B.A.S.E – A Security Assessment Methodology

Prepared By: Gregory Braunton
GSEC Practical Assignment Version 1.4b, Option 1
Submitted September 29th, 2004

Abstract

> *"A fundamental tenet of security is that a chain is only as strong as its* weakest link *and a wall is only as strong as its weakest point. Smart attackers are going to seek out that weak point and concentrate their attentions there."*[1]

At a fundamental level, much like a chain, the Internet is a collection of organizations' business networks inter-linked that form the digital infrastructure of the world. This infrastructure forms a global information grid that harnesses the potential (good and bad) for any node to access any other node worldwide. Some are personal home networks, some are small office networks, while still others are enterprise in size and scope. Regardless their size or purpose, the collective security posture of the Internet rests, metaphorically speaking, upon each link being fortified against the rampant swarm of malicious attacks and the infestation of pestilent viruses.

Presently, the information security industry recognizes this environment as one ripe for entrepreneurship to hock their procedural "best practices" and "best of breed" technologies. Yet to build a fortified chain, each link must have the relative strength of its neighbor. The weak link must be avoided! This can only be achieved by "forging" each link with nearly similar techniques and tools. So with the myriad of proprietary vendor hardware, software, and procedural solutions (complete with premium cost) available, which is universally adaptable, executable, and accessible to the Internet community en masse? The answer – none.

The purpose of this case study, then, is to propose and practically apply an elementary information security assessment protocol called BASE. BASE stands for **B**aseline, **A**udit and Assess, **S**ecure, **E**valuate and Educate. It outlines a basic Information Assurance (IA) vulnerability assessment protocol including the use of supplementary no-cost tools in an effort to build a universal information security "forge" that is affordable and executable by everyone from the home user to enterprise security engineer. The goal of all this? To evangelize the concepts of BASE to strengthen the collective security posture of the Internet.

[1] Chapman, Brent D. & Elizabeth D. Zwicky, Building Internet Firewalls, Nov 1995, Online Extract, Chapter 3

Security Strategies, URL: http://www.busan.edu/~nic/networking/firewall/ch03_04.htm

Contents

Background

The Proliferation of Insecure Networks

As previously stated, the Internet consists of the collective individual home, small office and enterprise networks. Easy to acquire and deploy, these networks are increasing in complexity and connectivity both within and without their logical boundaries.

The typical footprint of services provided or used in these proliferating networks include

- File and Print Sharing
- Email
- Document Processing
- Virus Protection
- Wireless Access Points
- Network Operating Systems
- Instant Messaging
- Basic backup services
- Always-on Internet Services
- Business or personal web presence

It requires minimal knowledge and expertise to deploy a fully functional network complete with internet access, print, email, ftp, web, wireless, and firewall services. With equipment in hand and a couple GOOGLE^{TM} searches later, using the myriad of “how-to” and “cookbooks” sites available, your average person could assemble the various pieces to produce a default operational network in just days or hours – presto, it works!

But what to do once you have all the technical pieces in place and the bits and bytes are flowing? The average person or business simply begins using these services in their default configuration. And they do so without any knowledge or awareness of the conduit for digital maliciousness they’ve just created. A few examples of how default configurations provide this conduit underscore this point:

HTTP Proxy: (September 2003) Some of the HTTP proxy default configurations by vendors such as CISCO, Symantec, IBM, and others “allow an attacker to make arbitrary TCP connections to internal or to external third-party hosts.”[2]
Potential Impact: direct compromise/exploit capability of internal and external hosts right out of the box.

Linux Services: (May 2004) “’The Achilles heel of many Linux servers come from insecure default configurations” The fundamental problem being that Linux has a history of enabling certain services (X Serve, remote configuration via Linux.conf, FTP, Apache, and Samba) services right out of the box.. (Ref 3)
Potential Impact: un-experienced administrators are unaware of default services enabled at installation which go unsecured, unmonitored, unused, and un-patched; leaving persistent open doors into a system.

[2] The US Computer Emergency Readiness Team. Vulnerability Note VU#150227, Jan 2004. URL: http://www.kb.cert.org/vuls/id/150227

[3] InstantSSL. Next Generation of Linux Servers Unveiled, New York, May 2004. URL: http://www.instantssl.com/ssl-certificate-news/ssl-260504.html

MAC OS X : (December 2003) Settings involving the default behavior of DHCP resolution and uid '0' combine to permit the MAC to trust a malicious machine on the network.[4]
Potential Impact: With relative ease, an attacker could gain full and complete administrative control of the system right out of the box.

WINDOWS 2000 Server : NTFS permissions of EVERYONE and permissive anonymous connections are defaults on both the Windows NT 4.0 workstation and server and Windows 2000 platforms.
Potential Impact: Without administrators hardening default configurations, servers can be readily probed for system information including domain affiliations, usernames and shares and connected to for easy exploit.

These examples are just the tip of the iceberg. The Internet is fraught with evidence and pinpoint (how-to) articles detailing services and application configurations that, in their default configuration provide an open conduit through which malicious hackers can easily compromise a single or chain of interconnected networks.

The Basic Network Structure

So, what does one of these interconnected networks look like? Mentioned previously were some services provided by a basic network structure and depicted in Figure 1 below is a simple diagram of such a network. Undoubtedly, not all networks are the one depicted. Some are simpler, yet others many times more expansive and complex. But, it is a suitably accurate assertion that the network characterized below is a common denominator of almost all networks supporting the same types of devices.

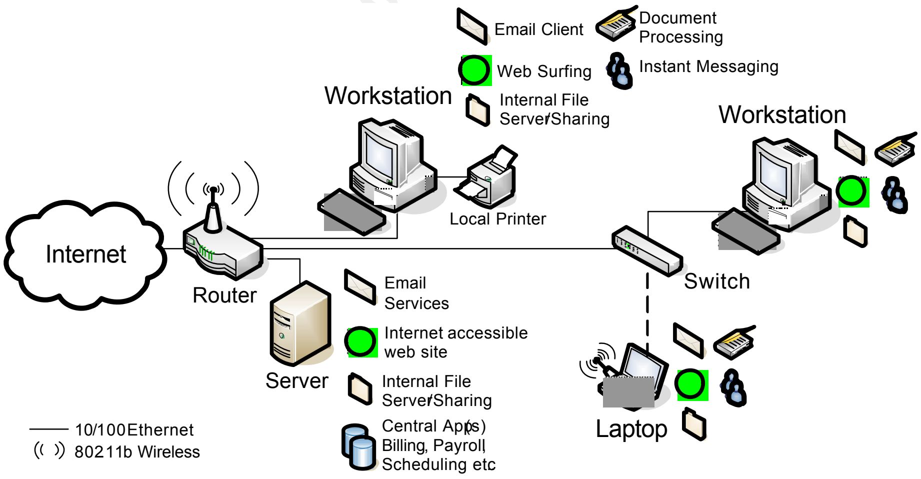


Figure 1 – Basic Network Structure

[4] Carrel, William. www.Carrel.org. MAC OS X Security Vulnerability, Jan 2004. URL:http://www.carrel.org/dhcp-vuln.html

Core components include email, internet accessible web site, and central file serving in a peer (typically home user) or domain (typically mid-sized office to enterprise) based network. And commonly, small to medium sized business (SMB) based networks round out server side services with a centralized application providing accounts receivable, finance and payroll, or patient or business scheduling.

Infrastructure hardware typically consists of a few workstations, cabling, a switch and a Small Office, Home Office ($100-$150) router/firewall combo to provide always-on internet connectivity for multiple internal hosts. With the pervasiveness of wireless devices and wireless connectivity being a highly desired function, many border routers like in the diagram above also double as Wireless Access Points (WAP). The dashed line indicates the mobility of the laptop as it comes in and out of the network.

The client side activities typically consist of document processing, internet surfing, instant messaging, central application access (AR, Billing, Payroll, Scheduling, etc…) and file and print sharing.

