Global Information Assurance Certification Paper

Ethernet over Low-Voltage Power Line Communication Networks

A Security Analysis and Audit of the HomePlug 1.0 Standard

An Auditor's Perspective

By

Todd W. Colvin

SANS GSNA Practical (v 2.1) – Option 1

October 29, 2003

Abstract/Summary

Individuals seeking GSNA certification are required to submit a practical assignment to address the auditing of an information system, network or combination of both. To this end, the following paper was developed to address the certification requirements by documenting a security analysis and audit of HomePlug Powerline Communication networks. HomePlug devices permit individual workstations or entire network segments to be bridged over standard AC power lines. To date, the security exposures presented by the HomePlug technology have not been evaluated. This paper was developed to address the gap in knowledge regarding HomePlug devices and their inevitable use in Small Office / Home Office (SOHO) or Remote Office / Branch Office (ROBO) environments. The HomePlug standard will be discussed, security risks will be identified and then an audit approach will be proposed to detect and mitigate any discovered vulnerabilities.

Table of Contents

1 ASSIGNMENT I – RESEARCH IN AUDIT, MEASUREMENT PRACTICES, AND CONTROL

1.1 Introduction

The options available for companies, in particular Small Office/Home Office (SOHO) or Remote Office/Branch Office (ROBO), to supplant or expand structured cabling networks for the interconnection of systems or populations of users are nearly limitless considering today's available technologies. Organizations may now extend networks in any imaginable direction through the installation of wireless or wire line carrier technologies over existing cable infrastructures, to include phone line and power line, without the need or expense of cabling new outlets or purchasing additional and often times costly network electronics.

To date much coverage has been provided on the topic of wireless communication technologies, examples of which include 802.11b, 802.11a and Blue Tooth, but the same may not be said for power line communications. Although power line communications have had a long history, both conceptual and actual, attempts made in the 1990's to utilize existing energy distribution infrastructures for last mile broadband access were met with limited success. In April of 2000, author David Hines investigates how "Many people thought that Powerline telecommunications (PLT) was dead, the final nail in the coffin being the withdrawal of NOR.WEB…from the PLT arena." However, as it turns out, the true purpose of his paper is counter to the argument that powerline is "dead." Rather, he uses the attention getting introduction to lure the reader into an article chock fill of newly introduced technologies and especially "PLT home networking products."

Hines further states that "PLT home networking products are already on the market, 10 megabit per second at every socket in the home [or small business] means that computers, printers and a host of other peripherals may all be networked together via existing…wiring in a simple, tidy and flexible way." Support for Hines' argument that PLT is on the move, may be found in the form of the HomePlug Alliance. The HomePlug Alliance (http://www.homeplug.org) has served to develop a communications standard based on several common protocols to produce the HomePlug Specification version 1.0 (Version 2.0 is currently under development and promises greater throughput). In doing so, the Alliance has returned low-voltage power line communications as a viable alternative to wireless and structured cabling technologies.

An information systems and network auditor should be keenly aware of the growing acceptance and deployment of alternative network technologies as presented by low-voltage power line communication devices. The unforeseen risks, which are often shielded by the economic and flexible attractiveness of such technologies to small and medium sized companies, are the threat of data loss, manipulation or exposure.

However, before an auditor can effectively inspect for and report on the presence of low-voltage power line communication devices, they will need a high-level understanding of the benefits and limitations of the technology to gain a business perspective on their use. They too will need tools, techniques, methods and processes

to detect the presence of such devices and alternatives should standard measures be met with failure.

1.2 Focus

The focus of this paper, as assigned during the San Diego SANS Conference in March 2003, will be to address the topic of low-voltage power line communications via the HomePlug standard (also referenced as LPLC, PLC or PLN) throughout this document, within the framework of requirements identified by the Auditing Networks, Perimeters, and Systems GSNA Practical version 2.1, option 1.

1.3 Scope

ABC Corporation, primarily located in the United States, has received internal reports from it's Kansas based branch office and warehousing facility that unauthorized low-voltage power line devices based on the HomePlug 1.0 Standard are deployed on its local area network. It was further reported that said devices are being used to extend network capabilities, to include unfiltered Internet access, to offices on the warehouse floor, while subverting recent corporate efforts to detect wireless (e.g., 802.11a or 802.11b technology) access points.

Of additional concern to the ABC Corporation, is the use of non-enterprise workstation operating systems (i.e., Windows 9x (95/98) and Millennium Edition (ME)), within the Kansas facility. The ABC Corporation is aware of the security and control limitations presented by such operating systems and fears the workstations contained within that facility would present likely targets for malicious entities should they be directly exposed to the Internet. ABC Corporation further realizes that such direct exposure could lead to a domino effect presenting backdoor access into the corporate wide area network that is presently without inter-facility firewalls providing access to enterprise information assets located at its headquarters.

XYZ Company of Kansas, a recognized information systems and network auditing organization engaged by the ABC Corporation, is tasked with auditing the local area network housed within the Kansas facility, reporting on the results of the audit and providing recommendations to management to improve the overall security posture of the facility.

Accordingly, XYZ Company will audit the Ohio facility specifically for the presence of Ethernet traffic being transmitted across low-voltage power line communication devices based on the HomePlug 1.0 Standard and if discovered, expand the assessment to review any Windows 9x or ME workstation determined to be actively engaged in the support or use of such PLC devices.

To that end, XYZ Company will research:

1. Low-Voltage Powerline Communication (PLC) devices and specifically those based on the HomePlug 1.0 standard
2. History
3. Technology
4. Benefits
5. Limitations
6. Form Factor
7. Tools and methods to detect the presence of HomePlug devices
8. Evaluate and document the risks presented by the use of HomePlug devices
9. Research and document the current state of practice.
10. Create an audit checklist
11. Conduct the audit
12. Present a written report containing the 10 key findings (visual evidence of the audit) and associated recommendations.

ABC Corporation, having agreed to the terms and conditions of the audit as listed above, have approved and granted the XYZ Company with the authority to proceed immediately. Additionally, ABC Corporation has responded to XYZ Company's request for pre-audit materials as listed in Table 1-1:

Table 1-1 – Pre-Audit Materials Requested

Pre-Audit Materials Required	Provided	Comments
Escorted facility access for length of contract	Yes	None.
Work Area with network connectivity in main warehouse office	Yes	
Work Area in warehouse floor office	Yes	
Access to written security policy	Yes	
Map of property	Yes	
Map of building (with electrical and network outlets displayed)	Yes	A map will be provided but may or may not contain electrical/network outlets as requested.
Network documentation including map of devices	No	Current network documentation is non-existent.
Log files from network devices (i.e., routers, firewalls, etc.)	Yes	Syslog file available from firewall.
The assignment of two static IP addresses or permission to utilize local DHCP if available for two separate devices. Additionally, a network or domain login will be necessary to perform some of the tests listed below	Yes	Permission granted to use DHCP.

Table 1-1 – continued

Permission to utilize the following applications while on the network: Tools SuperScan – Network mapping Nessus-Network Vulnerability Assessment Ethereal-packet capture and analysis CAIN-NetBIOS Enumeration CAIN-Brute Force Share Passwords.	Yes	Caveat provided by XYZ regarding possible interference created by these tools and the goal of preventing downtime.
Permission to utilize ad hoc tools or techniques while inspecting individual workstations in addition to the following specific applications: Tools AntiVirex Virus Scanner AdAware Spyware Detection/Removal Screen Saver Bypass version 3.1 CAIN ScreenSaver Password Analysis CAIN Local Share Password Techniques Software Currency (windows update utility or wulog.txt wuhistv3.log inspection)	Yes	Caveat provided by XYZ regarding possible interference created by these tools and the goal of preventing downtime.
Permission to utilize necessary electronic surveillance equipment during physical security assessment to include: Tools True RMS DVM Field Strength Meter Frequency Counter Radio Scanner Radio Scanner with Oscilloscope software	Yes	Caveat provided by XYZ regarding possible interference created by these tools and the goal of preventing downtime.

1.4 Understanding Low-Voltage Power Line Communications

***1.4.1** History*

In April of 2003, a series of articles discussing power line communications were published within the IEEE Communications Magazine. Of particular interest to the history of PLC, as noted in the article titled *Power Line Communications: State of the Art and Future Trends* on page 34, is the fact that the concept as well as the practical application of said technology has been in existence for a considerable period of time. To this point the article states:

> In 1838 the first remote electricity supply metering and in 1897 [3] signaling the first patent on power line signaling were proposed in the United Kingdom. In 1905 applications were patented in the United States, and in 1913 the first commercial production of electromechanical repeaters took place. By late 1980,

relatively sophisticated error control coding techniques within the hardware of PLC modems were proposed. PLC standard have evolved constantly over the years, especially in the last 20, and resulted after 1994 in the digital power line boost promising new revenues for energy utilities and cheap Internet access for consumers (Tengdin 321-26).

Until the year 2000, the focus of powerline communication technology had "concentrated primarily on automatic meter reading, selective load control and demand-side management (PALAS). That position changed in March of 2000 when "Thirteen industry-leading companies formed the HomePlug Powerline Alliance…[with the belief that] Since most electronic devices already use power outlets to receive power, the goal of the alliance...[would be to] create a way that these same power outlets could be used to connect to the Internet and connect the devices to each other. The alliance achieved this by evaluating technologies and creating a specification. The HomePlug 1.0 specification was released in June of 2001" (HomePlug FAQ).

While the original goal of the alliance appeared to be the creation of a technology utilizing existing power outlets to focus on tech savvy homes for marketing and sales, their target has and will experience scope creep. What an expanding scope creep means, is that inevitably these devices will make their way into the SOHO/ROBO environment and quite possibly a medium or large enterprise given sufficient opportunity. To borrow from a cliché, history repeats itself.

A brief examination of the wireless marketplace from introduction to current state will show that it too started as a home technology on the shelves of many local computer stores before it spread like wild fire throughout 2001 and 2002. Once ample momentum is gained for HomePlug networks, history may repeat itself. If HomePlug devices do find their way into business networks, how will an auditor know? A high-level analysis of the technology may help to answer that question.

1.4.2 *Powerline Communications Technology*

What is interesting to note, is that the heart of a PLC device is the same as what may be found within voice or data wireless devices. The heart is the Crystal Oscillator responsible for the generation of radio frequencies. The difference however, is that rather than broadcast signals via an antenna, as is the practice with wireless devices, the PLC device utilizes power lines as a frequency carrier to superimpose it's radio signal or signals.

While other wireless technologies may be discussed for comparative reasons throughout this document as in the previous paragraph, the real focus here is on PLC and specifically the HomePlug Standard. There are many comprehensive articles and one known book, *Powerline Communications* by Klaus Dostert, written about powerline communications and the HomePlug technology of which most prove extremely complex by providing references to physics and mathematics. The articles, while useful to broaden an understanding of the technology, provide little in terms of presenting the

PLC concepts in lay terms. As an example, a paper published by members of the IEEE Computer Society titled *Field Performance Comparison of IEEE 802.11b and HomePlug 1.0* provides the following basic definition of the HomePlug protocol:

> HomePlug 1.0 uses a Physical Layer (PHY) protocol [6] based on equally spaced, 128-carrier Orthogonal Frequency Division Multiplexing (OFDM) [2, 11] from 0 HZ to 25 MHz, in conjunction with concatenated Viterbi and Reed Solomon coding with interleaving for payload data and turbo product codes for control data. 84 carriers are used to transmit data. BPSK, DBPSK, DQPSK or ROBO (a robust form of DBPSK) modulation us used for data, with a cyclic prefix for synchronization.
>
> A pair of nodes first determines which subcarriers are usable, and what form of modulation and error correction should be applied to the channel. This 'tone map' is used for subsequent communication between them. Broadcast packets and frame delimiters use all subcarriers with robust modulation and forward error correction codes so that all nodes can interpret them; the rest of a unicast frame uses the higher speed specified by the tone map.

The difficulty with most available documentation on this topic, as may be noted above, is that it assumes the reader is implicitly familiar with radio communications.

What if the reader is not entirely familiar with radio technology, where are they to turn? One of the first reference guides that I would recommend, if one desired a better foundational understanding of radio technology, would be a book written by Carl J. Weisman titled *The essential Guide to RF and Wireless – Second Edition.* To quote from the preface of the book:

> *The Essential Guide to RF and Wireless* takes an overly simplistic approach to the subject matter. In this vein, it accomplishes two main objectives: it provides a conceptual understanding of RF components and wireless systems, and it exposes you to the main vocabulary used in the industry.

Mr. Weisman's book should provide sufficient background to understand the creation, control, transmission, reception and processing of radio signals. If after reading Mr. Weisman's book one still craves for a better understanding of radio communications.

I would next recommend the *Certified Wireless Network Administrator (CWNA) Official Study Guide* published by McGraw Hill / Osborne. This book too provides a lot of fundamental information but then applies it towards the design, installation and management of a wireless network. It also discusses current RF standards (minus powerline) and relevant industry associations. A must have reference for those seeking to better understand radio communications. Do you still desire more knowledge regarding radio communications? If so, it is strongly recommended that you become a Federal Communications Commission (FCC) licensed amateur radio operator.

Licensed amateur radio operators are permitted to, based on their licensed privileges, transmit and receive radio communications across the bulk of the radio spectrum, in comparison to the more restricted communication applications such as Citizens Band (CB) and Family Radio Service (FRS). Furthermore, to dispel a common misconception regarding amateur radio operators, it is no longer just Morse code. Rather, amateur radio operators are involved in everything from, Single-Side Band (SSB), Upper-Side Band (USB), AM, FM, Packet, Digital (i.e., PSK, BPSK, etc.), microwave and satellite to name a few. If there is a broadcast signal to be found, there is usually an amateur radio operator nearby. To get to the point of this digression, most amateur radio operators make their start via a book published by the American Radio Relay League (ARRL) titled, *Now You're Talking – All You Need for your first Amateur Radio License.* The book is another recommended source of reading for those wishing to further their understanding of radio communications.

Broadening one's knowledge, by developing a solid background in radio communications, will serve system and network auditors well into the future as the world continues to unplug and go wireless. Fundamental radio communications knowledge is also highly portable and may be applied to a myriad of technologies to include, 802.11 devices, HomePlug (PLC), BlueTooth, HomePNA, IRDA and converged PDA/Mobile devices to name a few. These are all areas where technical auditing skills will be highly essential for better securing private or sensitive information resources.

Unfortunately, there is insufficient room or time within this paper to truly dive into the HomePlug standard. Just to begin to make sense of its acronyms and methods would require at a minimum, several weeks of continuous reading. For this reason, it is proposed that only the most necessary details be provided to enable sufficient awareness of HomePlug capabilities, benefits and limitations before wrapping up this section.

1.4.3 *The HomePlug Standard*

It appears that the best way to read and understand the HomePlug standard, is to find a HomePlug manufacturer capable of providing a sufficiently detailed reference, without directly publishing or communicating the standard itself. It sounds confusing, but the standard itself is not publicly accessible. In order to gain access to the standard, an individual or business entity must be a member of the HomePlug Alliance at a yearly cost of thousands of dollars. The monetary restriction makes it very difficult to find enough detail on the topic.

However, as mentioned, all that is necessary is to find a vendor with detailed documentation. In this case such documentation may be found in the *Open Powerline Management (OPM)- Simple Network Management (SNMP) Manual* from Corinex Communication (http://www.corinex.com). The OPM application will be discussed in more detail later in the paper so for now, let's peer into the world of HomePlug.

The following excerpt from the Corinex Manual, details the basic concepts regarding powerline networking and specifically the HomePlug standard:

> Sending millions of bits per second over common electric wires in premises, requires sophisticated algorithms running on fast silicon. House wiring is in principle a hostile environment for high data rate communications. Brush motors in hair dryers, vacuum cleaners and kitchen appliances are a significant source of interference. Turning appliances on and off, using dimmer switches, and using halogen lights injects noise spikes into the transmission line. Each branch off the main circuit breaker panel acts as a stub, causing multi path interference. Plus, the whole network of house wiring acts as an antenna, picking up RF interference from all radio and wireless transmitters.
>
> Signal attenuation is another challenge. Long runs between outlets are one cause, but the common surge-suppressor power strip often contains a filter to block high frequencies—the very ones HomePlug® uses to carry data. And most houses take power from both sides of the neighborhood distribution transformer's secondary windings, creating in the USA for example two 120V phases and one 240V phase. Power-line signals must go through this winding if you use an outlet on one phase and a second outlet on the other phase. The secondary winding acts as a low-pass filter, attenuating the signal. All these factors create a unique, often-complex, over time varying transfer function for each outlet- to-outlet channel in a home.
>
> HomePlug® technology overcomes these obstacles using a combination of approaches… Before a transmitter sends data to a receiver, the two nodes agree on what carriers to use based on the characteristics of the channel between them. Deselecting "bad" carriers helps prevent the loss of data that would otherwise be transmitted on those carriers.
>
> HomePlug® addresses security by creating a logical network based on a password and a 56-bit DES (Data Encryption Standard) key. Although power-line networks don't broadcast their data to the world like a wireless network, data can travel to other[s]…connected to the same power transformer.
>
> HomePlug® tries to be a good neighbor by avoiding frequencies used by other power-line technologies. The technology also limits its power spectral density around the amateur-radio bands by inserting 30-dB notches in the 4.5- to 21-MHz HomePlug® frequency range.

In the opening two paragraphs of the Corinex excerpt, many of the limitations and obstacles are identified when attempting to utilize an electrical circuit for the purpose of data networking. Electricity presents a temperamental medium subject to rapid fluctuations with literally the flip of a switch. However, as is evidenced in the remainder of the excerpt, the current HomePlug standard has made great strides in terms of function and performance in such a "hostile environment" (Corinex). Beyond the basic description of HomePlug, there are far more categories for consideration with respect to the true technical specifications. Table 1-2 presents the HomePlug technical specifications.

Table 1-2 – HomePlug Technical Specifications

Technical Specification	Description
Network Throughput	14 Mbps
Range (Distance)	There is a little deviation between manufacturers on this particular item but the bulk of them estimate distance between 200 to 300 meters. Considerably further than 802.11 devices or even Ethernet at 105 meters.
Frequency Range	Approximately 4.3 MHz to 20.9 MHz. Also referred to as the range from 100 Hz through 30 MHz.
Modes of Operation	
Node	A node is one device connected directly to the powerline network (PLN). There may only be 16 Nodes per PLN. If more than 16 exist the network switches to ROBO.
Bridge	A bridge connects one network segment to another, via the PLN. There is a limit of two bridges per PLN. However, as the bridge acts as a concentrator, it is only limited by the physical Ethernet limitations of the devices connected behind it.
Robust (ROBO) Mode	The following is an excerpt from the Corinex Users Manual: A Powerline device switches itself into ROBO mode under one of the following conditions: • There is so much noise on the line that it is impossible to get connection with other devices using OFDM modulation • There are more than 16 devices willing to communicate with the particular device. This number of devices will not fit into the tone map table, which is 16 devices long and therefore the device will switch into ROBO mode. In ROBO mode the highest possible speed is 0,9 Mbps
Supported Operating Systems	
Windows 98SE, ME, 2000, XP	Currently, Windows is the only approved operating system capable of using the necessary configuration software. However, an open source utility exists for Linux and Macintosh named PLConfig by Manuel Kasper. For additional information (http://www.neon1.net/prog/plconfig.html)
All others	Just about everything else can be supported in bridge mode. Software will need to be installed on a Windows machine to change the default "HomePlug," password. However, once changed the software is no longer required to operate a PLC bridge device.
Supported Interfaces	
Ethernet	May be used as a node or a bridge.
USB	May only be used as a node limiting connectivity to a single device.

Device Supported Protocols	
802.2 (MAC)	
802.3U (Ethernet)	
Network Topologies	The most common topologies are bus and star.
Common Device Form Factors	Auditors should note that some form factors have been discontinued. However, they may already be in production and as such, the auditor should be aware of the approximate dimensions during physical inspection.
Desktop-Single RJ-45 	~5.5" x 4" x 1.1" (W x D x H)
Wall Plug (Ethernet or USB) 	~2.68" x 4.25" x 2.60"(W x D x H)
Combined Wireless and HomePlug DSL/Cable Router	~8" x 5" x 1.1" (W x D x H)
Powerline DSL/Cable Router	~(W x D x H) Vendor specific
WallPlug with 802.11	~2.68" x 4.25" x 2.60"(W x D x H)
Encryption	56bit-DES encryption, hardware based.
Price	Average between $69 and $119 dollars (based on local computer stores sales flyers).
Device LED's	The bulk of the devices provide the following LED's 1. Power LED - lights up in green when plugged into a power outlet 2. Collision LED - lights up in green whenever there is collision 3. Link LED - lights up in green after plugged into a power outlet 4. ACT LED - blinks in green when there is network activity 5. Ethernet port - connecting to the computer 6. Normal/Uplink button - you only need to use this button when connecting the bridge to a switch/hub. Any device with less than the Power, Collision, Link and Activity lights is not useful to an auditor when used for PLC device detection (more on this later in the paper).
Cabling	
Ethernet	(10Base-T) Cat 3, 4, 5 UTP Cable
Electrical	National Electric Code approved in the United States

Certainly some of the technical specifications could make the technology desirable for a SOHO/ROBO environment, but there has to be other drivers involved. To this point lets briefly explore some of the benefits of HomePlug networks.

1.4.4 Benefits

1.4.4.1 Cost as a Factor

One of the greatest benefits of HomePlug PLN's for businesses is the fact that no new structured wiring is required. Rather, HomePlug uses the ubiquitous availability of AC power lines to bridge data communication networks. By removing the requirement to install or upgrade a cabling infrastructure, the topics of cost and mean time to completion become more palatable. Table 1-3 provides a high-level cost comparison between the installation of HomePlug and the typical costs associated with the installation of network cabling (the cable run in this example is for a 295 foot segment)

Table 1-3 – Comparison of Ethernet vs. HomePlug Installation Costs

	New Cabling* (CAT5E Plenum)	PLC**
Average Time to Install (based on experience)	~4 to 8 hours depending on complexity of ceiling environment	~1-2 hours
Cable Cost	$ 113.00	$ 0.00
Patch Cables ($5.00 each)	$ 10.00	$ 5.00
Labor ($37.00 per hour)	$ 74.00	$ 37.00
PLC Electronics	$ 0.00	$ 80.00
Total	$ 197.00	$ 122.00

Data source: North Carolina Structured Cabling Services Contract discovered on Internet (see works cited for additional details).
* Assumes existing structured cabling with no requirement for new electronics
** Assumes existing PLC LAN and a contiguous or non-limited power segment

1.4.4.2 Other Benefits

Beyond cost, the other drivers include greater distance, hardware encryption, multiple form factors and two unique interface options that all address today's networked small office.

1.4.5 Limitations

As with any radio frequency based technology, there are limitations too, of which many were identified in the HomePlug technology section. However, technology is not the only drawback when using PLC devices. There are non-technical limitations as well and those will be explored briefly. Table 1-4 will address the technical limitations and Table 1-5 will address the non-technical limitations.

Table 1-4 – Technical Limitations

Technical Limitations	Description
Distance	HomePlug devices display an impressive ability to communicate at great distances however, the farther apart a pair of communicating devices are the more opportunity for signal loss (attenuation).

	802.11b has and always will suffer from attenuation. However, more recently "signal boosters," have been introduced to help reduce the effects of signal loss over a given distance.
Throughput	The Corinex guide states: The throughput of…[HomePlug] adapters is shared 14 Mbps half duplex, and the TCP throughput you can achieve between 2 workstations can be up to 7.5 Mbps.
Interference	
Impedance	The amount of resistance with an alternating current circuit. Increased resistance equates to a weaker signal.
Radio Signal	Any radio signal operating in the same frequency band as PLC devices which is approximately 4.3 MHz to 20.9 MHz.
Noise	Typical categories discussed in Intellon's Application Note titled *PowerPacket Lab Environment* include: universal motors, broad spectral and impulse. Also, the book *Powerline Communications* by Klaus Dostert provides an in depth review of the various noise categories and their implications.
Powerline Filer	The Corinex guide states: A Powerline Filter is a device, which, when applied on an electrical circuit will disable a powerline connection between powerline devices connected in front and behind the Filter.
Device quantity	The Corinex guide states: Tables in each device, where each is keeping the frequencies, which are best to connect to each particular other device, is 16 devices long. However, as the medium is shared, so is the bandwidth. The bandwidth for each adapter will drop with the increasing number of adapters in the same segment.
Security	More detail regarding security will be addressed at the end of this section as well as within the risk assessment section.
56bit DES	Should businesses be concerned with the fact that 56bit DES has already been broken?
Extended broadcast	Due to its ability to broadcast further, signals may be communicated to other facilities connected to the same side of power transformer.

Table 1-5 Non-Technical Limitations

Non-Technical Limitations	Description
Regulatory	
United States	Domestic Regulations (FCC Part 15)
European	European Regulations (ETSI, CENELEC, CEPT)
International	Regulations (ISO, IEC, ITU)

Radiation and Emissions	(IEC CISPR22)
Competing PLC Developers	Motorola, DS2 and Enikia are examples of competitors to Intellon the primary HomePlug chip manufacturer.
Activists	The range used by the HomePlug standard and similar technologies encompasses portions of the amateur radio bands. For this reason amateur radio enthusiasts are actively seeking to ban the further introduction of powerline communication technologies and more specifically broadband PLC as it proposes the use of radio signals up to 80Mhz effectively squashing the aforementioned amateur radio bands. For additional information (http://www.arrl.org/tis/info/HTML/plc)

1.4.6 Overcoming Limitations

HomePlug PLC is just as susceptible to technical limitations as is any electronic device. However, continued innovations as well as the development of new standards (HomePlug 2.0 is in development) many of these limitations will be reduced or removed as barriers.

As an example, transformers may appear to present a sufficient obstacle for PLC devices. However, much like wireless signal-boosters designed to overcome the broadcast barriers of 802.11 devices, manufacturers of PLC equipment have developed "repeaters" to bridge the gaps presented by the physical or mechanical limitations of the technology. One such manufacturer is CEPCO (http://www.cepcoproducts.com) who have created a "Transformer Coupler/Repeater" to overcome transformer barriers. While their technology appears to be aimed at command and control functions for energy providers, minor modifications could ideally harness the same technology with respect to low power PLC devices.

Another potential obstacle, with regard to security, is the current HomePlug 1.0 standard that only provides for DES 56 bit encryption. Although this may immediately appear as an insecure key length, especially with respect to the work produced by the Electronic Freedom Foundation in their book titled "Cracking DES," the technology and methods required to penetrate the HomePlug 1.0 implementation of DES 56 are quite possibly sufficient to guard against immediate compromise. Are there alternatives to purchasing HomePlug 1.0 devices, certainly?

In fact, one vendor in particular has noted the insecurities associated with this level of encryption and sought to incorporate the Advanced Encryption Standard (AES) into their integrated circuits. The manufacturer is EasyPlug and their technology supports AES with varying key strengths to include 128, 196 and 256 bit key lengths in accordance with commercial encryption export controls as established by the Department of Commerce (please see http://www.bxa.doc.gov/Encryption/Default.htm for more details). The only downside is that the PLC method implemented by the EasyPlug technology is not HomePlug compatible.

Increasing the key length is a step in the right direction for the protection of the data, however concerns still exist regarding the monitoring and management of PLC devices without regard for authentication and authorization. All of these are concerns that should and will be factored into a formal risk assessment.

To summarize the review of HomePlug PLC technology thus far, there has been a long history of innovation, development and application of technology pertinent to the communication of data over common electric lines. Despite a century or so of history surrounding this technology, it is still in relative infancy. As PLC technology, especially Broadband PLC (BPLC) and more specifically HomePlug compliant devices continue to mature and find their way into SOHO/ROBO environments, the risks associated with their use must be identified now and sufficient controls applied to prevent the introduction of a technology that presents an opportunity for the exposure of information assets.

1.5 Risk Evaluation

Since HomePlug networks operate on radio signals, many of the risks that currently target wireless networks may be applicable. For this reason much of the research for this section has been focused on the identification of existing threats, vulnerabilities and exposures that present risk to wireless networks. Table 1-6 is a compilation of the many sources referenced but formatted as a Risk Evaluation Matrix.

The Risk Matrix pertains to the usage of HomePlug devices in a SOHO/ROBO environment along with any identified risks, profiles (i.e., level, probability, financial loss, etc.) or consequences accordingly. Additionally, the table calculates a value for each identified risk. The higher the calculated score the greater the risk. Higher numbered risks present excellent opportunities for management to remove the "low-hanging fruit," presented by these items and in doing so, improve the overall security of the systems and networks exposed to HomePlug devices.

Table 1-7 presents a list of the sources referenced during the development of the risk evaluation matrix. The table is a truncated version of the full works cited and additional references contained herein.

Table 1-6 – Risk Identification Matrix

IDENTIFIED RISKS			RISK PROFILE																				CALCULATED RISK VALUE	CONSEQUENCES
			Method		Risk			Probability			Complexity			Popularity			Financial Loss			Security Impact(s)				
			Accidental	Deliberate	High	Medium	Low	High	Medium	Low	High	Medium	Low	Widespread	Popular	Obscure	High	Moderate	Inconsequential	Confidentiality	Integrity	Availability		
		POINTS	1	2	3	2	1	3	2	1	3	2	1	3	2	1	3	2	1	1	1	1		
Physical security perimeter permits electronic eavesdropping or observation.				D		M			M			M			P			M		C	I		14	Radio signals extend the physical perimeter. An unmonitored perimeter allows opportunity for eavesdropping.
RISK ID: 1	Source	SCORE		2		2			2			2			2			2		1	1			
	EXPR																							
Physical security perimeter contains multiple power outlets permitting external access to HomePlug powerline network.				D		M			M				L			O		M		C	A		12	Opportunity to implant HomePlug devices to conduct espionage.
RISK ID: 2	Source	SCORE		2		2			2				1			1		2		1	1			
	POLI																							

Table 1-6- continued

IDENTIFIED RISKS			RISK PROFILE																			CALCULATED RISK VALUE	CONSEQUENCES
			Method		Risk			Probability			Complexity			Popularity			Financial Loss			Security Impact(s)				
			Accidental	Deliberate	High	Medium	Low	High	Medium	Low	High	Medium	Low	Widespread	Popular	Obscure	High	Moderate	Inconsequential	Confidentiality	Integrity	Availability		
		POINTS	1	2	3	2	1	3	2	1	3	2	1	3	2	1	3	2	1	1	1	1		
Physical access to receiving area, computer facilities or data closets is uncontrolled.				D			L		M			M				O		M		C	I	A		Opportunity to implant HomePlug devices to conduct espionage.
RISK ID: 3	Source	SCORE		2			1		2			2				1		2		1	1	1	13	
	POLI																							
Computer system administration performed by untrained personnel.			A			M		H				M		W				M		C	I			Operating system is open for administration permitting the introduction of malicious or illegal software.
RISK ID: 4	Source	SCORE	1			2		3				2		3				2		1	1		15	
	POLI																							
Computer CMOS password is disabled.			A	D		M			M				L	W				M		C	I	A		Permits modification to boot sequence, reported device quantities, as well as the ability to load local key-logging software.
RISK ID: 5	Source	SCORE	1	2		2			2				1	3				2		1	1	1	16	
	EXPR																							
Computer operating system is insufficient to enforce adequate controls.			A	D		M			M				L	W				M		C	I	A		Operating system is open for administration permitting the introduction of malicious or illegal software.
RISK ID: 6	Source	SCORE	1	2		2			2				1	3				2		1	1	1	16	
	EXPR																							
Screensaver either not enabled or properly configured to lock after periods of inactivity.			A	D		M			M				L	W				M		C	I	A		Operating system is open for administration permitting the introduction of malicious or illegal software.
RISK ID: 7	Source	SCORE	1	2		2			2				1	3				2		1	1	1	16	
	EXPR																							

Table 1-6- continued

IDENTIFIED RISKS			RISK PROFILE																				CALCULATED RISK VALUE	CONSEQUENCES
			Method		Risk			Probability			Complexity			Popularity			Financial Loss			Security Impact(s)				
			Accidental	Deliberate	High	Medium	Low	High	Medium	Low	High	Medium	Low	Widespread	Popular	Obscure	High	Moderate	Inconsequential	Confidentiality	Integrity	Availability		
		POINTS	1	2	3	2	1	3	2	1	3	2	1	3	2	1	3	2	1	1	1	1		
Screensaver password composition does not meet policy.			A	D		M		H					L	W				M		C	I	A		Operating system is open for administration permitting the introduction of malicious or illegal software.
RISK ID: 8	Source	SCORE	1	2		2		3					1	3				2		1	1	1	17	
	EXPR																							
Operating system permits screensaver bypass utilities to execute due to CDROM autorun feature enabled.			A	D		M			M			M			P			M		C	I	A		Opportunity for data loss or manipulation.
RISK ID: 9	Source	SCORE	1	2		2			2			2			2			2		1	1	1	16	
	ISRA (p. 111)																							
Operating system permits remote sharing of files and folders.			A			M			M				L		P			M		C	I			Opportunity for data loss or manipulation.
RISK ID: 10	Source	SCORE	1			2			2				1		2			2		1	1		12	
	ISRA (p. 111)																							
Both employees and non-company personnel have access to computer system.			A	D	H				M			M				O	H			C	I			Disclosure of classified information. Possible violation of privacy laws.
RISK ID: 11	Source	SCORE	1	2	3				2			2				1	3			1	1		16	
	ISRA (p. 103)																							
Local storage of passwords or password lists is uncontrolled and unencrypted.			A	D	H			H					L	W			H			C	I	A		Open access to passwords allows for identity masquerading.
RISK ID: 12	Source	SCORE	1	2	3			3					1	3			3			1	1	1	19	
	ISRA (p. 110)																							

Table 1-6- continued

IDENTIFIED RISKS			RISK PROFILE																			CALCULATED RISK VALUE	CONSEQUENCES
			Method		Risk			Probability			Complexity			Popularity			Financial Loss			Security Impact(s)				
			Accidental	Deliberate	High	Medium	Low	High	Medium	Low	High	Medium	Low	Widespread	Popular	Obscure	High	Moderate	Inconsequential	Confidentiality	Integrity	Availability		
		POINTS	1	2	3	2	1	3	2	1	3	2	1	3	2	1	3	2	1	1	1	1		
Anti-virus detection is not present, active or current on the computer system.			A	D	H			H					L	W			H			C	I	A		Virus infections are a clear and present danger causing excessive data loss.
RISK ID: 13	Source	SCORE	1	2	3			3					1	3			3			1	1	1	19	
	POLI																							
Spy-ware detection is not present on the computer system.			A	D	H			H					L	W				M		C				Internet usage monitoring or keystroke capturing poses a threat to confidentiality. Internet tracker could review company details.
RISK ID: 14	Source	SCORE	1	2	3			3					1	3				2		1			16	
	EXPR																							
Unapproved, illegal, or malicious software is installed on the system.			A	D	H				M				L	W			H				I	A		Software license violations are punishable by law and may pose a financial threat to the company.
RISK ID: 15	Source	SCORE	1	2	3				2				1	3			3				1	1	17	
	POLI																							
Computer system used to access Internet sites of questionable content.				D	H			H					L	W			H			C				Could lead to public cases of sexual harassment posing a financial loss to the company.
RISK ID: 16	Source	SCORE		2	3			3					1	3			3			1			17	
	EXPR																							
Incomplete or non-existent computer hardware/software configuration information.			A			M			M				L		P			M				A		A current computer inventory is essential for troubleshooting and maintenance procedures. Failure to maintain a current inventory may lengthen issue resolution.
RISK ID: 17	Source	SCORE	1			2			2				1		2			2				1	11	
	POLI																							

Table 1-6- continued

IDENTIFIED RISKS			RISK PROFILE																			CALCULATED RISK VALUE	CONSEQUENCES
			Method		Risk			Probability			Complexity			Popularity			Financial Loss			Security Impact(s)				
			Accidental	Deliberate	High	Medium	Low	High	Medium	Low	High	Medium	Low	Widespread	Popular	Obscure	High	Moderate	Inconsequential	Confidentiality	Integrity	Availability		
		POINTS	1	2	3	2	1	3	2	1	3	2	1	3	2	1	3	2	1	1	1	1		
Incomplete or non-existent network inventory.			A			M			M				L		P			M				A		A current network inventory is essential for troubleshooting and maintenance procedures. Failure to maintain a current inventory may lengthen issue resolution.
RISK ID: 18	Source	SCORE	1			2			2				1		2			2				1	**11**	
	NIST (p. 11)																							
Incomplete or non-existent depiction of network topology.			A			M			M				L		P			M				A		A current network inventory is essential for troubleshooting and maintenance procedures. Failure to maintain a current inventory may lengthen issue resolution.
RISK ID: 19	Source	SCORE	1			2			2				1		2			2				1	11	
	NIST (p. 11)																							
Computer operating security patches not current or not configured properly.			A	D	H			H				M		W				M		C	I	A		Failure to maintain current operating system security patches provides an opportunity for system compromise due to documented vulnerabilities.
RISK ID: 20	Source	SCORE	1	2	3			3				2		3				2		1	1	1	19	
	EXPR																							
HomePlug devices constitute a new and untested technology that may lead to a breach of security.			A	D	H				M		H					O		M		C	I	A		HomePlug devices are untested and pose a unknown risk due to a lack of security testing and documentation.
RISK ID: 21	Source	SCORE	1	2	3				2		3					1		2		1	1	1	17	
	EXPR/ISRA (p.114)																							
HomePlug devices do not enforce local end-user authentication permitting unauthorized access to system and network resources.			A	D	H			H			H					O		M		C	I			HomePlug PLN's perform device authentication and not end-user authentication, permitting bridged access to network resources.
RISK ID: 22	Source	SCORE	1	2	3			3			3					1		2		1	1		17	
	EXPR/ISRA (p.103)																							

Table 1-6 - continued

IDENTIFIED RISKS			RISK PROFILE																			CALCULATED RISK VALUE	CONSEQUENCES
			Method		Risk			Probability			Complexity			Popularity			Financial Loss			Security Impact(s)				
			Accidental	Deliberate	High	Medium	Low	High	Medium	Low	High	Medium	Low	Widespread	Popular	Obscure	High	Moderate	Inconsequential	Confidentiality	Integrity	Availability		
		POINTS	1	2	3	2	1	3	2	1	3	2	1	3	2	1	3	2	1	1	1	1		
HomePlug device emits radio signals permitting interception or eavesdropping.				D	H				M		H					O		M		C	I	A		Malicious entities capable of discovering powerline network devices may actively target the information assets behind them.
RISK ID: 23	Source	SCORE		2		2			2		3					1		2		1	1	1	16	
	EXPR/CORX																							
HomePlug device is susceptible to radio signal jamming.			A	D	H				M		H					O		M				A		Malicious entities could knowingly broadcast on the HomePlug frequencies in an attempt to block communications.
RISK ID: 24	Source	SCORE	1	2	3				2		3					1		2				1	15	
	CORX																							
HomePlug device is susceptible to electrical interference.			A	D	H				M		H					O		M				A		A denial of service attack could be introduced to a PLN by turning on the right combination and quantity of electrical devices.
RISK ID: 25	Source	SCORE	1	2	3				2		3					1		2				1	15	
	CORX																							
HomePlug device is susceptible to electrical failures.			A	D	H				M		H					O		M				A		Plugging a home plug device into a socket controlled by a wall switch presents an opportunity for disruption.
RISK ID: 26	Source	SCORE	1	2	3				2		3					1		2				1	15	
	CORX																							
HomePlug device is susceptible to electrical spikes and sags.			A	D	H				M		H					O		M				A		Hypothetically, HomePlug devices may be susceptible to spikes and sags as thy may not be used with power filtering strips.
RISK ID: 27	Source	SCORE	1	2	3				2		3					1		2				1	15	
	EXPR																							

