GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at http://www.giac.org/registration/gsna

Auditing Nokia Communicator 9500 in Enterprise Context

GIAC Systems and Network Auditor
(GSNA)

Practical Assignment
Version 4.0
Option 1
Topic 1

Leonard Ong
GCFA, GCIH, GSNA, GAWN, GHTQ
CISM, CISSP [ISSMP,ISSAP], CISA, PMP
April 08 2005

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Table of Contents

Abstract iii
Document Conventions iii
Introduction 1
Section 1: Identification 2
1.1. Auditable Entity 2
1.2. Device Specifications 3
1.3. Role of Communicator in GIAC Enterprise 5
Section 2: Risk Analysis 7
2.1. Risk Analysis Fundamentals 7
2.2. Top 3 Risks with highest impact 9
2.3. Details of Top 3 Risks 9
2.3.1. Device may be lost or stolen 10
2.3.2. Lack of security controls for device operation in Intranet 11
2.3.3. Device may be compromised remotely by TCP/IP sessions 12
Section 3: Testing 13
3.1. Device may be lost or stolen 13
3.2. Lack of security controls for device operation in Intranet 18
3.3. Device may be compromised remotely by TCP/IP sessions 20
Section 4: Audit 25
References 30
Appendix 1 – Test Network Diagram 31
Appendix 2 – Risk Ranking 33
Appendix 3 – Device Registration Form 34
Appendix 4 – Nmap Result 35
Appendix 5 – LanGuard NSS Report 40
Appendix 6 – eEye Retina Report 43
Appendix 7 – Nessus Result 54

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

List of Figures

Figure 1 Nokia Communicator 9500 3
Figure 2 Setting-up password for MMC storage 14
Figure 3 Power-on and Inactivity Lock 15
Figure 4 Enabling and configuring Auto Lock period 16
Figure 5. Changing default lock code 16
Figure 6 Confirmation of lock code change 16
Figure 7 Enabling lock code for SIM card change 17
Figure 8 Enabling remote lock 17
Figure 9 Setting-up remote lock message 17
Figure 10 Enabling and setting up PIN request 18
Figure 11 Details of wireless network discovered 19
Figure 12 Wireless security options 19
Figure 13 Supported EAP modules 19
Figure 14 Supported EAP Modules (Continued) 19
Figure 15 Settings on LANGuard NSSv6 21
Figure 16 Retina Ports selection 22
Figure 17 Retina Audit Groups 23
Figure 18 Retina Options 23
Figure 19 Nessus options 23
Figure 20 Symantec Client Security is disabled 24
Figure 21 Symantec Client Security is enabled 24
Figure 22 Nokia Communicator 9500 Firmware version 25
Figure 23 Symantec Client Security version 25
Figure 24 Default display after power-on if system lock is configured 27
Figure 25 Test / Audit Topology 31
Figure 26 LanGuard NSS reported false positives 41
Figure 27 No vulnerability noted on UDP 54
Figure 28 Low risk on ICMP 54

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Abstract

Nokia Communicator 9500 is an indispensable business tool. It provides mobile phone functionality, modern Personal Digital Assistant (PDA) features together with complete ubiquitous connectivity. In a way, it transforms the way people work. Users can virtually work anywhere without having to bring laptops and find a wireless hotspot or wired business centers. It increases productivity by having always-available information and connectivity on one's fingertip.

Devices with similar functionalities have just been introduced to the market in 2004, and most companies have not anticipated regulating such devices. Companies' confidential information can be stored in the device, and a compromise on the device will pose risks to companies.

The paper aims to describe an audit on Nokia Communicator 9500 implementation in Enterprise context. The benefits offered by the device should be utilized at its maximum while minimizing or eliminating potential risks with appropriate controls.

Document Conventions

When you read this paper, you will see that certain words are represented in different fonts and typefaces. The types of words that are represented this way include the following:

`command`	Operating system commands are represented in this font style. This style indicates a command that is entered at a command prompt or shell.
`filename`	Filenames, paths, and directory names are represented in this style.
`computer output`	The results of a command and other computer output are in this style
URL	Web URL's are shown in this style.
Quotation	A citation or quotation from a book or web site is in this style.

© SANS Institute 2005 Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Introduction

The first step in auditing an Information System (IS) system is to have an Audit Charter in place[1]. The charter outlines overall authority, scope, and responsibilities of an audit function. It is normally signed-off by senior executives from the management and is an important element of a successful audit. With the management support in written documents, an audit can be commissioned.

Law of economics applies to audit function, there are limited resources to complete an audit, yet the result has to be as complete and as accurate as possible. Therefore, audit professionals should have sufficient competencies, both hard and soft skills, to perform their work effectively. An audit professional that understand and can manage audit as a project would be preferred. Project methodologies can be used to minimize any deviations from available constraints. The constraints are time, quality and cost[2].

Both audit and project management best practices explicitly specify that a well-defined scope is very important. A scope that is too narrow might not be able to convey sufficient report of an audit. Likewise a scope that is too broad will implicate audit process and might not receive management attention and follow-ups due to excessive areas involved. When a scope has been defined, it has to be maintained. Changes to scope are possible, as long as they are supported by valid business reasons. The changes should be documented and signed-off to record that customers understand and accept any possible impacts to the audit constraints. Gold plating (adding additional items that are not within the scope without any proper change control) practice should be avoided.[3]

Audit planning comes next after early preparation. This phase involved both clients and auditors to discuss how the audit will be conducted. Good IS auditors will be able to involve the clients actively and hence gain support and needed assistance from them. Good planning supports good execution. Audit execution and reporting comes afterwards.

The paper will be written according to the recommended outline by SANS for GSNA certification. It aims to discuss the identification of auditable entity, conduct risk analysis, develop test plan, and execute the test accordingly. Therefore, it will not include a complete audit planning, process and report.

[1] ISACA. Certified Information Systems Auditor Review Manual 2005 Edition.
[2] Project Management Institute. Project Management Body of Knowledge (PMBOK) 3rd Edition.
[3] Project Management Institute. Project Management Body of Knowledge (PMBOK) 3rd Edition.

© SANS Institute 2005 Author retains full rights.

Section 1: Identification

1.1. Auditable Entity

The scope of the audit is Nokia Communicator 9500 usage within "GIAC Enterprise" premises and network. GIAC Enterprise is a large multi-national company that has presence in more than 70 countries with 16 regional hubs in all five continents. As like other large multi-national companies, HR policy allows employees to work from home or anywhere else when physical presence is not needed in the role of duty. Therefore, mobility and telecommuting have been one of the company culture that viewed by many employees as a benefit to achieve balance between life and work. The company also viewed that mobility is a way to increase productivity.

Nokia Communicator 9500 is state-of-the-art mobile phone that works in most of the countries where GSM services available, with modern PDA/PIM functions (calendar, task, notes, contacts, browser, and calculator). It is also equipped with office productivity software such as word processor, spreadsheet, and presentation writer. One of its strong feature is unified messaging, where all faxes, SMS, MMS[4], and Emails are in one place. The device also caters for personal usages such as games, camera, video recording and streaming.

It offers complete connectivity from modem via GSM[5], GPRS[6], EDGE[7], Bluetooth and Wireless LAN. The connectivity options virtually enable users to stay connected anywhere. In most of Asia and Europe countries, GSM and GPRS coverage is available in most areas, while wireless LAN hotspots are catching up in numbers. Users are practically spoilt with many choices to stay connected.

As with previous models, Communicator 9500 allows user to install additional applications to expand its functionalities. Previous models have been adopted by companies for their specific needs such as GPS navigation and logistics. It will be very soon that the device will be further adopted by enterprises due to connectivity options. One application could be in factory, where the phone is always connected to company's servers to input or retrieve information in real-time. More case study of Communicator application can be read at http://www.nokia.com/nfb/referencecases.html

[4] SMS is Short Message between mobile subscriber, while MMS add multimedia context to the message (video clip, voice clip, images, animations, emails, applications)
[5] GSM is cellular communication technology that is very popular in Europe, most of Asia, and some area in United States.
[6] GPRS is General Packet Radio System. It offers data service up to 53,6 kbps with GSM coverage
[7] EDGE is Enhanced Data-rate for GSM Evolution. EDGE offers up to 236.8 kbps data service

© SANS Institute 2005 Author retains full rights.

1.2. Device Specifications

Figure 1. Nokia Communicator 9500

Full Specifications

Size

- Weight: 230g
- Dimensions: 148 x 57 x 24 mm

Tri-Band Operation

- EGSM 900, GSM 1800/1900 networks in Europe, Africa, Asia-Pacific, North America, and South America where these networks are supported
- Automatic switching between bands

Display and User Interface

- Cover display: active matrix with 65,536 colors in 128 x 128 pixels
- Communicator (interior) display: transflective LCD with 65,536 colors in 640 x 200 pixels
- Five-way scroll key on the cover and nine-way scroll key on the (interior) Communicator side
- Full keyboard with 8 shortcut keys
- Symbian operating system version 7.0S
- Series 80 platform

Connectivity

- High-speed, flexible data connections with Wireless LAN, GPRS and EGPRS (EDGE)
- IPv4 and IPv6 (dual stack) support
- Bluetooth wireless technology
- Infrared
- USB 2.0 connectivity (Nokia Connectivity Cable DKU-2)
- Pop-Port™ interface

Messaging*

- **Multimedia messaging (MMS):** combine image, video, text, and voice clips and send as MMS to compatible phone or PC; use MMS to tell your story as a multi-slide presentation
- **Email:** access your email accounts to send and receive emails with attachments**; supports SMTP, POP3, and IMAP4 protocols
- **Text messaging:** supports concatenated SMS; picture message receiving and SMS distribution lists
- **Fax:** send and receive faxes through your GSM number

* Network-dependent

** Nokia 9500 Communicator supports email with attachments compatible with the file formats supported by the device.

© SANS Institute 2005 Author retains full rights.

Imaging and Media

- **Camera:** 640 x 480 pixel resolution; Viewfinder in cover, digital zoom and support for recording video clips
- **Video player:** RealVideo, MPEG4, and H.263 formats supported
- **Music Player:** AMR, WAV, MIDI, AAC, MP3 and AWB formats supported

Memory Functions

- 80 MB built-in memory for saving contacts, messages, files, images, sounds, applications and more
- MultiMediaCard (MMC) slot with hotswap functionality for additional memory

Business Applications

- Document, Sheet, Presentation editor and viewer*
- Other applications: Calculator, Voice Recorder and Music Player
- Applications in product CD-ROM: Nokia mobile VPN client, Zip Manager, Converter, Bounce and Adobe Reader
  * Nokia 9500 Communicator supports the most common features of Microsoft Word, PowerPoint and Excel (Microsoft Office 97, 2000, XP and 2003).

Internet Browsing

- Opera Internet browser
- Support for HTML, XHTML, and JavaScript™
- Macromedia Flash plug-in version 5.0 and earlier

Data Transfer

- Up to 11 Mbit/s in Wireless LANs
- Up to 236.8 kbps in EDGE networks
- Up to 53.6 kbps in GPRS networks

Call and Contact Management

- Log Viewer for communication incidents retrieval
- Advanced contacts database with support for multiple numbers and addresses (email, Web and street) per contact, also supports thumbnail pictures and groups
- Easy contact copy from SIM to device and vice versa
- Contacts and calendar data transfer over Bluetooth wireless technology or Infrared between compatible Nokia devices

Advanced Voice Features

- Handset and handsfree options for convenient call handling
- Integrated speakerphone
- Conference calling with mute functionality enables usage of several applications at the same time
- Bluetooth wireless technology audio headset connectivity enables handsfree communication

Power Management

Battery	Capacity	Talk time	Standby	
			WLAN off	WLAN idle
BP-5L	1300 mAh	Up to 4-10 hours	Up to 200-300 hours	Up to 180-240 hours

Nokia Communicator 9500 picture was taken from:
http://www.symbian.com/images/library/9500_lores_800.jpg

Nokia Communicator 9500 full specification was quoted from:
http://www.nokia.com/nokia/0,,54108,00.html

© SANS Institute 2005 Author retains full rights.

1.3. Role of Communicator in GIAC Enterprise

GIAC Enterprise provides laptops to most of their employees and the policy has proven to be a good one. Employees often travel to other offices or work in customer premises for a period of time, the laptops enabled them to get company's resources remotely. Business meetings within the company or customer sites can be carried out with laptops instead of printed presentation. Virtual meetings with collaboration tools have been encouraged by widespread adoption of laptops.

While laptops had transformed the way people work, Communicator 9500 brings the evolution into the next level. At times, laptops are not friendly to be used at certain situations such as when one is on public transport or on customer premises where outsiders are not allowed to use their network. Laptops often weigh between 2.5 to 3.5 kg, and carrying them for prolonged period of time is not practical.

GIAC Enterprise acknowledged the need for mobility in their workforce, and thus adopted Nokia Communicator 9500. First phase adoption targets employees who travel frequently or involved in meetings. Second phase adoption includes all executives. The third phase will include most of the employees that have been identified with the need to be mobile.

VPN connection is enabled on the device, providing secure remote access to the company. With VPN, employees can read their emails, browse intranet, check their calendar and contacts, communicate to other employees through internal instant messenger, create and view documents anywhere. On many occasions, this simplifies working with virtual teams, and increase responsiveness.