So pervasive is the concept of a network, that it has emerged in the commercial market in the form of turn-key network kits sold on eBay^{TM}, Amazon^{TM}, and a host of technology and vendor sites. Noticeably (but not surprisingly) absent from the technical setup and support for these kits is any reference to security cautions, notices or instructions which warn the consumer of the potential threat, exposure and loss of personal or business information to miscreants that roam the global information grid.

The Threat

Without the proper knowledge and rudimentary skills to secure these default network setups and refine security configurations as technology and needs change, the net effect is the creation of a breeding ground for digital malefactors.

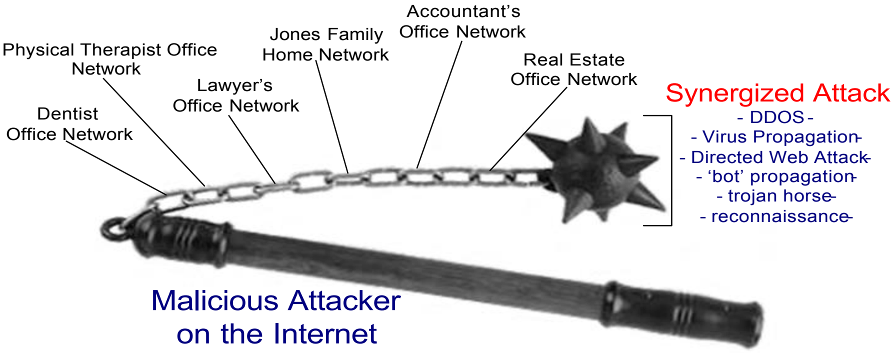


Figure 2 – The Malicious Mace[5]

[5] Medieval Weaponry. Morning Star (Rubber Ball) Ref: DX620 Graphic. URL: http://www.medieval-weaponry.co.uk/acatalog/index.html?http%3A// www.medieval-weaponry.co.uk/acatalog/catalogbody.html&CatalogBody. Quick Search: Mace.

Exploited and undetected, an attacker inventories the compromised network for later use; effectively building a chain of offensive capabilities. As visualized in Figure 2, with each additional link in the chain, an attacker lengthens the strike radius and increases the potential lethalness of an attack. Then, at the attacker’s discretion, he or she can combine the resources of numerous, previously compromised systems, to mount and execute a more lethal, concentrated and difficult attack to trace. So, how to keep the thousands of burgeoning networks safe from becoming the target of, or link in the chain, of an attacker’s menacing mace? Further, how can this protection be accomplished in an affordable, practical manner?

BASE Defined

Certainly there are a litany of formal principles and best practices involving the implementation of a security model; policies and procedures, qualitative/quantitative risk analysis, single loss expectancy (SLE), exposure factor (EF), annualized rate of occurrence (ARO), risk avoidance, risk transference, counter measures, contingency operations, incident handling and response teams, etc, etc. . .[6] Yet this level of effort is only realistic in an organization with the resources (and desire) commensurate to the task – the preponderance of which are large organizations hosting enterprise networks spanning multiple campuses supporting hundreds to thousands of users.

What is needed is a basic strategy grounded in the fundamentals of information assurance concepts yet lends itself to utilization in an ad-hoc style directly suited to securing a basic network. To meet this requirement, this paper proposes an assessment protocol called BASE which stands for Baseline, Audit and Assess, Secure, and Evaluate and Educate.

Baseline. The most detail oriented, but important step is baselining. Baseline the environment in terms of access patterns, performance, hardware configurations, services, installed applications, application and human behaviors etc. . It is difficult, if not impossible to detect and isolate anomalies and changes in a system or network if normal, daily operational behavior is not known and documented. In this step, the baseline as a measuring stick for detecting intrusion is not the only derivative. The baseline provides patterns and insight into the operational and maintenance needs of the system. And a critical end-state to this step is documentation. Documenting the baseline information collected becomes essential to troubleshooting and serves as an invaluable foundation in establishing a disaster recovery path which is an essential precursor to ensuring system availability.

Audit & Assess. Using both manual tasks and automated tools, plan and execute audits of the operational environment against the previously established baseline and against evolving information security practices. The supplementary task to this step is assessing the results of the audit both in terms of technical configuration and business needs. Technically, the assessment reveals what additional hardening measures are required, but they should not be implemented to the exclusion of required system functionality. Where security encroaches on functional business need, a risk analysis must be performed. Using risk analysis, a determination is made to apply additional security at the risk of lost functionality or productivity or revenue. Or, to instead accept the risk of continued operations in a vulnerable state. Whether risk analysis is invoked or not, the end state of this step is an accounting of the potential vulnerabilities identified and deciding which will be remediated in the next step.

[6] Chappel, Mike, The GSEC Prep Guide, Mastering SANS GIAC Security Essentials, Indianapolis, Wiley Publishing, Inc., 2003: 59-92.

Secure the Environment. The assessment feeds directly into this step. Here, the plan for remediation is executed to remediate those areas previously assessed to be a potential area of vulnerability. This includes technical changes to the environment as well as policies or procedures which govern the usage and management of IT resources.

Evaluate & Education. Evaluate the results of the 'securing' that was executed. Primarily to ensure that functional business need was not adversely impacted by errant or too restrictive settings, but also as a follow-up to determine if the configurations/changes made *actually* remediated the assessed threat(s). Where increased security impacts functional business requirements, risk acceptance must be evaluated and a decision weighed, justified and documented in favor of security at the risk of lost or reduced functionality, or in favor of functionality at the risk of lost security. Further, to avoid duplication of effort, adapt and integrate the resulting configurations where possible as a recommended standard across like environments in the organization. Successful or unsuccessful, capture the lessons learned to serve as a tool to further educate, as appropriate, technical, administrative, and user staff. The education element is essential as it will continue to increase awareness and competency at many levels, thus permanently raising the bar for the collective security posture of the organization.

Tools

When combined with automated assessment and configuration tools, BASE becomes a powerful, fundamental vulnerability assessment protocol. Table T-1 enumerates many of the freeware or 'trialware' products, that when used effectively together and in connection with BASE, provide a potent and functional toolkit for executing vulnerability assessments.

Table T-1 : Scanning, Detection, and Remediation Tools

Tool Name and Web Site	Platform Supported	Functional Comment	TW – useful Trial Ware FF&F – Full Featured & Free CM$ – Full Commercial Version
Nessus www.nessus.org	Linux	Port scanner and penetration testing TCP, UDP, SNMP, URL, Comment: very potent network assessment tool with myriad of options and penetration vectors, and fairly robust and friendly reports engine supporting a couple different formats	FF&F
NeWT www.tenablesecurity.com	Windows	In its humble beginning, NeWT was a version of Nessus ported to Windows. More mature now, the Tenable product line offers more than just scanning.	TW CM$
GFI LANGuard www.gfi.com/lansim	Windows	Thorough port scanning and vulnerability enumerations. Bugtraq reference, well done reporting function	TW CM$
GFI System Integrity Monitor www.gfi.com	Windows	Host based monitoring. Monitors specified file/directory structures with alerting functions	TW CM$
Brutas http://www.hoobie.net/brutus/	Windows	Remote password recovery across various network services, FTP, HTTP, RPC, dictionary and brute	FF&F
LOphtCrack 5 (LC5) www.atstake.com/products/lc	Windows	Password recovery, local, remote, network. Dictionary and brute force password cracking	TW-dictionary attack only CM$
Cain and Abel www.oxid.it	Windows	MAC address network enumeration, poison packets, man-in-the-middle, tracert, LSA Secret, brute force and dictionary password recovery	FF&F
Regmon ProcessExplorer TCPView ListDLLs TDIMon Filemon www.sysinternals.com	Windows	Registry monitoring, active/loaded DLL tool View processes and their associated port status. Comment: This site has a set of very useful utilities that fit various needs. Some tools have enhanced retail versions.	FF&F CM$
SuperScan www.foundstone.com	Windows	Port scanner, URL scanner.	FF&F