Table 1-6- continued

IDENTIFIED RISKS			RISK PROFILE																				CALCULATED RISK VALUE	CONSEQUENCES
			Method		Risk			Probability			Complexity			Popularity			Financial Loss			Security Impact(s)				
			Accidental	Deliberate	High	Medium	Low	High	Medium	Low	High	Medium	Low	Widespread	Popular	Obscure	High	Moderate	Inconsequential	Confidentiality	Integrity	Availability		
		POINTS	1	2	3	2	1	3	2	1	3	2	1	3	2	1	3	2	1	1	1	1		
HomePlug Network Encryption Key (NEK) password is set to default.			A	D	H			H					L	W				M		C	I			Failure to change the default NEK will permit open access to any HomePlug device connected to a PLN.
RISK ID: 28	Source	SCORE	1	2	3			3					1	3				2		1	1		17	
	CORX																							
HomePlug Network Encryption Key (NEK) password composition does not meet policy.			A	D	H			H					L	W				M		C	I			An easily guessed NEK password or one that doesn't subscribe to standards presents an exposure to the PLN
RISK ID: 29	Source	SCORE	1	2	3			3					1	3				2		1	1		17	
	EXPR																							
HomePlug Network Encryption Key (NEK) password storage does not meet policy.			A	D	H			H					L	W				M		C	I	A		The NEK controls access to a configured PLN. Gaining access to the NEK password gains access to the PLN.
RISK ID: 30	Source	SCORE	1	2	3			3					1	3				2		1	1	1	18	
	EXPR																							
HomePlug Device Encryption Key (DEK) is not controlled and may be used to bypass network security to gain access to the data.			A	D	H			H					L	W				M		C	I	A		The DEK permits remote administration of a HomePlug device in conjunction with the NEK.
RISK ID: 31	Source	SCORE	1	2	3			3					1	3				2		1	1	1	18	
	EXPR																							
Any HomePlug device may gain open access to a powerline network configured with the default or a known NEK password.				D	H			H				M			M			M		C	I	A		Inability to monitor and maintain a PLN permits an opportunity for device insertion and data manipulation or theft.
RISK ID: 32	Source	SCORE		2	3			3				2			2			2		1	1	1	17	
	CORX																							

Table 1-6- continued

IDENTIFIED RISKS			RISK PROFILE																			CALCULATED RISK VALUE	CONSEQUENCES
			Method		Risk			Probability			Complexity			Popularity			Financial Loss			Security Impact(s)				
			Accidental	Deliberate	High	Medium	Low	High	Medium	Low	High	Medium	Low	Widespread	Popular	Obscure	High	Moderate	Inconsequential	Confidentiality	Integrity	Availability		
		POINTS	1	2	3	2	1	3	2	1	3	2	1	3	2	1	3	2	1	1	1	1		
HomePlug remote administration and configuration on the Ethernet side is susceptible to interception.				D	H				M			M		W				M		C		A		It is unknown whether HomePlug administration permits password sniffing yielding device or identity masquerading.
RISK ID: 33	Source	SCORE		2	3				2			2		3				2		1		1	16	
	EXPR																							
HomePlug powerline network traffic may be sniffed or easily capture using inexpensive and readily available radio electronics.				D	H				M		H					O		M		C	I			Hypothetically all radio signals may be captured presenting the premature release or manipulation of proprietary information.
RISK ID: 34	Source	SCORE		2	3				2		3					1		2		1	1		15	
	EXPR																							
HomePlug network administrative activity is not logged.				D	H			H				M				O		M			I	A		Inability to log HomePlug administrative activities restricts the ability to monitor for inappropriate usage or device manipulation.
RISK ID: 35	Source	SCORE		2	3			3				2				1		2			1	1	15	
	EXPR																							
HomePlug powerline encryption (56bit) may be compromised.				D	H				M		H				P		H			C	I			56bit DES has already been broken but it is uncertain if it can be duplicated in a HomePlug PLN. Doing so would allow for data compromise.
RISK ID: 36	Source	SCORE		2	3				2		3				1		1			1	1		14	
	CDES																							
HomePlug devices present an opportunity for data manipulation.			A	D	H				M		H					O		M		C	I			Data broadcast over power lines is susceptible to interception and possibly manipulation.
RISK ID: 37	Source	SCORE	1	2	3				2		3					1		2		1	1		16	
	EXPR																							

Table 1-6- continued

IDENTIFIED RISKS			RISK PROFILE																			CALCULATED RISK VALUE	CONSEQUENCES
			Method		Risk			Probability			Complexity			Popularity			Financial Loss			Security Impact(s)				
			Accidental	Deliberate	High	Medium	Low	High	Medium	Low	High	Medium	Low	Widespread	Popular	Obscure	High	Moderate	Inconsequential	Confidentiality	Integrity	Availability		
		POINTS	1	2	3	2	1	3	2	1	3	2	1	3	2	1	3	2	1	1	1	1		
HomePlug devices present an opportunity for data destruction.			A	D	H				M		H					O		M		C	I			Data broadcast over power lines is susceptible to interception and possibly manipulation.
RISK ID: 38	Source	SCORE	1	2	3				2		3					1		2		1	1		16	
	EXPR																							
HomePlug devices present an opportunity for data leakage.			A	D	H				M		H					O		M		C	I			Data broadcast over power lines is susceptible to interception and possibly manipulation.
RISK ID: 39	Source	SCORE	1	2	3				2		3					1		2		1	1		16	
	EXPR																							
HomePlug devices open additional ports on the computer hosting the configuration software.			A	D	H				M			M		W				M		C	I			Installing the software necessary to administer HomePlug devices may open additional network ports on the host computer.
RISK ID: 40	Source	SCORE	1	2	3				2			2		3				2		1	1		17	
	EXPR																							
Firewall permits external access to the network.			A	D		M		H					L	W				M		C	I	A		Network perimeter firewalls may be providing unauthorized access due to Trojans installed within the network.
RISK ID: 41	Source	SCORE	1	2		2		3					1	3				2		1	1	1	19	
	EXPR																							
Firewall permits outbound access to Internet sites containing known or questionable content.			A	D		M		H					L	W				M		C	I	A		Accessing websites of known or questionable content may expose a corporation to litigation.
RISK ID: 42	Source	SCORE	1	2		2		3					1	3				2		1	1	1	19	
	EXPR																							

Table 1-7 – SOURCES USED TO IDENTIFY RISKS

Source Title	Source Author	Assigned Source Code
Personal experience or recommendation	Colvin, Todd	EXPR
Information Security Risk Analysis	Peltier, Thomas R.	ISRA
Providing a Risk Analysis Framework for Potential Users of Wireless Technology	Jamaluddin, et al.	RAFW
ABC Company Policy	BS 7799	POLI
NIST Network Security Testing – 800-42	Wack, John	NIST
Cracking DES	Electronic Frontier Foundation	CDES
Hacking Exposed: Network Security Secrets and Solutions	McClure, Scambray and Kurtz	HAEX

1.5.2 *Risk Summary*

The risks are many but that is partly due to the unknown threat that HomePlug devices present for the confidentiality, integrity and availability of information assets. Only through careful analysis of the technology and addition of appropriate security controls will some of the fog be lifted. Upon completion of the system and network audit, an overall risk categorization, with applicable observations and recommendations, will be presented in the management report to address many of the risks identified in this section.

1.6 Current State of Practice

To date, research for existing audit practices for low-voltage power line networks and specifically HomePlug devices have yielded few positive results. It appears that the only documentation accessible and comparable to HomePlug PLN's may be discovered in the form of numerous wireless security manuals and guides. It is labeled comparable for the obvious reason that HomePlug utilizes radio communications, yet not a single text references HomePlug security. It may be that HomePlug is assumed to belong to a class of wired devices despite its use of RF.

Perhaps it was in the approach towards researching the topic that errors were made preventing the discovery of current audit practices. While that may seem likely, a list has been provided below to reinforce and highlight the research effort made (also as required by the practical assignment guidelines) to exhaustively investigate and report on the topic. The list of research activities on the topic of PLC and HomePlug includes but is not limited to the following activities:

1. An inestimable number of hours spent on the Internet tracking down relevant PLC, radio and security articles.
2. Several weekends dedicated to researching the volumes of technology and patent information at the Linda Hall Library at the University of Missouri at Kansas City.
3. Purchasing memberships within organizations identified for the involvement in the research and development of PLC (e.g., IEEE Communications Society, IEEE Computer Society, American Radio Relay League) at a cost of nearly $350.
4. Purchasing numerous texts that directly relate to PLC technology, Radio Technology, Test and Measurement methods and Wireless Security. At last count the expense of all books purchased to date totaled nearly $500 (what a great way to expand a library).
5. Purchasing assorted vendor PLC devices to test capabilities for discovery and compromise at a cost of over $400.
6. Purchasing specialized software designed for remote management of HomePlug powerline devices at a cost of $125.
7. Purchasing specialized hardware purportedly capable of detecting radio emissions at a cost of $750.
8. Approximately ten hours of domestic long distance and international calls attempting to locate and converse with individuals possessing specialized knowledge of PLC, HomePlug or radio interception methods.
9. An inbox stuffed with emails sent out in search of information.
10. Approximately 48 hours of face time tugging people's ears at work, Radio Shack and any place else I could corner somebody else that might be knowledgeable about PLC.

So did any of the research pay off? Well, it was believed that a couple of small breaks were finally made when in April of 2003 the IEEE Communications Magazine ran a

series of articles on Power Line Communications. Then another break occurred in May of 2003, when the issue of Broadband Power Line Communications (BPLC) attracted the attention of American Radio Relay League Members (ARRL). However, in the end the articles and information, though valuable, only addressed the technology and glossed over the security by briefly discussing the use of 56bit DES.

So rather than continue to look for information pertaining to just the state of practice for HomePlug, a decision was made to look at other practice areas (e.g., Wireless, Network Security Testing, etc.), then hopefully tie them together to develop a new state of practice for HomePlug powerline networks. To properly address the many facets involved in HomePlug networking it must be broken down into two best practice areas to include: Radio Frequency (a.k.a. Wireless--offering the first door into the network), and existing system and network practices. As many practices already exist for systems and networks, they will be briefly reviewed prior to shifting over to the topic of radio frequency detection.

1.6.1 *Existing Guidelines and Practices*

Although not entirely applicable, many of the wireless, network and system practices currently in existence, do have some areas that may be considered partially transferable to HomePlug powerline networks. This section will review several of the potentially applicable practices as listed in table 1-8.

Table 1-8 – Existing Guidelines and Practices

ASSIGNED SOURCE NAME	SOURCE NAME	SECTION OR PAGES REFERENCED
WE2E	Wireless Security: End to End	Entire book and specifically pages 172 thru 174
NIST	NIST 800-42 Guideline on Network Security Testing	Entire Paper
CWNA	Certified Wireless Network Administrator	Entire book and specifically Chapter Eleven
SBIT	Small Business IT Auditing	Sections specific to auditing Windows 98
TLAH	Thinking Like a Hacker	Entire paper
MICR	Microsoft Support Knowledgebase	Articles specific to Windows 9/X security
PEOC	Personal Experience or Contribution	None

Beginning with the book *Wireless Security: End to End*, the authors propose the following steps beginning on page 172:

1. Establish a security baseline for all equipment
2. Create a network diagram and list of all equipment
3. Check each piece of equipment for compliance with the baseline
4. Gather specific firmware versions for each piece of equipment
5. Determine if current security problems exist in any of the firmware versions currently deployed.
6. Check for any unnecessary services on the equipment
7. Discover any unauthorized access points

8. Determine the maximum distance that wireless traffic can be received from each access point.
9. Verify that unencrypted traffic is not traversing the wireless network
10. Verify that weak forms of WEP are not in use
11. Document deficiencies and begin to plan corrections.

The recommended approach contains many items that may be transferred or modified so that they may be applied to a HomePlug PLN audit. However, the first stumbling block in the list is also the first item in the list. In the case of Wireless devices, the authors proceed to recommend baselines over the course of pages 172 through 174. As insufficient data is available for properly configuring a HomePlug device at this time, a baseline standard will have to be postponed and then delivered to ABC Corporation upon the successful completion of an audit checklist.

While the previous method is specific to wireless, a broader approach may be discovered in the Special Publication number 800-42 and titled, *Guideline on Network Security Testing* as published by the National Institute of Standards and Technology (NIST). The document is brief, yet identifies an approach that is most often utilized in one fashion or another by many network auditors. The guide recommends the "following types of testing:"

1. Network Mapping
2. Vulnerability Scanning
3. Penetration Testing
4. Security Test and Evaluation
5. Password Cracking
6. Log Review
7. Integrity Checkers
8. Virus Detection
9. War Dialing

With the exception of perhaps items 7 and 9, the remaining items present a very effective method for testing network security and if coupled with an appropriate review of applicable controls, would provide an overall perspective on the posture of the ABC Corporations network within the Kansas facility.

Additionally, there are other contributing sources from which select recommendations may be considered for their merit as best practices. As an example, the *Certified Wireless Network Administrator* proposes an approach for performing a wireless site survey. Of course the purpose of the survey within the context provided is to assess a facility prior to the installation of a wireless network, the site survey method may too be applied towards the discovery of wireless or in this case RF transmitting HomePlug devices. The following is the site survey list extracted from the aforementioned book (pages 449 and 450):

1. Building blueprints (including power source documentation)
2. Previous wireless LAN site survey documentation
3. Current network diagram (topology map)
4. A meeting with the network administrator
5. A meeting with the building manager
6. A meeting with the security officer
7. Access to all areas of the facility to be affected by the Wireless LAN
8. Access to wiring closets
9. Access to roof (if outdoor antennas are anticipated)
10. Future construction plans, if available.

Ideally, these items reflect steps that are helpful during a physical facility inspection that is designed to locate the presence of a HomePlug PLN. They proposed a method of discovery by talking with key representatives of the facility, examining blueprints containing power source locations, and walking the facility to identify the best areas for access point placement. The same approach of talking, walking and identifying the best places to insert HomePlug devices for either intentional use or covert activities will be defined within the proposed checklist presented later in this document.

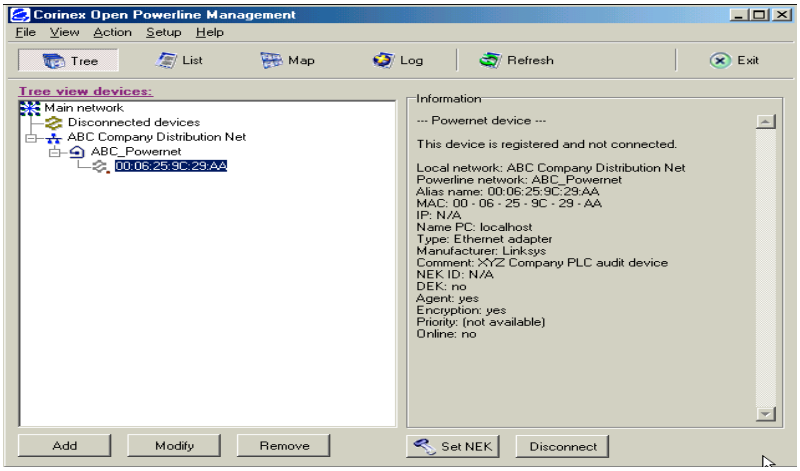
Beyond the sources presented thus far are other references that too contain helpful steps or recommendations that should and will be considered during the development of the HomePlug checklist. Example references may be found in the form of white papers such as the one written by Eric Shultze titled *Thinking Like A Hacker* as well as previously developed GSNA audit guides including the one created by David Eaves titled *Small Business IT Auditing*. All of the aforementioned references will be considered during the development of a HomePlug Audit Checklist and if utilized will be referenced and documented accordingly.

In addition to the references listed above, there exists a purpose built software application as mentioned previously in this paper, capable of HomePlug Detection. That is the *Open Powerline Management (OPM)- Simple Network Management (SNMP)* application from Corinex Communication. The tool will be briefly examined so that its usefulness may be highlighted in the discovery and management of HomePlug devices.

1.6.2 *Corinex Open Powerline Management Software*

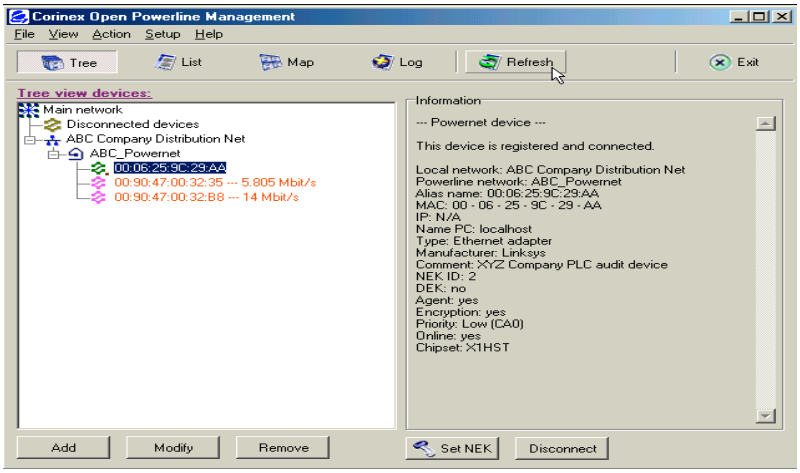
This section will discuss the use of the Corinex Open Powerline Management (OPM) software to observe a PLC network in conjunction with the previously installed Linksys PowerLine Etherfast 10/100 Bridge. After double-clicking the Corinex icon, the user is prompted to enter an appropriate User ID and Password. The documentation provides default settings for the initial login, but it is highly recommended that the authentication settings be changed prior to placing the system in production. It should also be noted that there are a series of steps that must be performed to install and utilize the Corinex software. However, due to space constraints these steps will not be shown rather the discussion will open by previewing the main console screen (Figure 1-1) just after having completed the software installation.

Figure 1-1



Selecting the refresh key will force the auto-discovery to initiate and seek other powerline devices on the powerline network. As screenshot shows in figure 1-2, there were two additional powerline devices discovered on the local power segment.

Figure 1-2



The console utilizes symbols to relay information regarding the currently monitored powerline network. The symbols are:

Table 1.9 Corinex OPM Symbols

	One powerline adapter is assigned to one PowerNet Agent and is responding as a connected item
	This powerline adapter is responding (will be any powerline device recognized in a defined Powerline network)
	Unregistered Powerline device (or Powerline device first discovered in a Powerline network)
	Device is currently not responding (for e.g. switched off)
	A device found in multiple powerline networks

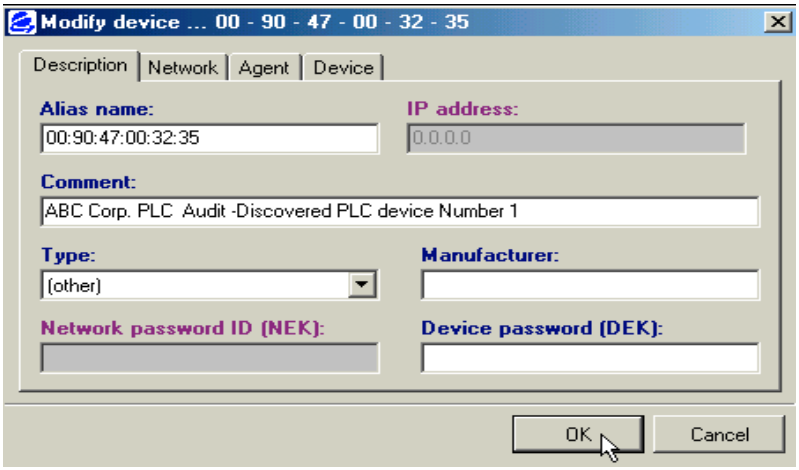
All symbols contained in the above table are the registered property of Corinex.

Based on the console display and the symbols listed in table 1-9, it can be determined that one device is configured within the OPM and an additional two devices are discovered but not registered PLC devices.

Each discovered device may be configured and added to the existing powerline network by first double-clicking the MAC address of one of the displayed devices.

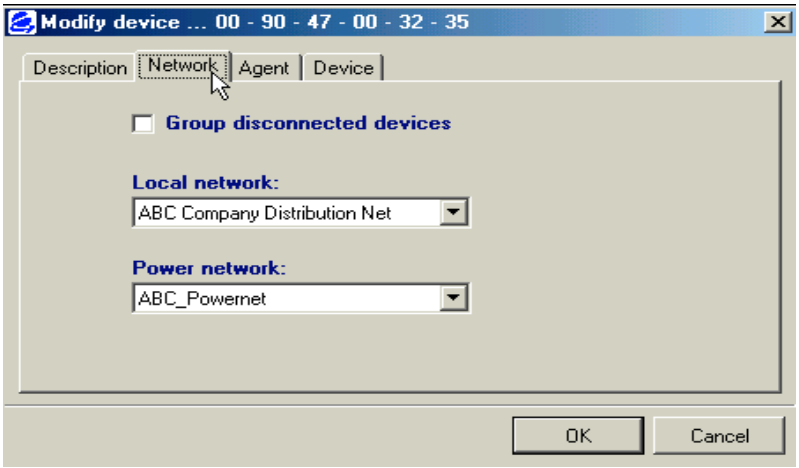
Then proceeding to enter information into each of the tabs. The “Description” tab allows additional comments to be made about the selected device that is useful for documentation purposes. Note the addition of information to the comments field in figure 1-3.

Figure 1-3



The network tab permits the selection of the Local Network and Powerline network for the selected device. These settings should match the local attached device for documentation purposes.

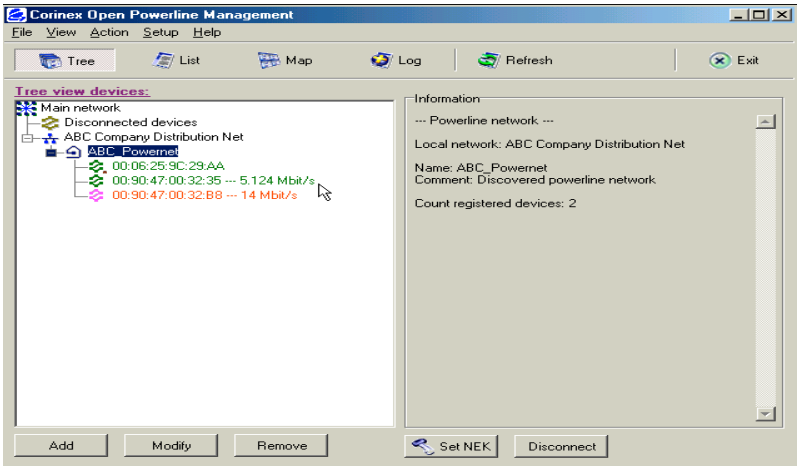
Figure 1-4



The “Agent” and “Device” tabs serve no purpose at this time so click on the “OK” button to proceed. When prompted to confirm the decision, click “Yes.”

Once returned to the console display, it may be observed that the status symbols as well as text color have changed to denote that the device is now a part of the local powerline network is depicted in figure 1-5.

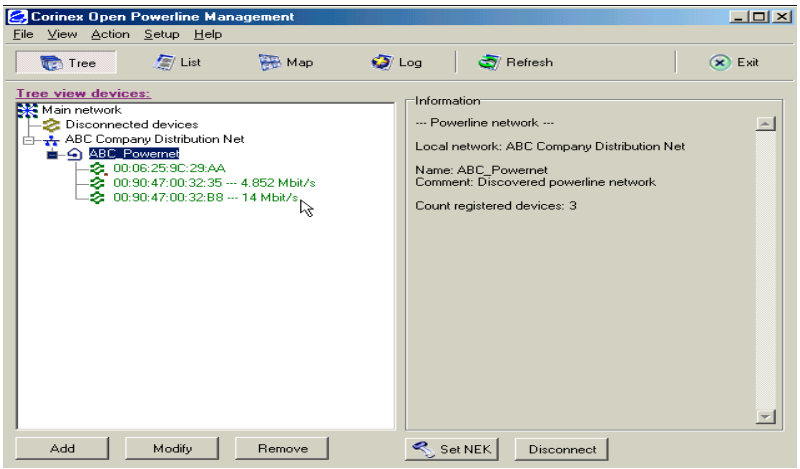
Figure 1-5



Proceed to configure the second device identical to the first with the exception of the comments field (for the purpose of space these steps will not be shown).

All devices should now be associated with the local “ABC_Powernet” powerline network as displayed in figure 1-6.

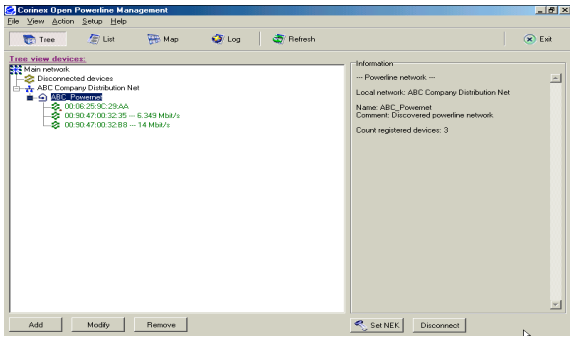
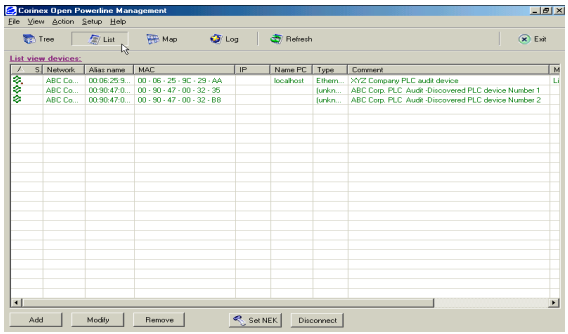
Figure 1-6



The OPM console provides additional options for displaying the powerline network that include: Tree (default), List and Map. In addition to the viewing options is the ability to

review the console log file where configuration activities are captured. Of the available choices, network and systems auditors will find the tree, list and log views most useful for documenting the discovery of a powerline network. For reporting audit findings, screen captures of the tree and list views along with the exported log file should be included to provide evidence of discovery.

The following screenshots of the tree and list views, as well as importing the log file aids to demonstrate the level of information available for reporting.

TREE	LIST
	

IMPORTED LOG FILE

```
10/10/2003 6:44:55 PM   admin   Info    Start application ...
10/10/2003 7:19:31 PM   admin   Info    Add NEK, id = 2
10/10/2003 7:24:49 PM   admin   Info    Set new application options
10/10/2003 7:30:58 PM   admin   Info    Add local network, name: ABC Company Distribution Net
10/10/2003 7:33:58 PM   admin   Info    Add powerline network, name: ABC_Powernet
10/10/2003 7:38:03 PM   admin   Info    Close application ...

10/10/2003 7:48:31 PM   admin   Info    Start application ...
10/10/2003 7:49:14 PM   admin   Info    Close application ...

10/10/2003 8:10:28 PM   admin   Info    Start application ...
10/10/2003 8:18:16 PM   admin   Info    Add device MAC: 00 - 06 - 25 - 9C - 29 - AA
10/10/2003 8:40:05 PM   admin   Info    Modify device, MAC: 00 - 90 - 47 - 00 - 32 - 35
10/10/2003 8:43:09 PM   admin   Info    Modify device, MAC: 00 - 90 - 47 - 00 - 32 - B8
```

The log file captures the addition of one HomePlug device and then the modification of two uniquely addressed devices. The modified devices indicate the automatic discovery of two additional HomePlug devices proving the detection capabilities of the Corinex OPM tool.

The Corinex OPM tool certainly presents a viable option for system and network auditors for the discovery and documentation of locally attached HomePlug PLC devices. However, it should be stated that locally means specific to the power segment where the auditor is performing their data collection as opposed to local within a given facility. This distinction must be drawn as the powerline segmentation issues identified

during the technology section of this paper may restrict the auditor's ability to see HomePlug PLC devices. That is where a facilities map indicating power segments and outlets may assist the auditor in identifying all segments where the OPM tool should be performed to determine if HomePlug PLC devices are present.

Corinex also offers a hardware diagnostics kit consisting of a transmitting and receiving unit that provide power and segmentation characteristics via an onboard LCD display. The diagnostics kit in addition to the OPM software could greatly expedite a PLC audit. It was intended that the diagnostics kit should be purchased and included within this audit documentation, yet production issues delayed the release of the kit prohibiting their inclusion.

There remains one last task before combining all of the existing practices and tools into a HomePlug audit checklist. The last task requires the investigation and experimentation with tools capable of detecting radio signals. Certainly identifying tools capable of remotely and rapidly discovering HomePlug radio signals would benefit network auditors, as much as those available for the discovery of 802.11x networks. So with the goal of rapid discovery by radio technology in mind, the next section will explore radio frequency detection.

1.6.3 Radio Frequency Detection

Radio Frequency detection too may be broken into two further practices areas, novice and professional. Professionals in the RF arena concerning electronic and RF device detection really fall into the realm of Telecommunication Surveillance Countermeasures (TSCM) Professionals. The separation then between novice and professional only exists due to inaccessibility to TSCM knowledge as well as the cost of RF detection equipment. To draw further on that separation the area of TSCM will be explored further before contrasting it with the novice.

All throughout the research of methods for the detection of HomePlug devices, much information was drawn from websites or resources specializing in radio communications or technical surveillance and counter measures (TSCM). Special attention was paid to information provided on TSCM, as that is an industry specializing in the detection of radio frequency devices and carrier communications. As briefly identified within the risk assessment matrix, HomePlug devices may be used for industrial espionage purposes by bridging an organizations network over the power lines to a remote or hidden location. It is for this reason that TSCM specialists look for RF and Carrier communications.

Additional research regarding Technical Surveillance Countermeasures (TSCM) firms may be found online at:

Information Security Associates, Inc. (http://www.isa-tscm.com/)
Granite Island Group TSCM (http://www.tscm.com)
TSCM Technical Services (http://www.tscmtech.com)

The whole discussion of TSCM brings to mind the topic of computer espionage and a great reference for this topic is currently available in a book aptly titled, *Secrets of Computer Espionage: Tactics and Countermeasures* by Joel McNamara. Mr. McNamara's book goes beyond a casual conversation of espionage by pointing out various methods and tools freely available to assist with the performance of computer espionage. Another referenced that may be used in conjunction with Mr. McNamara's is the Third Edition of the book titled *Hacking Exposed: Network Secrets and Solutions* published by McGraw Hill-Osborne. Combined these sources promoted the development of several checklist items that should be examined during a system audit to reduce the likelihood of system compromise by novice practitioners.
While on the topic of novice practitioners and in contrast to TSCM professionals, they should be considered more of a wild card. Whereas a TSCM professional may benefit a corporation by rapidly identifying undesirable RF devices, they too present an imposing force should there skills be called upon for espionage. If a TSCM is turned against a corporation there is little that can be done, and that is a risk that anyone using modern electronic devices must face. A novice on the other hand is typically motivated by the removal of barriers.

Anything that prevents access to system and network resources presents a challenge. Time-after-time the challenges have been met and defeated by novice wildcards and that is why they may present an even greater threat to the security of information assets. They cannot and should not be ruled out of any risk assessment but rather should be considered as a threat agent possibly taking advantage of any number of listed risks.

Therefore, focus on the identification of readily accessible, relatively low cost RF detection equipment was extensively researched. Encompassing this category of tools and equipment includes items that may be purchased off the shelf at many radio stores or over the Internet from specialized radio manufactures and or built from scratch at home.

Contained throughout the various TSCM websites, RF vendor websites and reference manuals were suggestions for tools that may be used for Radio Frequency (RF) detection and as with most technologies; they too have benefits and limits. It is best to describe the available methods for RF detection, by categorizing them as physically connected or connectionless. They may also be considered in terms of cost, purpose, proximity and effectiveness and to this point; they will be introduced from least costly with marginal effectiveness to most costly and highly effective.

Finally, where experimentation with these devices occurred, the location of the test, the results of the test and any observations or recommendations will be included. The purpose for providing this level of detail is that the experimentation helped to develop the proposed state of practice and for this reason it will be shared with the hopes that it may be improved upon to further simplify HomePlug device detection.

1.6.3.1 True RMS Digital Voltmeter (DVM)

The Radio Shack 22-816 was selected for power quality measurements to determine whether PLC devices may be detected on selected power segments. The concept if intermodulation interference as described in Chapter Thirteen of *The ARRL RFI Book: Practical Cures for Radio Frequency Interference* will serve as the basis for testing for the presence of HomePlug carriers via a True RMS DVM. It should be noted that frequency limitations of the selected DVM will prevent the detection of RF emissions on the power line above 9.999 MHz.

In the case of the RS22-816, it was configured based on manufacturer's instructions to detect five specific frequency ranges. The manufacturer's instructions state that to perform frequency measurements the user must [RS22-816 Extech Instruments User's Guide]:

1. Insert the black test lead banana plug into the negative COM jack and the red test lead banana plug into the positive HZ jack.
2. Turn the rotary switch to the FREQ % position.
3. Press the Hz/% button to select "Hz" or "%".
4. Touch the test probes to the circuit or under test and read the frequency or duty cycle on the display.

The test will require selecting a series of locations around and within the facility for the purpose of detecting and recording intermodulation via the DVM. The results of the experiment are contained within table 1-10 and the map locations align with those identified in Appendix B of the final report. Prior to initiating the test, control readings were established in a facility with no known HomePlug devices for comparison against the discovered values. Additionally, observations regarding the use of the DVM may be found immediately following the table.

Table 1-10 – True RMS DVM Test Results

Map Location (See final report for map details)	Frequency Range Results (RS22-816 configured for the 9.999 MHZ)
Control Measurement	59.95 to 59.96 Hz
External Area 5	25.44 to 72.00 Hz
External Area 2	50.0 to 50.6 Hz
Internal Area 1	50.0 Hz
Internal Area 3	32.8 to 50.0 Hz

Observations: The test results were inconsistent and inconclusive. The same readings were obtained at the ABC Corporation Kansas Distribution facility as were at the control location. The intent of this test was to discover harmonic interference due to non-linear intermodulation. It is theoretically possible that harmonics exists, however the device scale is not sufficient to reach the multiples associated with the HomePlug frequencies.

1.6.3.2 AC Current Clamp

Similar to a True RMS (root mean square) Digital Voltmeter (DVM) but may be clamped around a line whereas a DVM usually requires that the probes are in direct contact with the wire. Unless properly trained exposing a bare wire carrying electricity for the purpose of taking measurements may be detrimental to your health. AC Current Clamps remove the hazard by encircling the shielding of the wire rather than the wire directly. This in turn makes them faster, safer and more convenient than traditional voltmeters. As testing was performed with a DVM it was determined that testing with an AC current clamp would be redundant.

1.6.3.3 Field Strength Meter

Field Strength Meters according to MFJ Enterprises, Inc. "show the strength of the actual field being radiated from your antenna…You can use it to check for RF floating around…[as well as] Find hidden transmitter bugs at [the] office." The device operates in the range of 100 KHz to 500 MHz, which supports the HomePlug frequency range.

Prior to using the field strength meter, tests were performed with the Kenwood TH-F6A by transmitting on the 2-meter band at 5 watts to attempt to ascertain the sensitivity of the device. The only observation regarding this control test was that the meter needle deflected greater when in close proximity to the radio. The opposite being true as well in that the further away from the transmitting source, the less observable needle deflection. This will be taken into consideration when using the field strength meter for HomePlug RF detection.

The test will require selecting a series of locations around and within the facility for the purpose of detecting and recording field strength with the MFJ-802. The results of the experiment are contained within table 1-11 and the map locations align with those identified in Appendix B of the final report. Prior to initiating the test, control readings were established in a facility with no known HomePlug devices for comparison against the discovered values. Additionally, observations regarding the use of the field strength meter may be found immediately following the table.

Table 1-11 - Field Strength Meter Test Results

Map Location (See final report for map details)	Field Strength Meter Results
Control Measurements	Test broadcast on the 2 Meter Band (~ 144MHz to 148 MHz) at 5 watts tied to a dummy load, caused the needle to deflect across the entire meter range based on proximity to transmitting source
External Area 5	No deflection
External Area 2	No deflection
Internal Area 1	No deflection
Internal Area 3	No deflection

Observations: The test results were inconsistent and inconclusive. The meter did not detect the presence of HomePlug radio signals in either near field or far field distances. It is hypothesized that the HomePlug radio signals are impacted by the inability to escape the copper media due to insufficient output power causing standing waves on the AC lines. Boosting the transmit power of the HomePlug device may cause detection however this approach may also cause RFI issues with other devices attached to the power segment.

1.6.3.4 Radio Frequency Counter

Simply put, frequency counters are used to detect RF transmissions and then display the results of the detected frequency. In Haskell Moore's on line reference titled *Counter Intelligence*, the topic of frequency counters is reviewed in terms of capabilities and limitations. Haskell explains that, "a frequency counter is an electronic device used to measure the frequency of a nearby transmitter. The counter will only acquire an accurate reading when the signal source is relatively close by (referred to as "near field") and is approximately fifteen to twenty decibels stronger than the ambient signal level for a period long enough to acquire a reliable reading."

The frequency counter is one of two devices, with the spectrum analyzer ranking first, most recommended by TSCM documentation to be used for the detection of RF transmitters. As HomePlug equipment broadcasts an RF signal and frequency counters are both readily available and reasonably priced, they make an ideal choice for an auditor's toolkit. In this case, the MFJ Enterprises, Inc. (http://www.mfjenterprises.com) frequency counter model MFJ-886 will be purchased for the purpose of experimenting with the detection of HomePlug PLN's via frequency detection. The MFJ-886 provides selectivity between a 10 Hz to 300 MHz range and a 10 Hz to 3 GHz range. As HomePlug devices operate in an approximate range of 4.5 MHz to 21 MHz, the lower band selection will be used.

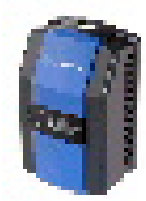
The test will require selecting a series of locations around and within the facility for the purpose of detecting and recording frequencies with the MFJ-886. The results of the experiment are contained within table 1-12 and the map locations align with those identified in Appendix B of the final report. Prior to initiating the test, control readings were established in a facility with no known HomePlug devices for comparison against the discovered values. Additionally, observations regarding the use of the frequency counter may be found immediately following the table.