A couple examples of use cases of Communicator in GIAC Enterprise are:

1. Sales workforce
   The employees on this group normally meet with customers on daily basis. During meetings, any information that they need can be retrieved in real-time with VPN over wireless LAN or GPRS. The availability of real-time information reduces the number of meeting due to lack of information on discussion with customers. They can receive faxes and view it on the spot, or escalate issues through instant messaging with back-end support.
2. IT Specialists
   Specialists are mobile time to time and may be needed to be always reachable for any issues in the network or incidents. The ability to read emails and receive messages through instant messaging anytime will improve the response time to any issues or incidents. They can establish SSH session to appliances (firewalls, proxy servers, web servers) from anywhere using available VPN over wireless LAN or GPRS.

© SANS Institute 2005 Author retains full rights.

In summary, Communicator's roles in GIAC Enterprise are as follows:

No.	Functionality	Description
1.	VPN Client	Enables access to company's Intranet
2.	Personal Information Manager (PIM)	Provides access to calendar, contacts, to-do lists, notes. The PIM is synchronized with company's server.
3.	Messaging client	Provides almost real-time emails, faxes, SMS, MMS
4.	Instant Messenger	Enables instant communication with other colleagues regardless of the location.
5.	Office productivity	Create and view Microsoft Office documents, and view Adobe Acrobat documents.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Section 2: Risk Analysis

2.1. Risk Analysis Fundamentals

Computer-based information systems are subject to some degree of vulnerabilities, threats, risks and exposures[8]. A risk materializes when a threat exploits one or more vulnerabilities to cause harm. Risk is inherent by nature and can be either voluntary or involuntary. Voluntary risks could exist when management accept uncertainties to enter new market for example. Involuntary risk is undesirable and not assumed by management.

Definitions:

1. Vulnerability is
   Software, hardware or procedural weaknesses in computer systems that could be exploited to attackers' gain. An example of vulnerability is default settings of Communicator without any password or authentication.
2. Threat is
   Any potential danger to information systems. Malicious software and untrusted applications are threats to Communicator.
3. Risk is
   The likelihood or probability of a vulnerability being exploited. Disclosure of company confidential information in Communicator due to theft or loss is a risk.
4. Countermeasure is
   implemented to reduce or eliminate risks. It is also known as control. A countermeasure against loss of company confidential information when a Communicator is stolen is by having encrypted memory and Multimedia Card (MMC). The information will not be disclosed when the phone lost or stolen.
5. Exposure is
   The instance of being exposed to loses from threats or attacks. A business bid that is loss due to sensitive information being disclosed by a stolen communicator is an exposure to business.

Derived from: McGraw-Hill. S. Harris. All-in-One CISSP Certification 1st Ed. Pg. 66

Risk analysis (assessment) identifies the risks to a system security and determines the probability of occurrence, the potential impacts and controls that mitigate the impacts. The process should involve cross-functional representatives in a company. Risk analysis is a part of risk management process. The other element of risk management is risk mitigation. Generally, there are two risk analysis methodologies: quantitative (by numbers) and qualitative (by degree).

[8] S.Rao. SRV Publications. CISSP Examination Textbook Vol. 1, 2nd Edition, Pg. 157

© SANS Institute 2005 Author retains full rights.

When conducting risk analysis, the following steps and question would be useful:

1. Assets identification
   The first step is to find out what assets that we want to protect against any undesirable risks. This should include tangible and non-tangible assets of a company, and has organization-wide coverage. Therefore, a good risk analysis process requires involvement from representatives from all departments in an organization. Tangible assets could be hardware, building, and others, while intangible assets include intellectual property rights, copyrights, brand, reputation and others.
2. Risk identification
   The following step is to identify potential risks associated with assets to be protected. A few questions that is quite useful to answer on this step:
   - What could go wrong, in regards to potential for harm or loss? (threat event)
   - How bad could it be when it happens? (Impact, Single loss exposure value [SLE])
   - How often it might happen? (frequency)
   - What is the confidence level of the assumption used? (Uncertainty)

Formula that may describe relationship between risk, threat, vulnerability and cost is as follows:

Risk = Threat x Vulnerability x Cost

Quoted from:
International Charter. The Risk Equation. http://www.icharter.org/articles/risk_equation.html

A system may have no risk if there is no threat to exploit vulnerability. Risk could be insignificant if the cost or consequences are insignificant, although the threat and vulnerability may be high. In summary, a risk could exist if there are all three elements in a computer system: threat, vulnerability and cost.

The value of SLE is important, as we may not want to implement control or safeguard that exceeds any protections it may offers. Let say annualized loss exposure of server failure is $10,000; therefore it would not make sense to implement control that cost more than $10,000.

In order to conduct a successful audit, risk analysis has to be complete, relevant and accurate. For the purpose of this paper, we will identify three risks that have the most impact to GIAC Enterprise that may arise due to Nokia Communicator 9500 usage in the company. The company may have employees that purchase their own communicator and somehow use it for both personal and business use.

© SANS Institute 2005 Author retains full rights.

2.2. Top 3 Risks with highest impact

There are 14 risks in 12 security issues identified with Personal Digital Assistance (PDA) usage in organizations.[9] The security issues and risks that are relevant to Nokia communicator 9500 are as follow:

Security issues	Risks	Ranks*
Physical loss, theft, or damage	Device may be lost or stolen, including lost of sensitive information contained in the device.	**1**
	Device may be dropped or damaged	**12**
Mobile use	Information may be disclosed when device is used in public places. (Shoulder surfing)	**4**
Inadvertent connections	Users may send or receive information from/to other PDAs.	**5**
Unauthorized Connection	User may connect individually-own device to organization's computers without permission, bypassing security controls	**9**
Spread of malware	Device may be infected with malicious application from user's lack of security awareness.	**8**
Network connectivity	Device may be vulnerable to TCP/IP attacks and potentially compromised remotely	**3**
Poor access control	User may have access to disable the security controls.	**6**
Weak default security settings	Device security features are by default disabled	**7**
Lack of enterprise-wide security controls	Device may operate in enterprise premises without corresponding/ relevant security controls.	**2**
Inadequate event logging	Evidence may be hard/not available to obtain in case of incidents.	**11**
Personalization	Personal devices are not configured with enterprise standard for use in business.	**10**

*Ranks are derived from qualitative calculation (Appendix 2 – Risk Ranking). They are not derived from ISF report.

Top three risks with highest impact are consistent with their total risk score. These risks will be our scope in this paper. The risks summarized as follows:

Rank	Risks
1	Device may be lost of stolen, including lost of sensitive information contained in the device.
2	Device may operate in enterprise premises without corresponding/ relevant security controls.
3	Device may be vulnerable to TCP/IP attacks and potentially compromised remotely

2.3. Details of Top 3 Risks

In this section, we will look into details the impact, vulnerabilities, scenario of exposure and possible means of exploitations for each risk.

[9] Information Security Forum. Securing PDA. http://www.securityforum.org/assests/pdf/pda.pdf

© SANS Institute 2005 Author retains full rights.

2.3.1. Device may be lost or stolen

Description	For most of users, Nokia Communicator 9500 is their primary communication device. Therefore, they will bring the device to wherever they go, at anytime. It is simply hard to maintain two communication devices, and GIAC Enterprise employees will usually integrate their personal phone directory and calendar into the device. The device itself supports private items that can only be stored on the device and will not be synchronized to GIAC Enterprise' servers.
Primary vulnerabilities	• Device is stolen • Device is lost due to users' carelessness
Possible means of exploitation	• An attacker may target certain employees in GIAC enterprise to gain relevant information useful for their own gain. For an attacker, who is interested to compromise GIAC Enterprise servers, will try to steal system administrators' device. System Administrators usually keep their passwords on their device. It is very easy to find out who is the administrators of GIAC Enterprise, as normally it could be found from Google with 'GIAC Enterprise System Administrators' query to search mailing lists or newsgroup posts. The names could also be available from public events where system administrators may have left their business cards on the registration desks. • An attacker may steal the device from any employees of GIAC Enterprise and use any information retrieved to sell them to competitors. • Devices that are lost could be found and sold to people who exploit the information may contain therein.
Scenario of exposure	• GIAC Enterprise may lose sales due to disclosed sales information from theft of sales person's device. • GIAC Enterprise servers may be vulnerable to unauthorized access due to disclosure of password on stolen device. • As the device stores schedule details and phone book entries, it may be used to launch social engineering or identity theft.
Impact (cost to the company)	Very high

© SANS Institute 2005 Author retains full rights.

2.3.2. Lack of security controls for device operation in Intranet

Description	GIAC Enterprise security controls have not been redesigned to include additional controls for device adoption. The device is relatively new to the organization, and hence may have not been considered when policy, guidelines, and procedures of information security were written. While all laptops and workstations have been secured with operating system policies and personal firewalls, the devices are not. There is no way to stop employees from connecting the device to both internal and external networks. The employees do not have the understanding that the device has the capabilities of a workstation to some degree, and therefore should be treated with similar security.
Primary vulnerabilities	• Unauthorized connections between device and workstations (synchronization of Calendar, Phone directories, etc) • Unauthorized connections to Intranet from the device (Retrieving corporate emails, browsing) • Unauthorized transfer of organization information assets to device (Copying company confidential data to device).
Possible means of exploitation	• In a secured environment, where employees are not supposed to be able to copy any information from their workstation. • The device can be used to access company network and download sensitive information using wireless LAN and device's browser. • Contractors or R&D employees normally would have workstations without any output devices (floppy drive, USB ports, infrared), the malicious employees could use device built-in camera to capture information and send it using MMS, Emails or GPRS to external servers.
Scenario of exposure	• GIAC Enterprise may have its product design leaked out by contractors or imposters. • The device can be used by attackers imposing as a guest to scan available wireless network in the company and its protection. If the wireless network is open, or pre-shared keys are known beforehand, nobody would suspect the attacker accessing organization network resources while he is sitting in the lobby pretending that he is waiting for someone.
Impact (cost to the company)	Very high.

© SANS Institute 2005 Author retains full rights.

2.3.3. Device may be compromised remotely by TCP/IP sessions

Description	The device offers complete connectivity to Internet, by way of GSM (data circuit), GPRS (ubiquitous data service), EDGE (high-speed ubiquitous data service), Wireless LAN, and IP-passthrough via workstations. There are only very few places that is not covered by either one of possible connectivity methods above for normal city environment. The connections are normally made to Internet, and therefore are exposed to the same potential risks as any other computers in the Internet of possible remote compromise.
Primary vulnerabilities	• TCP/IP stack in device operating system. Historically, TCP/IP protocol weaknesses in many other platforms have been exploited that may allow remote control to device remotely or data being retrieved remotely • Denial of service by flooding device connections. This is especially true for slower connections such as GSM (usually 9.6-14.4 kbps), GPRS (up to 53.6 Kbps), EDGE (236.8 Kbps).
Possible means of exploitation	• An attacker may send ping packets with large payload to slow down device communication or even disable it. • An attacker may try to send malformed packets to cause the device to reach unpredictably.
Scenario of exposure	• On a real-time negotiation or bidding, GIAC employees may use instant messaging feature to work with supporting team in the office. The attacker may be able to launch denial of service and stop the team on the field to get required information from the organization. • GIAC employees that are presenting to clients using the device may be interrupted if they happen to be connected to the Internet and TCP/IP stack received malformed packet. The device is capable of connecting to projectors with additional device.
Impact (cost to the company)	High

© SANS Institute 2005 Author retains full rights.

Section 3: Testing

On previous section, I have identified possible risks and vulnerabilities. Out of the lists, three top risks were selected and discussed in great details. This section will develop tests to audit Communicator usage in GIAC Enterprise. It is possible that the tests described to be used in other organizations that provide Communicator 9500 to their employees.

There are tests that are developed to test organization's policies readiness to regulate Communicator adoption. GIAC Enterprise has a set of well-written policies. The policies could be found on http://www.sans.org/resources/policies/. The policies used on this paper are available from the URL as per 10th April 2005.

3.1. Device may be lost or stolen

The tests described in this section primarily concerns physical loss of the device.

Test Item 1 – PDA Security Policy on physical assets.	
Reference:	SANS Handheld Devices Audit Checklists[10]
Test Category:	Administrative, Preventive
Test Type:	Subjective
Test Procedure:	Compare PDA and related security policies against compliance criteria.
Compliance criteria:	1. Security policy governing the use of PDA/Handheld devices exist. 2. Security policies cover PDA/Handheld on top of existing devices.
Additional Information	Policy is fundamental to govern Communicator use in an organization. Therefore, it is mandatory to have policies in place before adopting Communicator.

Test Item 2 – User Awareness	
Reference:	SANS Handheld Devices Audit Checklists
Test Category:	Administrative, Preventive
Test Type:	Subjective
Test Procedure:	Check existing awareness security training and projects to include Communicator as organization valuable assets.
Compliance criteria:	Security awareness training has a section that describe Communicator do's & don'ts, roles and risks.
Additional Information	Users, who aware of roles and risks of Communicator, would minimize any risk and reduce the probability of loss by proper due care.

[10] E. Maiwald, A. Robb, J. Bern, JB. Bagby. Handheld devices audit checklist. Available from: www.**sans**.org/score/checklists/ Handhelddevicesauditchecklist.pdf

© SANS Institute 2005 Author retains full rights.