Table T-1 (continued)

Tool Name and Web Site	Platform Supported	Functional Comment	TW – useful Trial Ware FF&F – Full Featured & Free CM$ – Full Commercial Version
Snort www.snort.org	Linux Windows	IDS, Packet Sniffer, Packet Logging	FF&F
EagleX www.engagesecurity.com/downloads	Windows	Preconfigured IDS providing a friendly front end for configuration and reporting using snort as the IDS engine.	FF&F
IDScenter www.engagesecurity.com/downloads	Windows	Configuration and management front end that uses snort as the IDS engine	FF&F
Microsoft Baseline Security Advistor (MBSA) www.mircosoft.com/downloads	Windows	Microsoft only patch / service pack reporting tool, local security policy auditing, local user account security auditing, IE configuration auditing, service auditing. Very effective foundational scans.	FF&F
Shavlick HFNetCheck www.mircosoft.com/downloads	Windows	Command-line based patch and service pack reporting/validation tool.	FF&F
EventComb www.microsoft.com/downloads	Windows	Utility to connect to and search multiple Window machine event logs using all Win32 native event log filtering parameters.	FF&F
PortReporter www.microsoft.com/downloads	Windows	Establish baseline port status report and auditing integrated to Windows event logs. .	FF&F
Enterprise Log Manager (ELM) www.tntsoftware.com	Windows	Event log searching, real-time event notification on logs and performance monitors	TW CM$
Argent Guardian www.argent.com	Windows	Event log searching, GUI real-time event notification on logs and any performance counters, LDAP queries alerting, SMTP traffic and content alerting, command-line scripting, robust wizard driven pie, statistical, chart graph reporting	TW CM$
NetStumbler www.netstumbler.com	Windows	Wireless 802.11b WAP discovery and profiling	FF&F
SC-KeyLog http://www.soft-central.net/keylog.php	Windows	Wizard driven key logger Trojan horse builder. Very effective if no virus protection present.	FF&F
UserLogger http://chemware.co.nz/usrlog.htm	Windows	Software Key Logger	TW CM$

Table T-1 (continued)

HP JetAdmin www.hp.com	Windows	Central Console for managing JetAdmin devices and scanning for them on the network. A high percentage of network (IP addressable) printers use HP JetAdmin cards. This an excellent tool for connecting to and viewing the configurations of printers.	FF&F
Spybot Search and Destroy www.safer-networking.org/en/index.html	Windows	Spyware and adware prevention, detection and removal utility.	FF&F NOTE: donation based
Nmap www.insecure.org/nmap	Linux Windows	Port scanner, network enumeration and effective device finger printing. Can successfully guess device type and manufacturer as well or better than most commercially available scanners.	FF&F
Amap www.thc.org/releases.php	Linux	Unix port scanner similar in nature to nmap	FF&F
Ethereal www.ethereal.com	Linux Windows	Packet Sniffer Comment: Very quick and thorough sniffer. Ability to construct search expressions for quickly sifting through results.	FF&F
Netmon www.microsoft.com	Windows	Packet Sniffer Basic network sniffer with much the same interface and abilities as ethereal.	FF&F
Microsoft Security Templates www.microsoft.com	Windows	MMC Snap-in from Microsoft that allows you to build windows platform security templates for individual host or enterprise deployment.	FF&F
Tiny Personal Firewall www.tinysoftware.com	Windows	Host based firewall for guard hosts against unauthorized inbound and outbound TCP/IP connections. Most current version has a wealth of features; logging, IDS, real-time process viewer, and reporting mechanisms.	TW CM$
Windows Personal Firewall www.microsoft.com/downloads	Windows	Available for Windows XP. A host based firewall for guarding against unauthorized inbound TCP/IP connections. Includes an effective pop-up blocker to guard against spyware sites.	FF&F

Implementing an Assessment Methodology

In the context of an enterprise environment with sufficiently able resources, it's necessary to stress the applicability of BASE as a subset of, not a replacement for a formal information assurance program and infrastructure. Yet as a component of vulnerability assessment procedures in the enterprise or for rudimentary, small organizational or home audits, BASE is well-suited. See Sample Security Assessment using BASE starting on page ?? which covers a brief application of BASE to a typical home or small office network. The next section, then, is dedicated to explaining tasks associated with each component involved in BASE.

Baseline

To detect anomalies in a system, the normal operational behavior of a system must be established. This is the core purpose behind baselining the environment, regardless the size or complexity. Once a baseline is established and documented, abnormal behaviors or suspicious looking programs or services can be identified and isolated in the conduct of an audit. Additionally, many general operational conditions are discovered during baseline activities. While there are many services, applications, performance, bandwidth, connectivity measurements and baselines that can be executed, two of the most important baseline activities deal with evaluating the network as a whole and the host systems connected to it.

Network Baseline. There are several areas to examine when baselining the network. Some are physical in nature involving simple visual inspections and applying some common sense. Others include some very rudimentary bandwidth statistics which can later prove very useful in recognizing potential latency issues. This task should include tasks and activities which examine the following;

Physical Security.
Are network devices in locations that are well secured against physical tampering? Empty or occupied, are all ports active? Can someone simply plug into an open port and become an active node on the network? Are devices well ventilated and easily accessible? Are they positioned such that you can visually see status lights indicating activity or problems?

Tools:	Manual/Visual Inspections
In small office or home networks, this is typically a subjective, manual process. Usually two sets of eyes are better than one. In middle to enterprise size networks, when using 'managed' network devices, the management tools, in addition to visual queues, can natively provide a status of each of the ports' activity, speed, connection status and other statistics depending on the device.	

Cables and Cable Runs.
Is the cable type and quality adequate for the length of the run? Are the cable runs shielded from foot traffic or other electronic emanations which might cause interruption? Or are cables running through conduit in a wall or ceiling and does the conduit have an existing pull string to facilitate additional pulls if necessary? Are the cables hidden from obvious view or are they readily accessible (over head cable trays) by any passer by? Are the cable ends labeled at both ends identifying the connected node? In an enterprise, are network distribution panels labeled along with their corresponding desk-side network jacks?

Tools:	Manual/Visual Inspections
This is largely a manual process. Cables can be inspected visually where possible. Usually two sets of eyes are better than one. Cable integrity tests can be accomplished with line testing tools, but typically this is unnecessary and more value is derived from the visual considerations and inspections	

Power.
Is there adequate power to the devices. Are UPS or power strips used and are they dedicated, shared, or daisy chained? Is the shared power strip adequately rated for the load? Is the device at risk of damage event of power spike or malfunction?

Tools:	Manual/Visual Inspections
This is a subjective, manual process. In larger enterprises, power and circuitry should be handled by trained facility technicians. In SOHO environments, there are small GFI plugs available as most hardware stores which can do basic current and grounding checks. A basic multi-meter could also be employed to validate wall outlets and power strips.	

Next in dealing with the network, what are the base configurations of the core network devices and what devices live on the network to begin with? In the medium to large enterprise, this would consist of one or several very large capacity core switches whose configurations should be managed centrally via a management suite. In simpler home and small office networks, unmanaged switches and hubs combined with an Internet facing router are more common (Refer to Figure 1, page 5). Regardless the size, the core configurations should be documented.

Host Enumeration.
How many and what hosts/devices are connected on the network? How many and what are they; workstations? servers? printers?

Tools:	Nmap, Amap, LANGuard, SuperScan, Nessus – scan tools which can be given an IP range to scan and they will attempt to identify any devices on the network which responds. Nmap is particularly fast (Linux version) and accurate in host identification.
	Cain & Abel – a particularly adept tool which, given an IP range (or local subnet) provides results of enumerated MAC addresses in an organized GUI environment and attempts to ID the device type or manufacturer.
	HP Web Jet Admin – while above scanners will ID printers as well, this tool is specifically adept for printer discovery and Jet Admin can use the resulting scans to connect to and further explore individual printer configurations.