Table 1-12 – Radio Frequency Counter Test Results

Map Location (See final report for map details)	Radio Frequency Counter Results
Control Measurements	Detected frequencies fluctuated between 88 MHz and 108 Mhz.
External Area 5	Same as Control Measurements
External Area 2	Same as Control Measurements
Internal Area 1	Same as Control Measurements
Internal Area 3	Same as Control Measurements

Observations: The test results were consistent with the detection of FM broadcast stations that are prevalent in metropolitan areas. This is due in part to the lack of a notch filter on the frequency counter. A notch filter serves to block out a range of frequencies while permitting signals above and below the notched range to continue on to the counter. While the final test for this device is categorized as inconclusive, the use of a notch filter to block strong FM frequencies, may provide the proper environment for the counter to discover HomePlug signals. Further experimentation is recommended.

1.6.3.5 HomePlug Network Device



PLC devices are built to talk to other PLC devices presenting an opportunity for discovery. I discovered during my experimentations that the status lights that are present on most HomePlug 1.0 Compliant devices (i.e., Link, Activity, etc.) could be used as a simple detector to determine whether another PLC device is present on the power circuit. Although, this may not be as accurate a test as would be delivered by other detection technologies, it was still sufficient for identifying possible network traffic on a power line.

The test method is simple, plug the device into the wall and pause for 15-30 seconds allowing the activity light to illuminate if the presence of a PLN is detected. It is further recommended that the use of the wall plug form factor be employed for this purpose as opposed to a device requiring a separate power cable.

It's also important to remember that whatever manufacturer you chose at a minimum the device should have the following LED's in order to detect other HomePlug devices: Power LED, Collision LED, and most importantly an ACT LED – that blinks green when there is network activity.

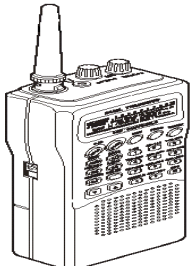
The test will require selecting a series of locations around and within the facility for the purpose of detecting and recording the presence of existing HomePlug devices by using another purchased HomePlug device. The results of the experiment are contained within table 1-13 and the map locations align with those identified in Appendix B of the final report. Prior to initiating the test, control readings were established in a facility with no known HomePlug devices for comparison against the discovered values. Additionally, observations comments regarding the use of the field strength meter may be found immediately following the table.

Table 1-13 –HomePlug Adapter Test

Map Location (See final report for map details)	FSM Test Results
Control Measurements	No HomePlug traffic detected by Activity LED
External Area 5	HomePlug traffic detected by Activity LED
External Area 2	HomePlug traffic detected by Activity LED
Internal Area 1	HomePlug traffic detected by Activity LED
Internal Area 3	HomePlug traffic detected by Activity LED

Observations: The results were positive and conclusive. Inserting a HomePlug standard 1.0 compatible device into a power segment with existing HomePlug traffic causes the Activity LED to illuminate despite incompatible vendor equipment. This test will be carried forward to the HomePlug Audit Checklist.

1.6.3.6 Radio Scanner with built in Signal Strength Meter



Purpose built radio designed to observe a range of frequencies while either pausing upon discovery or graphically displaying the strength of the detection signal.

The test will require selecting a single location, due to the time requirements for radio scanning, for the purpose of detecting and recording the presence of existing HomePlug devices by using a radio scanner. Only those signals whose strength is measured as seven or higher will be recorded. The results of the experiment are contained within table 1-14 and the map locations align with those identified in Appendix B of the final report. Prior to initiating the test, control readings were established in a facility with no known HomePlug devices for comparison against the discovered values. Additionally, observations comments regarding the use of the field strength meter may be found immediately following the table.

Table 1-14 – Kenwood Radio Frequency and Strength Meter Scanning

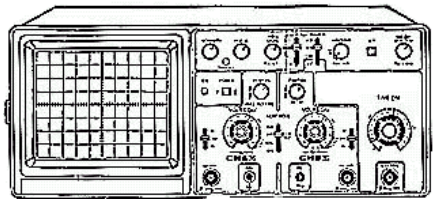
Range (Approximate)	Control Measurements	Site Measurement (Internal area 3)
100 kHz to 1 MHz (AM Radio Band)	.280 .285 .560 .570 .610 .750 .850 .980	.610 .710 .810 .980
1 MHz to 2 MHz (AM Radio Band)	.030 .200 .210 .230 .300 .310 .320 .340 .350 .360 .370	.120
2 MHz to 3 MHz	No strong signals detected	No strong signals detected
3 MHz to 4 MHz	.025 .030 .035	.035
4 MHz to 5 MHz	No strong signals detected	No strong signals detected
5 MHz to 6 MHz	No strong signals detected	No strong signals detected
6 MHz to 7 MHz	.055 .060 .065 .105	No strong signals detected
7 MHz to 8 MHz	No strong signals detected	No strong signals detected
8 MHz to 9 MHz	No strong signals detected	No strong signals detected
9 MHz to 10 MHz	No strong signals detected	.675 .680
10 MHz to 11 MHz	No strong signals detected	No strong signals detected
11 MHz to 12 MHz	No strong signals detected	No strong signals detected
12 MHz to 13 MHz	No strong signals detected	No strong signals detected
13 MHz to 14 MHz	No strong signals detected	No strong signals detected
14 MHz to 15 MHz	No strong signals detected	No strong signals detected*
15 MHz to 16 MHz	No strong signals detected	No strong signals detected*
16 MHz to 17 MHz	No strong signals detected	No strong signals detected*
17 MHz to 18 MHz	No strong signals detected	No strong signals detected
18 MHz to 19 MHz	No strong signals detected	No strong signals detected
19 MHz to 20 MHz	.795 .800 .805	.795 .800 .805
20 MHz to 21 MHz	No strong signals detected	No strong signals detected
21 MHz to 22 MHz	No strong signals detected	No strong signals detected

22 MHz to 23 MHz	No strong signals detected	No strong signals detected
23 MHz to 24 MHz	No strong signals detected	No strong signals detected
24 MHz to 25 MHz	No strong signals detected	No strong signals detected
25 MHz to 26 MHz	No strong signals detected	No strong signals detected
26 MHz to 27 MHz	No strong signals detected	No strong signals detected
27 MHz to 28 MHz	No strong signals detected	No strong signals detected*
28 MHz to 29 MHz	No strong signals detected	No strong signals detected*
29 MHz to 29.695 MHz	.485 .490	.485

*Denotes a range were numerous tones were discovered but weak signals were exhibited.

Observations: The test was inconclusive. However, a number of interesting audible tones were detected across nearly entire bandwidth ranges as indicated by asterisks in table 1-14. Additionally, the tones displayed a fairly consistent offset leading the auditor to believe that a tone map had been discovered. It should be noted that the tones were only discovered when proximity to a HomePlug device was approximately 4 feet. The audible tones grow weaker with distance complicating the desire for rapid detection. Even if a tone map was discovered, the difficulty still remains in the development of a radio receiver capable of monitoring the approximately 32 audible tones discovered in the frequency range between 14 MHz and 17 MHz, and determining how many are transmitting data and at what intervals. Complicated yes, impossible no!

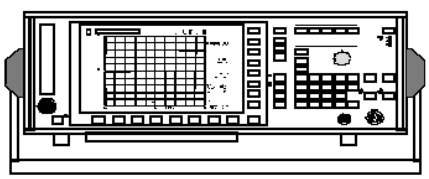
1.6.3.7 Oscilloscope



The website WhatIs (http://www.whatis.com) provides an excellent definition of an oscilloscope and it's purpose. WhatIs says "an oscilloscope is a laboratory instrument commonly used to display and analyze the waveform of electronic signals. In effect, the device draws a graph of the instantaneous signal voltage as a function of time." Oscilloscopes are available as analog devices, digital devices, hardware based or software based and everything else in between. Oscilloscopes can "display signals having frequencies up to several hundred gigahertz (GHz)" (WhatIs). While an excellent tool for detecting powerline frequencies the cost is prohibitive for the average auditor.

Software based oscilloscopes on the other hand, simulate many of the capabilities of their hardware cousins, but at a reasonable cost. One example, of a software-based oscilloscope may be found in the tool titled, "Oscilloscope for Windows," available from the Moscow State University (http://polly.phys.msu.su/~zeld/oscill.html) website. This particular tool will be coupled with the radio scanner for detailed testing later in this section.

1.6.3.8 Spectrum Analyzer



A Spectrum Analyzer (SA) is capable of detecting and displaying the radio frequency spectrum in a graphical format. Based on available research, the spectrum

analyzer is the tool of choice for detection professionals. Although it may be the tool of choice, costs for such a tool range from fifteen hundred to ten thousand or more. That does not include the training necessary to properly use the device to gather meaningful data. As always though, there are alternatives that may be explored when price is a limitation.

Spectrum analyzers are produced as purpose built hardware, computer software coupled with a compatible sound card or a combination of hardware and software. Ideally, the purpose built hardware device should yield better results. A variety of sources were researched with respect to the identification of Spectrum Analysis Devices. Examples of which included an exploration of Technical Surveillance Countermeasures (TSCM) firms, SA Test and Measurement Manufacturers and Homebrew resources (please see Poor Man's Spectrum Analyzer or W6/PA0ZN WeakSignal URL's in the reference section) for the do it yourself individual.

1.6.3.9 Combining Devices

Combining devices involves the coupling of one or more of the above methods to simulate the functions of a specific detection tool. For example, as the cost of an oscilloscope is relatively high in comparison to the cost of a Radio Scanner, it was decided that utilizing a Radio Scanner with pc based oscilloscope software might produce sufficient results for the purposes of HomePlug detection. To this point a Kenwood TH-F6A was coupled with Winscope to emulate waveform detection similar to a spectrum analyzer.

By utilizing the results of the radio scanner frequency detection in section 1.6.3.6 a range of signals of an unknown origin have been discovered. The frequencies while unknown do fall in the range of HomePlug bands from approximately 4.0 through 21.0. In this case, the following specific frequencies were identified with the Kenwood TH-F6A: 19.780, 19.785, 19.790, 19.795, 19.800 and 19.805 due to their relative strength.

Switching between each of the identified frequencies while observing the strength meter has identified 19.785 as having the strongest constant signal. This will be the selected signal to test with the WinScope software to attempt to determine if the signal(s) are related to the HomePlug devices.

While there are freeware, shareware and commercial based sound analysis packages (e.g., Winscope, Gscope, PicoScope) available, cost was a driver when selecting which package to work with. As such, the selection of a package simply titled Oscilloscope 2.51 for Windows95 (http://polly.phys.msu.su/~zeld/oscill.html) by Konstantin Zeldovich produced ample results considering the intended purpose.

The help section of the tool provides the following general overview:

> Oscilloscope for Windows95 version 2.51 (Oscilloscope 2.51) is an application showing how home PC peripherials, such as a sound card, can be used in an

unconventional way, emulating industrial ADC hardware. The Oscilloscope provides a complete functionality of a "standalone" scope in a familiar Windows ennvironment.

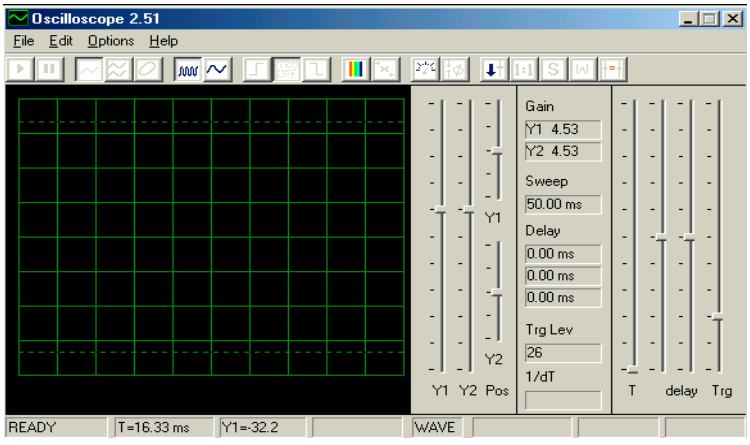
The Oscilloscope allows you, for example:
- To study in real time any signal envelope,
- To measure frequencies,
- To study realtime signal spectra,
- To plot Lissajous patterns.
- To measure a cross-correlation coefficient of two signals
  (In general, to do most things you can do with an oscilloscope and a spectrum analyzer).

When using this tool as with any, all recommended precautions should be observed to prevent damage or injury.

Input from the radio may be transferred from its speaker to a microphone attached to the computer; the results would be less than optimal. Therefore, it is recommended that a cable be purchased to connect the speaker-out port of the radio to the microphone port on the computer's soundcard. This will eliminate background noise that may interfere with the collection of signal characteristics.

When the application is first launched a blank slate is presented as shown in figure 1-7.

Figure 1-7

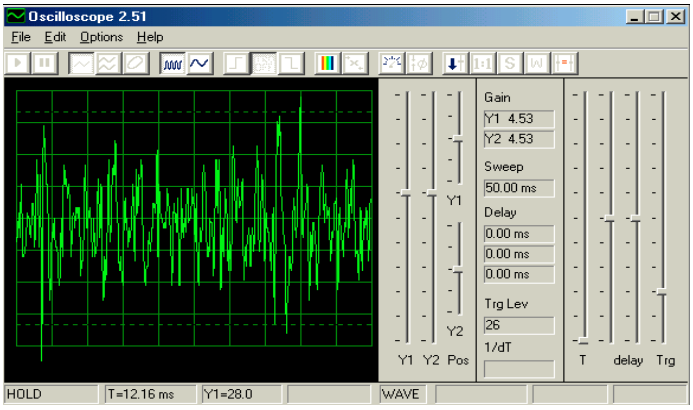


At this point, there is truly nothing required in terms of configuring the software, to begin a simple signal analysis. The steps are:

1. Ensure the cable is connected between the radio and soundcard.
2. Launch the oscilloscope application.
3. Turn on the radio and keep the volume setting as low as possible to prevent damage to the soundcard.
4. Tune to the desired frequency (19.785)
5. Click the play button on the oscilloscope toolbar.

If properly configured, the oscilloscope will spring to life with a continuous stream of peaks and valleys, or “waves,” moving from the right side of the screen to the left (as depicted in figure 1-8). At this point there is no correlation between the radio frequency and the display other than a continuous stream of noise.

Figure 1-8



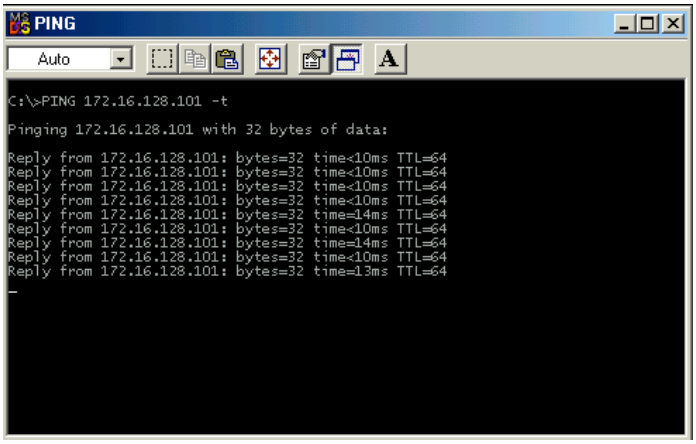
At this time, it is hypothesized that the generation of a consistent pattern of network traffic on the target system, such as a continuous PING test, should yield a consistent frequency response within the oscilloscope application.

To support this hypothesis a small adjustment to the Y1 slider is necessary. The effect of which is to reduce the amplitude displayed so that patterns of consistency may be more readily identified. Figure 1-10 illustrates the modification to the Y1 slider by clicking and dragging it down to a gain setting of approximately 1.30. Observably, the pattern now displayed within the oscilloscope window is less chaotic in appearance.

To perform the test, open a command prompt on the target system (Press Ctl+Esc, Select Run, type the word “Command” and press the enter key). Once at the command prompt, select an IP address from the list provided by the ABC Company and type the following (figure 1-9 illustrates the command) command to continuously PING the selected host:

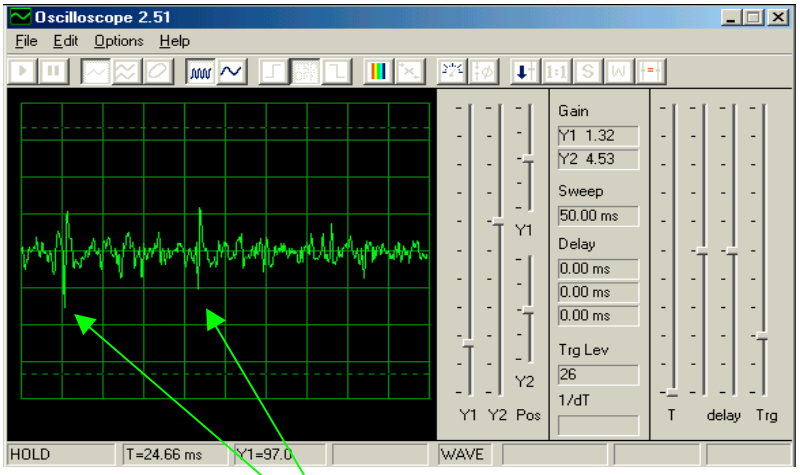
PING 172.16.128.101 –t <Press Enter Key>

Figure 1-9



After typing the PING command, return to the oscilloscope (Alt+Tab) and monitor for any consistent wave patterns. Within the current test environment a pair of signals are now visible and appear to be continuously repeated within the oscilloscope software as illustrated in figure 1-10.

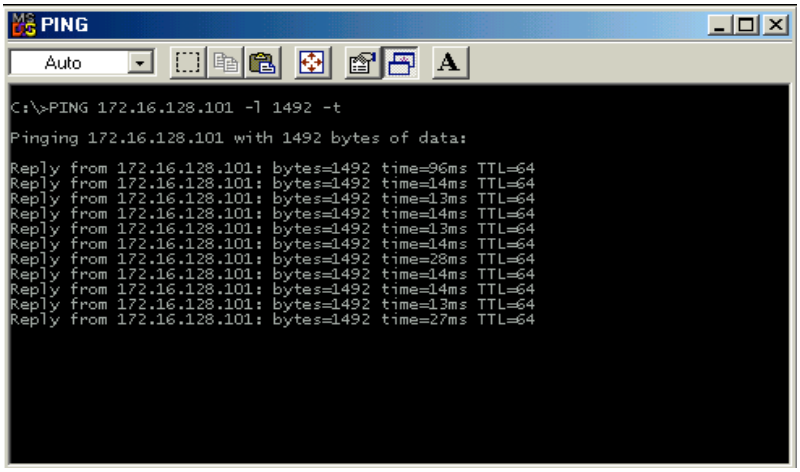
Figure 1-10



Pair of tall peaks displayed, possibly correlated to the PING test.

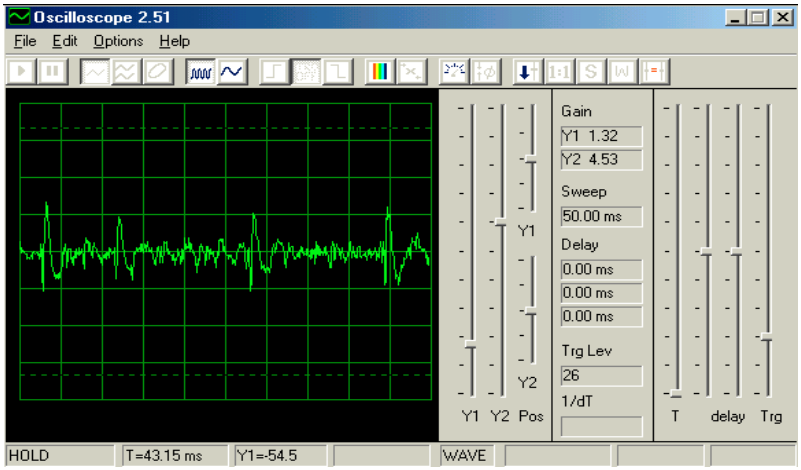
Still not certain that the results are influenced by the PING test; a further modification to the command line may force the issue. Returning to the command prompt (Alt+Tab), stop the previous PING test by pressing Ctrl+C then enter the following modified command to increase the size of the packets being transferred (please see figure 1-11 for an example of the command):
PING 172.16.128.101 –l 1492 –t <Press Enter Key>

Figure 1-11



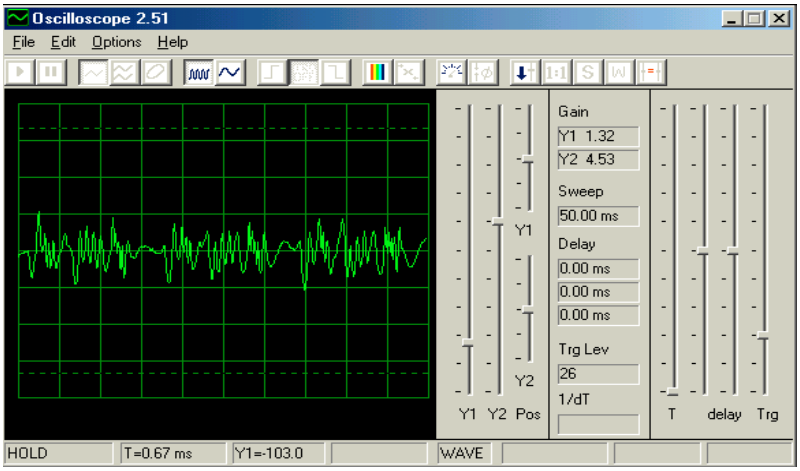
Quickly returning to the oscilloscope (Alt+Tab) to view the results of the current PING test, an entirely new pattern may be observed with an even greater frequency of waves (Figure 1-12).

Figure 1-12



If there were indeed a correlation, then turning off the ping would hopefully result in a reduction of waves. To test this final hypothesis, simply return to the command prompt (Alt+Tab) and press Ctrl+C to discontinue the PING test. Then quickly return (Alt+Tab) to the oscilloscope to monitor for any changes in wave patterns.

Figure 1-13



The results now show a series of bundled waves as opposed to the spiked waves observed in the previous trials. This may be a result of the conclusion of the PING test or again there may be no association with the HomePlug radio frequencies.

While the results of this test are inconclusive, the possibility of identifying HomePlug signals via an external radio is conceivable as evidenced by the purpose built device

constructed in the United Kingdom. Given time and modest capital resources, a simple device may be constructed to remotely "sniff" out HomePlug signals thus shortening the time necessary for auditors to detect their presence.

How likely is it then, that signals may be captured with the intent of deciphering their contents? The first hurtle of course is detection. The second is picking the correct frequency or range of frequencies, out of a possible 84 channels, to monitor and capture. Finally there is the issue of 56-bit DES that has been glossed over thus far.

If the initial challenge of rapid discovery of HomePlug signals could be surmounted, then logically the next step would be the pursuit of a means to capture and replay the signal. However, you cannot merely replay the signal from your Ethernet connected computer across a HomePlug PLC device and hope that the clear text message appears. What is likely to occur with this approach is that the HomePlug devices will hear the signal from the Ethernet side, think it is a music file and broadcast that fact to the rest of the network hoping to find a destination for the file.

Why would this occur? Encryption and decryption, according to block diagrams of the HomePlug standard, occurs on the powerline side of the device. If a captured stream of traffic were to be played back, it would have to be on the AC side. Hypothetically, a HomePlug device would treat the injected signal as noise and switch to a different frequency while blocking the injected signal in its tone map.

So how would the 56-bit DES message be decrypted? Assuming the first two obstacles could be conquered, the last step becomes transparent, as the 56-bit DES algorithm has already been broken.

1.6.3.10 Purpose Built PLC Detector

As of the writing of this document, there is only one known system that is purpose built to aid in the detection of PLC. The system was developed as the result of a "contract awarded to the University of Hertfordshire by the [United Kingdom] Radiocommunications Agency. The document pertaining to the development of the system, Ref. AY3920, is titled *Development of Practical Methods and Equipment to Facilitate Both Detection and Measurement of Radiation from, and Wideband Radio Frequency Currents in, Unstructured Distribution Networks.* The document dated January 5th of 2003 is available for review online at (http://www.radio.gov.uk/topics/research/topics/emc/ay3920.pdf). Upon conclusion of the contract, it was reported that:

> A portable measuring system for LF, MF and HF field strength measurements has been developed for use with a conventional EMC measuring receiver. The frequency range 80 kHz – 30 MHz is covered by a set of three tuned loop antennas, each with electronically controlled tuning and integral pre-amplifiers.

So there does exist a means to detect PLC communications at a distance (far field), however it may be some time before their availability and cost are in a range permitting system and network auditors to purchase them.

It should be noted that in addition to the purpose built PLC device created for the UK Radiocommunications Agency and posted to their websites, there too exists a considerable amount of documentation regarding Electromagnetic Compatibility (EMC) on their website that is pertinent to PLC communications. The documentation may be viewed online at: (http://www.radio.gov.uk/topics/research/topics/emc).

1.6.3.11 Miscellaneous and Unavailable Tools

There were many other tools identified throughout the research of RF detection methods. However, these tools were often discovered as unable to provide support for detection of the HomePlug frequencies, unavailable for purchase or still in development. A prime example of devices capable of detecting PLC but not at the HomePlug frequencies may be found online by visiting http://www.hometech.com/tools/signal.html. The tools initially appear promising but upon inspection turn out to be designed for X-10 PLN frequencies rather than HomePlug.

As for the category of tools unavailable for purchase there were many. Two specific examples would be the countermeasure equipment developed by Martin L. Kaiser (http://martykaiser.com) and a clamp-on detector detailed in the XXX 1992 edition of Radio Communications. In the case of Martin Kaiser, his website contained a number of potentially useful devices (e.g., 2030A Probe, etc.) that may produce positive results, however manufacture, support of these devices is limited, and the time constraints for this project restricted further pursuit. As for the article contained in the Radio Communications Magazine, it too suffered from the time constraints of the project. While the time constraints restricted short time viability, the aforementioned items still represent items worthy of further investigation in the pursuit of a device or devices that may be used by the lay-audit practitioner for the detection of RF emitting devices with respect to PLC.

There too remains the category of tools still in production as evidenced by the Corinex Diagnostics Kit. As of September the devices were still in developed and slated for fourth quarter production and accordingly, unavailable for purchase and experimentation. They should however, not be ruled out as a viable tool for future consideration when developing improved methods for PLC detection.

1.7 Summary of Current Practices for Radio Frequency Detection

In summary as observable in table 1-15, the current state of practice for discovering low-voltage power line communications by means of radio frequency detection is in its relative infancy. That is not to say that radio frequency detection is an immature practice as may be construed from other wireless networking technologies.

Table 1-15 – Comparison of Radio Frequency Detection Equipment

Detection Method	Purpose	Cost (in US dollars)	Proximity	Effectiveness (based on experimentation)
HomePlug Network Device	PLN Device	< $100	Access to electrical segment required	Highly Effective
True RMS Digital Voltmeter	Frequency display of detected harmonics	>$100	Access to electrical segment required	Ineffective
AC Current Clamp	Same as True RMS DVM	>$100	Access to electrical segment required	Untested
Field Strength Meter	Relative strength of an RF transmitter	>$100	Range undetermined	Ineffective
Frequency Counter	Detects frequency of nearby transmission	>$100	Range undetermined	Tested but Ineffective without a Notch Filter
Radio Scanner	Capable of scanning and tuning desired frequency	>$400	Range undetermined	Undetermined
Oscilloscope	Capable of displaying the waveform of a detected frequency	>$1000	Range undetermined	Undetermined
Spectrum Analyzer	Capable of measuring the RF spectrum	>$3000	Range undetermined	Untested
Purpose Built PLC Detector	Cable of detecting PLC devices.	>unknown		Assumed highly expensive and highly effective

For example, wireless “RF” mediums to include 802.11b, 802.11b and Blue Tooth are more readily discovered due to the outwardly emanating signals borne from antennas. Comparatively, low-voltage power line devices utilize the shielded cabling of power lines as their antennas thus tunneling the waves into the cable rather than away from it. This complicates matters as the broadcasted signal may be discovered at any point along an electric cable run without revealing the exact location of a PLC device. A field strength meter should provide some assistance but as discussed in previous sections, most are not tuned to the specific frequencies covered by PLC.

It should be observed that an auditor equipped with a combination of the tools listed above in conjunction with the training and experience necessary to operate them

expertly, has in essence stepped out of the realm of system and network auditing and into the world of Telecommunications Surveillance and Countermeasures (TSCM).

Further to that point, unless the art and science of Radio Frequency Detection is a direction the auditing profession seeks to attain, the recommended course of action would be the continued use of existing system and network auditing practices. That is until such time that improved methods for the observation and discovery of low-voltage HomePlug powerline network devices, becomes readily available at a palatable cost.

1.8 Summary of Current Practices

Despite repeated efforts to identify practices specific to HomePlug PLN's, all attempts were met with limited success. There are however, generally accepted practices available for system and network auditing that may be combined with the results of the experimentation that occurred during the exploration of radio frequency detection to produce a new and recommended approach towards implementing HomePlug PLN's with security in mind. The next section titled Audit Checklist will serve to unite all of the research and experimentation to date, in an easy to use HomePlug Audit Checklist.

2 ASSIGNMENT II – CREATE AN AUDIT CHECKLIST

The audit checklist was developed based on the requirements contained within the practical assignment. However, to address all of the required sections within a single table, other sections of this document will be cross-referenced rather than duplicated within the table. Examples of sections that will be cross-referenced include the references table from the end of this document and the risk table created in section one.

Building upon the references table from the beginning of this document, the risk table will be added as a reference item. Table 2-1 will be used in turn for documenting the source or sources referenced to develop each checklist item.

Table 2-1 – AUDIT CHECKLIST REFERENCES

ASSIGNED SOURCE NAME	SOURCE NAME	SECTION OR PAGES REFERENCED
CWNA	Certified Wireless Network Administrator	Entire book and specifically Chapter Eleven
MICR	Microsoft Support Knowledgebase	Articles specific to Windows 9/X security
NIST	NIST 800-42 Guideline on Network Security Testing	Entire Paper
PEOC	Personal Experience or Contribution	None
RISK	Risk assessment table from this guide.	Entire Table.
SBIT	Small Business IT Auditing	Sections specific to auditing Windows 98
TLAH	Thinking Like a Hacker	Entire paper
WE2E	Wireless Security: End to End	Entire book and specifically pages 172 thru 174
HAXP	Hacking Exposed: Network Security Secrets and Solutions	Chapters 2, 3 and 4
EICAR	EICAR Virus Test (http://www.eicar.org/anti_virus_test_file.htm)	Entire Website
CESP	Secrets of Computer Espionage: Tactics and Countermeasures	Entire Table

The assigned risk ID's contained within table 1-6, will be referenced throughout the audit checklist so that the identified risks, profile and consequences may be cross referenced as required.

Table 2-2, was created to address the GSNA practical requirement to identify and recommend controls. The primary source of information for the development of table 2-2 was extracted from Thomas Peltier's book titled *Information Security Risk Analysis* on pages 82-84. Additional resources were called upon to draft the list of controls and those sources are referenced in table 2-1 s well.

Table 2-2 - Controls

Control Number	Control Name	Control Category			Control Type			Control Description	Reference
		Preventive	Detective	Corrective	Management	Operational	Technical		
1	Security Policy	X			X	X	X	A current and documented security policy should be available to all employees and all employees should be familiar with its contents.	POLI
2	Monitoring & Supervising	X	X	X	X	X	X	Management controls should be in place to monitor and supervise employee activities.	POLI
3	Roles And Responsibilities	X	X		X	X	X	All organizational roles should be documented and their responsibilities clearly stated.	POLI
4	Personnel Procedures	X	X		X	X	X	Procedure for performing background investigations prior to any hiring decision should be documented. Disciplinary actions up to and including termination should be documented.	POLI
5	Awareness Training	X	X		X	X	X	Employees should attend yearly security awareness training to reinforce the organizations commitment to the security of its assets.	POLI
6	Authentication	X					X	Implement user authentication mechanisms (such as firewalls, dial-in controls, secure ID) to limit access to authorized personnel.	PELTIER
7	Authorization	X			X		X	Only individuals with a “need-to-know” and processed on an “event-by-event” basis will be authorized access to identified assets.	POLI
8	Encryption	X					X	Implement encryption mechanisms (data, end-to-end) to prevent unauthorized access to protect the integrity and confidentiality of information.	PELTIER
9	Audit Logs		X			X	X	Implement mechanisms to monitor, report, and audit activities identified, as requiring independent reviews, including periodic reviews of user ID’s to ascertain and verify business need.	PELTIER
10	Anti-Virus Software	X	X	X			X	Install corporate standard anti-viral software on all computers. Provide training and awareness of virus prevention techniques.	PELTIER
11	Spyware Software		X	X			X	Information resources must be guarded against the accidental or intentional installation of spyware (e.g., tracking cookies, key loggers, etc.).	POLI
12	Firewall	X	X				X	A firewall should be engineered, monitored and managed by the security organization to aid in the protection of perimeter security. Requests to permit traffic to traverse the firewall will be viewed for business need and approved or denied based on	POLI

								an analysis of the exposure created by said request. Furthermore logs must be viewed on a monthly basis to determine compliance with the corporations acceptable use policy. Failure to comply with the acceptable use policy may lead to disciplinary action.	
13	Alarms and Alerts		X			X		Security alarms and alerts must be monitored and responded to daily.	POLI
14	Restricted File Sharing	X			X		X	Open file sharing will be restricted to file servers, mail servers, or systems reviewed and approved by management based on business need.	Contribution
15	Password Composition	X					X	Password should be composed of: 1. Upper and Lower Case Alpha Characters 2. Numeric Characters 3. At least one special symbol character 4. No more than two characters should be repeated consecutively 5. The combination of characters must be between 6 and 8 characters in length. 6. The word must not be a common dictionary word 7. The word must not utilize the organizational name.	POLI
16	New or Advanced Technologies	X			X		X	Develop policies and procedure to prohibit the use of new technologies until reviewed and approved by corporate security organization.	Contribution
17	Physical Security	X	X		X			In consultation with facilities management, facilitate the implementation of physical security controls designed to protect the information, software, and hardware required of the system	PELTIER
18	Inventory (network, system)	X			X	X		All information systems and network elements must be inventoried. Inventories must be updated and maintained on a quarterly basis. A current inventory provides a ready reference for troubleshooting issues and incidents.	POLI
19	Network and System Topology	X			X	X		A detailed network and system topology depicting the interconnection between systems must be maintained. Topologies must be reviewed and updated on a quarterly basis. A current topology provides a ready reference for troubleshooting issues and incidents.	POLI
20	Network and System Monitoring		X			X	X	A centralized monitoring and management platform must be implemented to maintain software currency as well as to aid in the detection and resolution of issues and incidents.	POLI
21	HomePlug Detection, Monitoring and Management	X	X				X	Process must be enabled to routinely inspect for the presence of HomePlug devices. If HomePlug is used within any facility where sensitive corporate data is transmitted, processed or	Contribution

								stored (including vendor and third party facilities) then appropriate controls as outlined within the policy must be implemented. Controls should also provide for the monitoring, management and auditing of HomePlug devices.	
22	Screensaver Requirements	X				X	X	All information systems must utilize a password-protected screensaver. The password must comply with corporate composition standards.	POLI
23	Secure System Configuration	X	X			X	X	Systems will maintain current security patches and be configured according to corporate minimum-security baselines and recognized best practice guidelines.	POLI

Table 2-3 – HomePlug Audit Checklist

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
1	1 2 3	N	N	CWNA PEOC	17 18 19		S	Utilizing a map of the facility (with powerline source documentation if possible) walk the entire property boundary, internal and external building perimeter and office locations to visually inspect for: 1. The presence of powerline devices based on identified form factors. 2. The identification of areas where powerline devices may be covertly placed. The presence of power outlet locks for external locations.				TARGET: Locking AC covers should be identified in external locations. External AC outlets should not be obstructed from routine observation. There should be no Powerline devices attached to any external or internal AC outlets that are easily visible.
2	1 2 3 32	N	Y	PEOC	18 19 20 21	O		While performing the physical inspection identified in step one, locate unique power segments based on the provided facility map and perform a PLN activity audit by: 1. Plugging the auditor's HomePlug device into an AC outlet. 2. Permit 15-30 seconds to elapse 3. Record any observable HomePlug traffic based on the Activity LED. 4. Repeat steps 1 thru 3 until completed.				TARGET: The HomePlug Activity LED should not display PLN activity for any AC outlet connection.

Table 2-3 – HomePlug Audit Checklist continued

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose		Test Procedure	Test Results			Compliance (*Other requires a detailed explanation)
						Objective	Subjective		Pass	Fail	Other*	
3	18 19	Y	N	NIST PEOC HAXP	18 19	O		Utilize an automated network scanner to: 1. Identify systems connected to the network 2. Determine what ports are open on the identified systems. Compare the results of the scan with the inventory provided by ABC Corporation. Note any discrepancies and document them for the final report.				TARGET: The network scanner should not detect network addresses for previously unknown and non-inventoried equipment.
4	33	Y	N	HAXP PEOC	18 19 20 21	O		Utilize a packet capture and analysis utility to: 1. Identify the presence of HomePlug traffic 2. Identify the devices using the HomePlug protocol. 3. Examine the contents of HomePlug packets to determine if they contain any sensitive command and control details (i.e., passwords) that may be viewed in clear text. Compare the results of the packet capture and analysis tool with any devices identified in the previous step that were not on the provided inventory.				TARGET: HomePlug traffic should not be detected within the environment per contract with ABC Corporation. If HomePlug traffic is discovered, it should be analyzed to determine susceptibility to command and control monitoring.

Table 2-3 – HomePlug Audit Checklist continued

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
5	4 6 15 17 20	Y	N	NIST PEOC	18 20	O		Utilize an automated network vulnerability scanner to determine: 1. Operating system fingerprints 2. Open ports and running processes 3. Potential exposures or vulnerabilities Pay careful attention to any hosts discovered that were not listed in the inventory provided by the customer.				TARGET: Systems should be configured with only those network services and system processes required for business needs and approved by management. A vulnerability scan should produce negative results for widely known and often targeted system and network vulnerabilities.

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
6	6 10	Y	Y	HAXP TLAH	6 14 18 19 20 23	O		Commercial HomePlug configuration software requires a Windows based operating system; as such, a NetBIOS enumeration will be performed to determine whether any open shares exist on systems potentially identified as passing HomePlug traffic. First, attempt to connect to any discovered shares without a password (stimulus/response test with a desired outcome to connect without a password proving weak controls). If unable to connect without a password, attempt to utilize a brute-force password utility to attach to the share and determine whether the password meets corporate standards for composition. Finally, if unable to remotely brute force the password, use a local password utility to determine whether the password meets corporate standards for composition.				TARGET: Windows shares should not be permitted on non-enterprise class operating systems. If discovered, a share password must be enabled and the same password should be compared against the ABC Corporate policy to determine compliance with composition requirements.