Test Item 3 – Device Registration	
Reference:	SANS Handheld Devices Audit Checklists
Test Category:	Administrative, Preventive
Test Type:	Objective
Test Procedure:	Evaluate if organization requires registration for Communicator
Compliance criteria:	1. Device registration is mandatory 2. Periodic check is carried out to track devices
Additional Information	Device registration allows companies to keep track of their employees' Communicator and perform maintenance. Access control can be applied based on the registration. Periodically checking the devices is a good control against unreported lost devices. A sample of device registration form can be read on Appendix 3 – Device Registration Form.

Test Item 4 – Encryption	
Reference:	ISF Securing PDA: A Practical Approach
Test Category:	Technical, Preventive
Test Type:	Objective
Test Procedure:	Verify if there is file system encryption on Communicator for both main and card memory.
Compliance criteria:	File system encryption implemented for all storage areas
Additional Information	Loss of device is considered insignificant compared to loss of the information in the device itself. Therefore, the data must be encrypted in line with secure standard. When a device is lost or stolen, there should be sufficient confidence that lost is limited to the device itself but not the information. One of commercial product that offers the functionality for Communicator 9500 is PointSec (http://www.pointsec.com). Memory card can be also secured by setting up a password in the device.

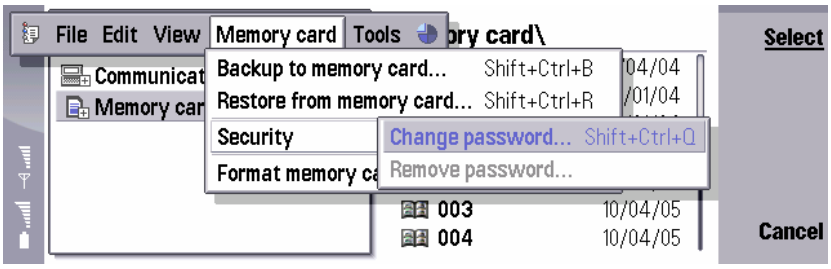


Figure 2 Setting-up password for MMC storage

© SANS Institute 2005 Author retains full rights.

Test Item 5 – Power-on Display	
Reference:	ISF Securing PDA: A Practical Approach
Test Category:	Technical, Preventive
Test Type:	Objective
Test Procedure:	Verify if there is any organization identifiable on power-on display.
Compliance criteria:	1. Device should not have any power-on message that lead thief or person who found the device to identify the organization and individual the device belongs to. 2. Contact information to return the device should be presented without revealing the organization.
Additional Information	The information of power-on screen is very useful to people who intend to abuse the information in the device.

Test Item 6 – Power-on Password	
Reference:	ISF Securing PDA: A Practical Approach
Test Category:	Technical, Preventive
Test Type:	Objective
Test Procedure:	Verify that Power-on password is enabled and system access is not possible before correct password entered.
Compliance criteria:	1. Power-on password enabled 2. Good password as described in security policy is used
Additional Information	Another good control to prevent thief or potential abuser to access the system is by having power-on password. A good password is needed to protect the system.

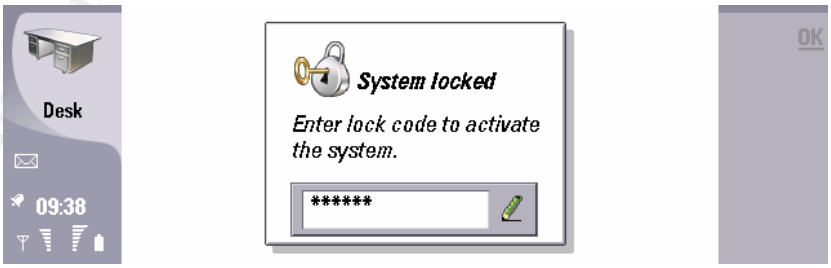


Figure 3 Power-on and Inactivity Lock

Test Item 7 – Inactivity lock interval	
Reference:	Original
Test Category:	Technical, Preventive
Test Type:	Objective
Test Procedure:	1. Verify that Communicator is configured to lock both phone and PDA interface at fixed interval. 2. Lock code is changed from default code. 3. Lock code is at least 6 digits strong.

© SANS Institute 2005 Author retains full rights.

Compliance criteria:	Inactivity lock is configured and enabled.
Additional Information	The phone should be locked if not used for a certain interval. It will greatly reduce the potential unauthorized access when the device is lost or stolen. The interval should be defined in PDA security policy, observing balance between convenience and security.

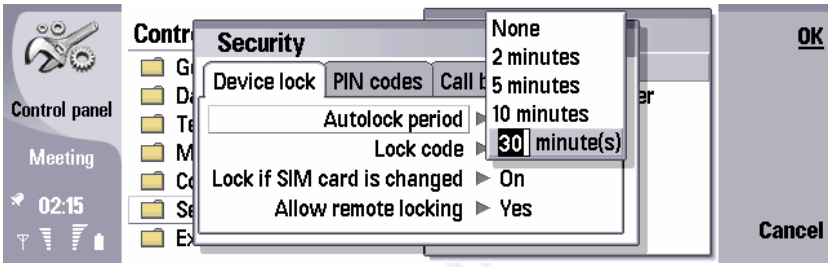


Figure 4 Enabling and configuring Auto Lock period

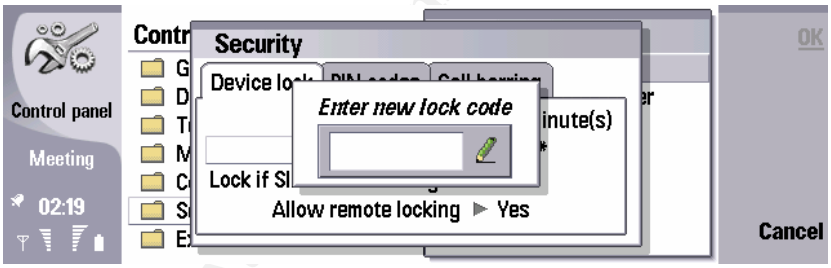


Figure 5. Changing default lock code

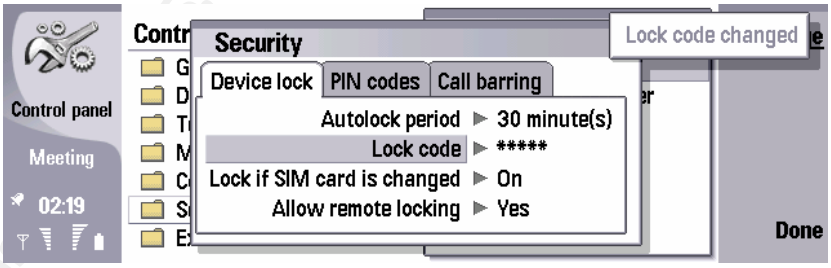
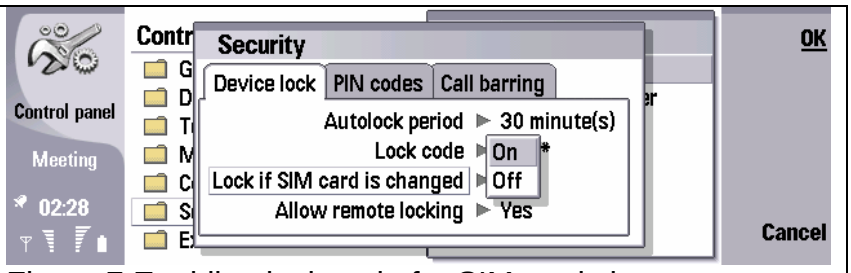
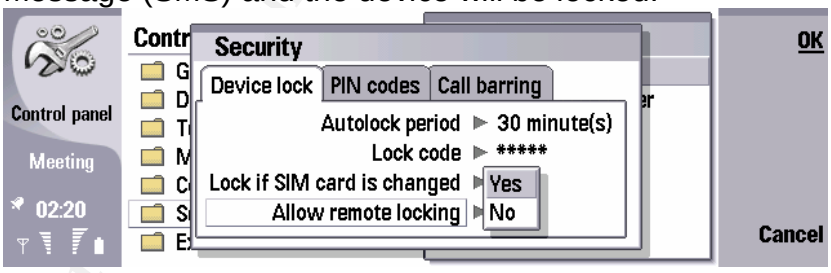


Figure 6 Confirmation of lock code change

Test Item 8 – SIM card change lock	
Reference:	Original
Test Category:	Technical, Preventive
Test Type:	Objective
Test Procedure:	Verify SIM card change lock status
Compliance criteria:	SIM card change lock is enabled.
Additional Information	The feature prevents the device from accepting new SIM card. This may be handy so that employees prevented from using personal SIM card on business phone or prevent abuser from using the device.

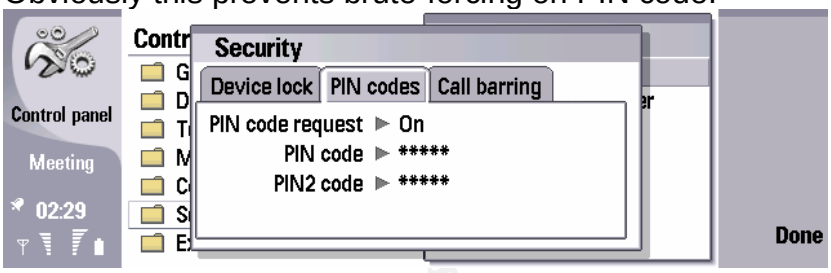
© SANS Institute 2005 Author retains full rights.

	 Figure 7 Enabling lock code for SIM card change

Test Item 9 – Remote lock	
Reference:	Original
Test Category:	Technical, Preventive and Reactive
Test Type:	Objective
Test Procedure:	Verify Remote Locking is configured and enabled
Compliance criteria:	Remote locking is configured and tested
Additional Information	This unique security feature allows organization to lock both phone and PDA interface, when the device is reported missing. The password must be secure and not dictionary-based. IT Security administrator in GIAC Enterprise can send the password to the device via Short Message (SMS) and the device will be locked.  **Figure 8 Enabling remote lock** **Figure 9 Setting-up remote lock message**

Test Item 10 – PIN code request	
Reference:	Original
Test Category:	Technical, Preventive and Reactive
Test Type:	Objective
Test Procedure:	Verify if PIN code is configured

© SANS Institute 2005 Author retains full rights.

Compliance criteria:	PIN code is asked when phone is turned on and PIN must not be easily guessed.
Additional Information	PIN (Personal Identity Number) is a security feature in GSM that will allow users to make calls only when correct code has been entered. Three wrong attempts will lock the SIM card at smart card level, and can only be unlocked with 8 digits PUK (Personal Unblock Key). Obviously this prevents brute-forcing on PIN code.  **Figure 10 Enabling and setting up PIN request**

3.2. Lack of security controls for device operation in Intranet

Some tests on this section have been described in previous section. With good user awareness training, employees may not synchronize their personal device to corporate laptops. Employees, who understand and accept AUP, will have to think twice before violating policy due to the liability may be incurred by the action.

Test Item 11 – Wireless LAN security	
Reference:	Original
Test Category:	Technical, Preventive
Test Type:	Objective
Test Procedure:	1. Verify if wireless LAN policy exists 2. Verify if wireless LAN policy covers Communicator
Compliance criteria:	1. Wireless LAN service is configured with proper and reasonably strong encryption 2. Wireless LAN policy covers Communicator
Additional Information	An insecure wireless LAN implementation will increase the risks with or without the use of Communicator. Access control in Communicator is normally weaker than laptops, not by design, but by default configuration. It is easier for a contractor to compromise a device lying on an employee table rather than the laptop. Communicator supports WEP, WPA, 802.1x (EAP-SIM, EAP-TLS, EAP-PEAP, EAP-PEAP, EAP-MSCHAPv2, EAP-GTC, EAP-LEAP). EAP is Extensible Authentication Protocol that allows Wireless authentication to support many protocol by using plug-ins. The device is Cisco

© SANS Institute 2005 Author retains full rights.

Certified CCX-1.0. With plenty of option, there is no reason to use insecure Wireless LAN for communicator, it is as good if not better than laptop's wireless authentication, for example, laptop needs additional software to support Cisco LEAP, or PEAP.