	NetStumbler – check the footprint and basic security configurations (WEP, SSID) of your wireless advertisement. Or, check to see if there are any rogue wireless access points on your network on your facilities.
This step cannot be emphasized enough. A good baseline will include a discovery, positive identification and documentation of all devices on the network. Rogue computers on your network are a threat to network resources and also represent an existing compromise of your physical security. Printers are commonly 'set and forget' devices, but the Jet Admin tool can quickly bring these neglected or forgotten devices into view.	

Configurations – Switches/Hubs.

Do you know which switch/hub ports connect which other network devices, terminate network hosts or are unoccupied? Do you have and maintain a port matrix which maps ports to hosts and what speeds should be configured?

Tools:	Native device management; small and home office are typically unmanaged switches/hubs which do not have export capabilities and are therefore unmanaged.
	Manual diagram and/or completed spreadsheet depicting hosts on the network and which ports they are attached to.
	There are sophisticated tools/applications that can discover and map entire networks, but this is beyond the scope of this paper.
In large enterprises involving managed devices and hundreds of hosts, a management suite is necessary. At smaller levels, depending on size and complexity, the majority of networks can be diagrammed by hand without a need to invoke network discovery tools which have a significant cost associated to them. With unmanaged devices, documenting the configuration is a manual process.	

Configurations – Routers/Firewalls.

What are the configurations of the router? What is the internal network IP subnet and what is its external WAN (Internet) address? Is it internet facing, or does it route traffic between internal networks (enterprise typically)? What protocols is it configured to route/filter/block? What Access Control Lists (ACLs) exist which control the flow of traffic? What network ports does the device have open for management purposes? telnet? http? ssh? Is it a SOHO router which combines firewall, DHCP and Wireless Access Point services? If yes, are the WAP services adequately secured etc?

Tools:	Nmap, LANGuard, SuperScan, Nessus – scan tools which will reveal what service protocols and ports are offered by the device.
	NetStumbler – check the footprint and basic security configurations (WEP, SSID) of your wireless advertisement.
	Native management tools to the device; web or command line interface obtain configuration information.
Large enterprises typically will have a 'border router' which is the perimeter device between the organization's network and the Internet (in reality the Internet Service Provider (ISP)). The same is true of many small or home networks. Regardless the size or configuration, these tools can be used to assess the service protocols advertised by these devices both externally and internally.	

Traffic Patterns.

What is the normal volume and pattern of network traffic? When are the high and low usage peaks and valleys? If sophisticated enough, what is the normal volume of traffic inbound and outbound through the border router/device or other core or distribution devices? What source and destinations is traffic routinely flowing to? What are some expected response times between hosts or network devices? Can you tell when they are experiencing normal volumes or are exhibiting overload conditions etc?

Tools:	Microsoft Netmon, Ethereal – sniffers which when placed appropriately on the network can record and save sessions of all traffic on the network, real-time or for later analysis.
	DOS command line tools – various DOS command line tool like ping, traceroute, arp, netstat, nbtstat to determine very basic IP configurations and response times.
In baselining traffic patterns, it's helpful to identify high volume talkers like switches, border routers, backup and file/print servers. If you don't know these ahead of time, the traffic baseline should help to yield some of this information.	

Workstation Host System Baseline. Hosts are arguable the most important devices on the network as the primary productivity tool for end users. They also are the most vulnerable because in the course of its daily use, a workstation, via file shares, instant messaging, streaming connections, application use, printing, and internet surfing, establish, maintain, and tear down tens of thousands of connections in a single day. With so much exposure to and processing of potentially malicious traffic, having a good understanding of the normal behaviors of a typical workstation will prove very useful in detecting anomalous behaviors or active exploits.

System Information.

What is the hardware configuration and components of the system? What services are installed, how are they configured? What applications are installed? Etc . . .

Tools:	winmsd – native tool on windows platform that can generate a system information file containing rudimentary system information that can be stored locally or archived off in a couple formats to access later.
Certainly there are powerful inventory applications that can inventory host systems in an enterprise environment. In smaller environments, though this simple built in tool can be very effective.	

Physical Security.

In large organizations, spanning multiple facilities, campuses, cities etc . . . supporting thousands of workstations and staff, host physical security is of paramount importance. Are host secured against physical theft or tampering? Are users trained in awareness to challenge the identity of unknown persons operating a workstation? Are unoccupied offices secured after hours. Are monitors and printers positioned out of common areas to prevent casual shoulder surfing or viewing etc?

Tools:	Manual/Visual Inspections

This is very much a manual, hands on process requiring physical inspection of the host environment. Usually two sets of eyes are better than one. In small office or home networks, physical security is less of an issue. Yet in middle to enterprise size networks, host physical security becomes a crucial first line of defense against exploits initiated from internal locations.

Policy/Governance.

Certainly a home user would not publish acceptable use policies governing the use of a single workstation. Yet this is an area where companies, big or small, are required by federal regulations like HIPAA, Sarbarnes-Oxley and Gramm-Leach-Bliley Act to have organizational policies governing computer usage and the data generated by them. While the purpose of recent government regulations is to improve computer security, much of the structure imposed by these regulations have been industry best practices for years. Recommended policies, while certainly not all inclusive, include:

Tools:	Published Organizational Policies	
• Acceptable Use	• Email Usage	• Client Privacy
• Incident Response	• Internet Usage	• Password Policy
• Patch Management	• Remote Access	• Disaster Recovery
• Vendor Access	• Encryption Policy	• Antivirus Policy
• Employee Monitoring	• Wireless Policy	• Data Classification

Policy requirements will differ based on industry and business needs. While not all inclusive of every need, www.sans.org/resources/policies/ has a very thorough list of policy templates ready for use.

Cables and Connectivity.

Is each available network cable occupied by a workstation or are there available connections for any device to be hooked up to the network? In small to mid-sized enterprises, conference and meeting rooms are frequent offenders; network cables are just left dangling from the wall ports, an open conduit to the network for the rogue laptop. Are there small switches or hubs present which turn a single active port to many ports? Many system administrators are often offenders of the under the desk switch or hub.

Tools:	Manual/Visual Inspections
This is largely a manual process. Cables can be inspected visually where possible. Usually two sets of eyes are better than one. Cable integrity tests can be accomplished with line testing tools, but typically this is unnecessary and more value is derived from the visual considerations and inspections of conference rooms and work areas, especially the IT department.	

Power.

Is there adequate power to the devices? Are UPS or power strips used and are they dedicated, shared, or daisy chained? Is the shared power strip adequately rated for the load? Is the device at risk of damage event of power spike or malfunction?

Tools:	Manual/Visual Inspections
This is a subjective, manual process. In larger enterprises, power and circuitry should be handled by trained facility technicians . In SOHO environments, there are small GFI plugs available at most hardware stores which can do basic current and grounding checks. A basic multi-meter could also be employed to validate wall outlets and power strips.	

NTFS and File System Permissions.
Permissions on workstations are traditionally more permissive to accommodate general usage by staff in the organization. Are the permissions too permissive? Do they allow basic users to install applications or write capabilities to key system files or directories?

Tools:	File Explorer [Security Tab], Regmon, Regedit/Regedt32, AccessEnum – enumerates and or edit NTFS file and Registry permissions and/or shares.
	Computer Management MMC, ShareEnum – enumerates any active shares on the host system.
The configuration of NTFS permissions is crucial in establishing a base security posture. As workstations are highly utilized devices and in a variety of ways, a functional set of file and registry permissions based on least privilege can be difficult to arrive at. Use a combination of these tools along with enabling auditing to document and isolate permission usage failures in NTFS and the registry. This step is crucial to determining the level of permissions that must be granted for proper operation of the workstation.	

Service Packs, Patches, Update Files.
Is the OS current with all service packs and any applicable host fixes? Are there any vendor application suits or products like Office or Internet Explorer that require patching? Is the Antivirus engine and signature current etc?