Table 2-3 – HomePlug Audit Checklist continued

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose		Test Procedure	Test Results			Compliance (*Other requires a detailed explanation)
						Objective	Subjective		Pass	Fail	Other*	
7	5	Y	Y	CESP	6 15 23	O		Properly shutdown the operating system and then reboot the computer to determine whether the BIOS password is enabled. Performing this step may lock the auditor out of the system. Therefore it is recommended that the auditor either prepare a system boot disk with appropriate CMOS password identification utilities or have the end-user for the selected system available during the BIOS password test.				TARGET: The BIOS password must be set to restrict access to the system configuration.
8	7	Y	Y	PEOX CESP HAXP	6 7 15 22 23	O		Determine if the system screensaver is configured to utilize a password by performing the following steps: 1. Click on Start and then Run 2. In the Run dialog box type the following without quotations "FLYING~1.SCR" 3. Allow 5-10 seconds to pass for the screen saver to activate. 4. Bump the mouse or press the spacebar to determine if the screen saver disappears or if a password dialog box appears.				TARGET: The screensaver must prompt for a password.

Table 2-3 – HomePlug Audit Checklist continued

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
9	9	Y	Y	CESP HAXP	6 7 18 22 23	O		Determine if the CDROM "autorun" feature is disabled by: 1. Enable and lock the screensaver password using the technique established in step XXX. 2. Insert the screensaver bypass CD and allow 15 to 30 seconds to elapse. 3. If autorun is enabled the screensaver will unlock and permit console access. If autorun is disabled nothing will happen.				TARGET: The autorun feature should be disabled to reduce the likelihood of unauthorized access
10	8	Y	N	CESP HAXP	6 18 22 23	O		Determine if the screensaver password meets corporate standards for composition by performing the following steps: 1. Insert the CAIN password utility CDROM or write protected floppy into system. 2. Click on Start and then Run. 3. Type the drive location and name of the file in the run dialog box or click on browse. Once the name is correctly entered, click on OK to proceed. 4. Select the appropriate tab within the password utility to display the currently assigned password.				TARGET: The screensaver password should be compared against the ABC Corporate policy to determine compliance with composition requirements.

Table 2-3 – HomePlug Audit Checklist continued

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose		Test Procedure	Test Results			Compliance (*Other requires a detailed explanation)
						Objective	Subjective		Pass	Fail	Other*	
11	13	Y	Y	EICAR	10	O		Determine if a corporate approved anti-virus application is: 1. Installed on the system 2. Using current virus string files 3. Configured to run automatically 4. Capable of detecting the EICAR test file Once the above steps have been completed, reboot the system and perform a second anti-virus scan using a write-protected floppy or bootable CDROM to further determined if the installed anti-virus software is functioning properly. Any commercial version of anti-virus software may be utilized as long as it is not the same manufacturer as the currently installed AV software.				TARGET: Per Corporate policy, the device must contain an approved anti-virus application with a current virus definition file and be configured to run routinely and automatically. The same anti-virus software must be capable of detecting the simplest of viruses as evidenced by the EICAR test. A secondary scan of the system using a competing anti-virus application should validate the cleanliness of the system.
12	14	Y	N	PEOC	11	O		Determine if the system contains spyware by: Utilizing a commercial malware scanner to identify known instances of spyware/adware. Report the results of the test but do not clean system at this time.				TARGET: The system should be clean of spyware.

Table 2-3 – HomePlug Audit Checklist continued

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
13	4 15 17 20	N	N	MICR	18 23 24	O		Microsoft provides the following manual process to determine if current operating system security patches have been installed in their 1. Click Start, point to Find, click Files Or Folders, type "wulog.txt wuhistv3.log" (without quotation marks) in the Named box, and then click Find Now. 2. Double-click the Wulog.txt file, and then note the update information. 3. Double-click the Wuhistv3.log file, and then note the update information.				TARGET: The system should have all current security patches installed.

Table 2-3 – HomePlug Audit Checklist continued

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
14	28 29 30	Y	N	PEOC	6 8 23	O		HomePlug devices may operate with the default Network Encryption Key (NEK) of "HomePlug" or with a user assigned NEK. If a HomePlug device is located, then an analysis of the attached computer should be performed by: 1. Install the HomePlug software provided with the PLC device purchased by the auditor for the ABC contract. 2. Examine the contents of the manufacturer's application directory (typically C:\Program Files\Manufacturer) to determine if any files exist that may contain passwords. 3. Examine the contents of the files to determine if a clear-text password may be discovered. 4. If a password is discovered, does it meet the corporate standards for composition? 5. Utilize a packet capture utility to determine if any PLN device command and control traffic is passed in the clear.				TARGET: The auditor should determine whether HomePlug configuration software is present. If it is, then the installation directory should be examined to determine if it contains a clear-text password. If a clear-text password is present, it should be compared against the ABC Corporate policy to determine compliance with composition requirements.

Table 2-3 – HomePlug Audit Checklist continued

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
15	41 42	N	N	PEOC	1 2 3 4 5 9 12	O		Examine inbound and outbound firewall logs to locate: 1. Previously unidentified outbound IP addresses 2. Suspicious inbound traffic destined for any IP addresses identified in step 1. 3. Destination IP addresses of known or questionable content.				TARGET: The auditor should not discover any previously unidentified outbound IP addresses when compared to the inventory. The auditor should not discover any inbound traffic destined for any IP Addresses discovered in step 1. If previously unidentified IP addresses are discovered, a thorough analysis of their destination traffic should be investigated to determine whether sites of known or questionable content are being accessed.

3 ASSIGNMENT III - AUDIT EVIDENCE

3.1 Conduct the Audit

Each test section will be introduced by the corresponding audit checklist item, in a table format, followed by the captured during testing. Comments regarding the results of the test and the ascertained level of compliance may be found at the end of each test section.

3.1.1 *Evidentiary Procedure One*

Table 3-1 – Requirements for Evidentiary Procedure One

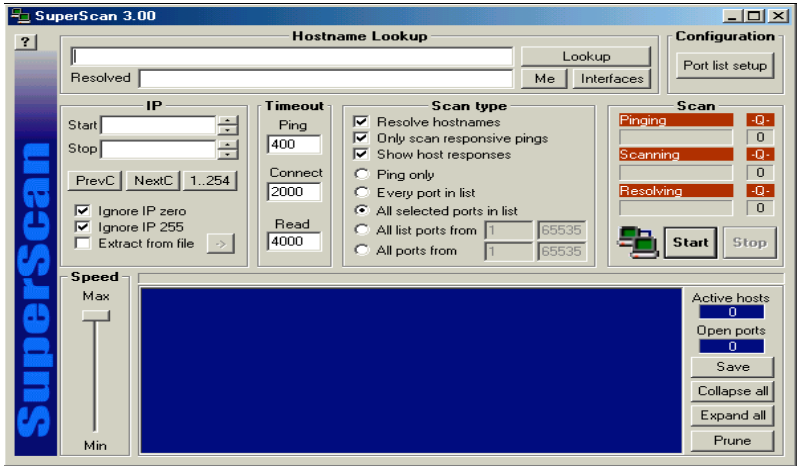
Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose		Test Procedure	Test Results			Compliance (*Other requires a detailed explanation)
						Objective	Subjective		Pass	Fail	Other*	
3	18 19	Y	N	NIST PEOC HAXP	18 19	O		Utilize an automated network scanner to: 3. Identify systems connected to the network 4. Determine what ports are open on the identified systems. Compare the results of the scan with the inventory provided by ABC Corporation. Note any discrepancies and document them for the final report.		X		ACTUAL: IP address 172.16.128.103 was discovered and compared against the ABC Corp. provided host inventory list and determined to be absent from said list. The system was identified as having the following ports open: 135/tcp 137/tcp 139/tcp 427/tcp 1032/tcp

3.1.1.1 Screenshots from Evidentiary Procedure One

There are two essential areas to configure prior to launching a network scan. The first requires the identification of the target IP subnet and the second requires the selection of a port list. SuperScan offers the ability to select specific ports and then permit the selected list to be saved for future use. It also provides pre-configured lists for the scanner and trojan ports. For the ABC scan, we will use a saved scan where all ports have been selected.

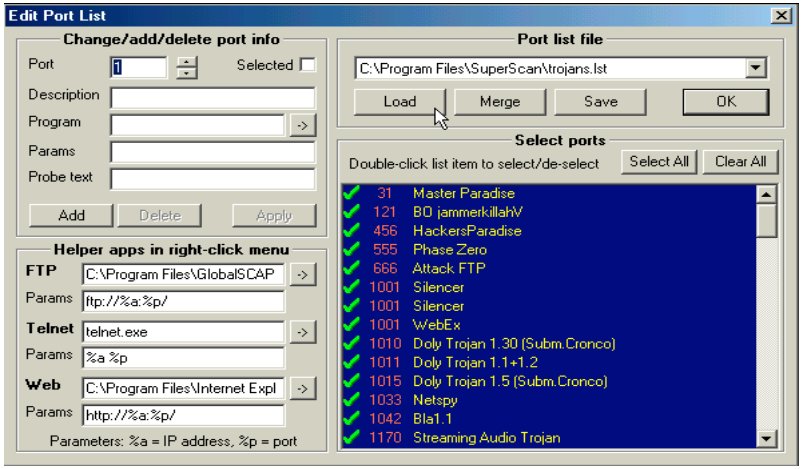
Step 1-Using SuperScan, version 3.0, to identify IP addresses and open network resources.

Figure 3-1



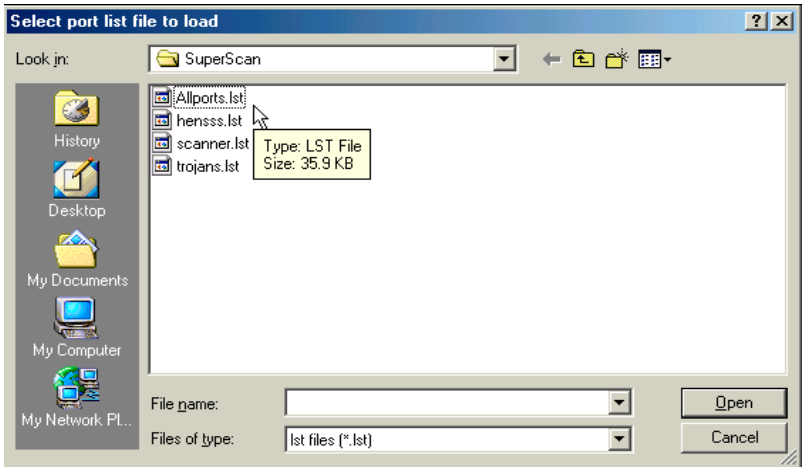
Step 2 – The first step is to configure the list of ports to for scanning as shown in figure 3-2.

Figure 3-2



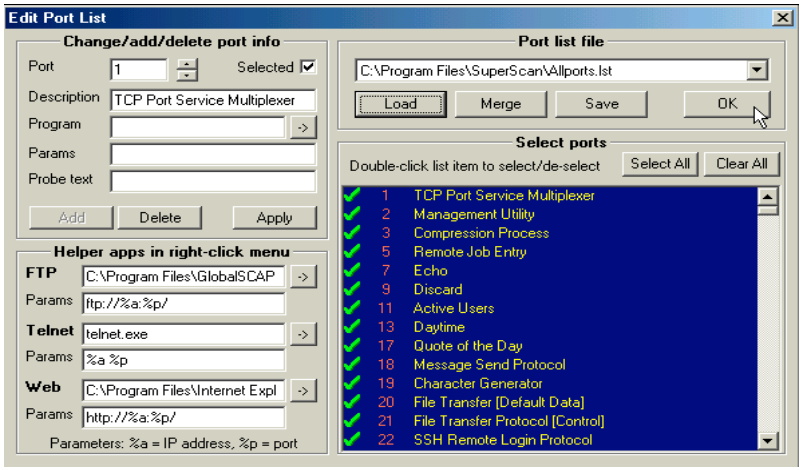
Step 3 – XYZ Company has selected the list titled “Allports.lst” for the ABC Corporation scan. After selecting the list, click “Open” to proceed as shown in figure 3-3.

Figure 3-3



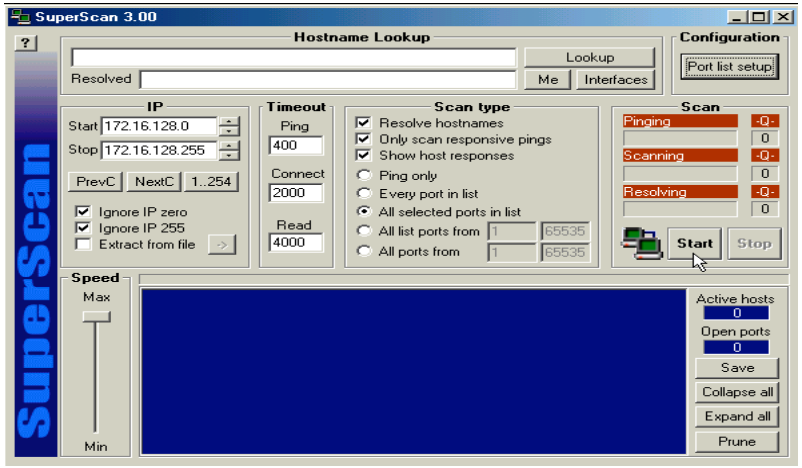
Step 4- After selecting the list you will return to the Edit Ports interface, just click “OK” to return to the main SuperScan interface as shown in figure 3-4.

Figure 3-4



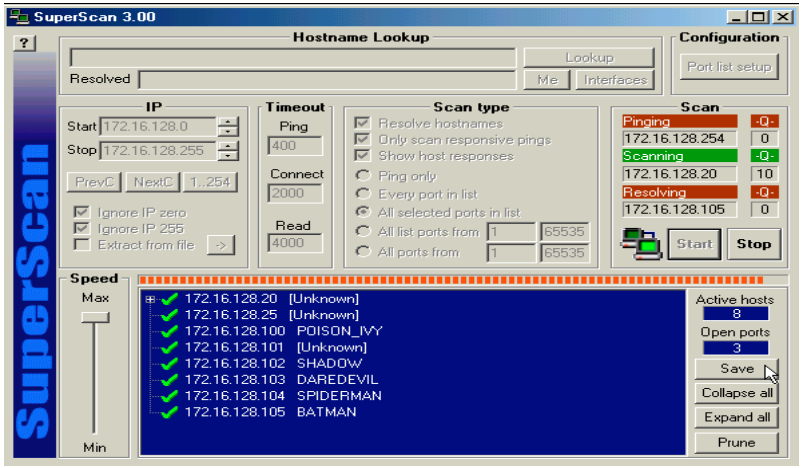
Step 5 - From the main SuperScan screen, select the “Start” button to initiate the scan as shown in figure 3-5.

Figure 3-5



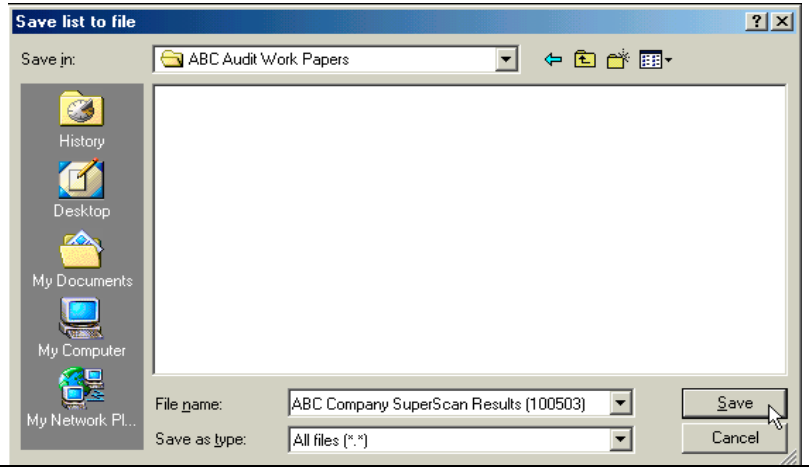
Step 6 - Once completed the box at the bottom of the screen will reflect the identified IP addresses as well as permit the opportunity to expand each IP address to discover what ports were identified as open by the SuperScan tool.

Figure 3-6



Step 7 – However, rather than expand the list now, it will be saved for inclusion in the audit findings report by utilizing the “Save” function to the right of the window as shown in figure 3-7.

Figure 3-7



3.1.2 *Evidentiary Procedure Two*

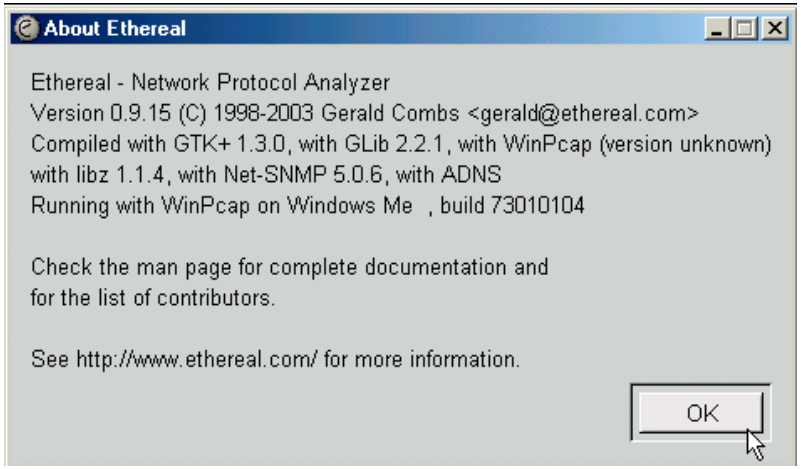
Table 3-2 – Evidentiary Procedure Two

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose		Test Procedure	Test Results			Compliance (*Other requires a detailed explanation)
						Objective	Subjective		Pass	Fail	Other*	
4	33	Y	N	HAXP PEOC	18 19 20 21	O		Utilize a packet capture and analysis utility to: 4. Identify the presence of HomePlug traffic 5. Identify the devices using the HomePlug protocol. 6. Examine the contents of HomePlug packets to determine if they contain any sensitive command and control details (i.e., passwords) that may be viewed in clear text. Compare the results of the packet capture and analysis tool with any devices identified in the previous step that were not on the provided inventory.		X		ACTUAL: HomePlug traffic based on the Intellon MAC management protocol (0x887b) was discovered emanating from host 172.16.128.103. This validates the results of step 2. Traffic generated by this workstation was captured and a detailed packet analysis was performed to determine if sensitive, clear-text information could be extracted from the packets. Upon completion of the analysis, it was determined that the captured packets did not contain information that could affect the availability or the HomePlug PLN. As an added precaution, a packet capture and analysis was performed during the configuration of a HomePlug device to determine the susceptibility to clear-text password theft of the NEK. This secondary test produced no useful details regarding the NEK.

3.1.2.1 Screenshots from Evidentiary Procedure Two

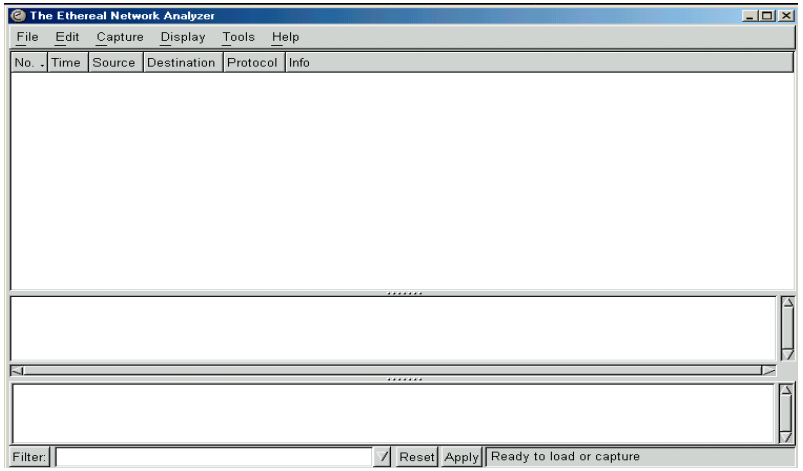
Step 1-Using the GUI version of Nessus, version 1.4.4, in conjunction with a SuSe Linux based Nessus daemon to perform a network vulnerability assessment.

Figure 3-8



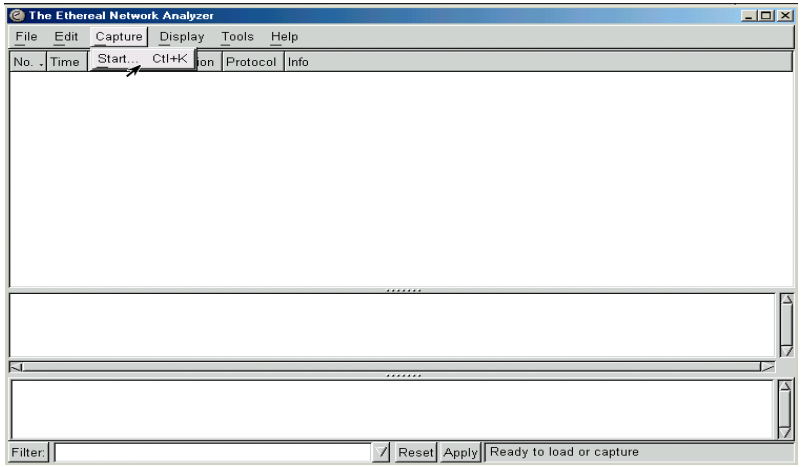
Step 2 –Launching Ethereal brings the auditor to the main console window as shown in figure 3-9.

Figure 3-9



Step 3 - Prepare for a new capture session by clicking on “Capture” and then “Start.”

Figure 3-10



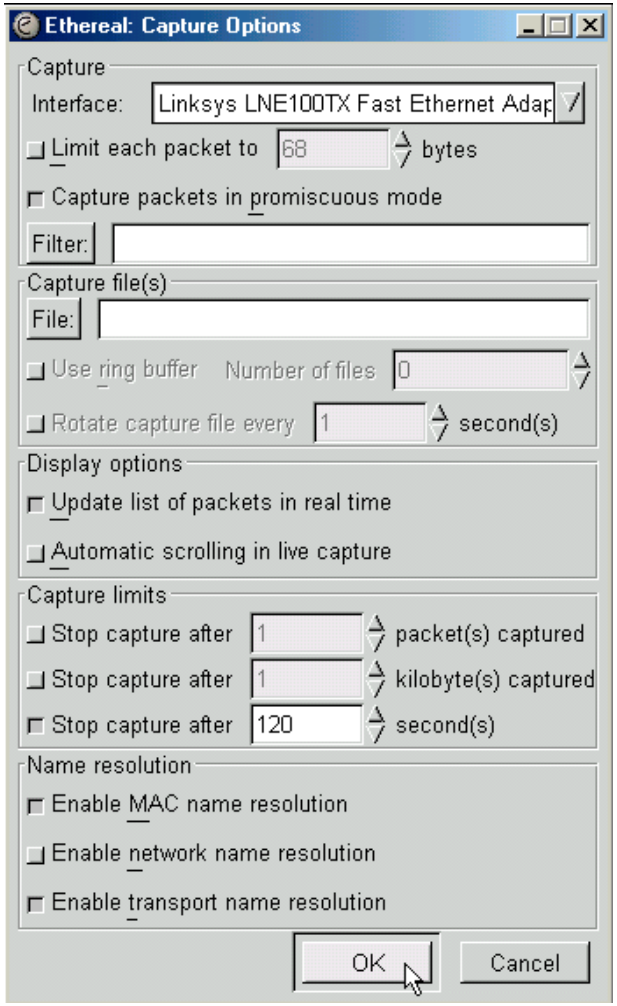
Additional Comments: Perform the following list of items to configure the capture options as shown in Step 4, figure 3-11:

1. Selecting the appropriate interface.
2. A personal preference is to update the list of packets in real time (this may also impact performance depending on the speed of the computer) by selecting the corresponding check box.
3. Configure the “Capture Limits” to stop capturing packets after one minute (this may be modified to run for as long as necessary, or until a specific quantity of packets or kilobytes is reached).
4. Finally, ensure that MAC and Transport Name resolution is selected.

Once configured click on the “OK” button to proceed.

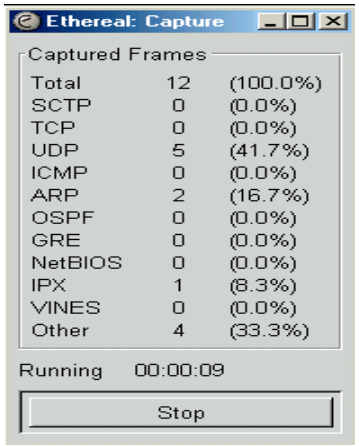
Step 4-Configuring the capture options.

Figure 3-11



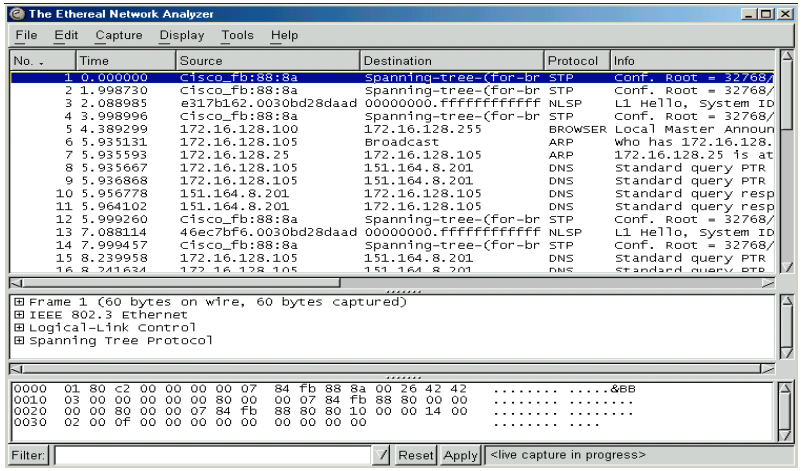
Step 5 –The capture begins immediately. A statistics window appears on the screen to address the types and quantities of files that are being captured.

Figure 3-12



Step 6- The main console window is also open for viewing. The live capture is shown in figure 3-13 as configured in the “Capture Options,” window from step 4.

Figure 3-13



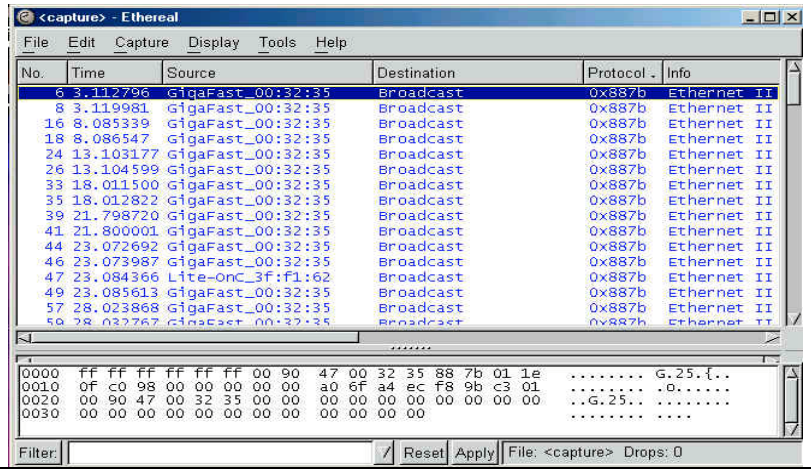
Additional Comments: A typical HomePlug configuration includes the installation of software that initializes during system start-up. The initialization calls and then loads a process into memory called “BridgeDecor.” BridgeDecor appears to call a second process named “WinPLCman.”

Experimenting with these processes by deleting them from the running program list does not appear to impact the ability for the device to communicate with the HomePlug network when running in BRIDGE mode (deleting them in NODE mode was not tested). Additionally, it was observed that allowing them to run severely impacts system performance. The cause of the impact appears to be tied to the routine broadcast requests generated by the pair of processes.

The broadcast requests, in turn, make the identification of HomePlug traffic fairly straightforward.

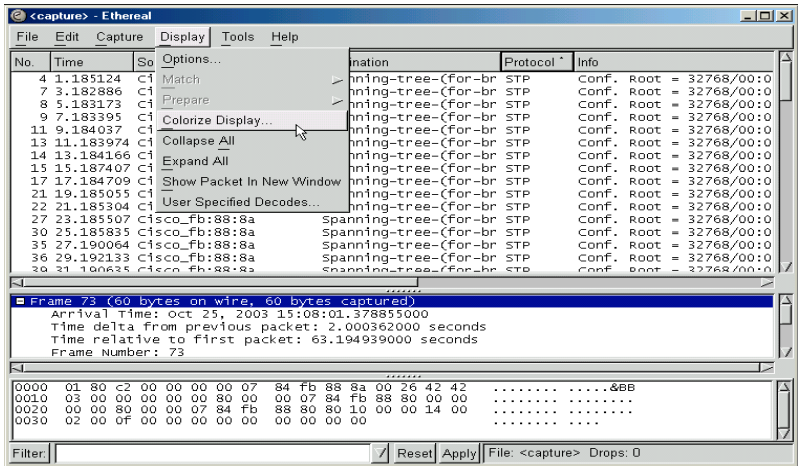
Step 7: The broadcasts occur at rapid intervals and will quickly fill a packet capture window as depicted in figure 3-14 (as well as clog a network segment).

Figure 3-14



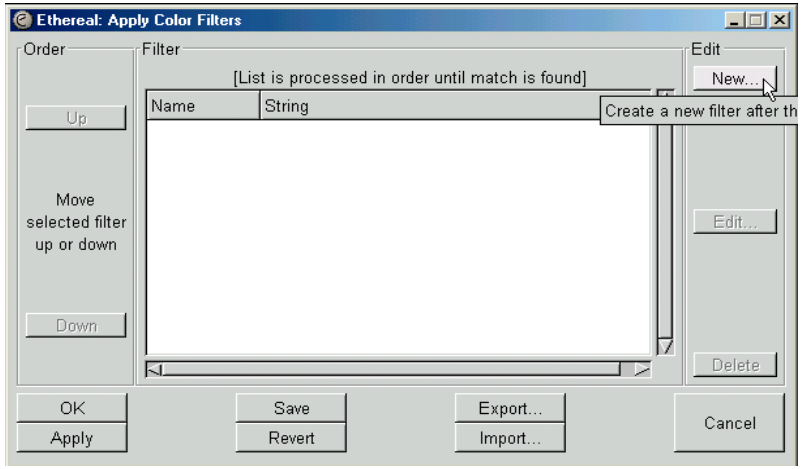
Step 8 – Optionally, Ethereal may be configured to “Colorize the display,” making HomePlug traffic identification even easier for an auditor. The first step to filtering for HomePlug traffic requires the auditor to click on “Display” and then “Colorize Display,” as shown in figure 3-15.

Figure 3-15



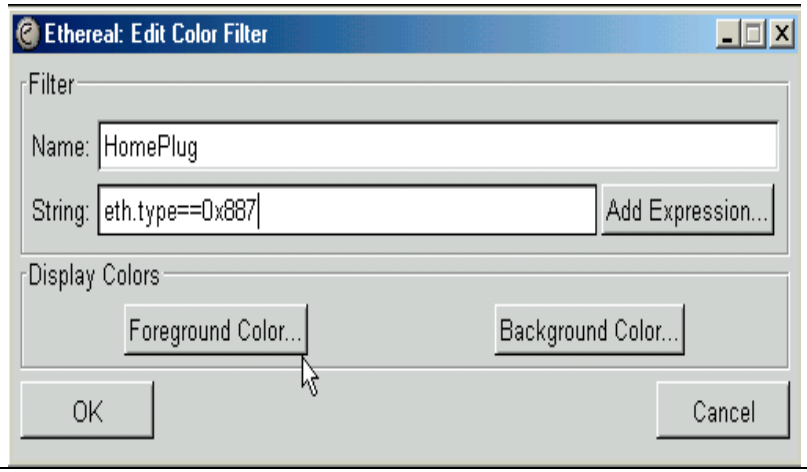
Step 9 – Next the auditor will click on the “New” button within the “Apply Color Filters” dialog window, as shown in figure 3-16.

Figure 3-16



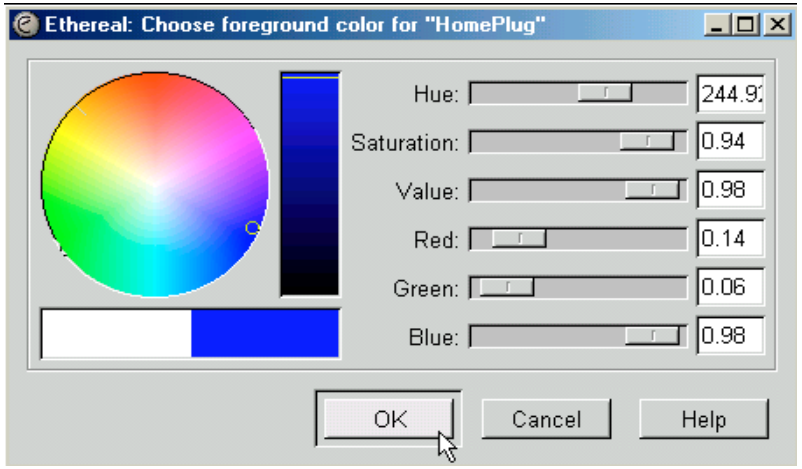
Step 10 - Enter a new name for the filter. Then use the expression builder or copy the string listed in figure 3-17 to define the "Intellon MAC management packets (ethertype = 0x887b)."

Figure 3-17



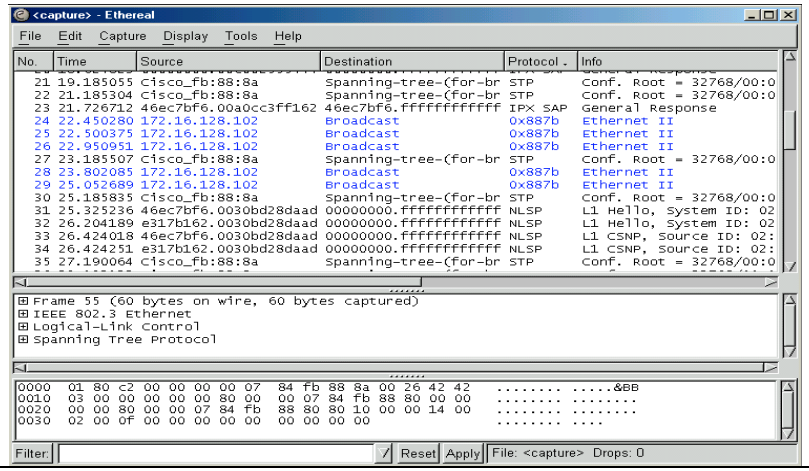
Step 11: Select a foreground color that will help the HomePlug protocol standout if detected by clicking on the "Foreground Color" button as shown in step 10. Select the desired color, in this case blue was chosen. Click the "OK" button when complete to return to the "Edit Color Filter" window and then click the "Apply" followed by the "OK" button from the "Apply Color Filters" window to return to the main Ethereal console.

Figure 3-18



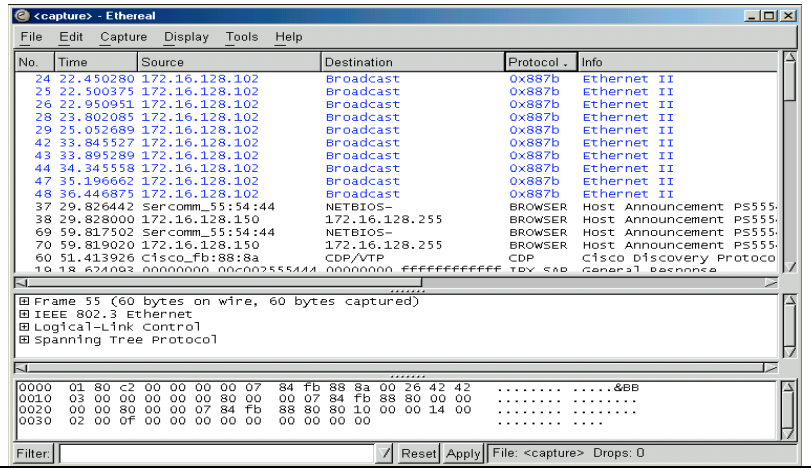
Step 12 - Any HomePlug packets will now stand out in the display during packet capture as shown in figure 3-19.

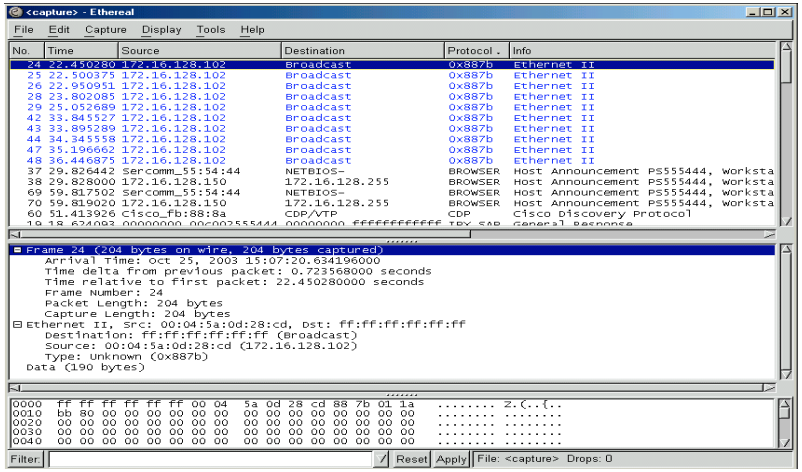
Figure 3-19



Step 13 – Optionally, by clicking on the "Protocol" column from the main console, the list will be sorted thus consolidating all HomePlug entries to the same section as shown in figure 3-20.

Figure 3-20



Step 14 - The middle console window displays the packet details while the bottom window displays the packet contents as shown in figure 3-21. Figure 3-21 	Additional Comments: Viewing the contents of all of the packets does not present any clear text information that may pose a threat to the configuration of a HomePlug device. However, the same packet capture and analysis will be performed during the PLC software installation and device configuration to determine if the NEK is passed in the clear, presenting an opportunity for compromise. Before quitting Ethereal, save the contents of the capture session for evidentiary purposes. To save the session, click on “File” and then “Save as.” The file should be placed along with the other evidentiary documentation on the local disk for later use.

3.1.3 *Evidentiary Procedure Three*

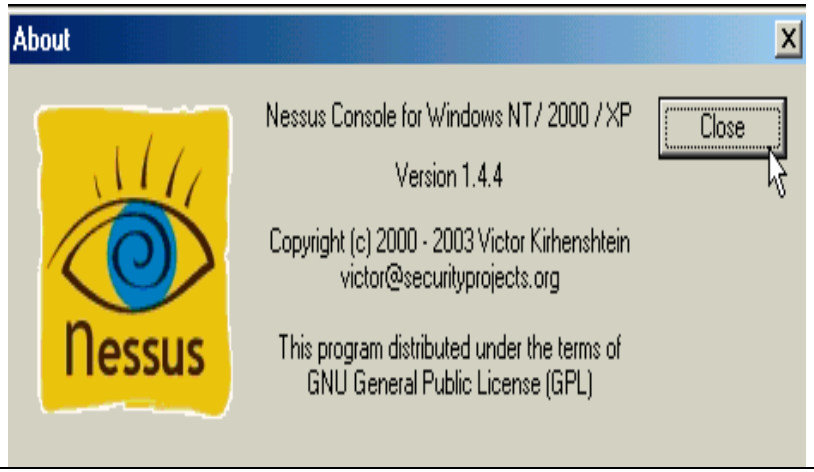
Table 3-3 – Evidentiary Procedure Three

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
5	4 6 15 17 20	Y	N	NIST PEOC	18 20	O		Utilize an automated network vulnerability scanner to determine: 4. Operating system fingerprints 5. Open ports and running processes 6. Potential exposures or vulnerabilities Pay careful attention to any hosts discovered that were not listed in the inventory provided by the customer.		X		ACTUAL: The Nessus network vulnerability-scanning tool discovered open ports and services that may be exploited with readily available tools. The results of the scan will be provided in the final report.