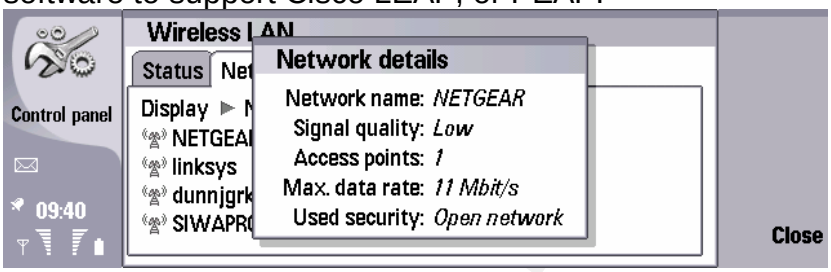


Figure 11 Details of wireless network discovered

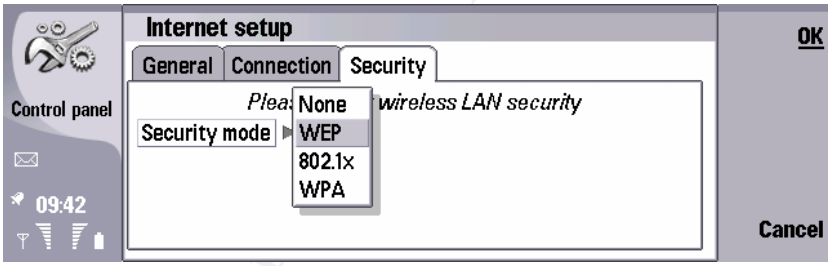


Figure 12 Wireless security options

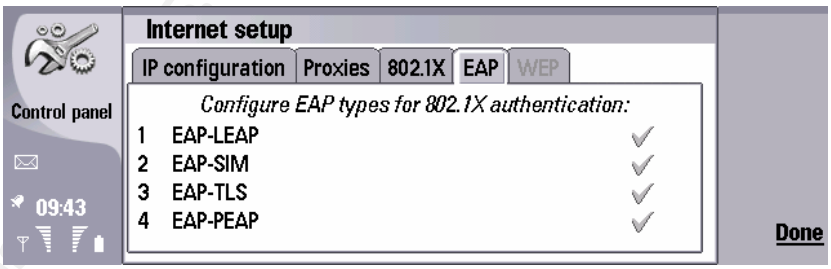


Figure 13 Supported EAP modules

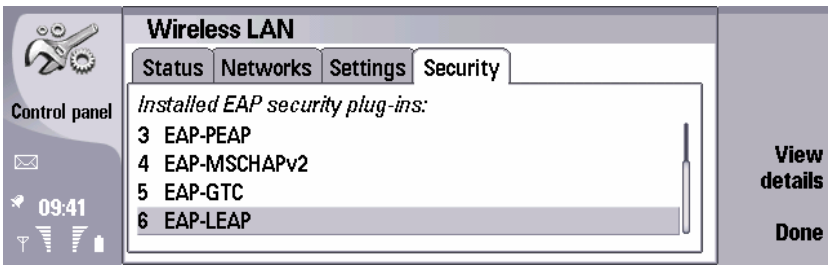


Figure 14 Supported EAP Modules (Continued)

© SANS Institute 2005 Author retains full rights.

Test Item 12 – Good host-based protection	
Reference:	Original
Test Category:	Technical, Preventive
Test Type:	Objective
Test Procedure:	1. Verify if Organization has means to set policy restricting employees from installing additional software. 2. Verify if Organization has personal firewall which policy can be set centrally to prevent IP Passthrough.
Compliance criteria:	1. Employees are restricted from installing additional software, hence stopping PC-suite[11] installation and possible synchronizations with organization laptops or workstations. 2. Personal firewall should be able to receive policy from management servers. It must be able to detect any extra unauthorized network interfaces and block the access. With IP-Passthrough, the device create additional interface in workstations, as if two computers connected via cross-cable.
Additional Information	To prevent unauthorized device from connecting to company's workstations, a good technical policy on Operating System level is required to limit employees' ability to install new software or install new hardware.

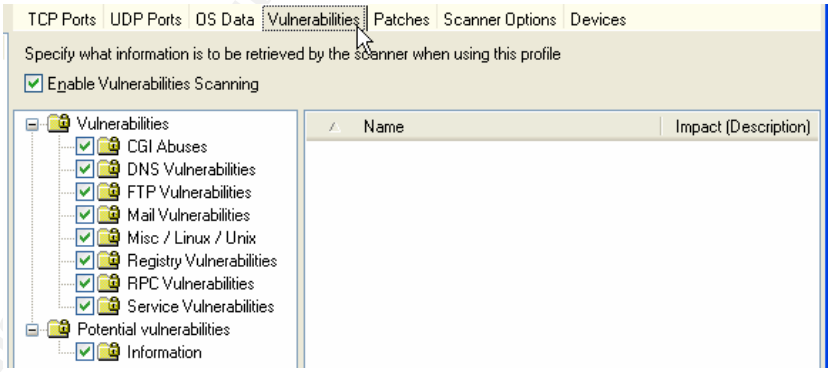
Test Item 13 – Camera Use	
Reference:	Original
Test Category:	Administrative, Preventive
Test Type:	Objective
Test Procedure:	Verify if company has policy against use of camera-enabled devices on sensitive areas.
Compliance criteria:	1. Sensitive areas identified 2. Security policy covers restriction of camera use
Additional Information	

3.3. Device may be compromised remotely by TCP/IP sessions

Test Item 14 – Open ports / Running services	
Reference:	http://www.insecure.org/nmap/data/nmap_manpage.html
Test Category:	Technical, Detective
Test Type:	Objective

[11] PC-Suite is a powerful suite of application to synchronize data between laptop and mobile phone, and transfer data between devices.

© SANS Institute 2005 Author retains full rights.

Test Procedure:	Run port-scanner to discover open ports by defaults. For this purpose, a number of vulnerability scanners and port scanners will be used. Different programs may have different results. 1. LanGuard Network Security Scanner v6 LanGuard NSS from GFI software is well known commercial software for vulnerability scanning. Latest version and database as per 10th April 2005 is used for this scan. The scanning profile is as follows: • Full TCP scan from port 1-65535 • Full UDP scan from port 1-65535 • All option enabled on "OS Data" Tab on scanning profile page. • All vulnerabilities checking on 'Vulnerabilities' tab • Disable all patches checking, as it applies to Microsoft Windows platform on 'Patches' tab. • Default settings on 'Scanner Option' tabs.  **Figure 15 Settings on LANGuard NSSv6** 2. nmap Nmap is a very well-known network mapping tool written by Fyodor. At times, target system does not react well to nmap active scanning and may crash or lose connectivity. Prior developing these tests, I have conducted tests and found that scanning all ports on most scans will cause device to lose its connectivity and need to be reconnected. The first tests will be thorough. If there are ports open, the same thorough tests will be conducted for the rest. In the case there are no ports open or nmap crashed the device, a simpler and faster

© SANS Institute 2005 Author retains full rights.

scans are chosen. The commands to be used in the tests are:

- `nmap –sS –sV –v –O –p 1-65535 <IP>`
  Detects open ports and running services using SYN scan. Target is all ports at device IP address with verbose and OS & service fingerprinting for additional options.
- `nmap –sT –sV –v –O –p 1-65535 <IP>`
  Detects open ports and running services using TCP connect() scan. Target is all ports at device IP address with verbose & OS and service fingerprinting for additional options.
- `nmap –sF -vv -O<IP>`
  Detects open ports and running services using Stealth FIN scan.
- `nmap –sX -vv –O <IP>`
  Detects open ports and running services using Xmas tree scan.
- `nmap –sN -vv –O <IP>`
  Detects open ports and running services using Null scan.
- `nmap –sU -vv –O <IP>`
  Detects open ports and running services using UDP scan.
- `nmap –sO -vv –O <IP>`
  Detects open ports and running services using IP Protocol scan.
- `nmap –sA -vv –O –p 1-65535 <IP>`
  Detects open ports and running services using Ack scan.
- `nmap –sR -vv –O –p 1-65535 <IP>`
  Detects open ports and running services using RPC scan.

3. eEye Retina
   Retine from eEye is another commercial vulnerability scanner that is well-known in the market. Test will be conducted in 'Audit' mode with all option selected.

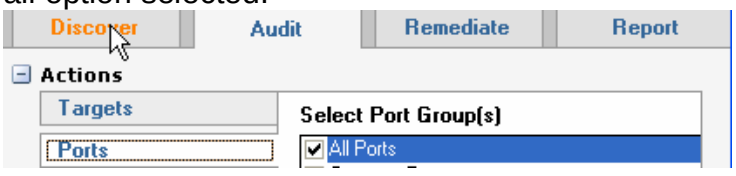


Figure 16 Retina Ports selection

© SANS Institute 2005 Author retains full rights.

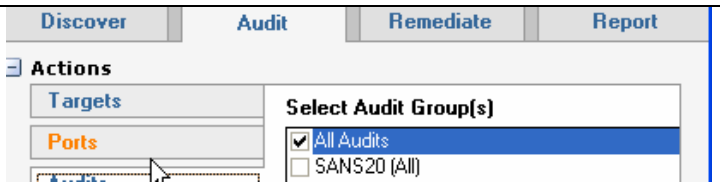


Figure 17 Retina Audit Groups

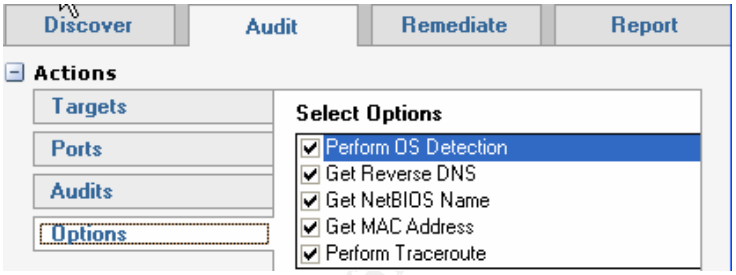


Figure 18 Retina Options

4. Nessus
   All plug-ins (5935 plug-ins) will be enabled and port scan is expanded to include all ports from 1 to 65535.

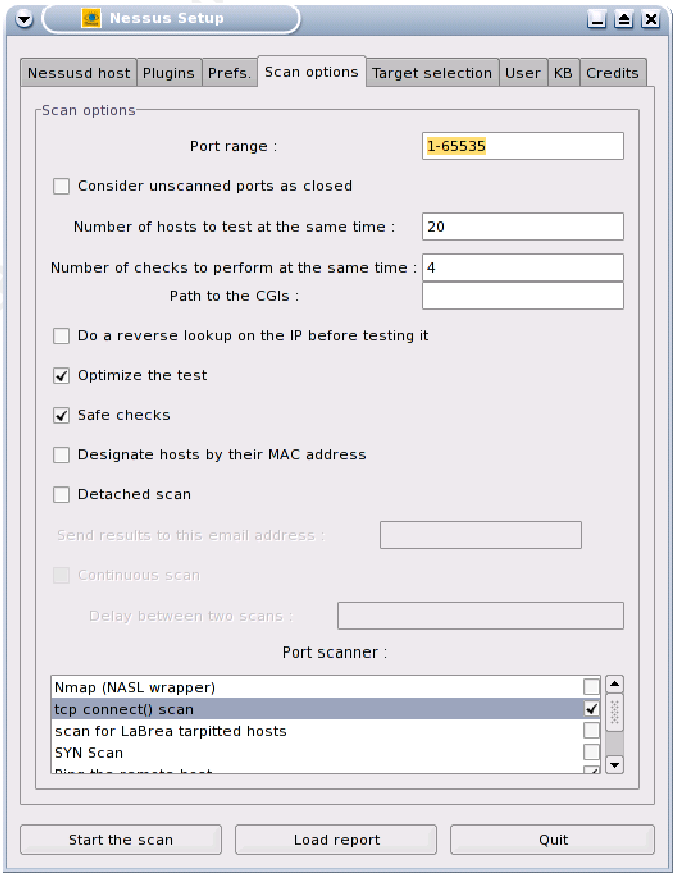
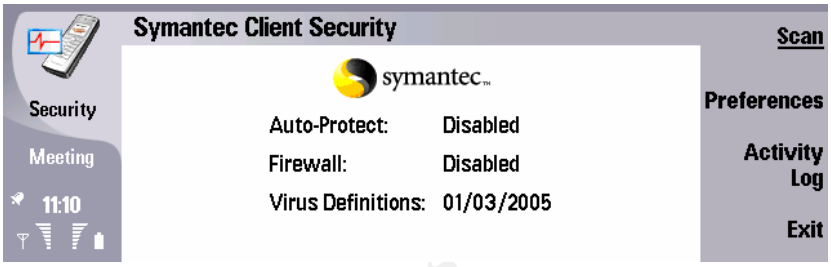
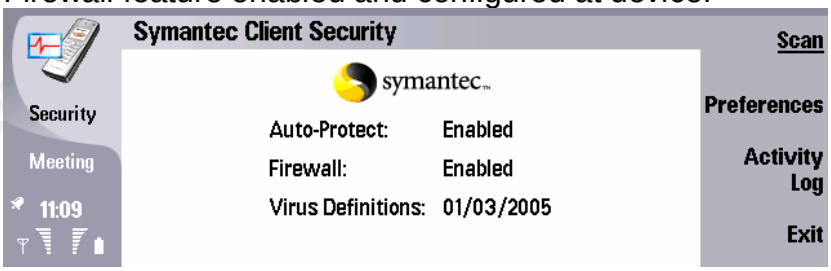


Figure 19 Nessus options

© SANS Institute 2005 Author retains full rights.

	Communicator is connected to an isolated network through wireless connection without any firewall on the network. Laptop with vulnerability and port scanner are in the same subnet and broadcast domain as the device is. Refer to Appendix 3 for network diagram. Symantec client security is disabled. The device is not running any personal firewall.  **Figure 20 Symantec Client Security is disabled**
Compliance criteria:	No unnecessary and vulnerable services should be running
Additional Information	The device will connect to various network anywhere, at anytime for enabling mobility, therefore, it should have secure TCP/IP stack. The test will verify this.

Test Item 15 – Effective device firewall.	
Reference:	Original
Test Category:	Administrative, Detective
Test Type:	Objective
Test Procedure:	Idem Test item 14 with Symantec Client Security's Firewall feature enabled and configured at device.  **Figure 21 Symantec Client Security is enabled**
Compliance criteria:	No unnecessary and vulnerable services should be running
Additional Information	The test will verify the effectiveness of device firewall (part of Symantec Client Security) in handling port or vulnerability scanning.

© SANS Institute 2005 Author retains full rights.

Section 4: Audit

This section will test items developed on previous section. The environment will be GIAC Enterprise. GIAC enterprise has a set of policies written that will be benchmarked against administrative test items. As the policies are living documents, the audit tests polices as per 10th April 2005. The policies are available online at http://www.sans.org/resources/policies/. Another assumption used in the testing is that IT department configures devices with secure settings before handing the device to end-users. Nokia Communicator 9500 tested has firmware version of 4.51(00) and installed with Symantec Client Security version 3.0.197.