Tools:	LANGuard, Nessus – scan tools which will reveal what service protocols and ports are offered by the device.
	Microsoft Baseline Security Advisor, HFnetCheck, Windows Update Site – patch/service pack validation tools specifically built for the windows platform that can check a host for compliance with the most recently released patches/service packs.
	Vendor Tools / Software Releases –vendors manage their software releases and updates in a variety of ways, best to check with the owning vendor.
When initially deploying a system, patching is almost always a necessary task to update the system to its most stable and/or secure release.	

Communications, System Processes and Ports.

What are the normal end point communications of the workstation? What port communications are outbound and what are inbound? Is the workstation knowingly or unknowingly hosting a service that is prohibited or should be on a managed server etc?

<table>
<tr><td rowspan="7"><b>Tools:</b></td><td>Nmap, LANGuard, SuperScan, Nessus – scan tools which will reveal what service protocols and ports are offered by the device.</td></tr>
<tr><td>MS Port Reporter – port reporting tool which upon installation conducts an initial inventory of port activity and then runs a periodic intervals to provide updated port activity reports..</td></tr>
<tr><td>Netmon, Ethereal – packet sniffers. Can be used to reveal a detailed IP packet level, the ingress and egress of traffic from a host computer.</td></tr>
<tr><td>TCPView, TDIMon useful utility which, via a friendly GUI, maps real-time the TCP connections of a host computer.</td></tr>
<tr><td>Tiny Personal Firewall – host firewall to monitor, restrict, report and alert on application behavior and TCP. Useful in the cursory investigation of inbound and outbound requests in real-time and to investigate what these request are attempting to do.</td></tr>
<tr><td>Task Manager – native windows platform utility that displays running programs, running processes, and real-time CPU and memory I/O.</td></tr>
<tr><td>Process Explorer, Filemon, AccessEnum, Regmon – various tools that display in real-time processes, DLLs, registry access, and NTFS permissions.</td></tr>
<tr><td colspan="2">At the workstations level, the bulk of valid connections are initiated as outbound connections. This makes sense because the intent of a workstation is for users to get work done which requires outbound connections. Typical connections are file servers, email servers, printers and internal web sites. In evaluating the communications and ports and processes active on a host, we’re looking for what is present and their ‘state’. Given this information, you can determine what processes are loaded, file accesses are occurring, and what communications the device is involved in or is advertising. This discovery process is important to establish what normal activity is expected so that anomalous behavior can be identified and isolated.</td></tr>
</table>

Baseline : Server Host Systems. Servers run the applications that users will connect to with their client in commonly referred to as the “client-server” model. In this role, servers too, establish, maintain, and tear down tens of thousands of connections a day, any one of which could be a malicious attempt to exploit an open port or published application. Just as we baseline the standard activity of a workstation, all the same tasks and tools would be involved on the server side with a slightly higher level of restrictions.

Physical Security.

While the common home user does not support servers, in small to midsized and enterprises, they are essential to the conduct of business; human resource, time and attendance, pay and financial applications to mention a few. As such, they can be high value targets and warrant a higher level of physical protection from your standard workstation.

Tools:	Manual/Visual Inspections
This is very much a manual, hands on process requiring physical inspection of the server environment. In small office or home networks, physical security is less of an issue. More applicable to medium to larger enterprises, the physical security of servers should be planned to the extent that there is a dedicated server room with adequate access and environmental controls. Structure of the walls, flooring, and ceiling should be evaluated as access avenues.	

NTFS and Windows Registry Permissions.

Newly built servers, if left in their default configuration, can be very insecure. Regardless the configuration, NTFS permission must be documented so that changes can be identified if they occur. Additionally, NTFS permissions must be frequently be modified to ensure functionality of a particular application.

Tools:	File Explorer [Security Tab], Regmon, Regedit/Regedt32, AccessEnum – enumerates and or edit NTFS file and Registry permissions and/or shares.
	Computer Management MMC, ShareEnum – enumerates any active shares on the host system.
The configuration of NTFS permissions is crucial in establishing a base security posture, especially on servers. The default builds in previous NT 4.0 and Windows 2000 platform environments were very insecure, typically with ‘Everyone’ permissions assigned on the root partition. NTFS permissions is the ideal component where baselining and auditing can converge to achieve improvement by using the results of an audit to capture insecure NTFS settings and then integrate recommended changes as part of the baseline build. Securing the registry takes the same patch, establish least privilege that works and then adapt as a standard configuration and note exceptions as necessary.	

Service Packs, Patches, Update Files.
Is the OS current with all service packs and any applicable host fixes? Are there any application suites or services (IIS, SQL server, Mail Servers) that require patching? Is the Antivirus engine and signature current etc?

Tools:	LANGuard, Nessus – scan tools which will reveal what service protocols and ports are offered by the device.
	Microsoft Baseline Security Advisor, HFnetCheck, Windows Update Site – patch/service pack validation tools specifically built for the windows platform that can check a host for compliance with the most recently released patches/service packs.
	Vendor Tools / Software Releases –vendors manage their software releases and updates in a variety of ways, best to check with the owning vendor.
When initially deploying a system, patching is almost always a necessary task to update the system to its most stable and/or secure release.	

Audit and Assess

Just like computer security, maintaining an operational system is not an end-state, but is a process. A process which includes the review of both technical configurations and governance related issues at schedule intervals. The established baseline is a good barometer, but a computer system is ever changing, and based on business or individual needs can morph from its original configuration to serve in a variety of roles. When services, patches, service packs, or applications are added or removed, the state of vulnerability of the system changes. Additionally, business needs, physical location, or leadership can shift in many directions, which warrants the review of policies and/or procedures governing IT security.

The size and method of the periodic audits, as a rule, is driven by the size and complexity of the network. Small networks of a couple dozen devices could reasonably be audited and assessed relatively quickly and by one to two staff members. Yet larger and more complex networks require a more segmented audit based on geography, department, or network segmentation - and in many instances, require a small team of dedicated staff to execute and manage.

Regardless the size, the scope of an audit and assessment should be well defined and narrow enough that the volume of data generated can be assessed and acted upon in a timely enough manner to avoid exploit or compromise. This in turn determines the frequency of audits. Frequency falls into two categories; periodic and event triggered.

Periodic.
Comes in many flavors; monthly, quarterly, semi-annual, etc. Regardless the defined interval, periodic audits are pre-scheduled events designed to be a comprehensive security accounting of the systems defined within the scope of the audit. These audits are planned and scheduled as part of an integral component of the security architecture. For example, an annual security review of a HR pay and accounting application. Or a monthly audit of mission critical applications, servers or key infrastructure devices.

Event Triggered.
Computer security is very often reactive and to be successful, mechanisms must be defined which trigger and set into motion reactive measures which counter compromises or exploits which could not otherwise be planned for in advance. Industry or vendor specific alerts or 'in the wild' or 'zero-day' exploit code propagating the internet all serve as triggers to auditing and assessing a network's susceptibility to compromise.[7]

So, whether periodic or triggered, what are the components of this step? Figure 4 shows a visual representation of BASE to compliment the steps as outlined here:

1) **Audit:** Review the baseline/documented/expected configuration against the operational state.
2) **Assessment:** Using the results of the audit, determine if a variance exists. If no, document audit as complete. If yes, then
   a) **Assign Risk.** Further assess the details of the variance and determine risk based on the computer security principles of Confidentiality, Integrity, and Availability (CIA Triad) of the system or its data. Conducting a risk analysis via quantitative and qualitative methods and other Risk Assessment (RA) tools can be a discipline in its own right. The end result of assigning risk is to use that information to guide decisions and actions that follow. [8]
   b) **Develop Mitigation Plan.** It is the level of risk assigned to each or a group of variances that will drive what remediation tasks will be applied to reduce (measures which decrease the severity of the risk), transfer (measures which transfer the risk somewhere else) or accept the identified risk (do nothing because any resources applied to remediation efforts exceeds the value of the asset being protected).[8]