3.1.3.1 Screenshots from Evidentiary Procedure Three

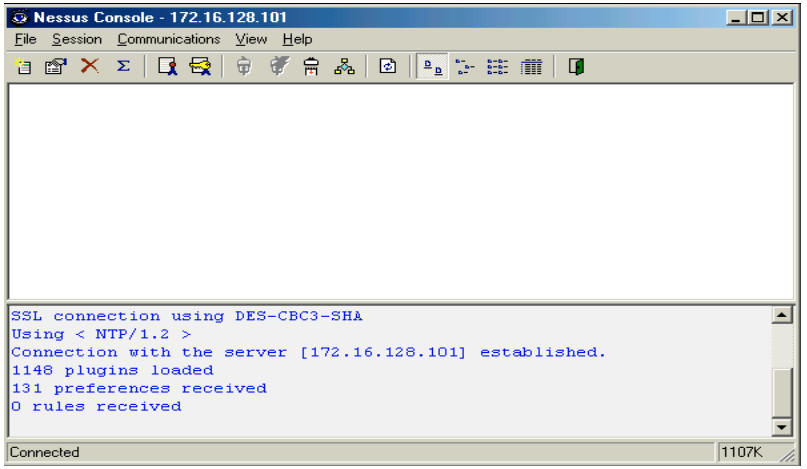
Step 1-Using the GUI version of Nessus, version 1.4.4, in conjunction with a SuSe Linux based Nessus daemon to perform a network vulnerability assessment.

Figure 3-22



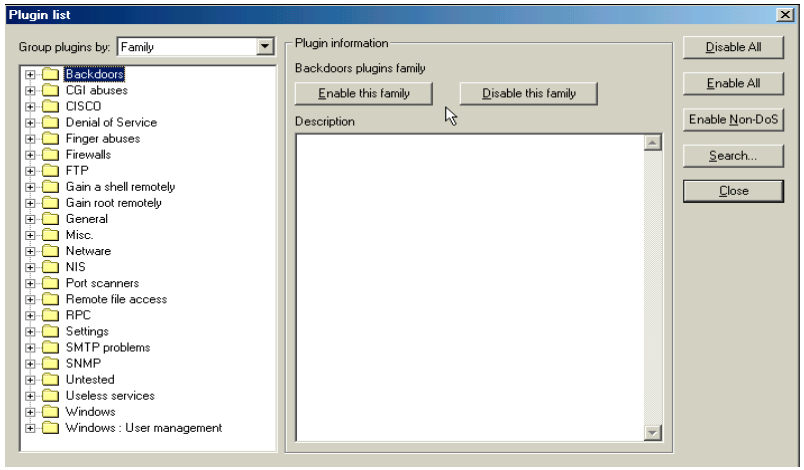
Step 2 – Requires connecting to the SuSe Server that was brought to the site. The server was assigned the IP Address of 172.16.128.101

Figure 3-23



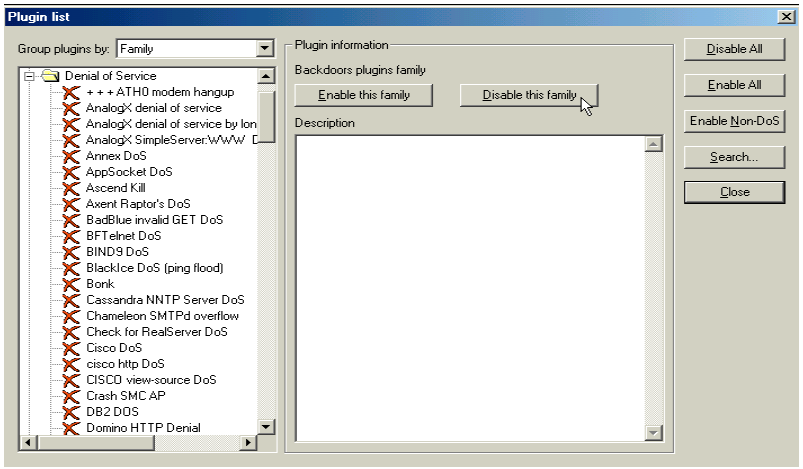
Step 3- Once connected, the auditor should configure the Nessus utility to perform a scan based on the target platform or environment. Figure 3-24 shows the available vulnerability "families" which may be performed during the assessment.

Figure 3-24



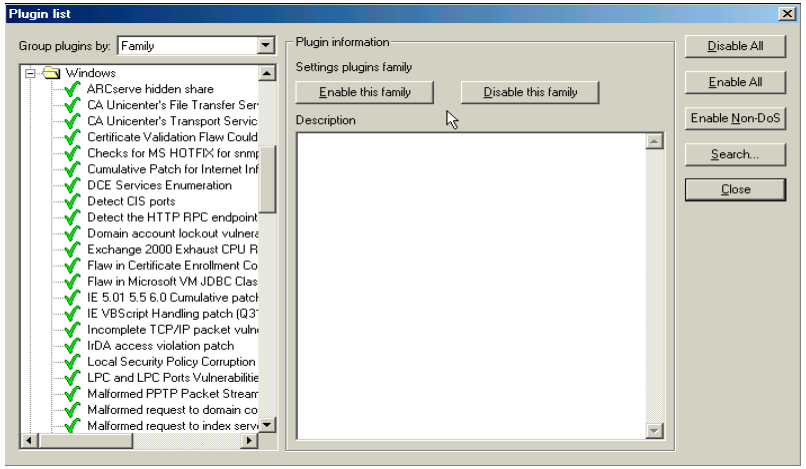
Step 4 – Unless preparing for a formal attack and penetration test, it is recommended that the Denial Of Service (DOS) family be disabled as it may cause network degradation or system outages that are not beneficial to the customer.

Figure 3-25



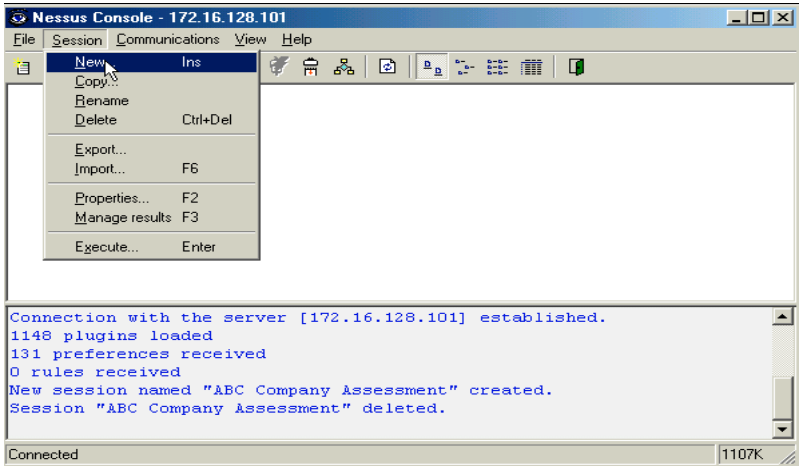
Step 5-The customer's environment is primarily Windows base that makes the selection of the "Windows Family" highly desirable as shown in figure 3-26.

Figure 3-26



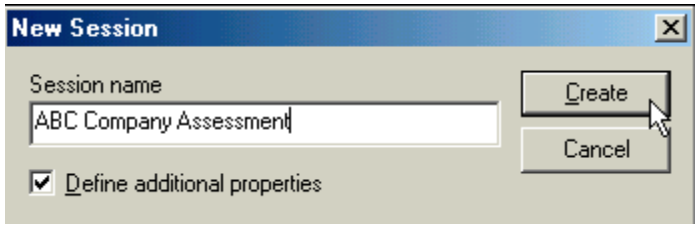
Step 6 – After all families have been selected, the auditor creates a new session from the Nessus Console.

Figure 3-27



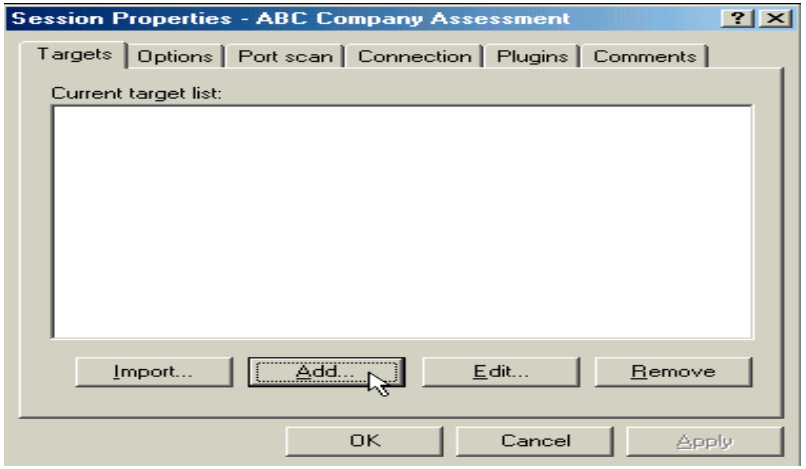
Step 7- Provide a proper name for the session and select "Define additional properties," then click create.

Figure 3-28



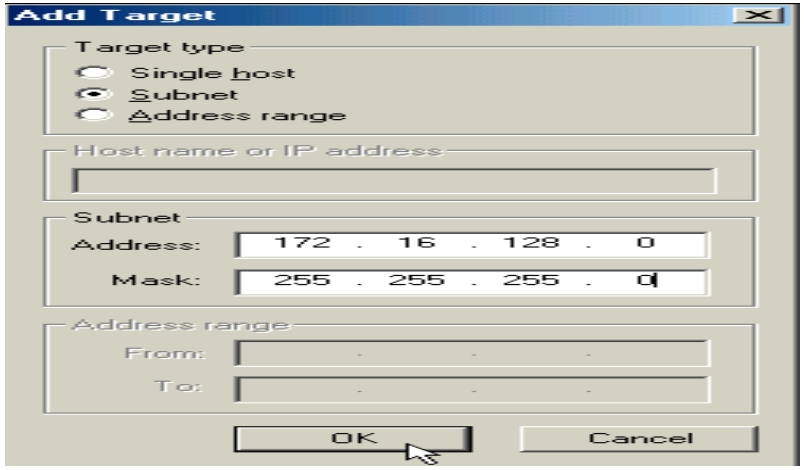
Step 8 – The first tab requires the identification of the ip address or addresses to target for the scan. Selecting "Add" will take you to the Targets window.

Figure 3-29



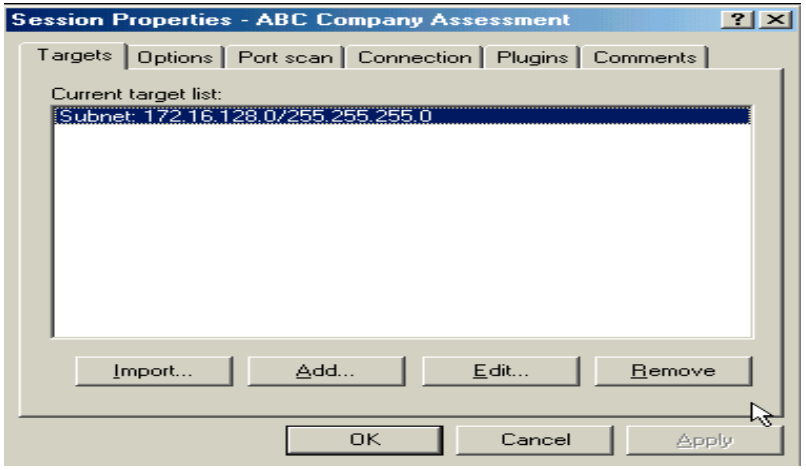
Step 9 - Inside of the add target window, enter the IP subnet details for the ABC Corporation facility by first selecting the Subnet radio button and the proceeding to complete the Address and Mask fields.

Figure 3-30



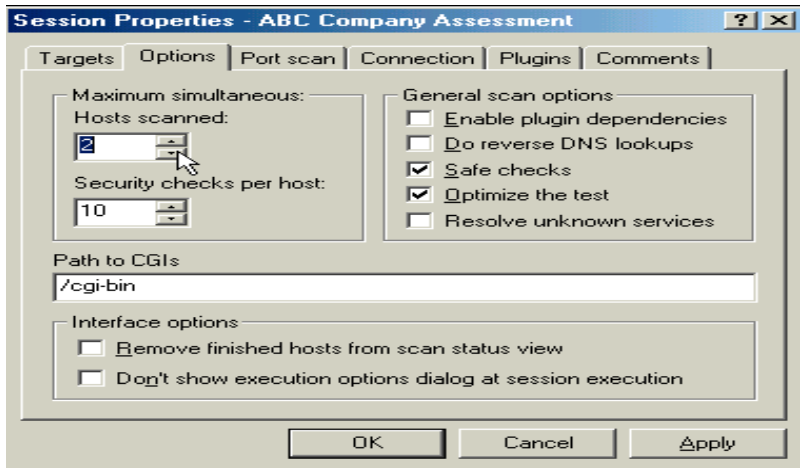
Step 10 – Once finished, click OK to return to the session properties window.

Figure 3-31



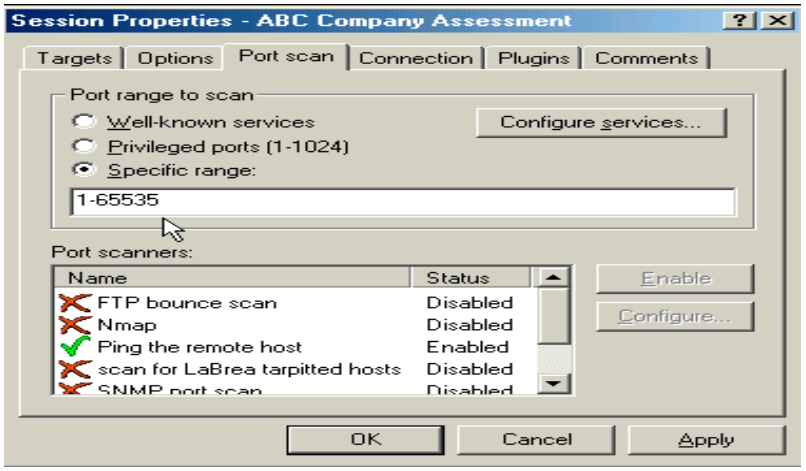
Step 11- The next available tab is the Options tab. As this is a small network, the auditor should limit the amount of traffic generated to avoid congestion. To support this approach, the auditor will only run an analysis of two hosts at a time.

Figure 3-32



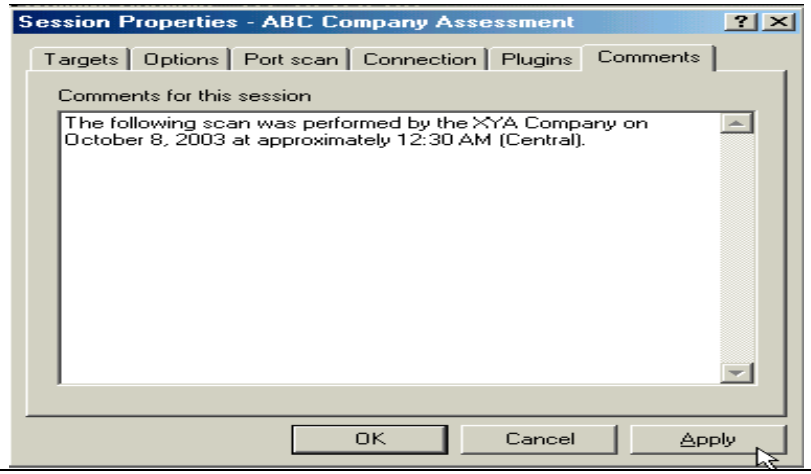
Step 12 – The auditor should scan the entire range of ports to see if any Trojans have been introduced into the network. The following screenshot captures the adjusted port range adjustment.

Figure 3-33



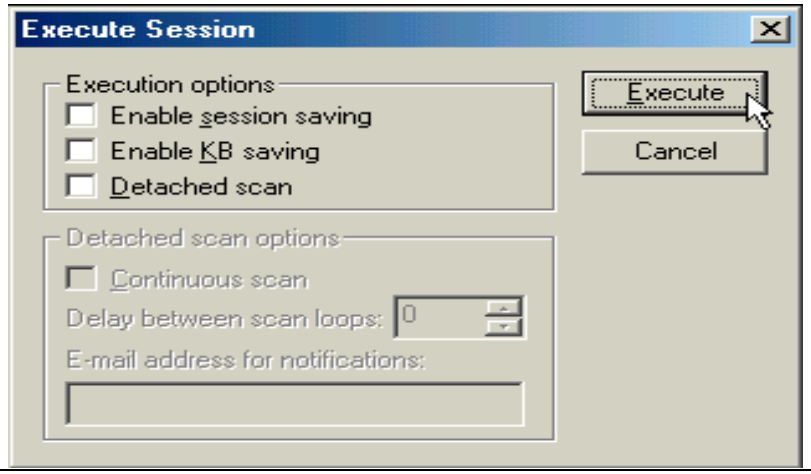
Step 13 - There are no adjustments required for the Connection and Plugins tabs. However, it may be desirable to properly document the date, time and purpose of the scan for future reference. This information will be captured in the Comments Tab.

Figure 3-34



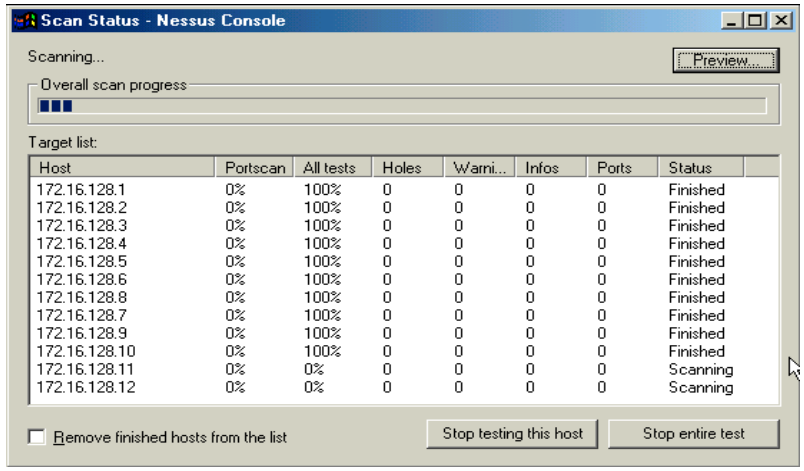
Step 14 – Press apply to save the changes and return to the main Nessus Console. To execute the scan, simply double-click the newly created session and left click execute. Optionally, right-click on the icon then highlight and click "execute" to initiate the scan.

Figure 3-35



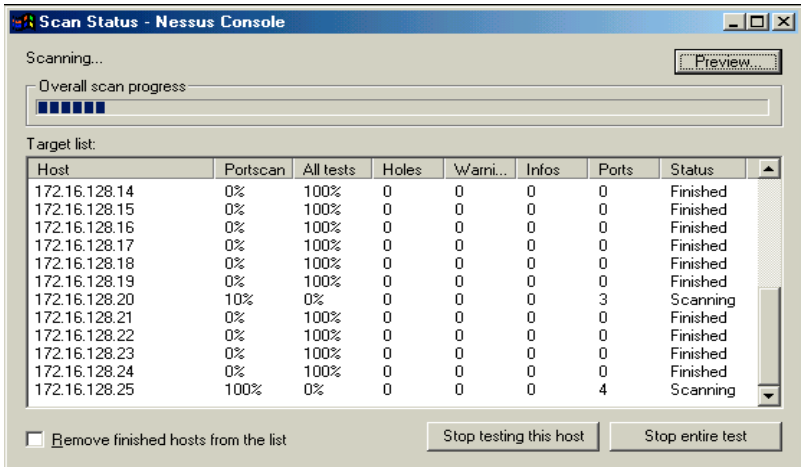
Step 15- Figure 3-36 illustrates the assessment in progress.

Figure 3-36



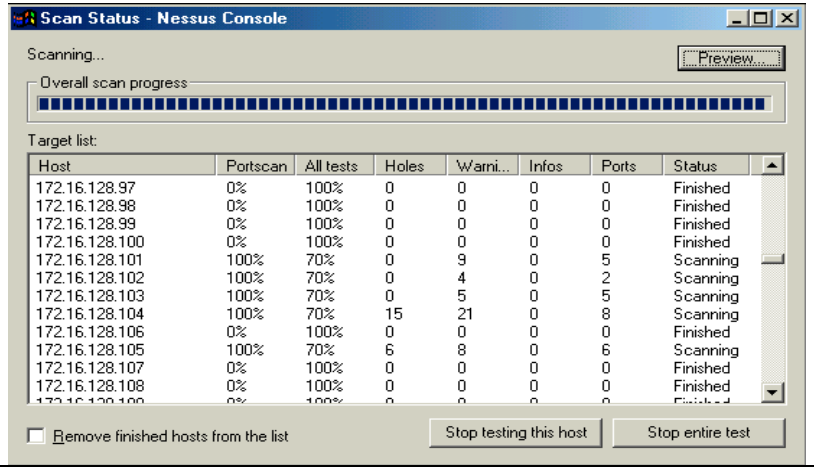
Step 16 – Figure 3-37 shows Nessus having completed its port scan of host 172.16.128.25 while it continues to port scan 172.16.128.20. However, the testing is still not completed for either system as may be determined by the zero percent (0%) shown in the "All tests" column.

Figure 3-37



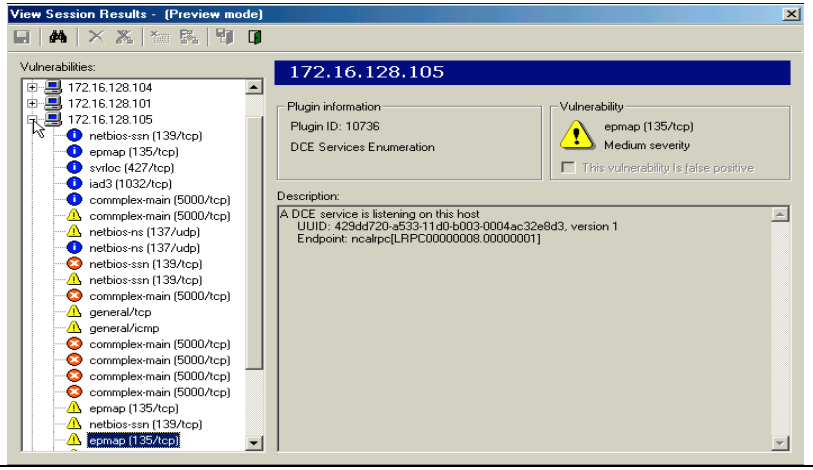
Step 17 – Figure 3-38 shows the scan nearing completion and already a number of vulnerabilities are reported in the console window (i.e., Holes, Warnings, etc.).

Figure 3-38



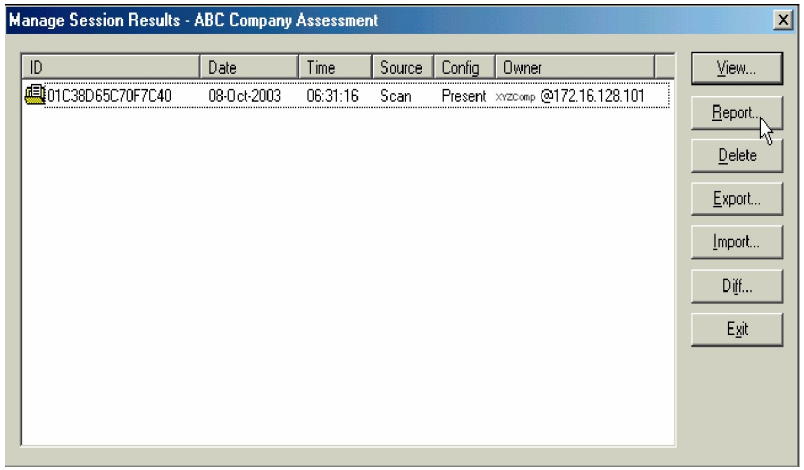
Step 18 – Once the scan completes the auditor has an opportunity to "preview" the report. Figure 3-39 contains a list of IP addresses that have been scanned by Nessus. To review further details about a specific host, simply click on the associated "+" sign to expand the results. In turn, individual results may be selected to review details regarding the purported vulnerability.

Figure 3-39



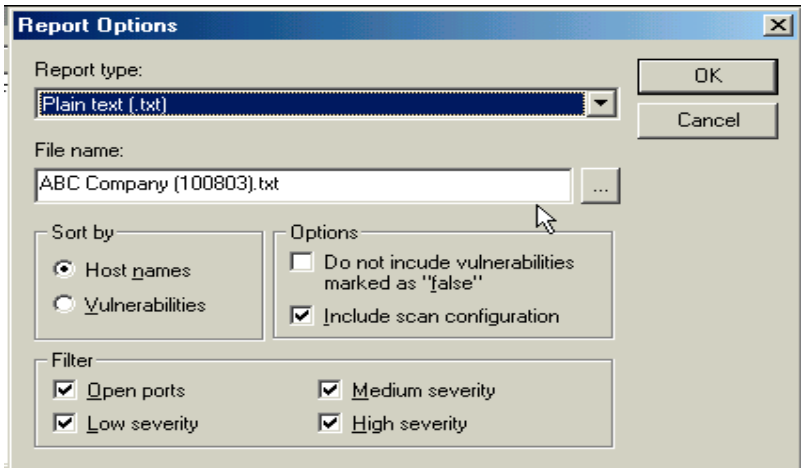
Step 19- As with other audit tests, the results will be exported for inclusion in the final report to the ABC Corporation. Figure 3-40 shows the report being prepared for export.

Figure 3-40



Step 20 – Figure 3-41 shows the "Report Options" window offering additional methods for report formatting.

Figure 3-41



3.1.4 Evidentiary Procedure Four

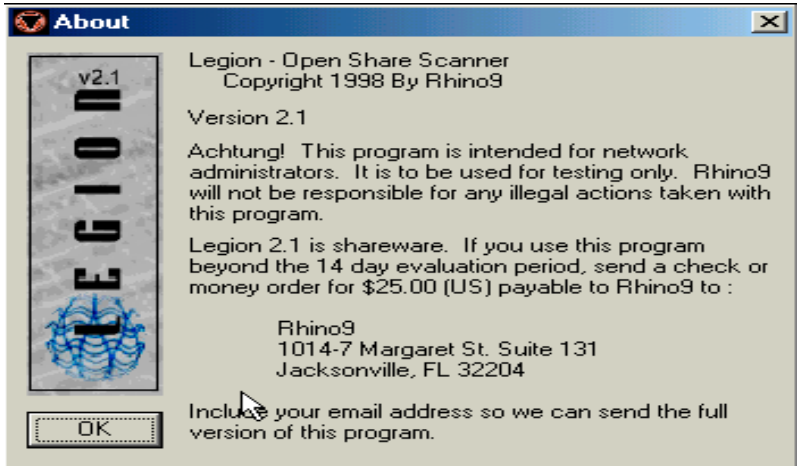
Table 3-4 – Evidentiary Procedure Four

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
6	6 10	Y	Y	HAXP TLAH	6 14 18 19 20 23	O		Commercial HomePlug configuration software requires a Windows based operating system; as such, a NetBIOS enumeration will be performed to determine whether any open shares exist on systems potentially identified as passing HomePlug traffic. First, attempt to connect to any discovered shares without a password (stimulus/response test with a desired outcome to connect without a password proving weak controls). If unable to connect without a password, attempt to utilize a brute-force password utility to attach to the share and determine whether the password meets corporate standards for composition. Finally, if unable to remotely brute force the password, use a local password utility to determine whether the password meets corporate standards for composition.		X		ACTUAL: Legion discovered the presence of a Windows share on the host at 172.16.128.103. The share name was \\DAREDEVIL\C The open workstation share fails to meet the control objective for Restricted File Sharing. The Cain remote share brute force failed to crack the password. The Cain local share password decryption utility successfully identified the password as "ABC03" (without quotation marks). This password fails to meet the corporate standards for composition.

3.1.4.1 Screenshots from Evidentiary Procedure Four

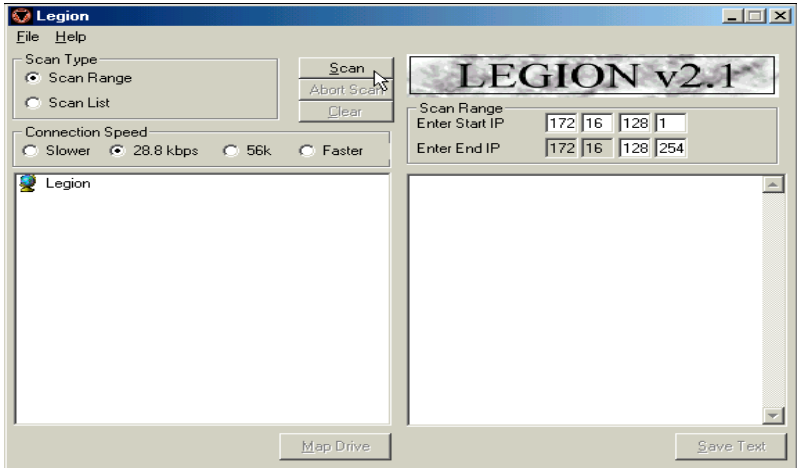
Step 1-The first step taken to discover Windows shares requires the use of a NetBIOS enumeration tool such as that presented by Legion in figure 3-42.

Figure 3-42



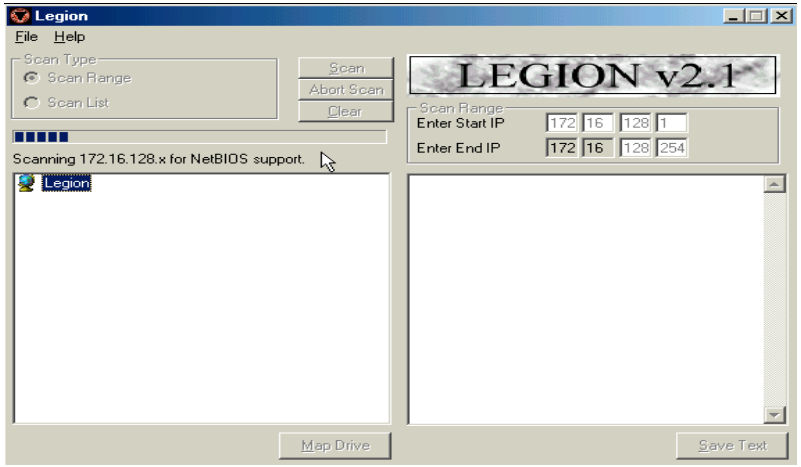
Step 2-Legion opens with an empty console window. You can configure it to scan a single IP address or a range of IP addresses as is shown in the top right corner of figure 3-43. Once the subnet details are configured, just click "Scan" to begin.

Figure 3-43



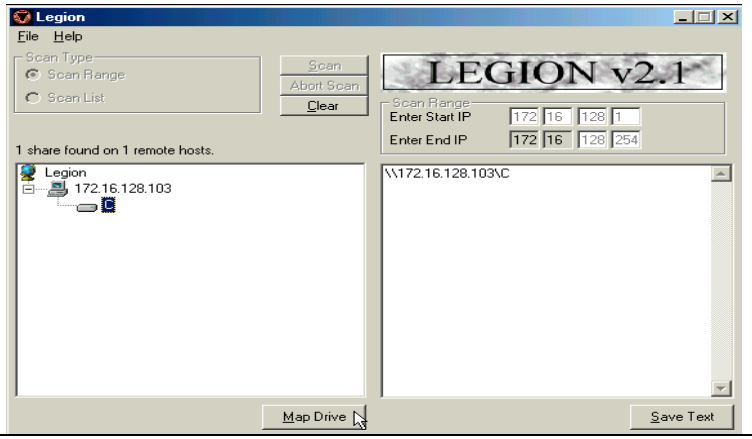
Step 3- Figure 3-44 shows Legion as it is scanning the subnet.

Figure 3-44



Step 4 – Legion discovered a host with a shared drive. Clicking on the plus sign will expand the host details. In this case the display shows that there is a share named "C" on the selected computer. Click on the share name and then click on Map Drive to attempt to connect to the folder share as shown in figure 3-45.

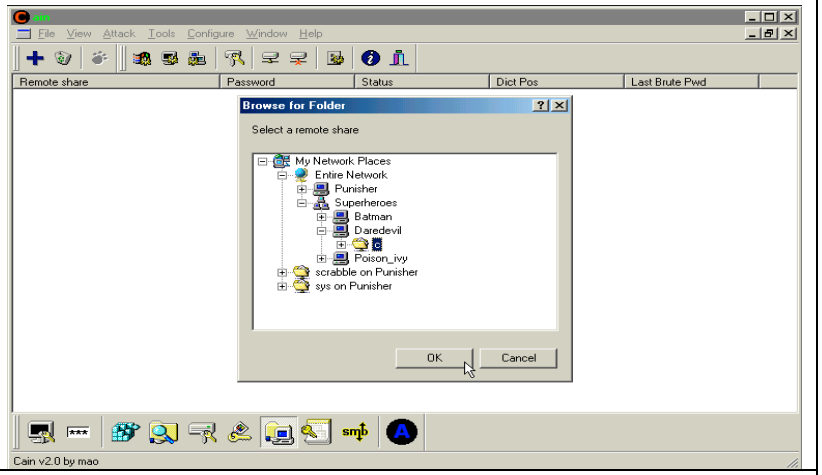
Figure 3-45



Additional comments: Two difficulties were observed while using Legion. The first was an inability for the tool to detect hidden shares. The second was difficulty mapping a password-protected share. So rather than continue to work with Legion, the auditor may instead take the discovered share information and plug the details into CAIN, which has the ability to perform dictionary and brute force attacks against remote shares.

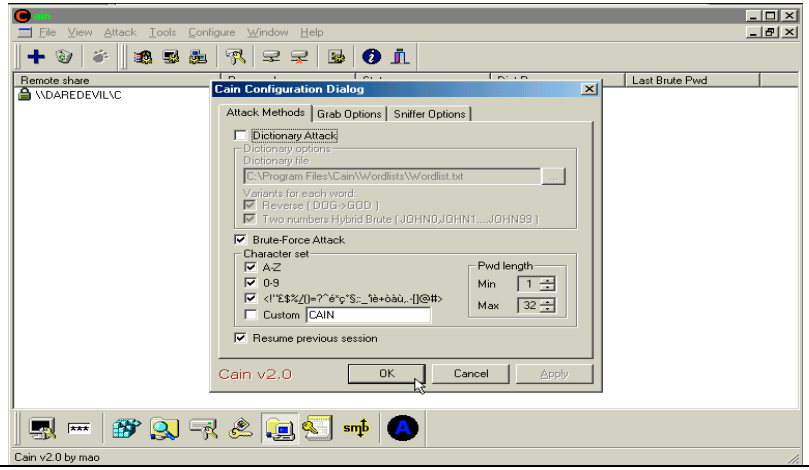
Step 5- Launch Cain and select "File" and then "Add to List." Using the Browse for Folder interface, locate the share identified with Legion, click on the share name and then click on OK to add it to the list.

Figure 3-46



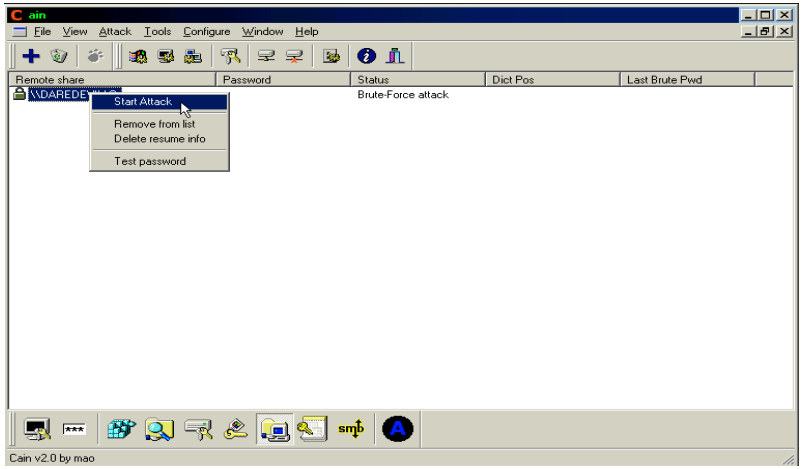
Step 6 - The tool can and should be configured to the audit environment prior to conducting an assessment. As an example, the default installation performs a dictionary attack and a brute force attack. For the purpose of assessing the security of the "C" share; a brute-force method will be used rather than a dictionary attack as show in figure 3-47. Click "OK" when the configuration has been completed to return to the remote share sub-console.

Figure 3-47



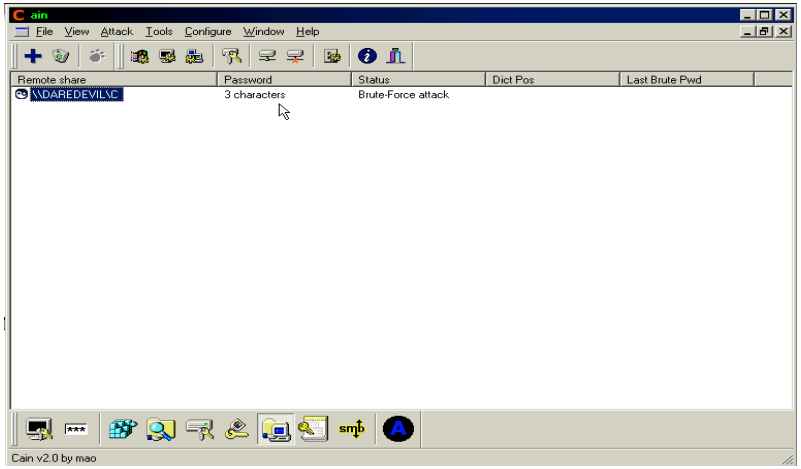
Step 7 - Once at the remote shares sub-console, right-click on the target share and then select "Start Attack" as shown in figure 3-48.