Figure 22 Nokia Communicator 9500 Firmware version

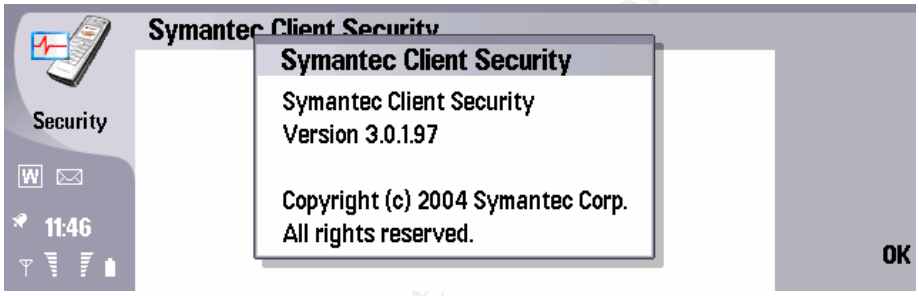


Figure 23 Symantec Client Security version

Test Item 1 – PDA Security Policy on physical assets.	
Evidence:	GIAC Enterprise has a set of policies defined in http://www.sans.org/resources/policies/ All policies are studied to find requirement on this test items.
Status:	**FAIL**
Findings and Comments:	1. There is no specific policy that governs the use of PDA (In this case Nokia Communicator 9500) in the enterprise. 2. Existing policies define hosts as servers, desktops, laptops. This excludes devices such as Communicator. In other word, existing policies are not specifically applied to Communicator. (Reference. Acquisition assessment policy) A specific policy must be written to govern Communicator use in the organization. Existing policies should be extended to include Communicator as well.

© SANS Institute 2005 Author retains full rights.

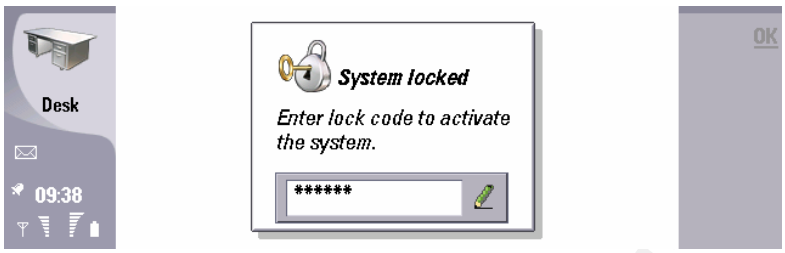
Test Item 2 – User Awareness	
Evidence:	Security awareness training is developed based on GIAC Enterprise policies above. The training syllabus consisted of all the company policies to educate users on the meanings.
Status:	**FAIL**
Findings and Comments:	Due to Communicator is not included in the policy, the security awareness training does not include user awareness on risks and best practices of Communicator.

Test Item 3 – Device Registration	
Evidence:	GIAC Enterprise policies does not have coverage on PDA (Communicator) usage in the organization
Status:	**FAIL**
Findings and Comments:	1. There is no policy requiring employees to register their Communicator 2. An example of Device registration from is on Appendix 3.

Test Item 4 – Encryption	
Evidence:	Ref. Acceptable Use Policy: 4.1.3. InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see InfoSec's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to InfoSec's Awareness Initiative.
Status:	**FAIL**
Findings and Comments:	While GIAC Enterprise has recommended the requirement for sensitive information encryption, it does not constitute mandatory requirement. Due to the mobile nature and high-risk of device theft & loss, encryption is a must on all Communicator storage areas. Third party software such as PointSec could be used to encrypt both main memory and MMC storage.

Test Item 5 – Power-on Display	
Evidence:	Nokia Communicator 9500 does not have any user-identifiable welcome screen such as Microsoft PocketPC devices. If security lock code is set, the first screen seen is Lock code dialog box. IT department has configured each device to have lock code upon power-on.
Status:	**SUCCESS**
Findings and Comments:	Nokia Communicator does not have welcome screen.

© SANS Institute 2005 Author retains full rights.

Test Item 6 – Power-on Password	
Evidence:	IT department has enabled and verifies power-on password enabled with end-users' preferred lock code of at least six digits.
Status:	**SUCCESS**
Findings and Comments:	 **Figure 24 Default display after power-on if system lock is configured** The device supports power-on password. Therefore, when turned-off, the system can't be accessed by unauthorized party just by turning it on.

Test Item 7 – Inactivity lock interval	
Evidence:	IT department has enabled and verifies inactivity lock interval enabled with end-users' preferred lock code of at least six digits.
Status:	**SUCCESS**
Findings and Comments:	Steps to enable inactivity lock interval and changing lock code as illustrated in Figure 4, Figure 5, and Figure 6 were taken.

Test Item 8 – SIM card change lock	
Evidence:	IT department has enabled and verifies SIM card change lock enabled with end-users' preferred lock code of at least six digits
Status:	**SUCCESS**
Findings and Comments:	Steps to enable SIM card lock and changing lock code as illustrated in Figure 7 were taken.

Test Item 9 – Remote Lock	
Evidence:	IT department has enabled and verifies remote lock enabled with password according to Password Protection policy
Status:	**SUCCESS**
Findings and Comments:	Remote lock enables GIAC enterprise IT security team to lock the device remotely, if it has been stolen or lost.

© SANS Institute 2005 Author retains full rights.

Test Item 10 – PIN code request	
Evidence:	IT department has enabled and verifies SIM card change lock enabled with end-users' preferred lock code of at least six digits
Status:	**SUCCESS**
Findings and Comments:	Necessary steps have been taken.

Test Item 11 – Wireless LAN security	
Evidence:	GIAC enterprise has a secure wireless LAN access as described in Wireless Communication, VPN Communication, and Remote Access policies. In addition to that, IT department has configured Wireless LAN on the device to match Enterprise security mechanism.
Status:	**SUCCESS**
Findings and Comments:	The device is very versatile and is supported by many Wireless security protocols, hence it is very possible to have the device secured.

Test Item 12 – Good host-based protection	
Evidence:	Ref. Acceptable Use policy
Status:	**FAILED**
Findings and Comments:	The policy does not restrict employees from installing additional software. Although malicious software is prohibited, synchronization software is not considered as malicious software.

Test Item 13 – Camera Use	
Evidence:	Ref. Acceptable Use policy
Status:	**FAILED**
Findings and Comments:	The policy does not cover restriction of exporting sensitive/confidential information using camera or similar devices. Despite the situation, it covers unacceptable use of exporting software, technical information, and encryption in accordance to government export control laws. It also covers unauthorized copying of copyrighted material. Not all sensitive information in the organization are copyrighted, mostly are not.

© SANS Institute 2005 Author retains full rights.

Test Item 14 – Open ports / Running services	
Evidence:	1. Vulnerability Scanning report using LanGuard NSS 2. Port Scanning result using Nmap (Appendix 4 – Nmap Result) 3. Vulnerability Scanning report using eEye Retina. (Appendix 6 – eEye Retina Report)
Status:	**SUCCESS**
Findings and Comments:	1. Full TCP and UDP scans from both eEye Retina and Nmap (with various combinations) show that there are no open ports on Communicator 9500. Therefore, there are no services that are accessible remotely. 2. Both applications could not fingerprint Symbian Operating system on Communicator 9500. 3. LanGuard NSS reported quite a number of open ports, but those are false positives. The reported open ports were tested using netcat (similar to telnet, but a much versatile tool) to access the ports. Ports are not accessible. 4. Some Nmap scans take a significantly long (UDP scan) 5. Nokia Communicator supports both IPv4 and IPv6. Overall, it supported IP, TCP, UDP, ICMP, IPv6, IPv6-frag, IPv6-icmp, and IPv6-nonxt

Test Item 15 – Effective device firewall.	
Evidence:	1. Vulnerability Scanning report using LanGuard NSS 2. Port Scanning result using Nmap 3. Vulnerability Scanning report using eEye Retina
Status:	**SUCCESS**
Findings and Comments:	1. Symantec Client Security detects port-scanning attempts and blocks the source. This is observed with network sniffer (a tool to listen packets on the network), Port scans are replied with RST packets by device, but device will stop sending RST packets after few seconds. 2. In stealth mode, all incoming traffic will be blocked even at the first packet. 3. As the application works as what it has claimed[12], it is a one of critical protection for the device against malicious application, viruses, worms, and network threats.

[12] Symantec. Symantec Client Security for Nokia Communicator. Available from: http://enterprisesecurity.symantec.com.au/ content/displaypdf.cfm?pdfid=1083&EID=0

© SANS Institute 2005 Author retains full rights.

References

1. SANS Institute. Courseware. Audit 507: Auditing Networks, Perimetes, and Systems. 2004
2. Calishain, Dornfest. Oreilly. Google Hacks. 2003
3. SANS Institute. Online. Security Policy Templates. Available at: http://www.sans.org/resources/policies/. Accessed at March 20, 2005
4. ISACA. Certified Information Systems Auditor Review Manual 2005 Edition.
5. Project Management Institute. Project Management Body of Knowledge (PMBOK) 3rd Edition.
6. Nokia. Nokia for Business: Reference Cases. Available from: http://www.nokia.com/nfb/referencecases.html
7. Symbian. Symbian Phone Gallery. Available from: http://www.symbian.com/images/library/9500_lores_800.jpg
8. Nokia. Nokia Communicator 9500 Full Specifications. Available from: http://www.nokia.com/nokia/0,,54108,00.html
9. McGraw-Hill. S. Harris. All-in-One CISSP Certification 1st Ed
10. S.Rao. SRV Publications. CISSP Examination Textbook Vol. 1, 2nd Edition, Pg. 157
11. International Charter. The Risk Equation. Available from: http://www.icharter.org/articles/risk_equation.html
12. SANS. SANS Policy Project. Available from: http://www.sans.org/resources/policies/.
13. ISF. Securing PDA: A Practical Approach. Available from: http://www.securityforum.org/assests/pdf/pda.pdf
14. Symantec. Symantec Client Security for Nokia Communicator. Available from: http://enterprisesecurity.symantec.com.au/content/displaypdf.cfm?pdfid=1083&EID=0
15. WinPcap. Online. The WinPcap manual and tutorial. Available at: http://winpcap.mirror.ethereal.com/docs/default.htm Accessed at March 20, 2005.
16. WinDump. Online. WinDump FAQ. Available at: http://winpcap.mirror.ethereal.com/misc/faq.htm. Accessed at March 20, 2005.
17. WinDump. Online. WinDump Documedntation. Available at: http://windump.mirror.ethereal.com/docs/manual.htm. Accessed at March 20, 2005
18. Auditor. Online. Available at: http://new.remote-exploit.org/index.php/Auditor_main

© SANS Institute 2005 Author retains full rights.

Appendix 1 – Test Network Diagram

Test environment is simulated to be inside company intranet, where there are no firewalls inside intranet. The setup also simplified and to ensure that tests are not influenced by other network devices in the networks.

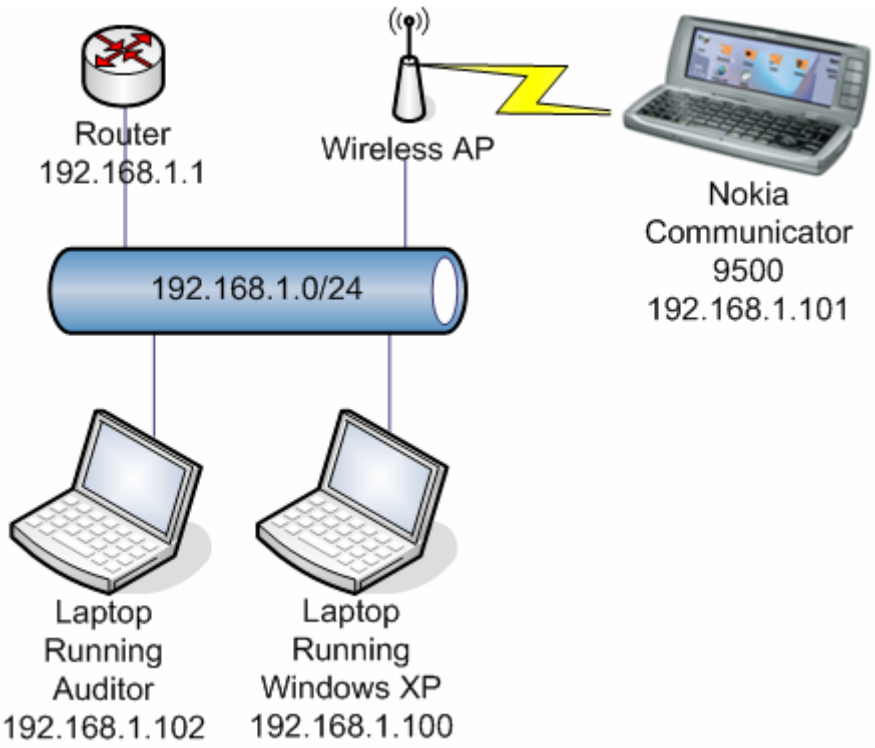


Figure 25 Test / Audit Topology

In the test, Auditor version 120305-1 was used. From official site (http://www.remote-exploit.com), Auditor is best defined[13] as:

"The Auditor security collection is a Live-System based on KNOPPIX. With no installation whatsoever, the analysis platform is started directly from the CD-Rom and is fully accessible within minutes. Independent of the hardware in use, the Auditor security collection offers a standardised working environment, so that the build-up of know-how and remote support is made easier. Even during the planning and development stages, our target was to achieve an excellent user-friendliness combined with an optimal toolset. Professional open-source programs offer you a complete toolset to analyse your safety, byte for byte. In order to become quickly proficient within the Auditor security collection, the menu structure is supported by recognised phases of a security check. (Foot-printing, analysis, scanning, wireless, brute-forcing, cracking). By this means, you

[13] http://new.remote-exploit.org/index.php/Auditor_main

© SANS Institute 2005 Author retains full rights.

instinctively find the right tool for the appropriate task. In addition to the approx. 300 tools, the Auditor security collection contains further background information regarding the standard configuration and passwords, as well as word lists from many different areas and languages with approx. 64 million entries. Current productivity tools such as web browser, editors and graphic tools allow you to create or edit texts and pictures for reports, directly within the Auditor security platform. Many tools were adapted, newly developed or converted from other system platforms, in order to make as many current auditing tools available as possible on one CD-ROM. Tools like Wellenreiter and Kismet were equipped with an automatic hardware identification, thus avoiding irritating and annoying configuration of the wireless cards.