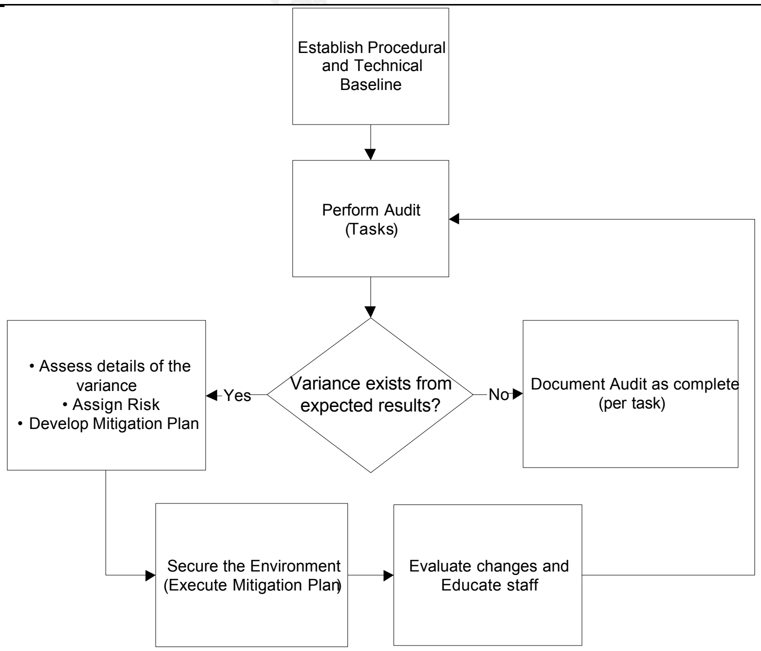

Establish Procedural and Technical Baseline
Perform Audit (Tasks)
• Assess details of the variance
• Assign Risk
• Develop Mitigation Plan
Yes
Variance exists from expected results?
No
Document Audit as complete (per task)
Secure the Environment (Execute Mitigation Plan)
Evaluate changes and Educate staff

Figure 4 – BASE Flow Diagram

[7] Tittel, Ed. "Security audit action list for CIOs." TechRepublic. 16 July 2003. URL: http://techrepublic.com.com/5100-6296-5054775.html (7 Sept 2004).
[8] Robinett, Jason. CISSP Cram Sheet Compilation. www.securitydocs.com. 10 April 2002. URL:

http://www.securitydocs.com/go/75 (7 Sept 2004).

Network Audit

The same steps involved in the baseline are also performed during the audit. The difference is how you look at the results. In the results of the audit, we are looking for conditions which are different from the baseline or are not expected among the authorized or known operational changes that have been implemented since the baseline. See the Sample Security Assessment using BASE on page

Audit: Physical Security, Cable Runs, Power.
Assessment: All of these elements require constant vigilance and should be validated to be within acceptable norms as outlined in the baseline. These areas are most effectively served through onsite physical inspections. The overriding concept here is to dirty your hands and "turn over some rocks.

Audit: Host enumeration. The same tasks for baselining are echoed here. Use a combination of scanning tools to enumerate the hosts on the network.
Assessment: If unidentified and/or unexpected hosts appear in the results, then every effort must be made to identify the hosts as friend or foe. In the case of the enterprise, there may be a policy which governs the addition of hosts to the network. Is this policy being violated? Or if your infrastructure devices were thought to be configured against this then these findings would lead to assessing their configurations as well.

Audit: Infrastructure Devices, Routers, Switches, Firewalls.
Assessment: Here again, the same activities (and tools) conducted in the baseline should be repeated; validate ports, routing/filtering rules, management protocols, ACLs etc.

Audit: Traffic and Traffic Patterns.
Assessment: Use IDS and packet sniffing tools to take periodic samplings of the traffic traversing the network. Are there source and destination addresses that look anomalous? Are you seeing a high volume of traffic on well know application ports that are prohibit or are particularly susceptible to malicious attacks? Although typically manifested by user complaints of "the network is slow", check current state of latency against the baseline – you may uncover network abuse or maybe discover the beginnings of a hardware issue before it causes downtime.

Audit: Logs.
Assessment: A feature component of most managed devices is an auditing and logging capability, some more robust that others. Regardless, auditing should be enabled on the devices and these logs should always be consulted when conducting an audit. Not only are they valuable discovering potential security issues, they can also give off operational or hardware alerts or failures which can help to avoid unscheduled service disruptions or downtimes.

Audit: Policy Governance.
Assessment: There are a handful of policies which are designed to govern network usage, like firewall, VPN, wireless access etc... While home and small offices understandably skip these, it is important to be aware of their requirement, regardless of organizational or network size, in certain regulatory conditions.

Host Server and Workstation System Audits

Perhaps repetitive, but the same steps involved in the host baseline are also performed during the audit. Again with the interpretation of the results being the key differentiator. Host systems are particularly dynamic and changing, making it very difficult to cope with subtle differences which in reality may or may not be malicious.

Audit: System Information.
Assessment: While simple, can be very effective. In your typical enterprise most users default to the IT department for H/W changes and workstation configurations. Included in the more useful information here is an inventory of the installed services and their startup configuration. One of the important configurations to check on a host is the existence of unfamiliar or Trojan services and this is an effective way to perform this check.

Audit: Cable Runs, Cables, Power, Physical Security.
Assessment: Akin to the network assessment, auditing these components requires a physical visit to the devices themselves. More rock turning. Are they behind a least one level of lock and key? If susceptible to physical theft, are they locked down. Is there adequate ventilation for the systems (on the carpet floor, or back in some enclosed desk corner)? In the case of servers, review the access control system to ensure past employees have had access revoked. With respect to a server room, check the access patterns if possible to discover any odd hours or frequent visits which might be later correlated to event data to piece together the details of an incident. Are the monitors inner facing such that passer-bys or folks outside a window cannot view the content of the screen from a distance?

Audit: Policy Governance.
Assessment: Relevant also to the network assessment, the policies and procedures which govern the usage of automated system are particularly applicable to the activities engaged in at the workstation level. The zealous small office user may draft policies governing workstation usage, but this is enterprise turf conditioned by productivity and business needs and again, regulatory compliance. Check for the existence of policies and then secondly their relevance in case they require updating. Also consider operational, cultural, and industry alerts and changes in general to anticipate emerging governance recommendations.

Audit: System Configuration. File System and Windows Registry, Communications, Application and OS Service Packs and hotfix level.
Assessment: This is by far the most time consuming task of the audit because very subtle changes to a host system can be near impossible to detect unless you are attempting to isolate something very specific. At the OS or application level, scan these hosts for permissive file system and windows registry settings, unauthorized or unused services, or suspicious port communications. Certainly one could not hope to audit every host and compare the scanned results against the baseline. There is neither a combination of enough time nor a robust enough set of tools with which to accomplish this. Nonetheless, it is important to be familiar with all these areas on a host in the event that a collection of events points to a particular host. More often than not, an event trail is the mechanism which would trigger the detailed evaluation of a host system.

Secure the Environment.

In the assessment phase, where necessary, a remediation plan was developed to remediate risk. 'Securing the environment', simply, is executing on the remediation plan; altering ACLs, configuring auditing, clearing and archiving logs, documenting trends, updating organizational policies, cleaning up user account directories, tightening or loosening file or application permissions, closing ports, disabling services, altering physical facilities, conducting awareness training, updating H/W code, reengineering cable runs, documenting changes, etc, etc. . .

It is paramount to understand that Securing the Environment and the next step of Evaluate and Educate are not mutually exclusive. In fact, they are very much an integrated, blended event.

Evaluate and Educate

At the same time that the environment is further secured based on the remediation plan, there must be a ongoing evaluation effort to balance increased security with functionality and productivity.

This requires emphasis in evaluating changes to ensure there is not adverse impact to production systems (hardware/software) or business flow and efficiency (policies and procedures). To achieve this it's necessary, nearly real-time, to conduct specific tests to evaluate configurations changes to avoid rendering a system or service useless through too many restrictions – the result of which amounts to a condition of self-inflicted denial of service.