Figure 3-48



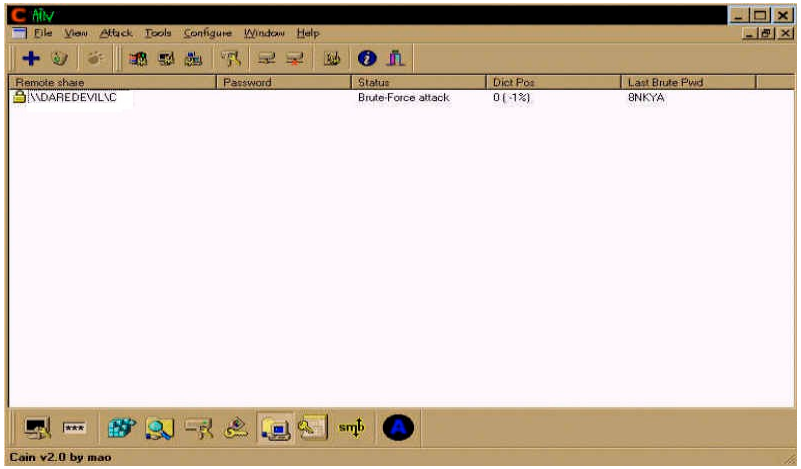
Step 8 - The tool provides status pertaining to the number of letters discovered during the brute force attack as shown in figure 3-49.

Figure 3-49



Step 9 – Once CAIN completes the brute force attack, it posts what it believes is the remote password which as shown in figure 3-50, is the combination "8NKYA."

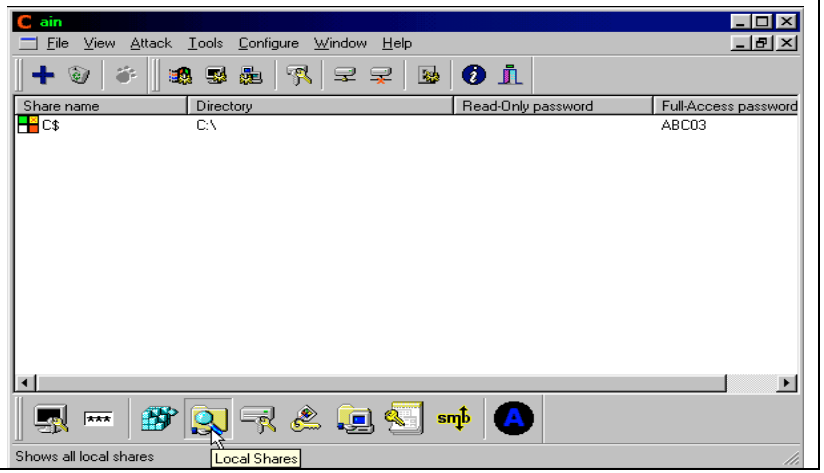
Figure 3-50



Additional Comments: Attempting to map a drive to the \\DAREDEVIL\C share with the password identified by CAIN fails. As such, the auditor will need to switch to the last step of the checklist that requires the use of CAIN installed local to the workstation under assessment.

Step 9 - To reveal the local share password click on the "shared folder" button at the bottom of the CAIN interface and instantly the password is revealed as demonstrated in figure 3-51. The password is "ABC03" which does not meet corporate standards.

Figure 3-51



3.1.5 *Evidentiary Procedure Five*

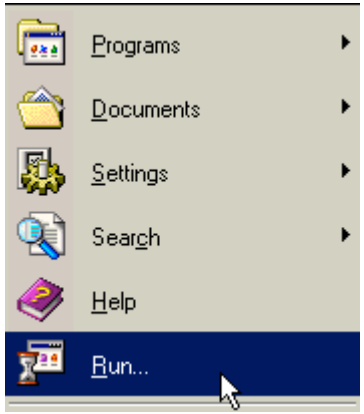
Table 3-5 – Evidentiary Procedure Five

Task ID	Risk ID's	Selected as an Evidentiary Procedure	Stimulus/ Response	Reference(s)	Control(s)	Test Purpose		Test Procedure	Test Results			Compliance
		Y=YES N=NO	Y=YES N=NO			Objective	Subjective		Pass	Fail	Other*	
8	7	Y	Y	PEOX CESP HAXP	6 7 15 22 23	O		Determine if the system screensaver is configured to utilize a password by performing the following steps: 1. Click on Start and then Run 2. In the Run dialog box type the following without quotations "FLYING~1.SCR" 3. Allow 5-10 seconds to pass for the screen saver to activate. 4. Bump the mouse or press the spacebar to determine if the screen saver disappears or if a password dialog box appears.	X			ACTUAL: The screensaver is password protected.

3.1.5.1 Screenshots from Evidentiary Procedure Five

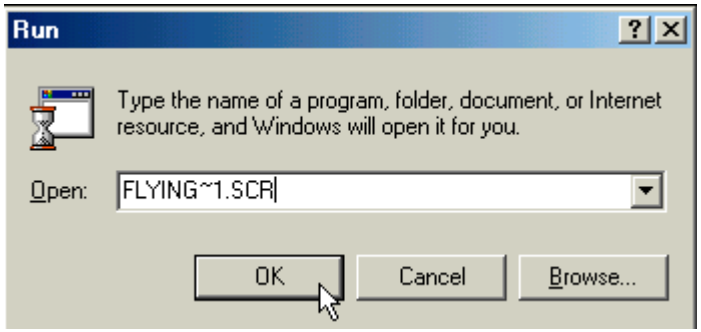
Step 1 – Figure 3-52 shows the first step of command execution

Figure 3-52



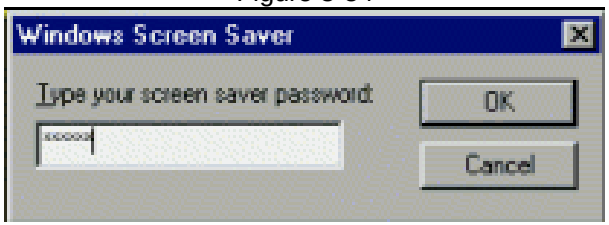
Step 2 – Figure 3-53 shows the second step of command execution

Figure 3-53



Step 3 – Bumping the mouse or pressing the space bar pulls up the screensaver password prompt, requiring the auditor to enter a password to proceed. This is the desired response for this test and sets up the system for the stimulus/response test to be conducted in step six (6).

Figure 3-54



3.1.6 *Evidentiary Procedure Six*

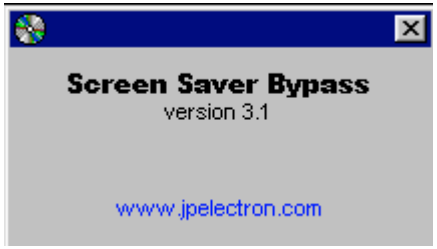
Table 3-6 – Evidentiary Procedure Six

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
9	9	Y	Y	CESP HAXP	6 7 18 22 23	O		Determine if the CDROM "autorun" feature is disabled by: 4. Enable and lock the screensaver password using the technique established in step XXX. 5. Insert the screensaver bypass CD and allow 15 to 30 seconds to elapse. 6. If autorun is enabled the screensaver will unlock and permit console access. If autorun is disabled nothing will happen.		X		ACTUAL: The bypass utility launched successfully indicating that the autorun feature has not been disabled. The autorun feature may allow for unauthorized access to system and network resources.

3.1.6.1 Screenshots from Evidentiary Procedure Six

Step 1 – Using a Windows 9/x Screen Saver Bypass Utility does not require the typing of any system commands. Rather, if the autorun feature is turned on just insert the CDROM, wait a few seconds, and the following screen shot will appear permitting open and unauthorized access to the system.

Figure 3-55 - Successful Execution of Screensaver Bypass

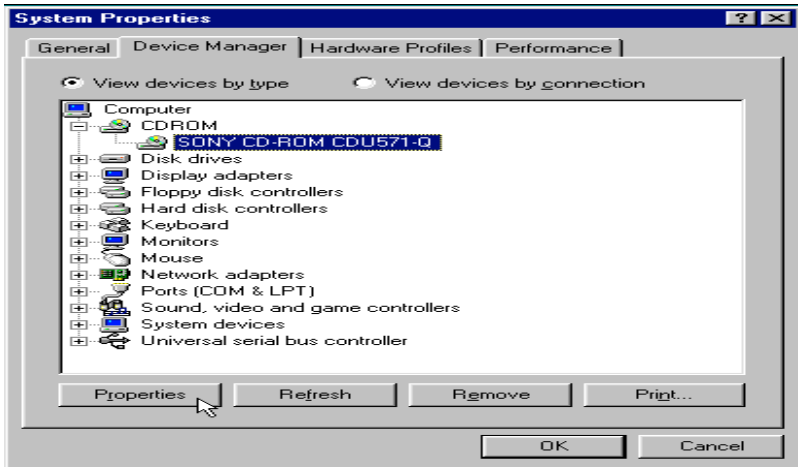


Step 2 – The way to prevent this from occurring is to disable the autorun feature by completing the following steps. From the desktop, right-click on “My Computer” then left-click on “Properties,” as shown in figure 3-56

Figure 3-56 - Viewing "My Computer" Properties

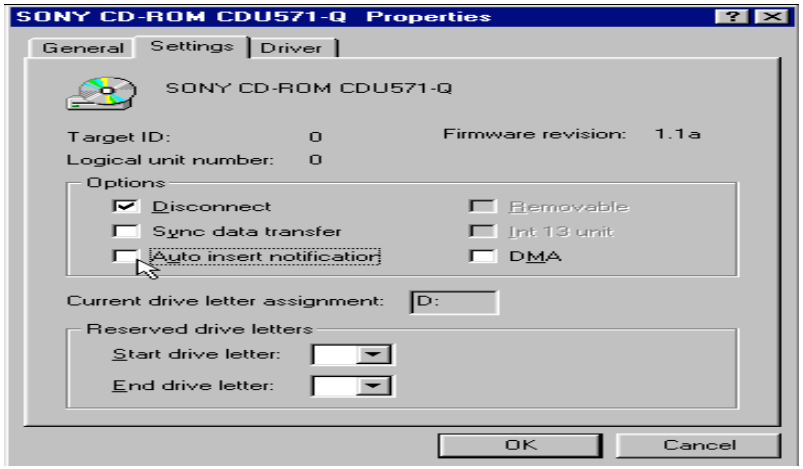
Step 3 – Figure 3-57 shows the location where the CDROM settings must be modified to disable the autorun. To access this location, first left-click on the “Device Manager” tab, then on the CDROM device type to expand the group, and then the available CDROM drive before finally clicking on the “Properties” button at the bottom of the screen.

Figure 3-57 - Accessing the CDROM Properties



Step 4 - Figure 3-58 shows the final steps necessary to disable the autorun feature. To access this location, first left-click on the “Settings” tab, then remove the check from the list box next to the “Auto insert notification” choice and finally click on the “OK” button to apply the change. The end-user will be returned to the Device Manager window.

Figure 3-58 - Remove the CDROM Autorun Feature



Step 5 – Click on the “Close” button from the device manager window to proceed with the properties modification. Finally, windows will prompt the end-user to reboot the system to complete the changes as shown in figure 3-59.

Figure 3-59 - Rebooting the system after modifying the CDROM properties

Step 6 – The autorun feature is now disabled. To validate that the change is operating as desired:

1. Restart the system
2. Enable the Screensaver
3. Insert the Screensaver Bypass CDROM

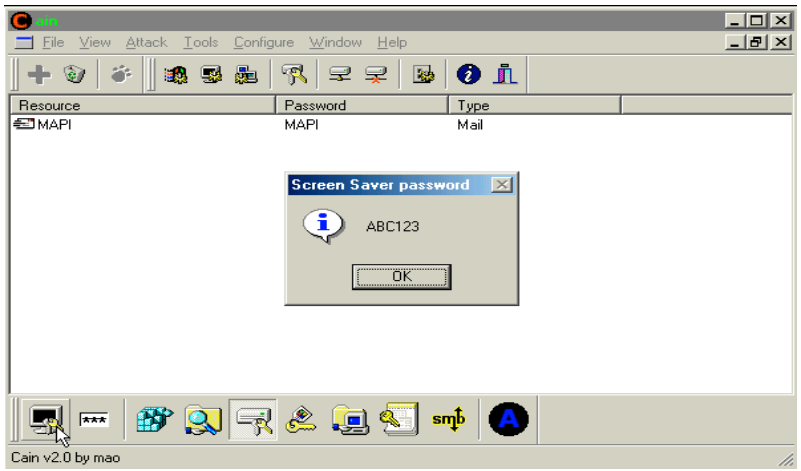
The utility CD should no longer allow the end-user to bypass the screensaver and gain access to the system. If access is still granted, repeat the property modification steps highlighted in this document to disable the CDROM autorun feature.

3.1.7 *Evidentiary Procedure Seven*

Table 3-7 – Evidentiary Procedure Seven

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
10	8	Y	N	CESP HAXP	6 18 22 23	O		Determine if the screensaver password meets corporate standards for composition by performing the following steps: 5. Insert password utility CDROM or write protected floppy into system. 6. Click on Start and then Run. 7. Either type the drive location and name of the file in the run dialog box or click on browse. Once the name is correctly entered, click on OK to proceed. 8. Select the appropriate tab within the password utility to display the currently assigned password.		X		ACTUAL: The screensaver password does not meet the corporate standards for composition.

3.1.7.1 Screenshots from Evidentiary Procedure Seven

Step 1 – The password analysis tool named CAIN & ABEL will be used to audit the screensaver password to determine compliance with corporate password composition requirements. To perform this test, CAIN must be run from the local system. Once executed, simply click on the Monitor Button on the bottom toolbar and the password is immediately identified as shown in figure 3-60. **Figure 3-60**  	Step 2 – The response is shown immediately which in this case the identified password is "ABC123." According to the ABC Corporations policy, password should be composed of: 8. Upper and Lower Case Alpha Characters 9. Numeric Characters 10. At least one special symbol character 11. No more than two characters should be repeated consecutively 12. The combination of characters must be between 6 and 8 characters in length. 13. The word must not be a common dictionary word 14. The word must not utilize the organizational name. All of these items will be considered during the assessment of the identified screensaver password.

3.1.8 *Evidentiary Procedure Eight*

Table 3-8 – Evidentiary Procedure Eight

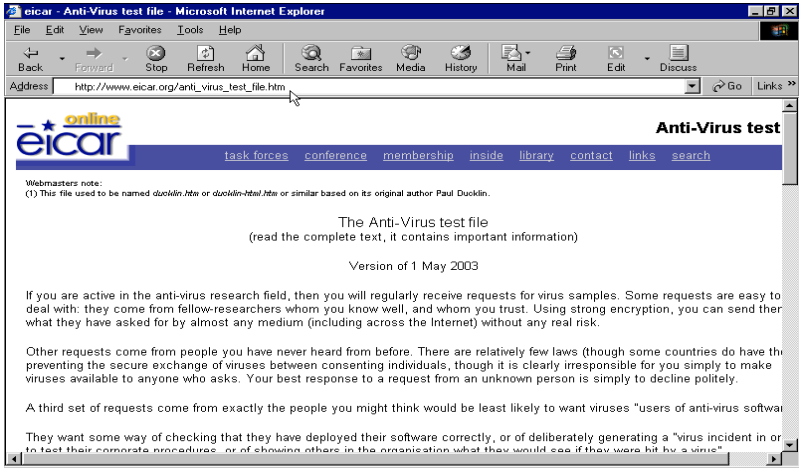
Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
11	13	Y	Y	EICAR	10	O		Determine if a corporate approved anti-virus application is: 5. Installed on the system 6. Using current virus string files 7. Configured to run automatically 8. Capable of detecting the EICAR test file Once the above steps have been completed, reboot the system and perform a second anti-virus scan using a write-protected floppy or bootable CDROM to further determined if the installed anti-virus software is functioning properly. Any commercial version of anti-virus software may be utilized as long as it is not the same manufacturer as the currently installed AV software.		X		ACTUAL: The installed anti-virus application did successfully detect the presence of the EICAR files. However, upon further inspection it was determined that the scanning engine and virus definition files are greatly outdated.

3.1.8.1 Screenshots from Evidentiary Procedure Eight

Introduction - The European Institute for Computer Anti-Virus Research (EICAR) project provides an opportunity for businesses to test the effectiveness of anti-virus detection and prevention applications. Freely available via the Internet, the EICAR approach provides a controlled environment where testing may build confidence without exposing information assets to live and potentially damaging viruses.

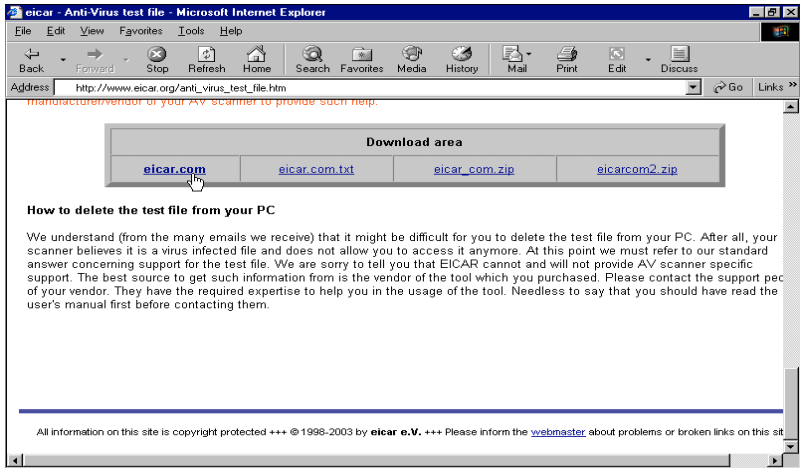
Step 1 – To begin, the EICAR test file must be downloaded from the website http://www.EICAR.org/anti_virus_test.htm as shown in figure 3-61.

Figure 3-61 - EICAR Website



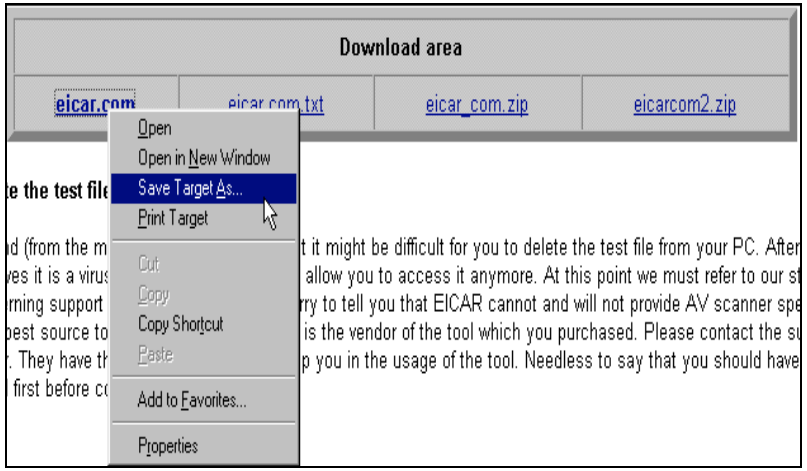
Step 2 - Hyperlinks for the test file and instructions may be found at the bottom of the page as shown in figure 3-62.

Figure 3-62 - EICAR Downloadable Files



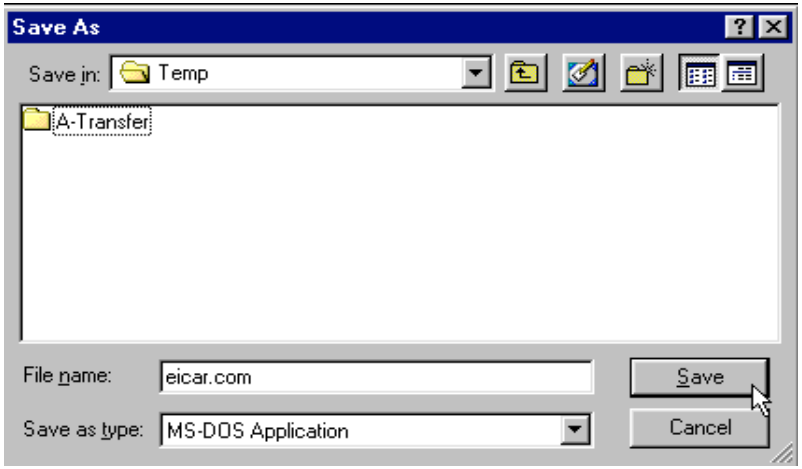
Step 3 - Right-Click on the file named “EICAR.com” and then left click on “Save Target As…”

Figure 3-63- Saving the EICAR Test File to a Local Drive



Step 4 - Select a local folder in the proceeding dialog box and then click on the "Save" button to proceed as shown in figure 3-64.

Figure 3-64 - Saving the EICAR Test File

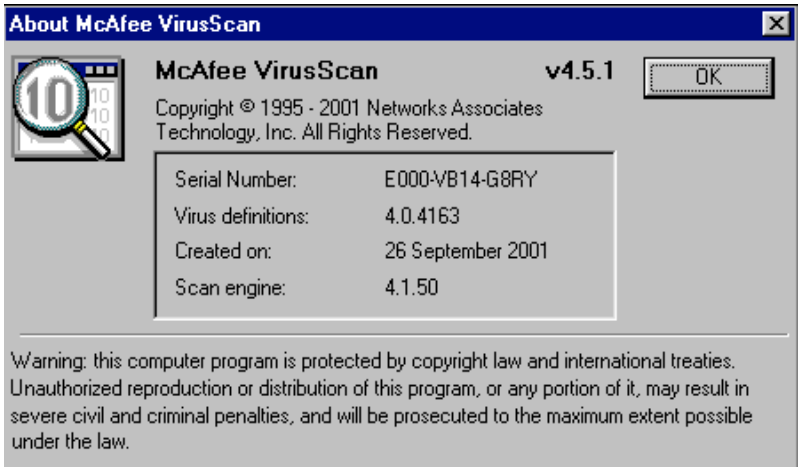


Steps 4 and 5 – Additional Comments: The EICAR project also provides two compressed files (*.zip) to further test detection effectiveness. You can repeat the steps above to save these files locally as well. The next step requires launching the anti-virus application and performing a local system scan.

In the case of the workstation under test, it is loaded with Network Associates McAfee ViruScan. It is important to determine the currency of the scanning engine and virus definitions file to provide for the detection of the most current virus strings.

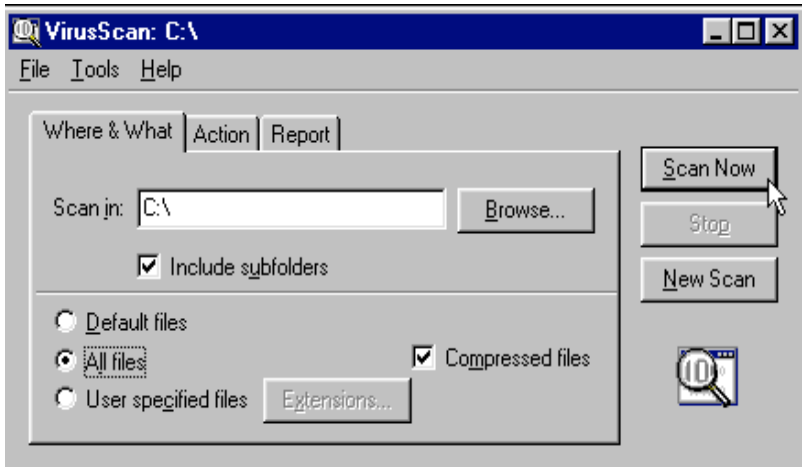
Step 5 - The quickest way to determine version information is to click on "Help" from the menu bar and then click on "About," to view a screen similar to the one shown in figure 3-65

Figure 3-65- Scanning Engine and Virus Definition Versions



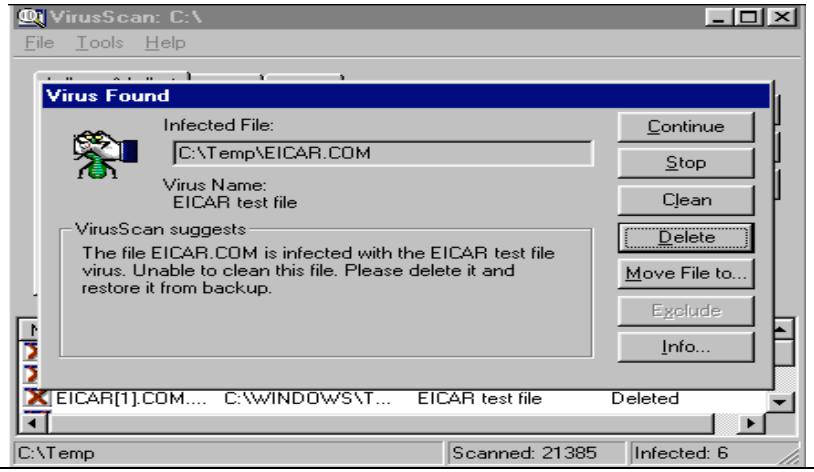
Step 6 - The viruscan interface requires little alteration prior to execution. In the case of the default configuration presented in figure 3-66, the only modification was to select the "all files" radio button and then click on "Scan Now" to begin.

Figure 3-66- Viruscan Configuration and Execution



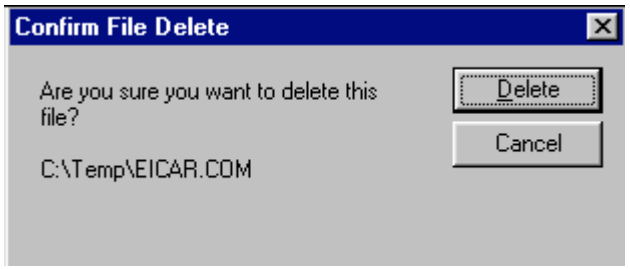
Step 7 - The scanner will initiate and if the EICAR files work properly, the anti-virus software should detect and report a virus as shown in figure 3-67. Each instance of virus should be removed as it is detected by clicking on the “Delete” button.

Figure 3-67 - EICAR Virus Discovered



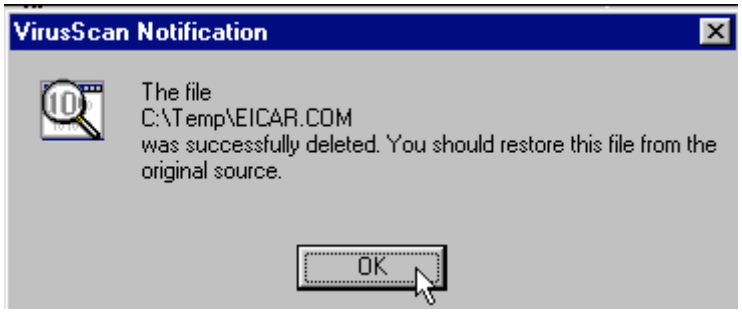
Step 8 - The anti-virus software will prompt the end-user a second time to confirm the request to delete the discovered file as shown in figure 3-68.

Figure 3-68 - Final Confirmation prior to Deletion



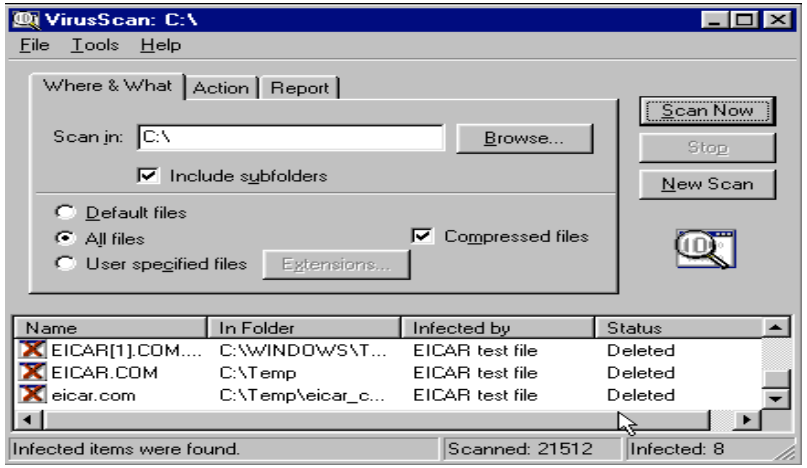
Step 9 - If successfully deleted the anti-virus software will inform the end-user as shown in figure 3-69. Repeat the previous steps to remove each detected instance of the downloaded EICAR files.

Figure 3-69 - Virus Successfully Deleted



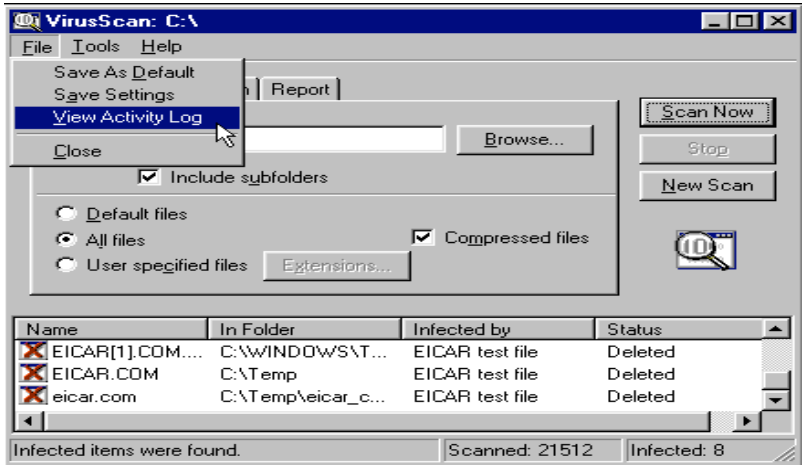
Step 10 - Upon completion, the end-user is returned to the main screen where the total number of viruses detected as well as their discovered location is reported as shown in figure 3-70.

Figure 3-70 - Virus Scan Completed



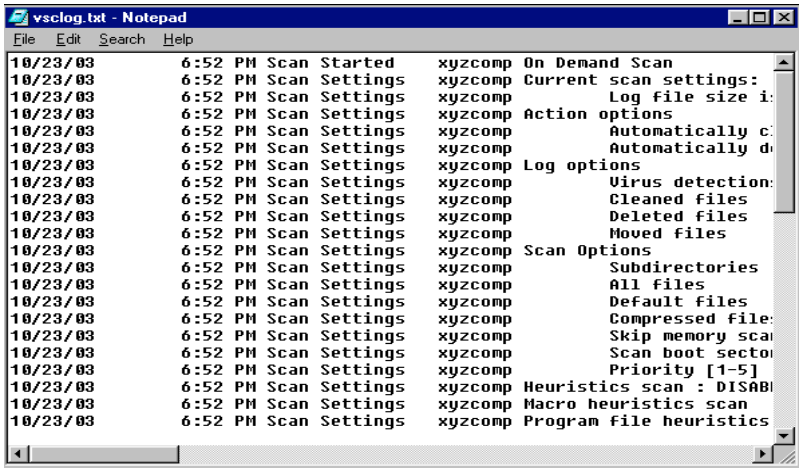
Step 11 – The last step will be to view and save the scanning log for evidentiary purposes to be delivered with the final report. To perform this step, left-click on "File," and then "View Activity Log," as shown in figure 3-71.

Figure 3-71 - Virus Scanning Log



Steps 12 - The scanning results are displayed in notepad (figure 3-72) which in turn may be saved as discussed previously.

Figure 3-72 – Scan Results



3.1.9 Evidentiary Procedure Nine

Table 3-9 – Evidentiary Procedure Nine

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
12	14	Y	N	PEOC	11	O		Determine if the system contains spyware by: Utilizing a commercial malware scanner to identify known instances of spyware/adware. Report the results of the test but do not clean system at this time.		X		ACTUAL: The spyware scanning discovered 42 instances of tracking cookies installed on the workstation.

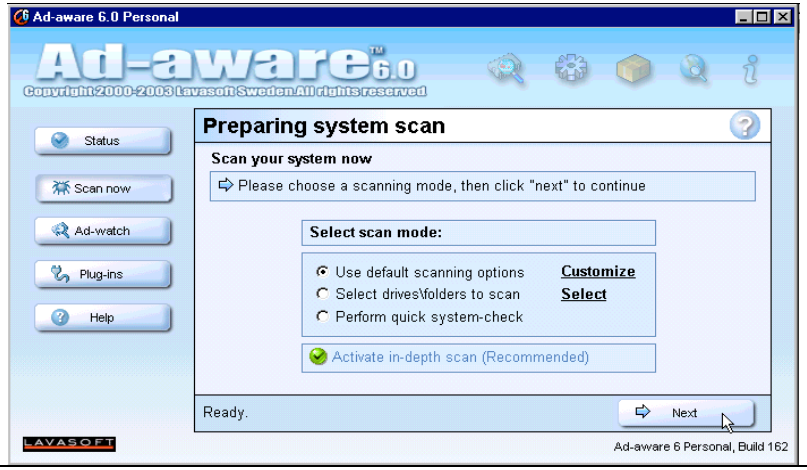
3.1.9.1 Screenshots from Evidentiary Procedure Nine

Step 1-Using AdAware, version 6 build 162, by Lavasoft to scan the system for spyware. Click the "Start" button to configure the scan.

Figure 3-73

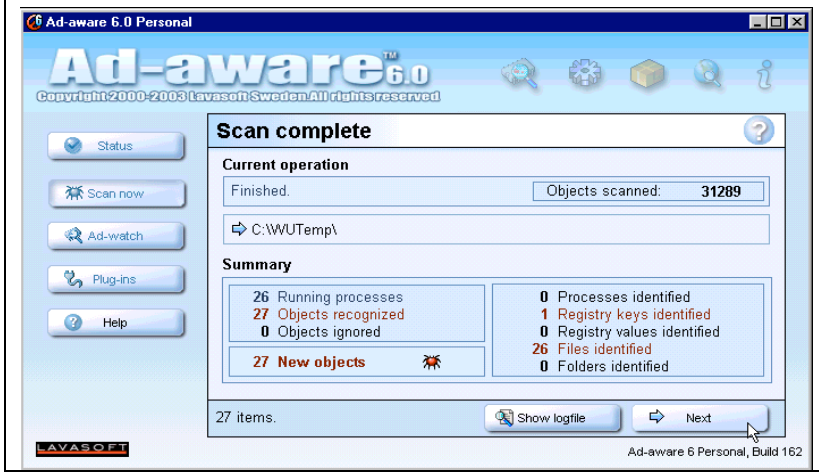
Step 2 – The tool offers the ability to customize the scan to meet the system and auditor requirements. In this case, the "default scanning options" are sufficient for the auditor's spyware test.

Figure 3-74



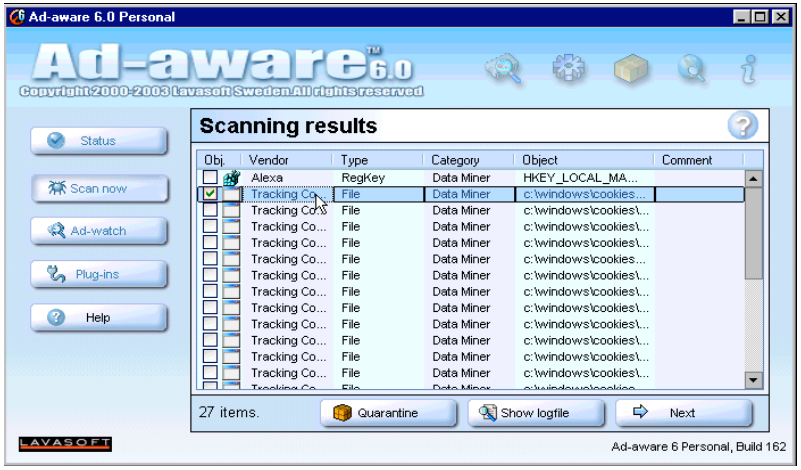
Step 3- The scan will run unattended and continuously update the main console screen to notify the auditor of its progress. Figure 3.75 shows the completed scan prior to clicking on the "Next" button to proceed with the removal of detected spyware.

Figure 3-75



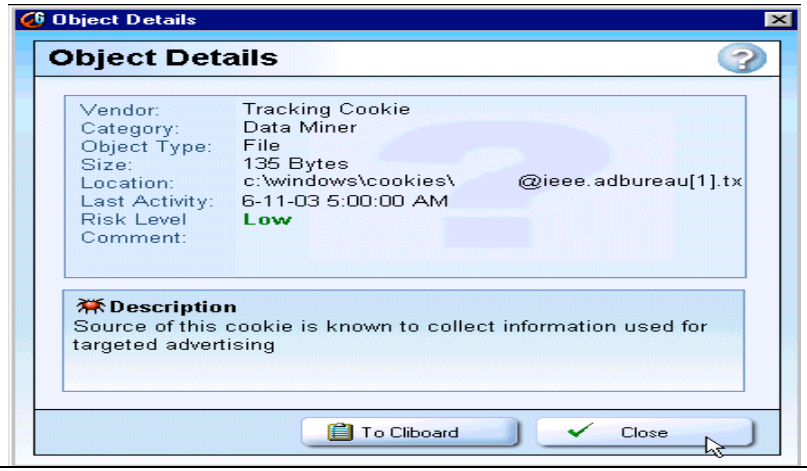
Step 4 – The tool provides the auditor with an option to quarantine some or all of the files based on their personal situation. However, for the purpose of this test the auditor should leave the files intact and report only on the discovery of spyware.

Figure 3-76



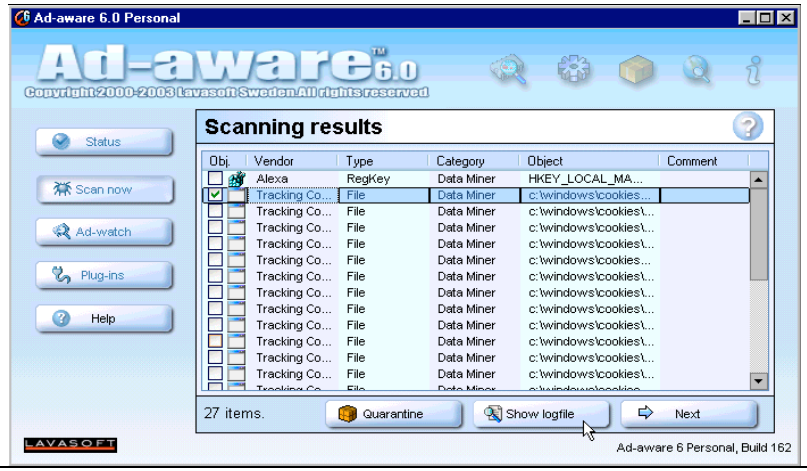
Step 5 –Double-clicking on any file listed displayed in step 4, will provide additional details regarding that object as shown in figure 3-77.

Figure 3-77



Step 6 – To view details about all objects or to export a file for report purposes, click on the "Show logfile" option. For the purpose of this audit, the results of the log file will be saved and reported to management as a part of the final audit findings.