© SANS Institute 2005, Author retains full rights

© SANS Institute 2005 Author retains full rights.

Appendix 2 – Risk Ranking

The following table is created to calculate total risks in regard to information security aspect of Nokia Communicator 9500 usage in GIAC Enterprise. The process exempts unavailability of data that may happen due to damaged device by user carelessness or wear and tear. The cost is determined in regard to cost incurred by lost of sensitive information that may be used adversely to organization interests. The impact of a risk is determined by the cost of exposure.

Risks	V	T	C	Total	Ranks*
Device may be lost or stolen, including lost of sensitive information contained in the device.	**3**	**3**	**3**	**27**	**1**
Device may be dropped or damaged	**2**	**0**	**0**	**0**	**12**
Information may be disclosed when device is used in public places. (Shoulder surfing)	**3**	**2**	**2**	**12**	**4**
Users may send or receive information from/to other PDAs.	**2.5**	**2**	**2**	**10**	**5**
User may connect individually-own device to organization's computers without permission, bypassing security controls	**3**	**2**	**1**	**6**	**9**
Device may be infected with malicious application from user's lack of security awareness.	**3**	**2.5**	**1**	**7.5**	**8**
Device may be vulnerable to TCP/IP attacks and potentially compromised remotely	**2**	**3**	**3**	**18**	**3**
User may have access to disable the security controls.	**3**	**3**	**1**	**9**	**6**
Device security features are by default disabled	**3**	**3**	**1**	**9**	**7**
Device may operate in enterprise premises without corresponding/ relevant security controls.	**3**	**3**	**2.5**	**21.5**	**2**
Evidence may be hard/not available to obtain in case of incidents.	**2**	**2**	**1**	**4**	**11**
Personal devices are not configured with enterprise standard for use in business.	3	2	1	6	**10**

Metrics (Qualitative):

	High	Moderate	Low
Vulnerability	3	2	1
Threat	3	2	1
Cost	3	2	1

© SANS Institute 2005 Author retains full rights.

Appendix 3 – Device Registration Form

GIAC Enterprise
Employee Communicator 9500 Registration Form

Employee Section		
First name	:	
Last name	:	
Employee ID	:	
Department	:	
Site	:	
Fixed phone number	:	
Mobile phone number	:	
Fax number	:	
Email address	:	
Device Section		
Device type	:	
IMEI number*	:	
Firmware version^	:	
Purchased by&	:	Company / Individual
Date purchased	:	
Authorized by	:	
Device configured by	:	
Device verified by	:	
Signed AUP on	:	

Most of the fields on the form are self-explanatory. IMEI number is a globally unique identifier of device (similar to NIC's MAC address). Before an employee could purchase a Communicator, Line manager should approve the purchase. The device should be configured by member of IT team and verified by security administrator. The concept is to segregate the duty so that Communicator configuration is secure and correct. Employee must sign Acceptable Use Policy (AUP) when receiving configured Communicator.

© SANS Institute 2005 Author retains full rights.

Appendix 4 – Nmap Result

1. nmap –sS –sV –v –O –p 1-65535 192.168.1.101

```
root@3[~]# nmap -sS -sV -v -O -p 1-65535 192.168.1.101

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-04-10 14:10 EDT
Initiating SYN Stealth Scan against 192.168.1.101 [65535 ports] at 14:10
SYN Stealth Scan Timing: About 12.81% done; ETC: 14:14 (0:03:24 remaining)
The SYN Stealth Scan took 235.99s to scan 65535 total ports.
Warning:  OS detection will be MUCH less reliable because we did not find at least 1
open and 1 closed TCP port
Host 192.168.1.101 appears to be up ... good.
All 65535 scanned ports on 192.168.1.101 are: closed
MAC Address: 00:11:9F:DD:21:DC (Nokia Danmark A/S)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo(V=3.75%P=i686-pc-linux-gnu%D=4/10%Tm=42596D00%O=-1%C=1%M=00119F)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 249.161 seconds
```

2. nmap –sT –sV –v –O –p 1-65535 192.168.1.101

```
root@3[~]# nmap -sT -v -O 192.168.1.101

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-04-10 19:21 EDT
Initiating Connect() Scan against 192.168.1.101 [1663 ports] at 19:21
The Connect() Scan took 6.69s to scan 1663 total ports.
Warning:  OS detection will be MUCH less reliable because we did not find at least 1
open and 1 closed TCP port
Host 192.168.1.101 appears to be up ... good.
All 1663 scanned ports on 192.168.1.101 are: closed
MAC Address: 00:11:9F:DD:21:DC (Nokia Danmark A/S)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo(V=3.75%P=i686-pc-linux-gnu%D=4/10%Tm=4259B51A%O=-1%C=1%M=00119F)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 40.627 seconds
```

Note: Scanning all port disconnected the device from Wireless connection. Port scan reduced to default setting, as first complete SYN scan found no open ports.

© SANS Institute 2005 Author retains full rights.

3. nmap –sF –sV –v –O –p 1-65535 192.168.1.101

```
root@3[~]# nmap -sF -v -O 192.168.1.101

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-04-10 19:19 EDT
Initiating FIN Scan against 192.168.1.101 [1663 ports] at 19:20
Increasing send delay for 192.168.1.101 from 0 to 5 due to 376 out of 1253 dropped
probes since last increase.
The FIN Scan took 23.37s to scan 1663 total ports.
Warning:  OS detection will be MUCH less reliable because we did not find at least 1
open and 1 closed TCP port
Host 192.168.1.101 appears to be up ... good.
All 1663 scanned ports on 192.168.1.101 are: closed
MAC Address: 00:11:9F:DD:21:DC (Nokia Danmark A/S)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo(V=3.75%P=i686-pc-linux-gnu%D=4/10%Tm=4259B4D7%O=-1%C=1%M=00119F)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 56.258 seconds
```

Note: Scanning all port disconnected the device from Wireless connection. Port scan reduced to default setting, as first complete SYN scan found no open ports

4. nmap –sX –sV –vv –O –p 1-65535 192.168.1.101

```
root@3[~]# nmap -sX -vv -O 192.168.1.101 | more

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-04-10 19:49 EDT
Initiating XMAS Scan against 192.168.1.101 [1663 ports] at 19:49
Increasing send delay for 192.168.1.101 from 0 to 5 due to 351 out of 1170 dropped
probes since last i
ncrease.
The XMAS Scan took 16.01s to scan 1663 total ports.
Warning:  OS detection will be MUCH less reliable because we did not find at least 1
open and 1 closed
 TCP port
Host 192.168.1.101 appears to be up ... good.
All 1663 scanned ports on 192.168.1.101 are: closed
MAC Address: 00:11:9F:DD:21:DC (Nokia Danmark A/S)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo(V=3.75%P=i686-pc-linux-gnu%D=4/10%Tm=4259BBB1%O=-1%C=1%M=00119F)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 49.390 seconds
```

Note: Scanning all port disconnected the device from Wireless connection. Port scan reduced to default setting, as first complete SYN scan found no open ports

© SANS Institute 2005 Author retains full rights.

5. nmap –sN –sV –vv –O –p 1-65535 192.168.1.101

```
root@3[~]# nmap -sN -vv -O 192.168.1.101 | more

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-04-10 19:47 EDT
Initiating NULL Scan against 192.168.1.101 [1663 ports] at 19:47
The NULL Scan took 6.91s to scan 1663 total ports.
Warning:  OS detection will be MUCH less reliable because we did not find at least 1
open and 1 closed
 TCP port
Host 192.168.1.101 appears to be up ... good.
All 1663 scanned ports on 192.168.1.101 are: closed
MAC Address: 00:11:9F:DD:21:DC (Nokia Danmark A/S)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo(V=3.75%P=i686-pc-linux-gnu%D=4/10%Tm=4259BB2A%O=-1%C=1%M=00119F)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 40.545 seconds
root@3[~]#
```

Note: Scanning all port disconnected the device from Wireless connection. Port scan reduced to default setting, as first complete SYN scan found no open ports

6. nmap –sU –sV –vv –O –p 1-65535 192.168.1.101

```
 root@3[~]# nmap -sU -vv -O 192.168.1.101 | more
Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-04-10 19:51 EDT
Initiating UDP Scan against 192.168.1.101 [1478 ports] at 19:51
Increasing send delay for 192.168.1.101 from 0 to 50 due to 11 out of 21 dropped
probes since last inc
rease.
UDP Scan Timing: About 9.00% done; ETC: 19:57 (0:05:03 remaining)
Increasing send delay for 192.168.1.101 from 50 to 100 due to 20 out of 65 dropped
probes since last i
ncrease.
Increasing send delay for 192.168.1.101 from 100 to 200 due to max_successful_tryno
increase to 4
Increasing send delay for 192.168.1.101 from 200 to 400 due to max_successful_tryno
increase to 5
Increasing send delay for 192.168.1.101 from 400 to 800 due to max_successful_tryno
increase to 6
Increasing send delay for 192.168.1.101 from 800 to 1000 due to max_successful_tryno
increase to 7
UDP Scan Timing: About 82.82% done; ETC: 20:16 (0:04:09 remaining)
The UDP Scan took 1551.52s to scan 1478 total ports.
Warning:  OS detection will be MUCH less reliable because we did not find at least 1
open and 1 closed
 TCP port
Host 192.168.1.101 appears to be up ... good.
All 1478 scanned ports on 192.168.1.101 are: closed
MAC Address: 00:11:9F:DD:21:DC (Nokia Danmark A/S)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo(V=3.75%P=i686-pc-linux-gnu%D=4/10%Tm=4259C22A%O=-1%C=-1%M=00119F)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 1585.923 seconds
```

Note: Scanning all port disconnected the device from Wireless connection. Port scan reduced to default setting, as first complete SYN scan found no open ports

© SANS Institute 2005 Author retains full rights.

7. nmap –sO –sV –vv –O 192.168.1.101

```
root@3[~]# nmap -sO -vv -O 192.168.1.101 | more

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-04-10 20:26 EDT
Initiating IPProto Scan against 192.168.1.101 [256 ports] at 20:27
Increasing send delay for 192.168.1.101 from 0 to 5 due to 11 out of 21 dropped probes
since last incr
ease.
Increasing send delay for 192.168.1.101 from 5 to 10 due to max_successful_tryno
increase to 4
IPProto Scan Timing: About 38.48% done; ETC: 20:28 (0:00:47 remaining)
Increasing send delay for 192.168.1.101 from 10 to 20 due to max_successful_tryno
increase to 5
Increasing send delay for 192.168.1.101 from 20 to 40 due to max_successful_tryno
increase to 6
Increasing send delay for 192.168.1.101 from 40 to 80 due to max_successful_tryno
increase to 7
IPProto Scan Timing: About 58.94% done; ETC: 20:29 (0:00:55 remaining)
Increasing send delay for 192.168.1.101 from 80 to 160 due to max_successful_tryno
increase to 8
Increasing send delay for 192.168.1.101 from 160 to 320 due to max_successful_tryno
increase to 9
Increasing send delay for 192.168.1.101 from 320 to 640 due to max_successful_tryno
increase to 10
IPProto Scan Timing: About 76.01% done; ETC: 20:30 (0:00:42 remaining)
Increasing send delay for 192.168.1.101 from 640 to 1000 due to max_successful_tryno
increase to 11
IPProto Scan Timing: About 80.32% done; ETC: 20:31 (0:00:44 remaining)
The IPProto Scan took 285.23s to scan 256 total ports.
Warning:  OS detection will be MUCH less reliable because we did not find at least 1
open and 1 closed
 TCP port
Host 192.168.1.101 appears to be up ... good.
Interesting protocols on 192.168.1.101:
(The 248 protocols scanned but not shown below are in state: closed)
PROTOCOL STATE         SERVICE
1        open|filtered icmp
4        open|filtered ip
6        open|filtered tcp
17       open|filtered udp
41       open|filtered ipv6
44       open|filtered ipv6-frag
58       open|filtered ipv6-icmp
59       open|filtered ipv6-nonxt
MAC Address: 00:11:9F:DD:21:DC (Nokia Danmark A/S)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo(V=3.75%P=i686-pc-linux-gnu%D=4/10%Tm=4259C58D%O=-1%C=-1%M=00119F)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 318.870 seconds
root@3[~]#
```


© SANS Institute 2005 Author retains full rights.