As the cycle of securing and evaluating continues, there will inevitable come the situation which requires a balanced decision. The situation is where the desired level of security to reduce risk cannot be achieved without loss of functionality. There are many cost analysis matrices and esoteric decision algorithms to help in this decision which are outside the scope of this paper. Home and small office users typically are not faced with this dilemma. But in the enterprise environment, such a decision can impact the financial bottom line in thousands or hundreds of thousands of dollars. Regardless the decision, it must be weighed, justified and documented.

Finally, the principles of BASE are rounded out as any good methodology should; internalizing the lessons learned from the entire process to further educate the staff. After completing an iteration of BASE, conduct knowledge-share sessions which discuss the entire process and highlight both the good and the bad. Then, strive to integrate what worked back into the process. Do this and you will continue to build depth and breadth in your staff, and grow towards being a robust and adaptive IT organization.

Sample Security Assessment using BASE

To illustrate the application of BASE as a basic security methodology, the following section covers the application of this proposed methodology to a small office network as depicted in Figure 5. This discussion begins with the Audit and Assess step because auditing and baselining would be the same except the results would be documented in a Baseline and analyzed in an Audit.

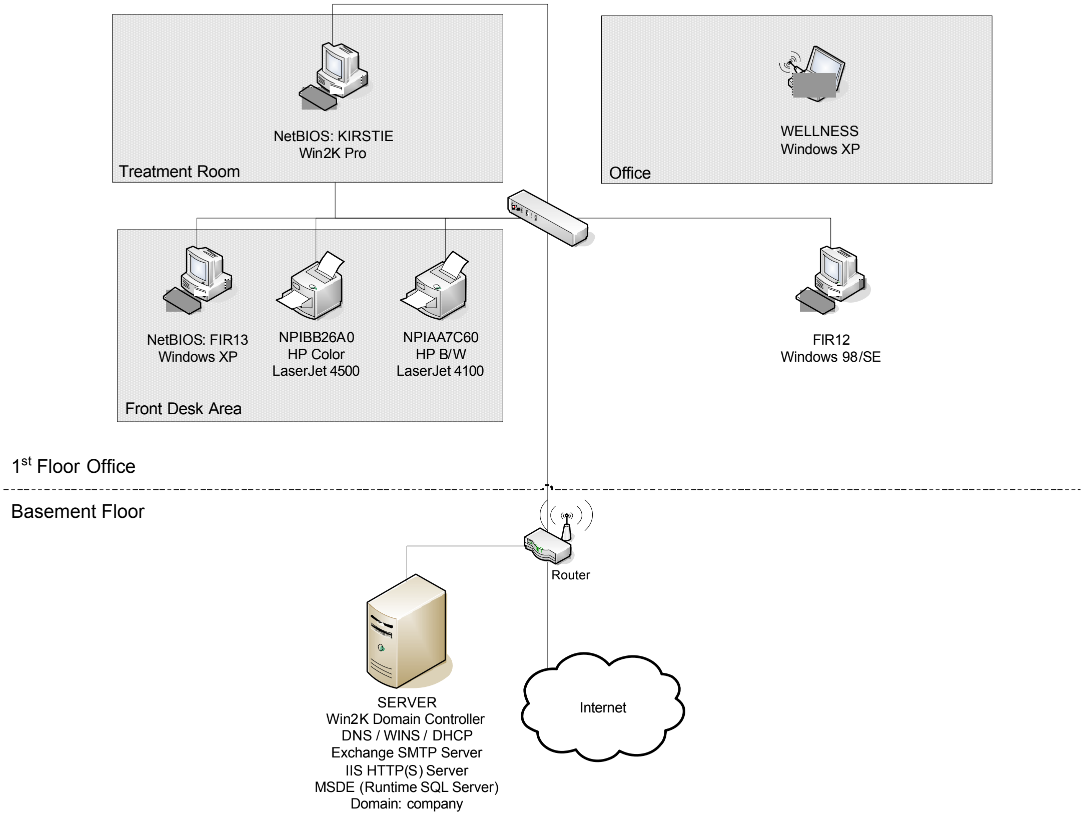


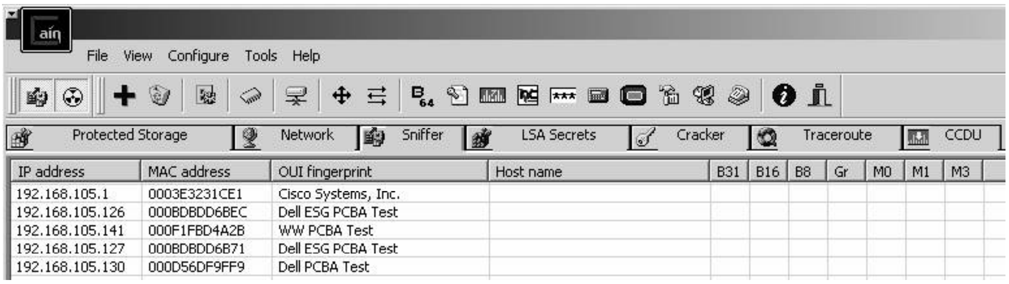
Figure 5 – Small Office Network

BASE and Network Host Enumeration

Audit: Network Host enumeration. Using Cain and Abel, connect to the target network and define the IP address range you want to enumerate. Figure 6a shows the baseline host enumeration of the network. Note that only 4 hosts and the router were enumerated because one of the hosts was not one the network at the time (perhaps the laptop?) and the printers were turned off. Note to self: Ensure that during a baseline that all hosts are on the network to maximize accuracy. A very similar baseline could be achieved using SuperScan or nmap, or Nessus etc…, but Cain and Abel provides a clear, concise (and exportable) list of the hosts discovered on the network.

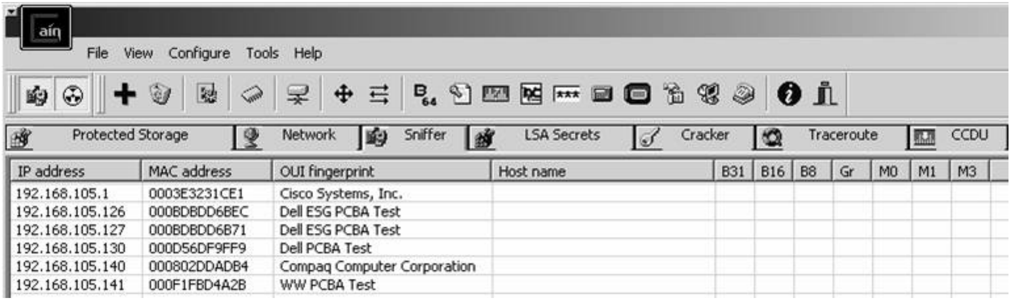
Assessment: Figure 6b shows a subsequent enumeration of registered IP hosts that reveals an additional host (IP 192.168.105.140) on the network. Is it authorized? Have you added any hosts to your network? If yes, then document and use these results in future audits as a new point of reference. In this case, we know that some hosts were not available. But for a second, assume that there was a unknown device on the network.

Assign Risk. Is this authorized? What is the risk of this unknown host on your network? In the case of an unknown host present on the network, the risk assigned should be high and steps taken to reduce it. High because what is this device doing on the network; sniffing and logging packets, conducting man-in-the-middle attacks, conducting illegal activities, launching external attacks using your internet connection?