Figure 3-78



3.1.10 *Evidentiary Procedure Ten*

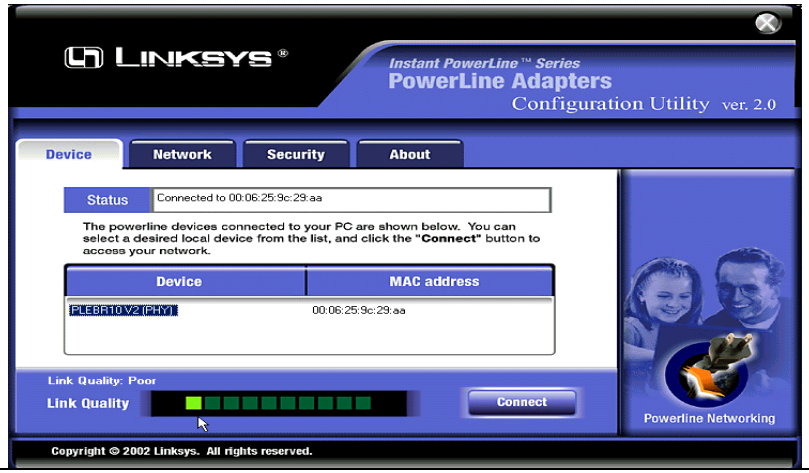
Table 3-10 – Evidentiary Procedure Ten

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
14	28 29 30	Y	N	PEOC	6 8 23	O		HomePlug devices may operate with the default Network Encryption Key (NEK) of "HomePlug" or with a user assigned NEK. If a HomePlug device is located, then an analysis of the attached computer should be performed by: 6. Install the HomePlug software provided with the PLC device purchased by the auditor for the ABC contract. 7. Examine the contents of the manufacturer's application directory (typically C:\Program Files\Manufacturer) to determine if any files exist that may contain passwords. 8. Examine the contents of the files to determine if a clear-text password may be discovered. 9. If a password is discovered, does it meet the corporate standards for composition? 10. Utilize a packet capture utility to determine if any PLN device command and control traffic is passed in the clear.		X		ACTUAL: A clear-text password was discovered using the steps prescribed in checklist item 14. Subsequently, the password was compared against corporate standards for password composition and determined to be out of compliance with said standards.

3.1.10.1 Screenshots from Evidentiary Procedure Ten

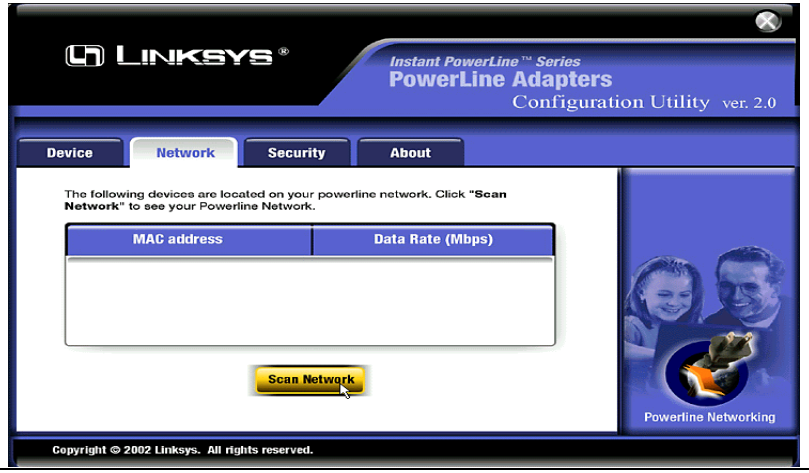
Step 1- Install and launch the HomePlug software provided with the PLC device purchased by the auditor for the ABC contract on the auditor's laptop. Figure 3-79 shows the initial configuration screen. It also shows that the software has detected the directly attached HomePlug device.

Figure 3-79



Step 2 – Attempting to scan the network produces no results. This is due to an incorrectly configured network encryption key (NEK).

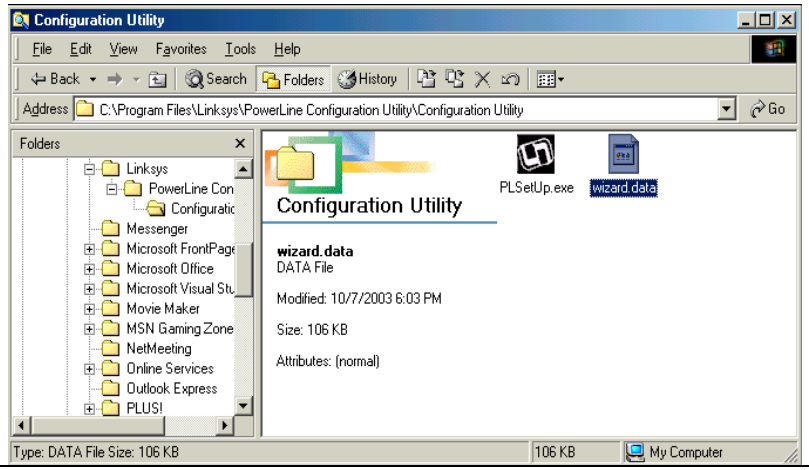
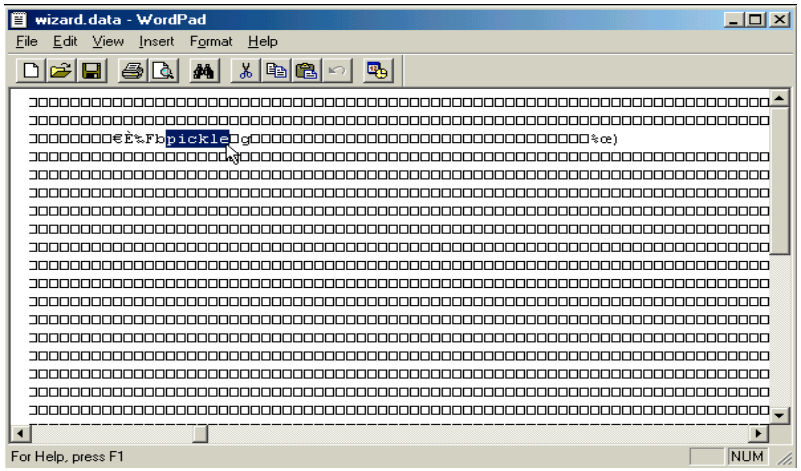
Figure 3-80



Step 3- The default password for all HomePlug devices, as required by the standard, is the word HomePlug. In figure 3-81, the word HomePlug has been replaced by a phrase indicating where the password is to be provided.

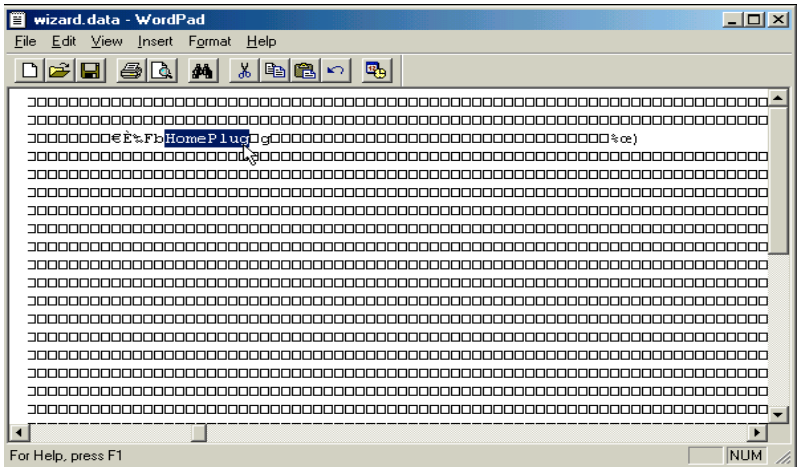
Figure 3-81

Additional Comments: – As the password is unknown to the auditor, an investigation of he local installation directory should be performed to determine if a clear text password might be discovered. If it is determined possible, then the same approach will be taken for the systems discovered in previous steps that are believed to be running HomePlug software

Step 4- Begin by investigating the default HomePlug installation directory for any files that may be reviewed with a simple word editor. Figure 3-82 shows the contents of the default installation folder for the auditor's purchased PLC device. It appears that a file named "wizard.data" exists and may offer an opportunity for examination. Figure 3-82  	Additional Comments: Carefully reviewing the contents of the "wizard.data" file with a text editor identified seven instances of the default. This does not prove that a password may be detected in this fashion. To better determine if a password is viewable in this manner, the PLC device will be changed to a more obvious word that in this case is "pickle." Searching the file again produces the following results
Step 5- Searching the "wizard.data" file again for the word pickle, produces the following results: Figure 3-83  	Additional Comments: – In this case the characters "Fb" preface the word "pickle". To test whether the identified prefix is a marker for the password location, we return to the default password of "HomePlug" and again edit the "wizard.data" file searching specifically for the combination of "FbHomePlug."

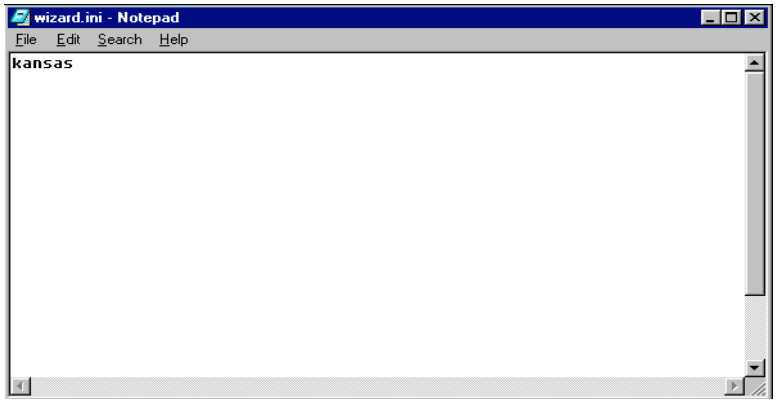
Step 6- The search successfully identifies the combination. With Fb as a marker it makes searching for the password a much simpler task.

Figure 3-84



Step 7 – Searching the computer named "DAREDEVIL" in the same fashion, identifies a subdirectory named "Encryption Management Utility" within the \\DAREDEVIL\Program Files\HomePlug directory. Contained within folder is a file named "wizard.ini" as shown in figure 3-85. The contents of this file are even easier to decipher as the only word contained within it, is the password "kansas"

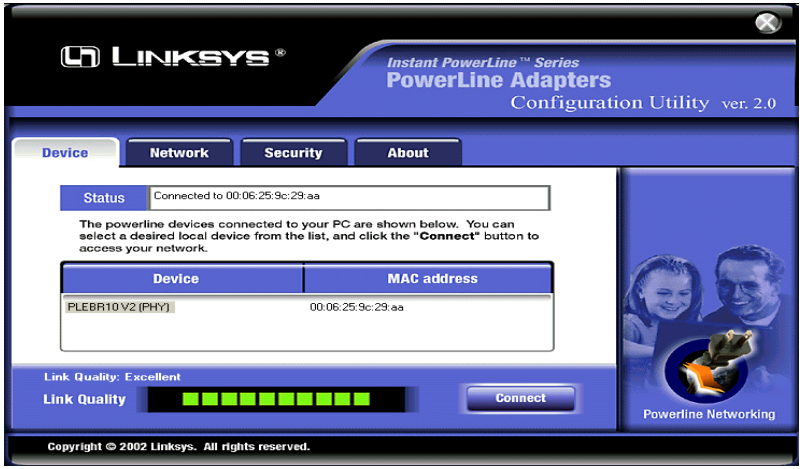
Figure 3-85

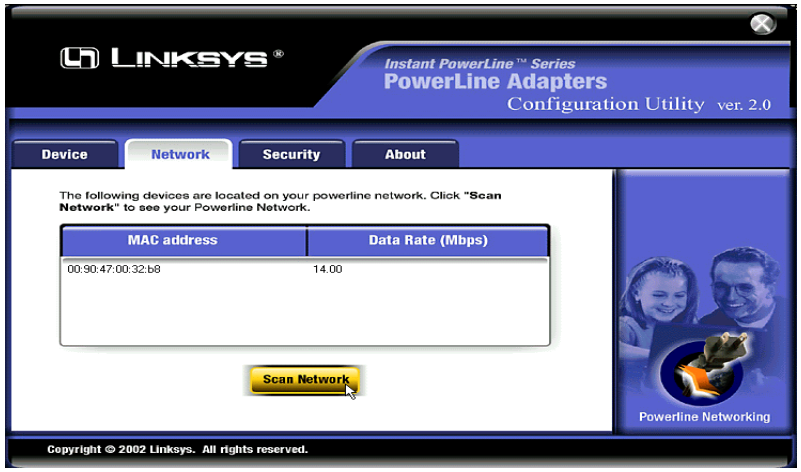


Additional Comments- Having discovered the NEK for the ABC Corporation's Kansas Facility PLN, it may be instantly observed that the password does not meet the Corporate Standards for composition. It also provides an opportunity to test the auditor's HomePlug device to ascertain if access may now be gained to the facility PLN.

Step 8 – Return to the HomePlug configuration software and enter the password discovered in step 7. The first observation is that the Link Quality instantly changes from one or two bars to nearly a full set of bars.

Figure 3-86



Step 9- A second observation is that the network tab now displays a second HomePlug device and its associated MAC address. Figure 3-87  	Additional Comments – One final observation regarding the storage of the NEK password. The NEK password file was deleted to determine if it was necessary to retain the file for device functionality. When the HomePlug device is functioning in BRIDGE mode, the absence of the NEK file does not impact access to the PLN. However, when later operating and testing the PLN in NODE mode, deleting the file caused the HomePlug device to disconnect from the network. Additional investigation should be pursued to determine if these responses are consistent across all vendor HomePlug offerings. If so, it may be advantageous to operate in Bridge mode (although restrictive) to allow for the deletion of the file that may permit the PLN to be compromised.

3.2 Measure Residual Risk

The following residual risks have been identified:

There are a number of AC power outlets available externally and internally where the placement of HomePlug devices could be concealed. Such concealment would permit espionage to occur unobserved and relatively undetectable.

HomePlug devices, compromised of solid-state technology, are susceptible to the random fluctuations of modern electric distribution networks. A power spike, surge or sag may pose as much damage to a HomePlug device as it would to any other electronic device.

HomePlug devices utilize radio communications to transmit specific frequencies via AC power lines. Therefore, due to the nature of the HomePlug technology and the current implementation of AC power distribution networks globally, these signals may be received beyond the bounds of the intended recipients. The use of RF also offers and opportunity to jam the HomePlug operating frequencies to directly impact network availability.

HomePlug devices are difficult to discover by means of common radio detection technologies. This permits the introduction of HomePlug devices, either by well-intentioned employees or by malicious individuals that may be difficult to detect.

HomePlug Standard 1.0 uses an outdated encryption algorithm. Although, based on current technology it would be difficult to capture and decrypt HomePlug traffic as it traverses an AC powerline network, it is not an improbability.

The HomePlug Network Encryption Key (NEK) mechanism stores passwords locally and in clear-text thus permitting an opportunity for PLN compromise.

The HomePlug environment may be implemented without centralized monitoring or management. The lack of a centralized management platform does not permit visibility into the availability of network elements. HomePlug devices, if not properly configured, are susceptible to network broadcast storms. The inability to monitor and manage the PLN in the event of a broadcast storm may permit unacceptable outage periods affecting system-processing cycles. Additionally, a HomePlug NEK may be unknowingly changed affecting the confidentiality, integrity and availability of a HomePlug PLN. A centralized management platform would log configuration changes providing an audit trail for investigation in the event devices are added, removed or modified without management and administrative permission.

The current operating system provides an insufficient level of control with respect to authentication and authorization.

Recommendations for the identified residual risks will be included in the final report to ABC Corporation.

3.3 Is the system auditable

The network and system is auditable by most standard tools or auditing mechanisms. However, some of the audit checklist items are not realistic given the time constraints experienced by information system auditors. The following are examples of unrealistic audit tests based on the results gained while performing the audit checklist.

Walking a facility with a HomePlug wall adapter may produce inconclusive results. If an auditor inspects the facility during the first shift of the day and a PLC device is not in use until the third shift, the auditor will leave the premise thinking that the facility is free and clear of HomePlug. Additionally, based on the size of a facility or access limitations that may be presented by locked doors, it may not be possible for the auditor to reach all powerline segments for testing. Of course testing for PLN traffic at the main breaker panel is a possibility, however it is not recommended unless the auditor is a licensed electrician. The main breaker panel presents electrical safety hazards that may be fatal to an auditor not properly trained to work in this environment.

There also exist difficulties when using detection and monitoring applications such as the Corinex OPM, as not all ac power segments may be accessible from the SNMP console. This too leaves the auditor blind to HomePlug devices that may be operating on other floors or in other areas of a building.

Attempting to brute force windows shares, although possible, is extremely time consuming and not the best use of an auditors time. There is significance to this approach however, and that is to open management's eyes to the reality of operating systems with inherent weaknesses. Using an operating system that permits end-users to configure them in an insecure fashion will only serve to expose the entire system, and quite possibly the network, to compromise. The desired effect of such an audit step would be to demonstrate the weaknesses of specific workstation operating system platforms. Highlighting these insecurities would hopefully motivate management to spend the necessary dollars to protect their information assets. In the case of the windows share password cracking checklist item, the desired result was to steal the clear text NEK password from the target system so that another powerline device could be added without observation. If successful, the resulting logs and documentation would present solid evidence of a system and network exposure.

Despite the current limitations for the rapid identification of HomePlug devices via purpose built detectors, it is still possible to detect the presence of a HomePlug device using conventional means. The best approach towards detecting powerline devices is to utilize the same methods that any auditor would with respect to network elements. The process of monitoring all local network traffic for later comparison against an inventory of known systems serves to identify newly added components.

Additionally, the using of a packet capture and analysis tool, such as Ethereal, allows the auditor to filter the traffic stream for specific protocols as was evidenced with the hunt for the Intellon MAC management protocol (0x887b). One final and common approach is to audit the log files from ingress/egress points (e.g., Internet gateway, firewall, etc.). This approach serves the same purpose as packet capture but narrows the auditors focus to specifically identifying new and suspicious traffic patterns at a point where network traffic is concentrated. Egress point auditing simplifies the hunt for equipment not previously inventoried.

XYZ COMPANY

AUDIT REPORT

REPORT OF HOMEPLUG SECURITY ANALYSIS AND AUDIT

ABC CORPORATION
KANSAS DISTRIBUTION FACILITY

October 26, 2003

Prepared by: Todd Colvin, XYZ Company, Kansas Office

Table of Contents

SYSTEM RISK LEVEL: HIGH

SUMMARY

The general risk level for the Kansas Distribution facility is categorized as *HIGH,* due to the discovery of numerous and serious cyber and physical vulnerabilities. In combination, these vulnerabilities effectively reduce the compensating controls of the system. These issues would enable system compromise resulting in the loss of data confidentiality, integrity, and availability.

The Kansas Management team is asked to please provide to ABC Corporate Staff, within the next thirty days, the action plans detailing the intended corrective measures to mitigate these vulnerabilities to reduce the overall risk of system exposure or compromise. XYZ Company is available to provide assistance in mitigating these issues.

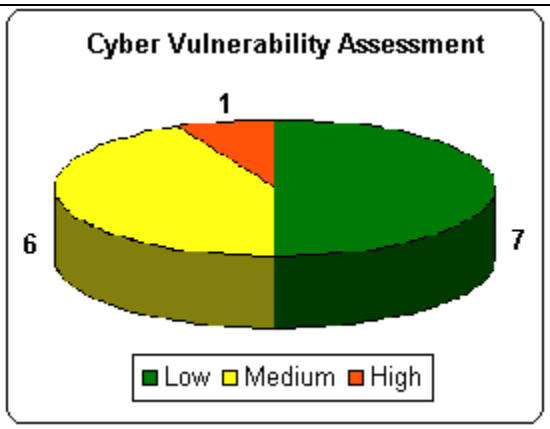
GENERAL FINDINGS

The Nessus network vulnerability tool discovered cyber vulnerabilities that if exploited, would allow for the compromise of the HomePlug NEK.

The external perimeter of the facility allows for the deployment and concealment of HomePlug devices that would permit the loss of information confidentiality and integrity.

The operating system hosting the HomePlug device lacks security controls that would normally restrict unauthorized access to system resources.

Password composition requirements are not systematically enforced.



Total Hosts Scanned: 6 (Print Server Excluded)
Hosts with HomePlug Installed: 1
Low Risk Vulnerabilities for HomePlug Sys: 7
Medium Risk Vulnerabilities for HomePlug Sys: 6
High Risk Vulnerabilities for HomePlug Sys: 1
Total cyber vulnerabilities for HomePlug Sys: 14

Symbols

Immediate action required

Review required

Awareness required

MANAGEMENT ACTIONS REQUIRED

The following actions must be taken by management to improve the overall physical and cyber security posture.

	Review and revoke generic administrative access to system resources by non-information technology personnel.
	Implement and enforce corporate password composition requirements for access to network and system resources.

		Purchase and implement an enterprise class operating system using accepted minimum-security baselines and best practices.
		Implement required security controls based on data classification.
		Harden the cyber security of the system through the application of patches and the configuration or removal of non-essential system processes.
		Install locks on all external AC power outlets or in locations where concealed access may be gained. Check with local codes prior to implementation.
		Investigate and implement a centralized monitoring and management console for HomePlug devices.

4.1 Security Analysis and Assessment Overview

4.1.1 Background

ABC Corporation, primarily located in the United States, has received internal reports from it's Kansas based branch office and warehousing facility that unauthorized low-voltage power line devices based on the HomePlug 1.0 Standard are deployed on its local area network. It was further reported that said devices are being used to extend network capabilities, to include unfiltered Internet access, to offices on the warehouse floor, while subverting recent corporate efforts to detect wireless (e.g., 802.11a or 802.11b technology) access points.

Of additional concern to the ABC Corporation, is the use of non-enterprise class workstation operating systems (i.e., Windows 9x (95/98) and Millennium Edition (ME)), within the Kansas facility. The ABC Corporation is aware of the security and control limitations presented by such operating systems and fears the workstations contained within that facility would present likely targets for malicious entities should they be directly exposed to the Internet. ABC Corporation further realizes that such direct exposure could lead to a domino effect presenting backdoor access into the corporate wide area network that is presently without inter-facility firewalls providing access to enterprise information assets located at its headquarters.

XYZ Company of Kansas, a recognized information systems and network auditing organization engaged by the ABC Corporation, is tasked with auditing the local area network housed within the Kansas facility, reporting on the results of the audit and providing recommendations to management to improve the overall security posture of the facility.

Accordingly, XYZ Company will audit the Ohio facility specifically for the presence of Ethernet traffic being transmitted across low-voltage power line communication devices based on the HomePlug 1.0 Standard and if discovered, expand the assessment to review any Windows 9x or ME workstation determined to be actively engaged in the support or use of such PLC devices.

To that end, XYZ Company will:

13. Research Low-Voltage Powerline Communication (PLC) devices.
14. History
15. Technology
16. Benefits
17. Limitations
18. Form Factor
19. Tools and methods to detect the presence of PLC devices

20. Evaluate and document the risks presented by the use of PLC devices
21. Research and document the current state of practice.
22. Create an audit checklist
23. Conduct the audit
24. Present a written report containing the 10 key findings (visual evidence of the audit) and associated recommendations.

ABC Corporation, having agreed to the terms and conditions of the audit as listed above, have approved and granted the XYZ Company with the authority to proceed without delay.

4.1.2 Summary

The general risk level for the Kansas Distribution facility is categorized as *HIGH,* due to the discovery of numerous and serious cyber and physical vulnerabilities. In combination, these vulnerabilities effectively reduce the compensating controls of the system. These issues would enable system compromise resulting in the loss of data confidentiality, integrity, and availability.

The Kansas Management team is asked to please provide to ABC Corporate Staff, within the next thirty days, the action plans detailing the intended corrective measures to mitigate these vulnerabilities and reduce the overall risk of system exposure or compromise. XYZ Company is available to provide assistance in mitigating these issues.

4.1.3 Document Scope

The HomePlug Security Analysis and Audit (HSAA) report provides detailed findings regarding the security posture of a defined network and system environment. Additionally, it serves to raise management awareness where specific security controls must be improved upon thus reducing short-term risks to the environment.

4.1.4 *Target Audience*

The HSAA report is categorized as “XYZ Company and ABC Corporation Restricted,” with distribution limited to personnel on a “case-by-case” basis with a management identified “need-to-know.”

4.2 Security Analysis and Audit Process

4.2.1 *Security Analysis and Audit Process*

4.2.2 *Audit Process Description*

The Security Analysis and Audit process is a progressive methodology aimed at risk identification and mitigation through management awareness. Steps taken during the assessment include:

1. Investigation
2. Analysis
3. Documentation and Review

4. Risk Mitigation
5. Verification

The first step requires a thorough investigation and definition of the systems and boundaries comprising an information asset environment. The resulting investigative documentation forms the framework for the system analysis.

The second step utilizes a combination of automated tools in conjunction with a manual review of the results to establish a security baseline for the target environment.

The third step provides for the development and review of recommendations by Corporate Security to improve, where possible, the security posture for the target system.

The fourth step seeks system owner and administrator support for the reduction of risk through the mitigation of identified vulnerabilities.

The fifth and final step closes the loop by verifying that some or all of the security recommendations for the target environment, using automated tools and manual processes, have been implemented.

4.3 Assessment Scope

For the purpose of analyzing, auditing and reporting on the security and policy compliance for the ABC Distribution Facility Network, XYZ Company is focused specifically on steps one (1) through three (3) of the methodology outlined in section 2.1 for the target environment.

XYZ Company is available to assist management representatives with steps four and five (4 and 5), the mitigation of identified issues and verification that controls have improved and security recommendations have been implemented.

To gain a broad perspective of the security posture of the target environment, an analysis of the HomePlug standard was initiated in March 2003. The result of which lead to the development of an audit checklist targeting the following areas:

- Architecture – Review the host inventory and network topology for comparison against automated discovery and assessment tools.
- HomePlug Communications – Inspect for the presence of obvious or subtle communications ingress points (i.e., HomePlug networks) to information assets.
- Operating System and Password Strength – Utilize automated tool(s) and manual analysis to detect operating system vulnerabilities.
- Physical – Review the controls employed to safeguard against unauthorized physical access.

- Firewalls – Firewall analysis examines the firewall rules and the firewall logs.

4.4 Assessment Tools

The following tools were used to identify system and network vulnerabilities:

- SuperScan network mapping
- Nessus network vulnerability scanner
- Ethereal-packet capture and analysis
- CAIN-NetBIOS Enumeration
- CAIN-Brute Force Share Passwords.
- AntiVirex Virus Scanner
- AdAware Spyware Detection/Removal
- Screen Saver Bypass version 3.1
- CAIN ScreenSaver Password Analysis

Additionally, the following tools were attempted in an effort to rapidly identify HomePlug devices radio signals:

- True RMS DVM
- Field Strength Meter
- Frequency Counter
- Radio Scanner
- Radio Scanner with Oscilloscope software

4.5 Detailed Findings

***4.5.1** Architecture*

ABC Corporations Information Policy requires a current visual depiction of the network topology comprising the environment and surrounding device(s) be maintained.

4.5.2 Topology Observations

OBSERVATIONS	A current topology was unavailable
RISK	A visual depiction of the current network topology surrounding the device(s) is useful for the rapid identification and resolution of security incidents.
CONTROL REQUIREMENT	
RECOMMENDATIONS	A network topology should be developed and maintained on a quarterly basis and retained in a centralized repository with highly restricted access.
COSTS	Less than $1000 dollars for an automated discovery and mapping tool.
COMPENSATING CONTROLS	None.

4.5.3 System and Network Inventory Observations

OBSERVATIONS	The ABC Corporation provided system and network inventory did not contain a listing for the host named Daredevil at IP address 172.16.128.103.
RISK	A current system and network inventory provides a baseline for comparison to aid in the identification of new or suspicious information systems.
CONTROL REQUIREMENT	All information systems and network elements must be inventoried. Inventories must be updated and maintained on a quarterly basis. A current inventory provides a ready reference for troubleshooting issues and incidents.
RECOMMENDATIONS	A system and network inventory should be developed and maintained on a quarterly basis and retained in a centralized repository with highly restricted access.
COSTS	Less than $1000 dollars for an automated discovery and mapping tool.
COMPENSATING CONTROLS	None.

4.6 HomePlug Communications

The HomePlug communications assessment, performed by representatives of XYZ Company, investigates the target environment for obvious means of alternative data access to ABC Corporations Information Assets with specific focus on HomePlug communications.

4.6.1 HomePlug Device Discovery via Radio Detection

OBSERVATIONS	HomePlug devices are difficult to detect by means of common radio detection technologies. This permits the introduction of HomePlug devices, by either well-intentioned employees or by malicious individuals while, that may be difficult to detect.
RISK	In due time, it is perceived that detection tools will become available permitting malicious users with an opportunity to remotely locate and compromise HomePlug Powerline Networks.
CONTROL REQUIREMENT	Process must be enabled to routinely inspect for the presence of HomePlug devices. If HomePlug is used within any facility where sensitive corporate data is transmitted, processed or stored (including vendor and third party facilities) then appropriate controls as outlined within the policy must be implemented. Controls should also provide for the monitoring, management and auditing of HomePlug devices.
RECOMMENDATIONS	Until purpose built PLC detection devices are developed, it is recommended that the ABC Corporation purchase at a minimum, a PLC wall-plug device with the minimum number of LED's outlined in the HomePlug technology review section of this document. Ideally, the use of PLN detection and monitoring software, such as that offered by Corinex, should be employed to routinely and remotely monitor PLN's for the introduction or modification of any HomePlug devices.
COSTS	Less than $100 dollars for a wall plug form factor HomePlug device. Less than $5000 dollars to purchase a monitoring and management laptop or workstation. Less than $200 dollars to purchase a commercial HomePlug monitoring and management application.

COMPENSATING CONTROLS	Develop policies and procedure to prohibit the use of new technologies until reviewed and approved by corporate security organization.

4.6.2 HomePlug Device Radio Signal Broadcasts

OBSERVATIONS	HomePlug devices utilize radio communications to transmit specific frequencies via AC power lines. Therefore, due to the nature of the HomePlug technology and the current implementation of AC power distribution networks globally, these signals may be received beyond the bounds of the intended recipients.
RISK	Data integrity and confidentiality may be compromised depending upon the configuration and management of the Network Encryption Key
CONTROL REQUIREMENT	Process must be enabled to routinely inspect for the presence of HomePlug devices. If HomePlug is used within any facility where sensitive corporate data is transmitted, processed or stored (including vendor and third party facilities) then appropriate controls as outlined within the policy must be implemented. Controls should also provide for the monitoring, management and auditing of HomePlug devices.
RECOMMENDATIONS	If eitherbound HomePlug broadcasts are a concern to an organizations information security program, then a qualified electrician should be sought to install “blocking capacitors or low-pass filters (blocking above 60 Hz) on AC power lines [to] negate carrier current devices” (Carrier).
COSTS	Electrician labor cost plus supplies.
COMPENSATING CONTROLS	Identify power segments that do not run outside of the facility via devices such as the Corinex Diagnostics Kit.

4.6.3 HomePlug Electronic Component Failure

OBSERVATIONS	HomePlug devices, compromised of solid-state technology, are susceptible to the random fluctuations of modern electric distribution networks. A power spike may pose as much damage to a HomePlug device as it would to any other electronic device.
RISK	Component failure may impact system and network availability.
CONTROL REQUIREMENT	Process must be enabled to routinely inspect for the presence of HomePlug devices. If HomePlug is used within any facility where sensitive corporate data is transmitted, processed or stored (including vendor and third party facilities) then appropriate controls as outlined within the policy must be implemented. Controls should also provide for the monitoring, management and auditing of HomePlug devices.
RECOMMENDATIONS	(It is recommended that spare HomePlug adapters be purchased and stored in reserve should a power line fluctuation damage the HomePlug circuitry).
COSTS	Less than $100 dollars for a spare HomePlug device in the event of a component failure.
COMPENSATING CONTROLS	Install fiber optic cable between offices within the facility.

4.6.4 HomePlug Encryption Algorithm

OBSERVATIONS	HomePlug Standard 1.0 uses an outdated encryption algorithm (DES 56 bit). Although, based on currently available technology, it would be difficult to capture and decrypt HomePlug traffic as it traverses an AC powerline network; it is only a matter of time.
RISK	Data integrity and confidentiality may be compromised depending upon the configuration and management of the Network Encryption Key
CONTROL REQUIREMENT	Process must be enabled to routinely inspect for the presence of HomePlug devices. If HomePlug is used within any facility where sensitive corporate data is transmitted, processed or stored (including vendor and third party facilities) then appropriate controls as outlined within the policy must be implemented. Controls should also provide for the monitoring, management and auditing of HomePlug devices.
RECOMMENDATIONS	If the information being transmitted by HomePlug devices is classified as sensitive to the ABC Corporation, then it is the auditor's recommendation that additional VPN technology be deployed to decrypt information prior to traversing the PLN.
COSTS	Hardware VPN end-point with client software or a pair of VPN end-points. Approximate cost is less than $5000.
COMPENSATING CONTROLS	Partition the HomePlug traffic to restrict the transmission of sensitive or classified information.

4.6.5 *HomePlug Network Encryption Key (NEK)*

OBSERVATIONS	The HomePlug Network Encryption Key (NEK) mechanism stores passwords locally and in clear-text thus permitting an opportunity for compromise. Additionally, the identified password for the HomePlug PLN does not meet the standards for composition.
RISK	Data integrity and confidentiality may be compromised depending upon the configuration and management of the Network Encryption Key
CONTROL REQUIREMENT	Process must be enabled to routinely inspect for the presence of HomePlug devices. If HomePlug is used within any facility where sensitive corporate data is transmitted, processed or stored (including vendor and third party facilities) then appropriate controls as outlined within the policy must be implemented. Controls should also provide for the monitoring, management and auditing of HomePlug devices. Password should be composed of: 15. Upper and Lower Case Alpha Characters 16. Numeric Characters 17. At least one special symbol character 18. No more than two characters should be repeated consecutively 19. The combination of characters must be between 6 and 8 characters in length. 20. The word must not be a common dictionary word The word must not utilize the organizational name.
RECOMMENDATIONS	Unless operating in a NODE configuration, it is recommended that the password files be located in the manufacturers installation directory and be deleted.
COSTS	No cost to delete the password when using HomePlug devices in

	BRIDGE mode.
COMPENSATING CONTROLS	Centralized monitoring and management of the NEK and HomePlug Powerline network when operating in a NODE configuration.

4.6.6 *HomePlug Network Services*

OBSERVATIONS	A typical HomePlug configuration includes the installation of software that initializes during system start-up. The initialization calls and then loads a process into memory called "BridgeDecor." BridgeDecor appears to call a second process named "WinPLCman."
RISK	System availability and performance may be degraded.
CONTROL REQUIREMENT	Process must be enabled to routinely inspect for the presence of HomePlug devices. If HomePlug is used within any facility where sensitive corporate data is transmitted, processed or stored (including vendor and third party facilities) then appropriate controls as outlined within the policy must be implemented. Controls should also provide for the monitoring, management and auditing of HomePlug devices.
RECOMMENDATIONS	Unless operating in a NODE configuration, it is recommended that the network processes be disabled by removing the run command for the BridgeDecor.exe file from the registry.
COSTS	No cost to modify the registry.
COMPENSATING CONTROLS	None required if removing the network processes from the registry (BRIDGE MODE ONLY).

4.7 Operating System

4.7.1 *Version Observations*

OBSERVATIONS	The workstation operating system was reviewed and observed to be lacking current patch levels as required by Microsoft for the Windows 98 platform. Additionally, the current operating system provides an insufficient level of control with respect to authentication and authorization.
RISK	Data confidentiality, integrity and availability may be compromised based on known and remotely exploitable system vulnerabilities.
CONTROL REQUIREMENT	Systems will maintain current security patches and be configured according to corporate minimum-security baselines and recognized best practice guidelines.
RECOMMENDATIONS	Utilize the Microsoft Windows Update service to routinely inspect and install current patches. The least expensive option to overcome the risks associated with the use of the Windows 9/X operating system would be the use of Microsoft's Policy Editor. The policy editor is available with the Windows 9/X Resource Kit. The policy editor may be applied to the default computer configuration to restrict access to passwords, file sharing, and network resources as examples. However, the recommended option would be to replace the existing operating system with an enterprise class operating system capable of better protecting information assets.
COSTS	No cost to licensed users. Windows Resource Kit for Policy Editor less than $300 Cost to upgrade to an enterprise class workstation operating system is less than $500.

COMPENSATING CONTROLS	Deploy a centralized monitoring and management application such as Microsoft's SMS to maintain current system configurations.

4.7.2 *Password Observations*

OBSERVATIONS	The following observations were made with respect to workstation passwords: BIOS password disabled Screensaver password does not meet composition requirements. The workstation is configured to share its entire local hard disk.
RISK	Data confidentiality, integrity and availability may be compromised if unauthorized personnel or permitted administrative access to system resources.
CONTROL REQUIREMENT	All information systems must utilize a password-protected screensaver. The password must comply with corporate composition standards. Password should be composed of: 1. Upper and Lower Case Alpha Characters 2. Numeric Characters 3. At least one special symbol character 4. No more than two characters should be repeated consecutively 5. The combination of characters must be between 6 and 8 characters in length. 6. The word must not be a common dictionary word The word must not utilize the organizational name. Open file sharing will be restricted to file servers, mail servers, or systems reviewed and approved by management based on business need. Implement user authentication mechanisms (such as firewalls, dial-in controls, secure ID) to limit access to authorized personnel.
RECOMMENDATIONS	The least expensive option to overcome the risks associated with the use of the Windows 9/X operating system would be the use of Microsoft's Policy Editor. The policy editor is available with the Windows 9/X Resource Kit. The policy editor may be applied to the default computer configuration to restrict access to passwords, file sharing, and network resources as examples. However, the recommended option would be to replace the existing operating system with an enterprise class operating system capable of better protecting information assets.
COSTS	Windows Resource Kit for Policy Editor less than $300 Cost to upgrade to an enterprise class workstation operating system is less than $500.
COMPENSATING CONTROLS	There is no way to systematically enforce password composition to meet standards.

4.7.3 CDROM Autorun Feature Observations

OBSERVATIONS	The CDROM Autorun feature is enabled permitting unauthorized users to bypass the screensaver password prompt.
RISK	Data confidentiality, integrity and availability may be compromised if unauthorized personnel or permitted administrative access to system resources.
CONTROL REQUIREMENT	Implement user authentication mechanisms (such as firewalls, dial-in controls, secure ID) to limit access to authorized personnel. Only individuals with a "need-to-know" and processed on an "event-by-event" basis will be authorized access to identified assets. Systems will maintain current security patches and be configured according to corporate minimum-security baselines and recognized best practice guidelines.
RECOMMENDATIONS	The least expensive option to overcome the risks associated with the use of the CDROM autorun feature is to disable it. However, the recommended option would be to replace the existing operating system with an enterprise class operating system capable of better protecting information assets.
COSTS	No cost to disable the autorun feature. Cost to upgrade to an enterprise class workstation operating system is less than $500.
COMPENSATING CONTROLS	None required if CDROM autorun disabled.