8. nmap –sA –sV –v –O –p 1-65535 192.168.1.101

```
root@3[~]# nmap -sA -vv -O 192.168.1.101 | more

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-04-10 20:35 EDT
Unexpected port state: 6

QUITTING!
Initiating ACK Scan against 192.168.1.101 [1663 ports] at 20:35
root@3[~]#
```

Note: Scanning all port disconnected the device from Wireless connection. Port scan reduced to default setting, as first complete SYN scan found no open ports. Nmap didn't get expected reply from Communicator and terminate the scan automatically.

9. nmap –sR –sV –v –O –p 1-65535 192.168.1.101

```
root@3[~]# nmap -sR -vv -O 192.168.1.101 | more

Starting nmap 3.75 ( http://www.insecure.org/nmap/ ) at 2005-04-10 20:43 EDT
Initiating SYN Stealth Scan against 192.168.1.101 [1663 ports] at 20:44
The SYN Stealth Scan took 8.85s to scan 1663 total ports.
Warning:  OS detection will be MUCH less reliable because we did not find at least 1
open and 1 closed
 TCP port
Host 192.168.1.101 appears to be up ... good.
All 1663 scanned ports on 192.168.1.101 are: closed
MAC Address: 00:11:9F:DD:21:DC (Nokia Danmark A/S)
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SInfo(V=3.75%P=i686-pc-linux-gnu%D=4/10%Tm=4259C861%O=-1%C=1%M=00119F)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(Resp=Y%DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

Nmap run completed -- 1 IP address (1 host up) scanned in 42.023 seconds
```

Note: Scanning all port disconnected the device from Wireless connection. Port scan reduced to default setting, as first complete SYN scan found no open ports

© SANS Institute 2005 Author retains full rights.

Appendix 5 – LanGuard NSS Report

```
========================================================================
STARTING SECURITY SCAN FOR MACHINE/RANGE: 192.168.1.101
Profile: Default
========================================================================
Validating targets...
      Building computers list...
      Resolving hosts...
      Determining computers that are alive...

-------> (sent 50 bytes)
 01 F8 00 00 00 01 00 00 00 00 00 20 43 4B 41      ........... CKA
 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41      AAAAAAAAAAAAAAA
 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21      AAAAAAAAAAAA..!
 00 01                                             ..

      Pong from 192.168.1.101

<------- (received 60 bytes)
 45 00 00 3C 0C 8E 00 00 45 01 E5 19 C0 A8 01 65      E..<....E......e
 C0 A8 01 64 00 13 52 49 02 00 01 00 61 62 63 64      ...d..RI....abcd
 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 71 72 73 74      efghijklmnopqrst
 75 76 77 61 62 63 64 65 66 67 68 69                  uvwabcdefghi

1 Computer(s) found.
========================================================================
COMPLETED SECURITY SCAN FOR MACHINE/RANGE: 192.168.1.101
Scan Start Time: 17:36:43
Scan Duration: 1 minutes, 22 seconds
========================================================================

========================================================================
STARTING SECURITY SCAN FOR MACHINE/RANGE: 192.168.1.101
Profile: Default
========================================================================
========================================================================
Starting security scan of host [192.168.1.101]...
Time: 17:36:51
========================================================================
Start WMI Network Detection ...
      No connection, remote registry not available on this computer
Collecting Windows OS Information...
Starting port scanning...
      TCP scanning started...
      2 TCP open port(s)
      UDP scanning started...
      29 UDP open port(s)
      Post scanning fingerprint...
      21 - ftp
            Anonymous logins accepted?

-------> (sent 14 bytes)
 55 53 45 52 20 61 6E 6F 6E 79 6D 6F 75 73            USER anonymous

Started vulnerability scan analysis...
      Checking for trojans...
      Checking black listed USB devices...
      Checking black listed Net devices...
      Checking FTP vulnerabilities...
      Checking DNS vulnerabilities...
      Checking mail vulnerabilities...
      Checking service vulnerabilities...
      Checking RPC vulnerabilities...
      Checking miscellaneous vulnerabilities...
      Checking registry vulnerabilities...
      Checking information vulnerabilities...
      CGI probing...
========================================================================
```


© SANS Institute 2005 Author retains full rights.

```
Completed security scan for [192.168.1.101]: 17:38:05.
Scan time: 1 minutes, 13 seconds
======================================================================
======================================================================
COMPLETED SECURITY SCAN FOR MACHINE/RANGE: 192.168.1.101
Scan Start Time: 17:36:43
Scan Duration: 1 minutes, 22 seconds
======================================================================
```

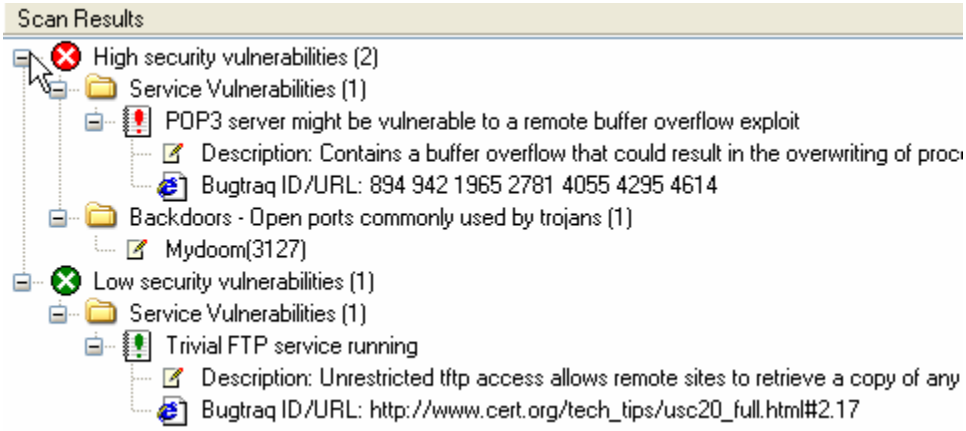
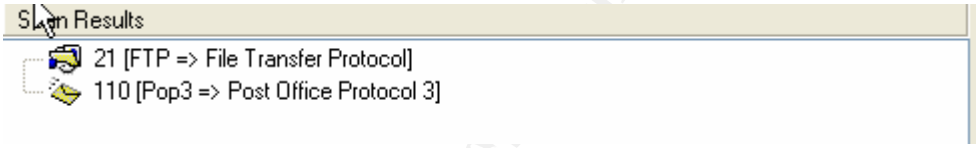
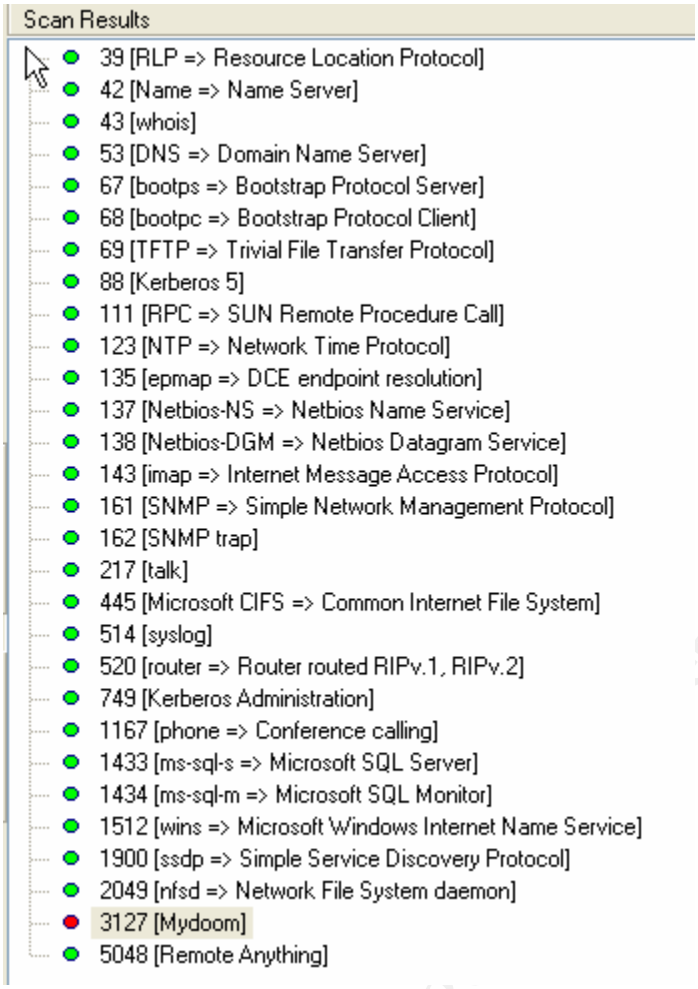
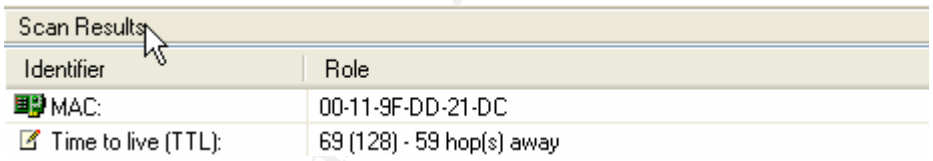


Figure 26 LanGuard NSS reported false positives



© SANS Institute 2005 Author retains full rights.





© SANS Institute 2005 Author retains full rights.

Appendix 6 – eEye Retina Report

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

NETWORK ANALYSIS RESULTS

Report Summary			
Scanner Name	Retina	Machines Scanned	1
Scanner Version	5.0.9.1067	Vulnerabilities Total	0
Scan Start Date	04/10/2005	High Risk Vulnerabilities	0
Scan Start Time	13:49:12	Medium Risk Vulnerabilities	0
Scan Duration	0h 8m 17s	Low Risk Vulnerabilities	0
Scan Name	N9500-All	Information only Audits	0
Scan Status	Completed	Credential Used	- - -

Top 5 Most Vulnerable Hosts
No Vulnerabilities Discovered

Num. of Vulnerabilities By Risk	% of Vulnerabilities By Risk	Avg. of Vulnerabilities By Risk
No Vulnerabilities Discovered	No Vulnerabilities Discovered	No Vulnerabilities Discovered

© SANS Institute 2005 Author retains full rights.

Retina - Network Security Scanner

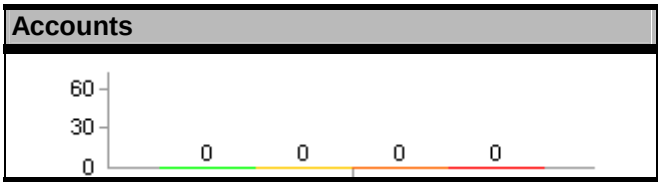
Network Vulnerability Assessment & Remediation Management

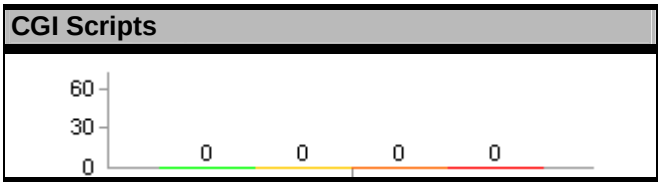
eEye® Digital Security

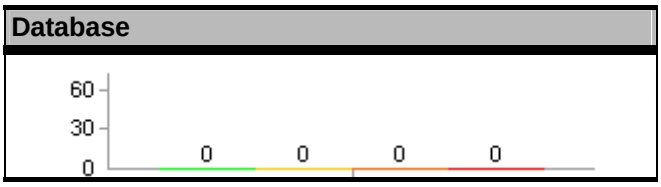
04 October 2005

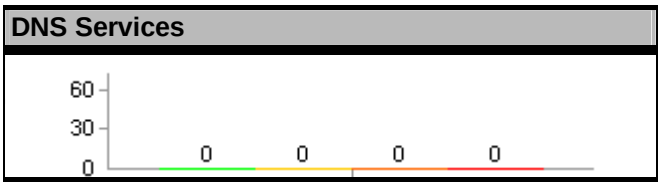
TOTAL VULNERABILITIES BY CATEGORY

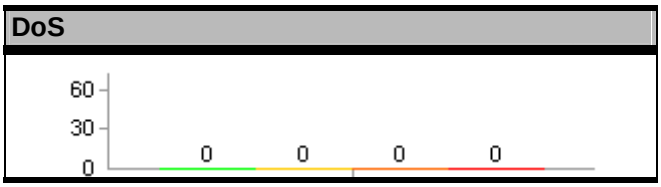
The following is an overview of the total vulnerabilities by audit category.