IP address	MAC address	OUI fingerprint	Host name	B31	B16	B8	Gr	M0	M1	M3
192.168.105.1	0003E3231CE1	Cisco Systems, Inc.								
192.168.105.126	000BDBDD6BEC	Dell ESG PCBA Test								
192.168.105.141	000F1FBD4A2B	WW PCBA Test								
192.168.105.127	000BDBDD6B71	Dell ESG PCBA Test								
192.168.105.130	000D56DF9FF9	Dell PCBA Test								

Figure 6a – Network Baseline of Host Enumeration



IP address	MAC address	OUI fingerprint	Host name	B31	B16	B8	Gr	M0	M1	M3
192.168.105.1	0003E3231CE1	Cisco Systems, Inc.								
192.168.105.126	000BDBDD6BEC	Dell ESG PCBA Test								
192.168.105.127	000BDBDD6B71	Dell ESG PCBA Test								
192.168.105.130	000D56DF9FF9	Dell PCBA Test								
192.168.105.140	000802DDADB4	Compaq Computer Corporation								
192.168.105.141	000F1FBD4A2B	WW PCBA Test								

Figure 6b – Subsequent audit scan revealing an additional registered host

Develop Mitigation Plan. In this small network, the first thing to do is determine where this host is located and discover its true identity and remove or reduce it as a threat. Or maybe it was an authorized addition to the network and simply represents a change.

Tool: Physical Inspection – plan to physically inspect network devices to ensure only authorized hosts are connected.

Tool: Nmap – can use nmap to further identify information about the host and confirm initial findings.

Tool: Netstumbler – can use a laptop and wireless NIC to physically walk at various distance to the WAP and determine the physical footprint of your WAP devices. If the unknown host is gaining access wirelessly, then it must be physically located within this footprint.

Tool: **Native Switch/Router Interface** – if access is achieved wirelessly, then the

BASE and Network Printer Enumeration

Audit: Network Printer enumeration. Most network today usually have some type of network printing services available. Use HP Web/JetAdmin to scan the local or destination subnet searching for network printers.

Assessment: Printers are notorious as 'set-and-forget' devices often listening on various network protocols and configured with no passwords and default Simple Network Management Protocol (SNMP) strings. Most network printers use JetAdmin cards. Along with accepting print jobs, previous default JetAdmin configurations also included an FTP servlet such that it will accept anonymous FTP connections.

Assign Risk. Printers are typically of little risk in terms of network disruptions such as denials of service or virus propagation. However, they can be of serious consequence if with the proper motivation and skills, someone could intercept those print jobs and use them for other purposes. And if those print jobs contain financial or personal health information, federal regulations are likely being breached and carry with them stiff fines.

Develop Mitigation Plan. In this small network, the first thing to do is determine where this host is located and discover its true identity and remove or reduce it as a threat. Or maybe it was an authorized addition to the network and simply represents a change.

Tool: HPJet/WebAdmin – plan to check the configurations of each printer to remove unneeded configurations.

Secure the Environment. Using Jet/WebAdmin, connect to the printers and turn off any protocols like AppleTalk or IPX if they are not being used. Configure an admin password to prevent others from altering the printer configuration at will. Change the default SNMP string to reduce the risk of someone reading the configurations remotely.

Evaluate. Can authorized hosts still print successfully to the printer(s)? Is the password effective in stopping 'no password' access? Use SuperScan or LANGuard to validate that turned off protocols are no longer listening.

Educate. You discovered some things about a default JetAdmin configuration and have properly added a level of security but still maintained function. Given this working configuration, you can adopt this as a standard when deploying new printers.

Audit: Host Physical Security. An unannounced move of servers occurred over a weekend. Users along with the system administrator were notified after the fact on Monday. The servers were up, connectivity good and the application working just fine. However, a physical visit to the new home of the servers revealed a significant risk as identified in Figure 6a-d below.

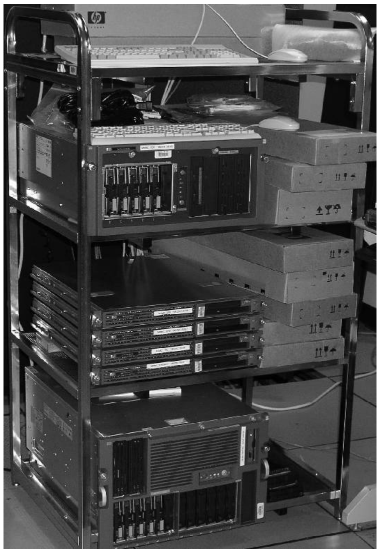


Figure 7a
Servers stacked on open, free standing shelf rack in server room.

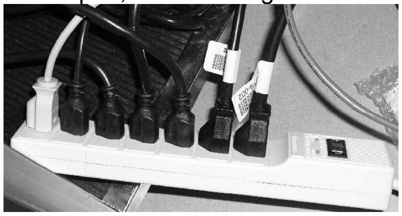


Figure 7b
All servers with singe PS plugged into basic power strip

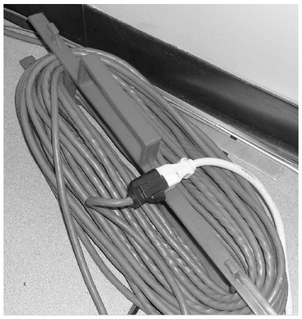


Figure 7c
Power strip plugged into 100ft extension cord

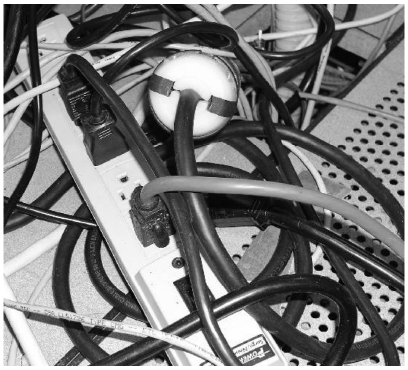


Figure 7d
Extension cord plugged into second power strip.

Assessment: Pretty obvious here. Servers are not secured to the rack and the rack is not

GLOSSARY

Information Assurance. The concept of all tasks, policies, procedures, education and configurations combined together to provide confidentiality, integrity and availability to information technology assets; including hardware, software, and the information they process, store or transmit.

Global Information Grid. The world-wide framework of interconnected devices and systems, connected via both wired and wireless infrastructure, both public and private, that engage in the continuous processing, storage, and transmittal of data and information.

Vulnerability Assessment. The process of evaluating the information assurance level of an organization administratively and technically to identify its weaknesses to protect and defend itself against malicious attack.

Network Scan. The practice of using an automated tool that enumerates and surveys the devices on a network to give an accounting of the configuration of the devices it locates based on .

Remediate. Steps, tasks, or configurations taken to further reduce or eliminate technical or administrative vulnerabilities in the environment.

Small Office, Home Office (SOHO) Network. Small networks run by a small office either from a commercial building or from home. These small network typically consist of a few workstations and/or servers networked together to provide mutually supporting access to business processing functions and for home internet access.

REFERENCES

Chapman, Brent D. & Elizabeth D. Zwicky, Building Internet Firewalls, Nov 1995, Online Extract, Chapter 3 Security Strategies, URL: http://www.busan.edu/~nic/networking/firewall/ch03_04.htm

The US Computer Emergency Readiness Team. Vulnerability Note VU#150227, Jan 2004. URL: http://www.kb.cert.org/vuls/id/150227

InstantSSL. Next Generation of Linux Servers Unveiled, New York, May 2004. URL: http://www.instantssl.com/ssl-certificate-news/ssl-260504.html

Carrel, William. www.Carrel.org. MAC OS X Security Vulnerability, Jan 2004. URL:http://www.carrel.org/dhcp-vuln.html

Medieval Weaponry. Morning Star (Rubber Ball) Ref: DX620 Graphic. URL: http://www.medieval-weaponry.co.uk/acatalog/index.html?http%3A//www.medieval-weaponry.co.uk/acatalog/catalogbody.html&CatalogBody. Quick Search: Mace.

Chappel, Mike, The GSEC Prep Guide, Mastering SANS GIAC Security Essentials, Indianapolis, Wiley Publishing, Inc., 2003.

Tittel, Ed. "Security audit action list for CIOs." TechRepublic. 16 July 2003. URL: http://techrepublic.com.com/5100-6296-5054775.html (7 Sept 2004).

Robinett, Jason. CISSP Cram Sheet Compilation. www.securitydocs.com. 10 April 2002. URL: http://www.securitydocs.com/go/75 (7 Sept 2004).