4.7.4 Antivirus Application Observations

OBSERVATIONS	The installed anti-virus application did successfully detect the presence of the EICAR files. However, upon further inspection it was determined that the scanning engine and virus definition files are greatly outdated.
RISK	Data confidentiality, integrity and availability may be compromised by the introduction of viruses or rojan .
CONTROL REQUIREMENT	Install corporate standard anti-viral software on all computers. Provide training and awareness of virus prevention techniques.
RECOMMENDATIONS	Implement a process to automatically inspect for and remove virus files. Modify the security settings of the web browser to restrict the types of applications or programming languages that may be run from the Internet. Purchase and install a real-time antivirus prevention utility. Block known website offenders at the firewall.
COSTS	Range from less than $100 dollars for local anti-virus detection and prevention with a yearly subscription to several thousand dollars for an enterprise virus-scanning gateway. It is recommended that both options be reviewed and installed, with unique vendor solutions for each, to layer the ABC Corporate defenses against virus attacks.
COMPENSATING CONTROLS	Restrict access to the Internet to only those with a management approved business need.

4.7.5 Spyware Observations

OBSERVATIONS	The presence of spyware was detected on the local system.
RISK	Data confidentiality may be compromised when using Internet resources.
CONTROL REQUIREMENT	Information resources must be guarded against the accidental or intentional installation of spyware (e.g., tracking cookies, key loggers, etc.).
RECOMMENDATIONS	Implement a process to routinely inspect for and remove instances of known spyware. Modify the security settings of the web browser to restrict the types of applications or programming languages that may be run from the Internet. Purchase and install a real-time spyware prevention utility. Block known website offenders at the firewall.
COSTS	Range from less than $100 dollars for local spyware detection and prevention to several hundred dollars for a web-filtering application with a monthly subscription.
COMPENSATING CONTROLS	Restrict access to the Internet to only those with a management approved business need.

4.7.6 Operating System Vulnerabilities

XYZ Company scanned six (1) unique IP addresses on the local network. The results of the scan identified one (1) workstation broadcasting HomePlug traffic. A further scan of the workstation identified one (1) high vulnerability present in addition to a number of medium and low vulnerabilities. A High, Medium or Low Risk vulnerability indicates an opportunity exists for system compromise.

The vulnerability scan produced the following results:

Total Hosts Reviewed	1
Distinct High Vulnerabilities	1
Distinct Medium Vulnerabilities	6
Distinct Low Vulnerabilities	7
Total Vulnerabilities Discovered	14

4.7.7 Vulnerability Scan Observation Number 1

OBSERVATIONS	The Nessus scanner was able to log into the host using the following login/password combinations: • ‘administrator’/’’ • ‘administrator’/’administrator’ • ‘guest’/’’ • ‘guest’/’guest’

	Furthermore, the Nessus scanner determined that: It was possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000). Note that this won't completely disable null sessions, but will prevent them from connecting to IPC$
RISK	Data confidentiality, integrity and availability may be compromised when remote access is open to unauthorized users.
CONTROL REQUIREMENT	Only individuals with a "need-to-know" and processed on an "event-by-event" basis will be authorized access to identified assets. Systems will maintain current security patches and be configured according to corporate minimum-security baselines and recognized best practice guidelines.
RECOMMENDATIONS	Configure system and services per vendor recommendations and in accordance with minimum security baselines and best practice guidelines.
COSTS	No cost.
COMPENSATING CONTROLS	Restrict network access to workstations and systems with a management approved business need.

4.8 Physical

The physical security assessment, performed by a representative of the XYZ Company, provides an on-site examination of physical controls in addition to policy and process interviews with management.

The areas examined include facility access control (e.g., employee access, card access system, lock & key program); guard services; alarm system; redundancy of power and HVAC; and areas were the concealed placement of HomePlug devices may occur.

4.8.1 *Locking Mechanism Observations*

OBSERVATIONS	There are a number of AC power outlets available externally and internally where the placement of HomePlug devices could be concealed. Such concealment would permit espionage to occur unobserved and relatively undetectable with existing tools.
RISK	Data confidentiality may be compromised when using Internet resources.
CONTROL REQUIREMENT	In consultation with facilities management, facilitate the implementation of physical security controls designed to protect the information, software, and hardware required of the system
RECOMMENDATIONS	It is recommended that locking ac outlet covers be installed if permitted by local law. Such covers are available from vendors such as Thomas & Betts (http://www.tnb.com) and TayMac (http://www.taymac.com).
COSTS	Range from less than $50 dollars for the cover and separate padlock.

COMPENSATING CONTROLS	Move plants, shrubs and trees away from AC outlets and increase perimeter security patrols. Train guard service to observe external AC outlets during rounds. Instruct maintenance personal and management to observe internal AC outlets were concealed access may be attempted. Request that routine inspections be performed.

4.9 Firewall Controls Analysis

An assessment of the firewall controls and logging features was performed to identify access to sites of known or questionable content.

4.9.1 *Firewall Hardware and Software*

OBSERVATIONS	The current firewall lacks enterprise class features.
RISK	Improper installation and configuration may result in unauthorized access to the ABC Company network.
CONTROL REQUIREMENT	A firewall should be engineered, monitored and managed by the security organization to aid in the protection of perimeter security. Requests to permit traffic to traverse the firewall will be viewed for business need and approved or denied based on an analysis of the exposure created by said request. Furthermore logs must be viewed on a monthly basis to determine compliance with the corporations acceptable use policy. Failure to comply with the acceptable use policy may lead to disciplinary action.
RECOMMENDATIONS	Purchase and install an enterprise class firewall.
COSTS	Range from less than $500 dollars to several thousand dollars depending on requirements.
COMPENSATING CONTROLS	Restrict network access to workstations and systems with a management approved business need. Monitor logs on a daily or weekly basis to identify suspicious activity.

4.9.2 *Firewall Logs*

OBSERVATIONS	The current firewall logs provide very basic traffic information to include source and destination IP addresses and Ports. Local personnel do not inspect the firewall logs.
RISK	Unobserved activity including access to ABC Corporation system and network assets as well as outbound access to sites of questionable content may pose a judicial threat to the Corporation.
CONTROL REQUIREMENT	A firewall should be engineered, monitored and managed by the security organization to aid in the protection of perimeter security. Requests to permit traffic to traverse the firewall will be viewed for business need and approved or denied based on an analysis of the exposure created by said request. Furthermore logs must be viewed on a monthly basis to determine compliance with the corporations acceptable use policy. Failure to comply with the acceptable use policy may lead to disciplinary action. Implement mechanisms to monitor, report, and audit activities identified, as requiring independent reviews, including periodic reviews

	of user ID's to ascertain and verify business need.
RECOMMENDATIONS	Purchase and install an enterprise class firewall.
COSTS	Range from less than $500 dollars to several thousand dollars depending on requirements.
COMPENSATING CONTROLS	Restrict network access to workstations and systems with a management approved business need. Monitor logs on a daily or weekly basis to identify suspicious activity.

5 Appendix A: ABC Provided Documentation

5.1.1 *Kansas Distribution Facility – System Inventory*

Host Name	O/S Platform	IP Address
Poison Ivy	Windows	172.16.128.100
Spiderman	Windows	172.16.128.104
Batman	Windows	172.16.128.105
Punisher	Novell	Non-IP Protocol
Gateway	Firewall	172.16.128.XX
Print Server	Print Server	172.16.128.150

5.1.2 *Firewall Log Files*

Logs were provided but due to space limitations only ten records from the incoming and outgoing logs will be presented.

Incoming
10/01/2003 22:48:18 61.40.224.249 1029 65.66.157.90 137
10/01/2003 23:02:50 198.36.22.18 4156 65.66.158.152 4156
10/01/2003 23:07:26 66.28.236.84 4156 65.66.158.152 4156
10/01/2003 23:22:01 200.83.146.57 4018 65.66.157.193 4662
10/01/2003 23:34:01 172.190.200.11 4166 65.66.156.163 1230
10/01/2003 23:35:41 64.94.89.221 80 65.66.156.163 1037
10/02/2003 00:02:54 24.184.219.175 4778 65.66.158.157 6346
10/02/2003 00:48:25 217.3.33.9 1280 65.66.156.86 6399
10/02/2003 00:49:33 200.204.176.202 1047 65.66.156.86 137
10/02/2003 01:04:08 172.181.131.63 2117 65.66.156.89 1214

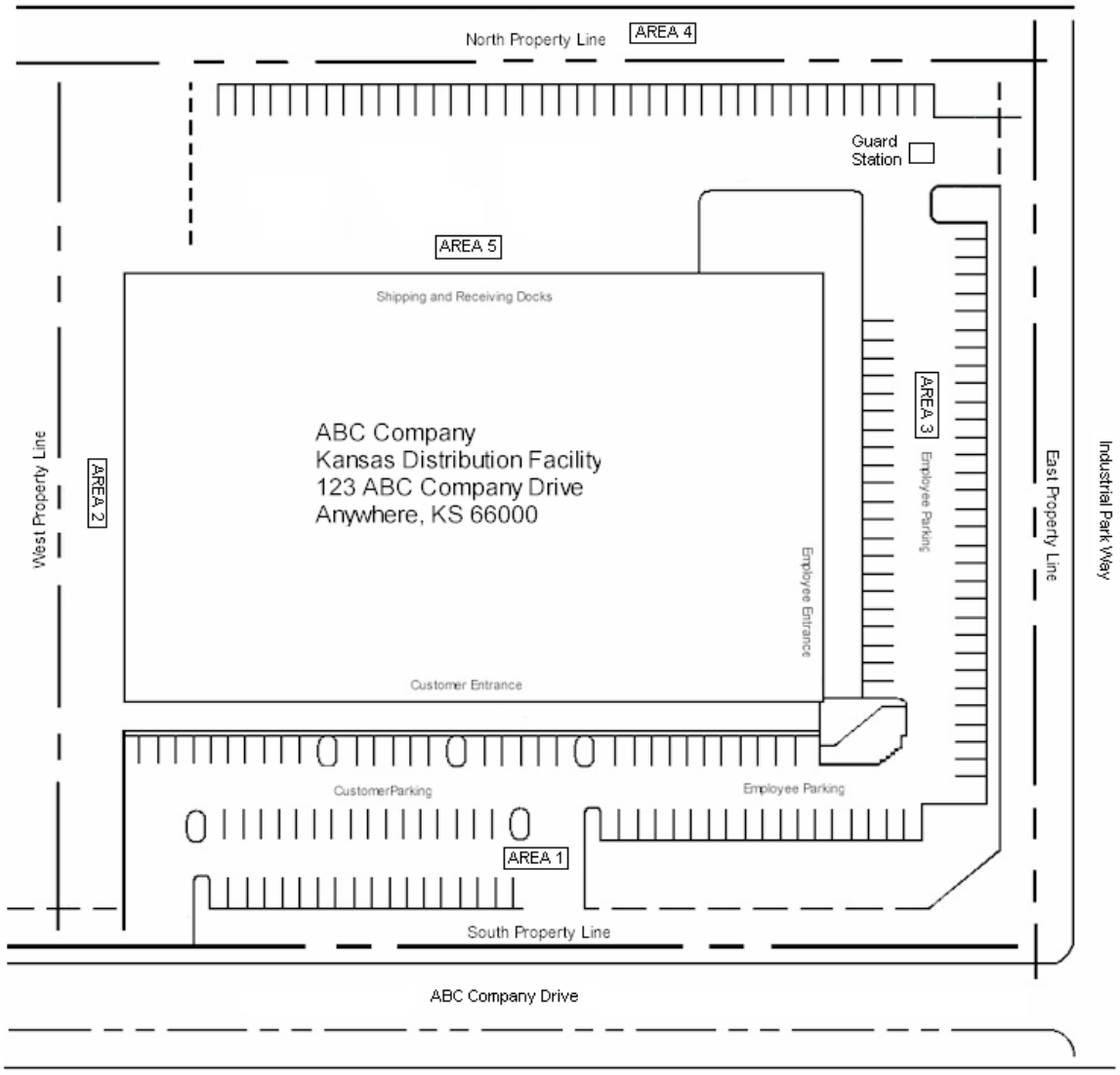
Outgoing
10/02/2003 11:24:29 172.16.128.103 1147 ad.doubleclick.net 80
10/02/2003 11:24:30 172.16.128.103 1149 ads.ah-ha.com 80
10/02/2003 11:25:03 172.16.128.103 1150 www.altavista.com 80
10/02/2003 11:25:04 172.16.128.103 1151 ad.doubleclick.net 80
10/02/2003 11:25:05 172.16.128.103 1155 m2.doubleclick.net 80
10/02/2003 11:25:05 172.16.128.103 1156 search.gator.com 80
10/02/2003 11:25:36 172.16.128.103 1157 www.altavista.com 80
10/02/2003 11:25:37 172.16.128.103 1160 66.150.1.141 80
10/02/2003 11:25:38 172.16.128.103 1166 ss.gator.com 80
10/02/2003 11:25:38 172.16.128.103 1167 bannerserver.gator.com 80

5.1.3 XYZ Company IP Address Assignment

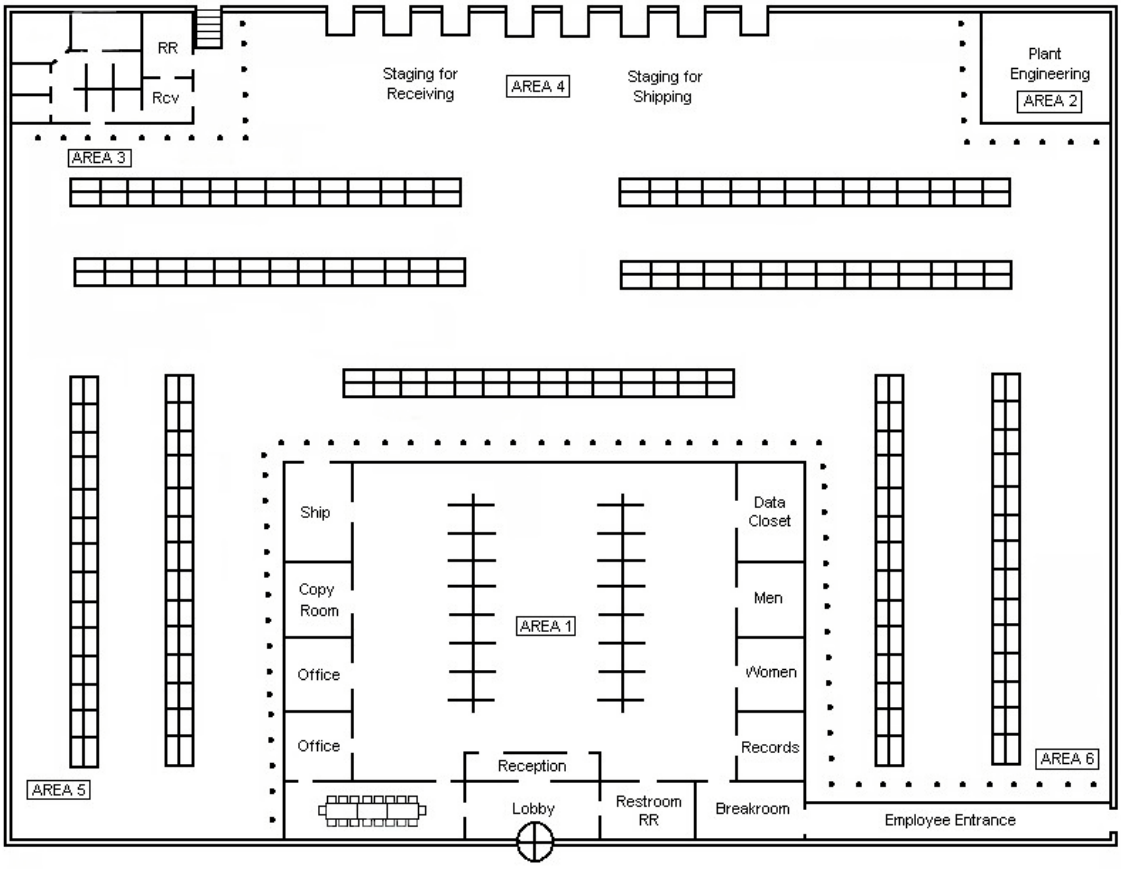
XYZ Company is authorized to use IP addresses 172.16.128.101 and 172.16.128.102 for the duration of the audit.

6 Appendix B: Kansas Distribution Facility Maps

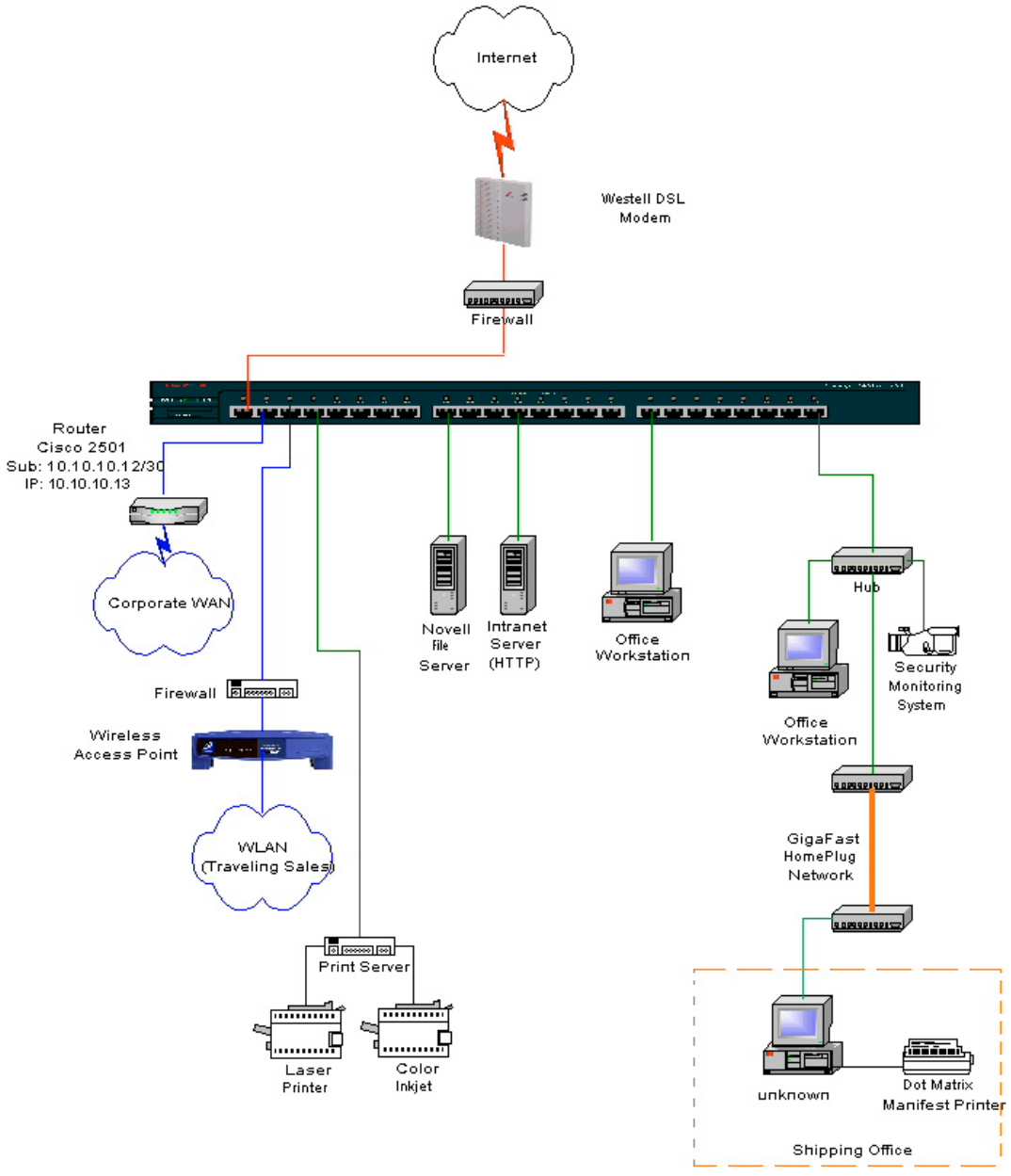
External Facility Drawing



Internal Facility Drawing



7 Appendix C: Network Topology



8 Appendix D: Audit Checklist and Results

Task ID	Risk ID's	Selected as an Evidentiary Procedure (Y=YES N=NO)	Stimulus/ Response (Y=YES N=NO)	Reference(s)	Control(s)	Test Purpose: Objective	Test Purpose: Subjective	Test Procedure	Test Results: Pass	Test Results: Fail	Test Results: Other*	Compliance (*Other requires a detailed explanation)
1	1 2 3	N	N	CWNA PEOC	17 18 19		S	Utilizing a map of the facility (with powerline source documentation if possible) walk the entire property boundary, internal and external building perimeter and office locations to visually inspect for: 1. The presence of powerline devices based on identified form factors. 2. The identification of areas where powerline devices may be covertly placed. The presence of power outlet locks for external locations.		X		TARGET: Locking AC covers should be identified in external locations. External AC outlets should not be obstructed from routine observation. There should be no Powerline devices attached to any external or internal AC outlets that are easily visible. ACTUAL: Locking covers were not observed anywhere on the premise. There were also areas discovered where HomePlug devices could be implanted and concealed offering the loss of data confidentiality and compromise.
2	1 2 3 32	N	Y	PEOC	18 19 20 21	O		While performing the physical inspection identified in step one, locate unique power segments based on the provided facility map and perform a PLN activity audit by: 1. Plugging the auditor's HomePlug device into an AC outlet.		X		TARGET: The HomePlug Activity LED should not display PLN activity for any AC outlet connection. ACTUAL: HomePlug traffic was discovered in the following tested areas: External Areas 2 and 5 as

								2. Permit 15-30 seconds to elapse 3. Record any observable HomePlug traffic based on the Activity LED. 4. Repeat steps 1 thru 3 until completed.				well as Internal Areas 1 and 3. The discovery of HomePlug traffic confirms ABC Corporations concern regarding the use of HomePlug PLN devices to subvert efforts to detect wireless access points.
3	18 19	Y	N	NIST PEOC HAXP	18 19	O		Utilize an automated network scanner to: 1. Identify systems connected to the network 2. Determine what ports are open on the identified systems. Compare the results of the scan with the inventory provided by ABC Corporation. Note any discrepancies and document them for the final report.		X		TARGET: The network scanner should not detect network addresses for previously unknown and non-inventoried equipment. ACTUAL: IP address 172.16.128.103 was discovered and compared against the ABC Corp. provided host inventory list and determined to be absent from said list. The system was identified as having the following ports open: 135/tcp 137/tcp 139/tcp 427/tcp 1032/tcp
4	33	Y	N	HAXP PEOC	18 19 20	O		Utilize a packet capture and analysis utility to:		X		TARGET: HomePlug traffic should not be detected within the environment per contract with

					21			1. Identify the presence of HomePlug traffic 2. Identify the devices using the HomePlug protocol. 3. Examine the contents of HomePlug packets to determine if they contain any sensitive command and control details (i.e., passwords) that may be viewed in clear text. Compare the results of the packet capture and analysis tool with any devices identified in the previous step that were not on the provided inventory.				ABC Corporation. If HomePlug traffic is discovered, it should be analyzed to determine susceptibility to command and control monitoring. ACTUAL: HomePlug traffic based on the Intellon MAC management protocol (0x887b) was discovered emanating from host 172.16.128.103. This validates the results of step 2. Traffic generated by this workstation was captured and a detailed packet analysis was performed to determine if sensitive, clear-text information could be extracted from the packets. Upon completion of the analysis, it was determined that the captured packets did not contain information that could affect the availability or the HomePlug PLN. As an added precaution, a packet capture and analysis was performed during the configuration of a HomePlug device to determine the susceptibility to clear-text password theft of the NEK. This secondary test produced no useful details regarding the NEK.
5	4 6 15 17	Y	N	NIST PEOC	18 20	O		Utilize an automated network vulnerability scanner to determine: 1. Operating system fingerprints		X		TARGET: Systems should be configured with only those network services and system processes required for business

	20							2. Open ports and running processes 3. Potential exposures or vulnerabilities Pay careful attention to any hosts discovered that were not listed in the inventory provided by the customer.				needs and approved by management. A vulnerability scan should produce negative results for widely known and often targeted system and network vulnerabilities. ACTUAL: The Nessus network vulnerability-scanning tool discovered open ports and services that may be exploited with readily available tools. The results of the scan will be provided in the final report.
6	6 10	Y	Y	HAXP TLAH	6 14 18 19 20 23	O		Commercial HomePlug configuration software requires a Windows based operating system; as such, a NetBIOS enumeration will be performed to determine whether any open shares exist on systems potentially identified as passing HomePlug traffic. First, attempt to connect to any discovered shares without a password (stimulus/response test with a desired outcome to connect without a password proving weak controls). If unable to connect without a password, attempt to utilize a brute-force password utility to attach to the share and determine whether the password meets corporate standards for composition. Finally, if unable to remotely brute force the password, use a local password utility to determine whether the password meets corporate		X		TARGET: Windows shares should not be permitted on non-enterprise class operating systems. If discovered, a share password must be enabled and the same password should be compared against the ABC Corporate policy to determine compliance with composition requirements. ACTUAL: Legion discovered the presence of a Windows share on the host at 172.16.128.103. The share name was \\DAREDEVIL\C The open workstation share fails to meet the control objective for Restricted File Sharing. The Cain remote share brute force failed to crack the password. The Cain local share password

								standards for composition.				decryption utility successfully identified the password as "ABC03" (without quotation marks). This password fails to meet the corporate standards for composition.
7	5	Y	Y	CESP	6 15 23	O		Properly shutdown the operating system and then reboot the computer to determine whether the BIOS password is enabled. Performing this step may lock the auditor out of the system. Therefore it is recommended that the auditor either prepare a system boot disk with appropriate CMOS password identification utilities or have the end-user for the selected system available during the BIOS password test.		X		TARGET: The BIOS password must be set to restrict access to the system configuration. ACTUAL: It was determined that the system is not presently configured to utilize a BIOS password, thus offering unauthorized access to system and network resources.
8	7	Y	Y	PEOX CESP HAXP	6 7 15 22 23	O		Determine if the system screensaver is configured to utilize a password by performing the following steps: 1. Click on Start and then Run 2. In the Run dialog box type the following without quotations "FLYING~1.SCR" 3. Allow 5-10 seconds to pass for the screen saver to activate. 4. Bump the mouse or press the spacebar to determine if the screen saver disappears or if a password dialog box appears.	X			TARGET: The screensaver must prompt for a password. ACTUAL: The screensaver is password protected.
9	9	Y	Y	CESP	6	O		Determine if the CDROM "autorun"				TARGET: The autorun feature

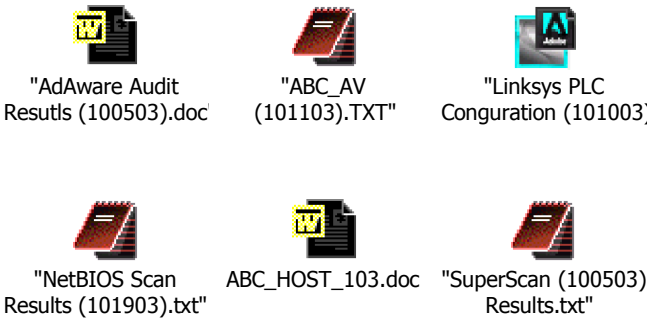
				HAXP	7 18 22 23			feature is disabled by: 1. Enable and lock the screensaver password using the technique established in step XXX. 2. Insert the screensaver bypass CD and allow 15 to 30 seconds to elapse. 3. If autorun is enabled the screensaver will unlock and permit console access. If autorun is disabled nothing will happen.		X		should be disabled to reduce the likelihood of unauthorized access ACTUAL: The bypass utility launched successfully indicating that the autorun feature has not been disabled. The autorun feature may allow for unauthorized access to system and network resources.
10	8	Y	N	CESP HAXP	6 18 22 23	O		Determine if the screensaver password meets corporate standards for composition by performing the following steps: 1. Insert the CAIN password utility CDROM or write protected floppy into system. 2. Click on Start and then Run. 3. Type the drive location and name of the file in the run dialog box or click on browse. Once the name is correctly entered, click on OK to proceed. 4. Select the appropriate tab within the password utility to display the currently assigned password.		X		TARGET: The screensaver password should be compared against the ABC Corporate policy to determine compliance with composition requirements. ACTUAL: The screensaver password does not meet the corporate standards for composition.
11	13	Y	Y	EICAR	10	O		Determine if a corporate approved anti-virus application is: 1. Installed on the system 2. Using current virus string files 3. Configured to run automatically 4. Capable of detecting the EICAR test file		X		TARGET: Per Corporate policy, the device must contain an approved anti-virus application with a current virus definition file and be configured to run routinely and automatically. The same anti-virus software must be capable of detecting the simplest of viruses as evidenced by the

								Once the above steps have been completed, reboot the system and perform a second anti-virus scan using a write-protected floppy or bootable CDROM to further determined if the installed anti-virus software is functioning properly. Any commercial version of anti-virus software may be utilized as long as it is not the same manufacturer as the currently installed AV software.				EICAR test. A secondary scan of the system using a competing anti-virus application should validate the cleanliness of the system. ACTUAL: The installed anti-virus application did successfully detect the presence of the EICAR files. However, upon further inspection it was determined that the scanning engine and virus definition files are greatly outdated.
12	14	Y	N	PEOC	11	O		Determine if the system contains spyware by: Utilizing a commercial malware scanner to identify known instances of spyware/adware. Report the results of the test but do not clean system at this time.		X		TARGET: The system should be clean of spyware. ACTUAL: The spyware scanning discovered 42 instances of tracking cookies installed on the workstation.
13	4 15 17 20	N	N	MICR	18 23 24	O		Microsoft provides the following manual process to determine if current operating system security patches have been installed in their 1. Click Start, point to Find, click Files Or Folders, type "wulog.txt wuhistv3.log" (without quotation marks) in the Named box, and then click Find Now. 2. Double-click the Wulog.txt file, and then note the update information. 3. Double-click the Wuhistv3.log		X		TARGET: The system should have all current security patches installed. ACTUAL: The Microsoft recommended procedures for manually inspecting a Windows 98 operating system to determine security software currency failed. An alternative method was attempted that involved searching the local system for any files that may contain a similar level of detail.

								file, and then note the update information.				During the course of exploration, a file named “iuhist.xml” was discovered in the V4 sub-directory of the hidden WUTemp directory. Upon further inspection of “iuhist.xml” it was determined that patch details where contained within the file that could be printed and compared against the online Windows Update Catalog. Proceeding with the alternative approach, it was determined that the system does not contain current security software patches.
14	28 29 30	Y	N	PEOC	6 8 23	O		HomePlug devices may operate with the default Network Encryption Key (NEK) of “HomePlug” or with a user assigned NEK. If a HomePlug device is located, then an analysis of the attached computer should be performed by: 1. Install the HomePlug software provided with the PLC device purchased by the auditor for the ABC contract. 2. Examine the contents of the manufacturer’s application directory (typically C:\Program Files\Manufacturer) to determine if any files exist that may contain passwords. 3. Examine the contents of the files to determine if a clear-text password may be discovered.		X		TARGET: The auditor should determine whether HomePlug configuration software is present. If it is, then the installation directory should be examined to determine if it contains a clear-text password. If a clear-text password is present, it should be compared against the ABC Corporate policy to determine compliance with composition requirements. ACTUAL: A clear-text password was discovered using the steps prescribed in checklist item 14. Subsequently, the password was compared against corporate standards for password composition and determined to be out of compliance with said

								4. If a password is discovered, does it meet the corporate standards for composition? 5. Utilize a packet capture utility to determine if any PLN device command and control traffic is passed in the clear.				standards.
15	41 42	N	N	PEOC	1 2 3 4 5 9 12	O		Examine inbound and outbound firewall logs to locate: 4. Previously unidentified outbound IP addresses 5. Suspicious inbound traffic destined for any IP addresses identified in step 1. 6. Destination IP addresses of known or questionable content.		X		TARGET: The auditor should not discover any previously unidentified outbound IP addresses when compared to the inventory. The auditor should not discover any inbound traffic destined for any IP Addresses discovered in step 1. If previously unidentified IP addresses are discovered, a thorough analysis of their destination traffic should be investigated to determine whether sites of known or questionable content are being accessed. ACTUAL: IP address 172.16.128.103 was discovered and compared against the ABC Corp. provided host inventory list and determined to be absent from said list. An intensive inspection of all Internet destination IP addresses was performed to determine whether sites of known or questionable content were accessed. The results of the analysis yielded no positive results concerning questionable sites.

9 Appendix E: Detailed Assessment Reports



10 Appendix F: HomePlug Minimum Security Baselines

Gaining access to the NEK via a poorly secured workstation opens the HomePlug PLN to attacks against data confidentiality, integrity and availability. To protect against the loss of the NEK, the following steps should be followed:

Systems responsible for the maintenance and monitoring of HomePlug devices must:

1. Follow hardening guidelines according to best practice.
2. Contain current security patches.
3. Use an automated anti-virus application with a current scanning engine and virus definition files.
4. Use an automated spyware application with a current scanning engine and spyware definition files.
5. Use a BIOS password.
6. Use a screensaver with a strong password.
7. Disable the CDROM autorun feature.

Facility Management seeking proactive measures to protect against the deliberate and malicious installation of powerline devices should:

1. Invest in locking covers for external power outlets.
2. Relocate any materials that may obscure visibility to an external or internal power outlet that would permit concealed placement of a HomePlug device.

Management representatives seeking proactive measures to protect their powerline networks should:

1. Invest in an enterprise class operating system.
2. Invest in a centralized monitoring and management console specific to powerline networks.
3. Provide security representatives with at least one HomePlug compatible device and require routine security assessments until such time that an alternative detection method is developed.
4. Modify policy to accommodate the use of HomePlug devices.
5. Provide awareness to employees regarding the security concerns presented by new technology.
6. Enforce the policy when violations occur.

11 WORKS CITED

American Radio Relay League. Now Your Talking – All you need for your first Amateur Radio License, 4th Edition. Newington: ARRL, 2000.

American Radio Relay League. Power Line Communications (PLC) and Amateur Radio. <http://www.arrl.org/tis/info/HTML/plc/> 4 September 2003.

American Radio Relay League. The ARRL RFI Book: Practical Cures for Radio Frequency Interference. Newington: ARRL, 1999.

Carter, Brian, Russell Shumway. Wireless Security: End To End. Indianapolis: Wiley Publishing, 2002.

CEPCO Products Incorporated, <http://www.cepcoproducts.com/ >.

Corinex. Open Powerline Management: SNMP Network Management Manual. <http://www.corinex.com/> 8 August 2003.

Dostert, Klaus. Powerline Communications. Upper Saddle River: Prentice Hall PTR, 2001.

Eaves, David M. Small Business IT Auditing. <http://www.giac.org/practical/David_Eaves_GSNA.zip> 27 August 2003

Electronic Freedom Foundation. Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design. Sebastopol: O'Reilly and Associates, 1998.

Granite Island Group, <http://www.tscm.com/>.

Hines, David. "Unlocking the potential of power distribution networks." Power Economics April 2000.

HomePlug Alliance, <http://www.homeplug.org/>.

Information Security Associates, Inc. <http://www.isa-tscm.com/>.

Jamaluddin, Jazilah, Edwards, Reuben, Coulton, Paul. Providing a Risk Analysis Framework for Potential Users of Wireless Technology. PostGraduate Networking Conference (PGNet) Liverpool: John Moores University, 2003.

Lauder, David. Development of Practical Methods and Equipment to Facilitate Both Detection and Measurement of Radiation from, and Wideband Radio Frequency Currents in, Unstructured Distribution Networks. <http://www.radio.gov.uk/topics/research/topics/emc/ay3920.pdf>. United Kingdom Telecommunications Agency Website, 2003.

Lee, M.K., et al. Field Performance Comparison of IEEE 802.11b and HomePlug 1.0. Proceedings of the 27th Annual IEEE Conference on Local Computer Networks <http://www.computer.org/proceedings/lcn/1591/15910598.pdf>. IEEE Computer Society, 2002.

McClure, Stuart, Joel Scambray, George Kurtz. Hacking Exposed: Network Security Secrets and Solutions, Third Edition. Berkeley: Osborne / McGraw-Hill, 2001.

McNamara, Joel. Secrets or Computer Espionage: Tactics and Countermeasures. Indianapolis: Wiley Publishing, Inc. 2003.

Microsoft. Q194796 - How to Determine Your Installed Windows 98 Updates. <http://support.microsoft.com/?kbid=194796> 1 September 2003.

Moore, Haskell. Counter Intelligence. <http://www.radio-scanning.fsworld.co.uk/frex_counter.html>, 8 May 2003.

North Carolina. Office of Information Technology Services. 920A –Structured Cabling Services. <http://www.its.state.nc.us/ITProcurement/TermContracts/Contracts/920A/ITS-00276 Contract Info.pdf> 8 May 2003

PALAS. Powerline as an Alternative Local AcceSs, Deliverable D6: State of the Art and Initial Analysis of PLC Services. <http://palas.regiocom.net/> 26 April 2003

Peltier, Thomas R. Information Security Risk Analysis. Boca Raton: Auerbach, 2001.

Planet3 Wireless. CWNA: Certified Wireless Network Administrator Official Study Guide. Berkeley: McGraw-Hill / Osborne, 2003.

Schultze, Eric. Thinking Like A Hacker. <http://www.shavlik.com/Whitepapers/Thinking like a hacker.doc.pdf> 3 September 2003.

TayMac. <http://www.taymac.com/> 3 October 2003.

TSCM Technical Services. <http://www.tscmtech.com>.

Tengdin, J. Distribution Line Carrier Communications – an Historical Perspective IEEE Trans. Power Delivery, 1998.

Thomas & Betts. <http://www.tnb.com/> 3 October 2003

United States. Dept. of Commerce. Commercial Encryption Export Controls. <http://www.bxa.doc.gov/Encryption/Default.htm> 28 June 2003.

W6/PA0ZN Weaksignal Site. Homebrew Spectrum Analyzer Project. <http://www.nitehawk.com/rasmit/sa50.html> 17 April 2003.

Wack, John, Miles Tracy, Murugiah Souppaya. NIST Special Publication 800-42: Guideline on Network SecurityTesting. <http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf > 28 June 2003

Weisman, Carl J. The Essential Guide to RF and Wireless. Upper Saddle River: Prentice Hall PTR, 2002.

11.1 Glossary

Word or Acronym	Definition
Attenuation	Reduction in signal quality over a given distance
BPLC	Broadband Power Line Communications.
BRIDGE	Layer 2 device used to segregate collision domains.
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
EMC	Electromagnetic compatibility
EMI	Electromagnetic interference
Extended Perimeter	The area beyond the physical property line for which broadcast information may be susceptible to interception.
HVL	High-Voltage Line
Impedance	
LPLC	Lower-Voltage Power Line Communications
LVL	Low-Voltage Line
MAC	Media Access Control
MVL	Medium-Voltage Line
OFDM	Orthogonal Frequency Division Multiplexing
Perimeter	The physical boundary or property line of a business facility
PHY	Physical Layer
PLC	Powerline Communciations
PLN	Powerline Network
PLT	Power Line Telecommunications (also means broadband access)
Propagation	
RFI	Radio frequency interference
ROBO	Remote Office, Branch Office
SOHO	Small Office, Home Office
Standing Waves	Radio signals still present on the transmitting medium often caused by reducing the amount of power necessary for the signal to escape the surface of the medium.