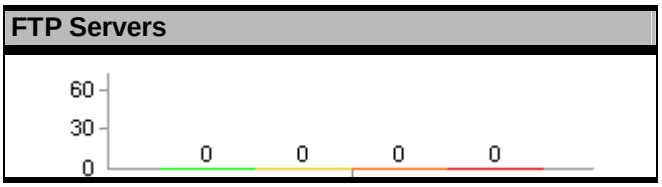


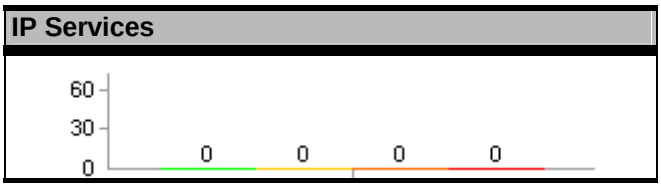


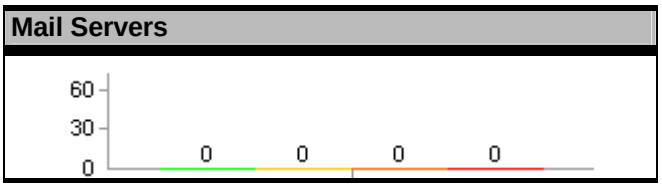


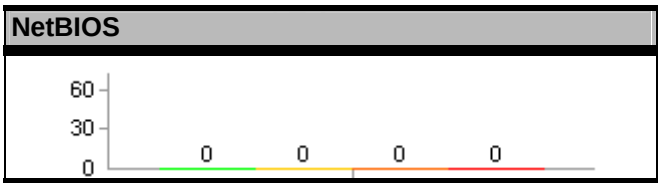


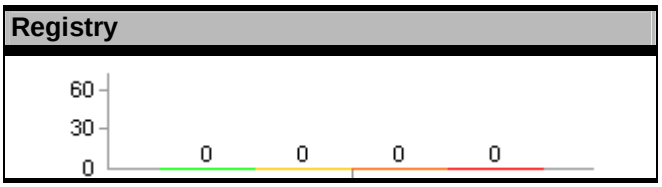


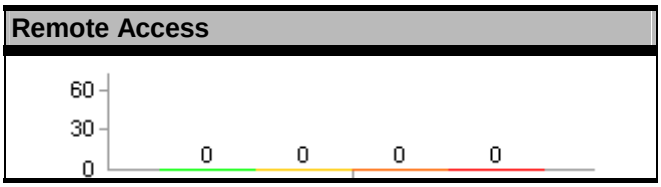


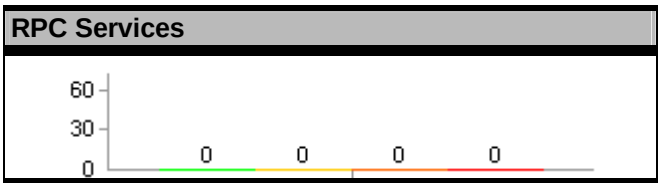


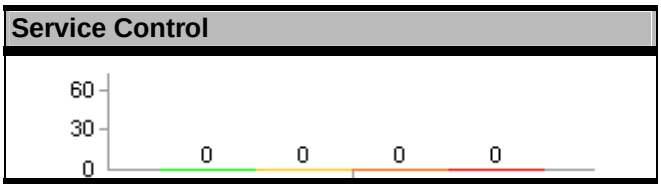


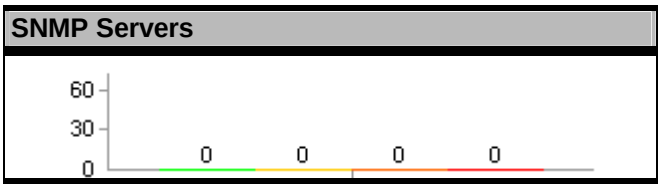




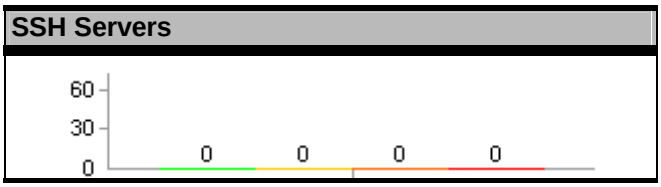


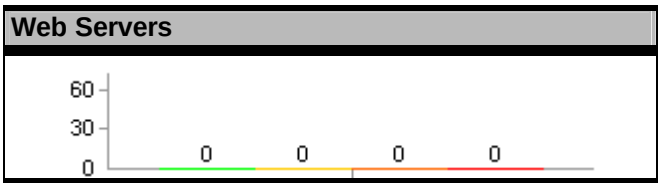


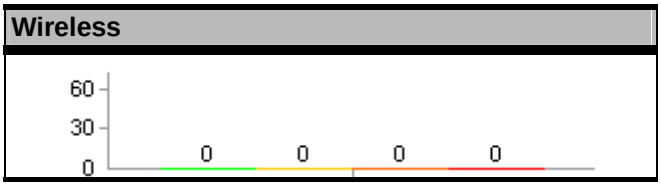


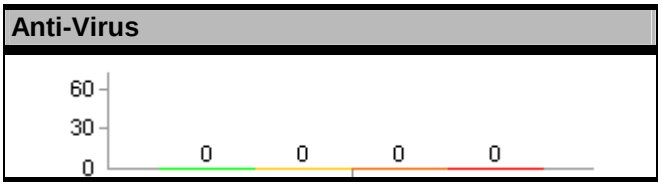


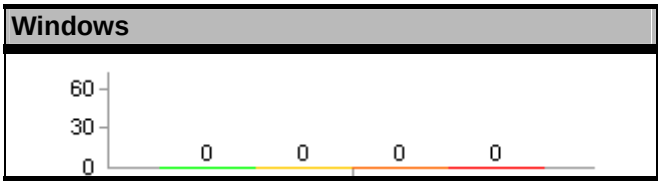
© SANS Institute 2005 Author retains full rights.

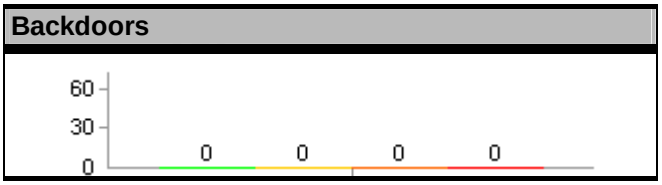


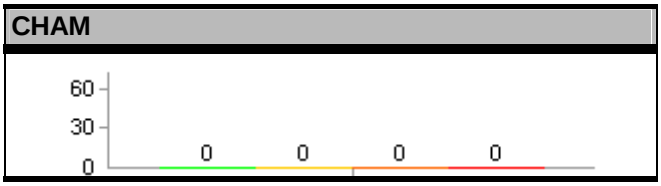


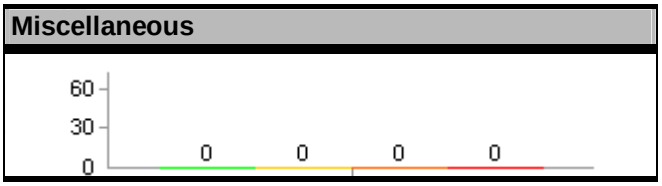


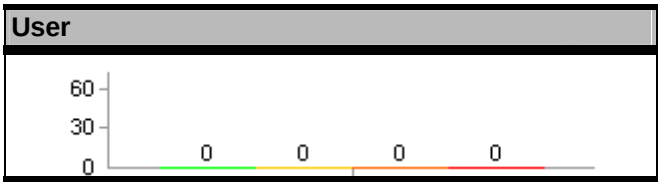


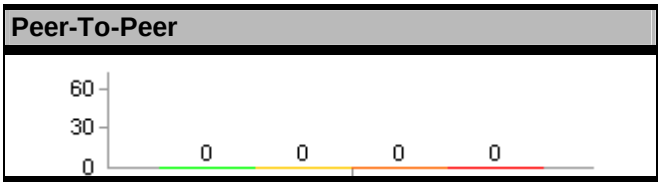












Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

TOP 20 VULNERABILITIES

The following is an overview of the top 20 vulnerabilities on your network.

Rank	Vulnerability Name	Count
No Vulnerabilities Discovered		

© SANS Institute 2005 Author retains full rights.

Top 20 Vulnerabilities
No Vulnerabilities Discovered

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

TOP 20 OPEN PORTS

The following is an overview of the top 20 open ports on your network.

Rank	Port Number	Description	Count
No Ports Discovered			

Top 20 Open Ports
No Ports Discovered

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

TOP 20 RUNNING SERVICES

The following is an overview of the top 20 running services on your network.

Rank	Name	Description	Count
No Services Discovered			

Top 20 Running Services
No Services Discovered

© SANS Institute 2005 Author retains full rights.

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

TOP 20 OPERATING SYSTEMS

The following is an overview of the top 20 operating systems on your network.

Rank	Operating System Name	Count
No Operating Systems Discovered		

Top 20 Operating Systems
No Operating Systems Discovered

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

TOP 20 USER ACCOUNTS

The following is an overview of the top 20 user accounts on your network.

Rank	Account Name	Count
No Users Discovered		

Top 20 User Accounts
No Users Discovered

© SANS Institute 2005 Author retains full rights.

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

TOP 20 NETWORK SHARES

The following is an overview of the top 20 network shares on your network.

Rank	Share Name	Count
No Shares Discovered		

Top 20 Network Shares
No Shares Discovered

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

BOTTOM 20 VULNERABILITIES

The following is an overview of the bottom 20 vulnerabilities on your network.

Rank	Vulnerability Name	Count
No Vulnerabilities Discovered		

Bottom 20 Vulnerabilities
No Vulnerabilities Discovered

© SANS Institute 2005 Author retains full rights.

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

BOTTOM 20 OPEN PORTS

The following is an overview of the bottom 20 open ports on your network.

Rank	Port Number	Description	Count
No Ports Discovered			

Bottom 20 Open Ports
No Ports Discovered

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

BOTTOM 20 RUNNING SERVICES

The following is an overview of the bottom 20 running services on your network.

Rank	Name	Description	Count
No Services Discovered			

Bottom 20 Running Services
No Services Discovered

© SANS Institute 2005 Author retains full rights.

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

BOTTOM 20 OPERATING SYSTEMS

The following is an overview of the bottom 20 operating systems on your network.

Rank	Operating System Name	Count
No Operating Systems Discovered		

Botom 20 Operating Systems
No Operating Systems Discovered

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

BOTTOM 20 USER ACCOUNTS

The following is an overview of the bottom 20 user accounts on your network.

Rank	Account Name	Count
No Users Discovered		

Bottom 20 User Accounts
No Users Discovered

© SANS Institute 2005 Author retains full rights.

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

BOTTOM 20 NETWORK SHARES

The following is an overview of the bottom 20 network shares on your network.

Rank	Share Name	Count
No Shares Discovered		

Bottom 20 Network Shares
No Shares Discovered

Retina - Network Security Scanner

Network Vulnerability Assessment & Remediation Management

eEye® Digital Security

04 October 2005

GLOSSARY

The following is glossary of common terms used throughout this report.

- **DoS Attack:** A Denial of Service (DoS) attack is a remote attack against a servers TCP/IP stack or services. DoS attacks can saturate a servers bandwidth, saturate all available connections for a particular service, or even crash a server.

- **Exploit:** A script or program that takes advantage of vulnerabilities in services or programs to allow an attacker to gain unauthorized or elevated system access.

- **Host:** A node on a network. Usually refers to a computer or device on a network which both initiates and accepts network connections.

© SANS Institute 2005 Author retains full rights.

- **IP Address:** The 32-bit address defined by the Internet Protocol in STD 5, RFC 791. It is usually represented in dotted decimal notation. Any device connected to the Internet that used TCP/IP is assigned an IP Address. An IP Address can be likened to a home address in that no two are alike.

- **Netbios:** Network Basic Input Output System. The standard interface to networks on IBM PC and compatible networks.

- **Ping:** A program used to test reachability of destination nodes by sending them an ICMP echo request and waiting for a reply.

- **Port:** A port in the network sense is the pathway that a computer uses to transmit and receive data. As an example, Web Servers typically listen for requests on port 80.

- **Registry:** The internal system configuration that a user can customize to alter his computing environment on the Microsoft Windows Platform. The registry is organized in a hierarchical structure of subtrees and their respective keys, subkeys, and values that apply to those keys and subkeys

- **Risk Level - Info:** Retina may provide additional information about a host that does not necessarily represent a security threat, but may be useful to the administrator in order to better assess the security of the host, or the network at large. These alerts are displayed with the list of discovered vulnerabilities, and are indicated by a green 'I' icon.

- **Risk Level - Low:** A low-risk vulnerability is typically one that only presents a threat in specific and unlikely circumstances. Such a vulnerability may provide an attacker with information that could be combined with other, higher-risk vulnerabilities, in order to compromise the host or its users.

- **Risk Level - Medium:** Medium-risk vulnerabilities are serious security threats that would allow a trusted but non-privileged user to assume complete control of a host, or would permit an untrusted user to disrupt

© SANS Institute 2005 Author retains full rights.

service or gain access to sensitive information.

- **Risk Level - High:** A vulnerability is designated as high-risk if it would allow a user who has not been given any amount of trust on a susceptible host to take control of it. Other vulnerabilities that severely impact the overall safety and usability of the network may also be designated as high-risk.

- **Service:** A service is a program running on a remote machine that in one way or another provides a service to users. For example, when you visit a website the remote server displays a web page via its web server service.

- **Share:** A folder, set of files, or even a hard drive partition set up on a machine to allow access to other users. Shares are frequently set up with incorrect file permissions which could allow an attacker to gain access to this data.

- **Sniffer:** frequently attackers will place a sniffer program on a compromised machine. The sole purpose of a sniffer is to collect data being transmitted on the network in clear-text including usernames and passwords.

- **Subnet:** A portion of a network, which may be a physically independent network segment, which shares a network address with other portions of the network and is distinguished by a subnet number.

- **Vulnerability:** A weakness or a flaw in a program or service that can allow an attacker to gain unauthorized or elevated system access.

© SANS Institute 2005 Author retains full rights.

Appendix 7 – Nessus Result

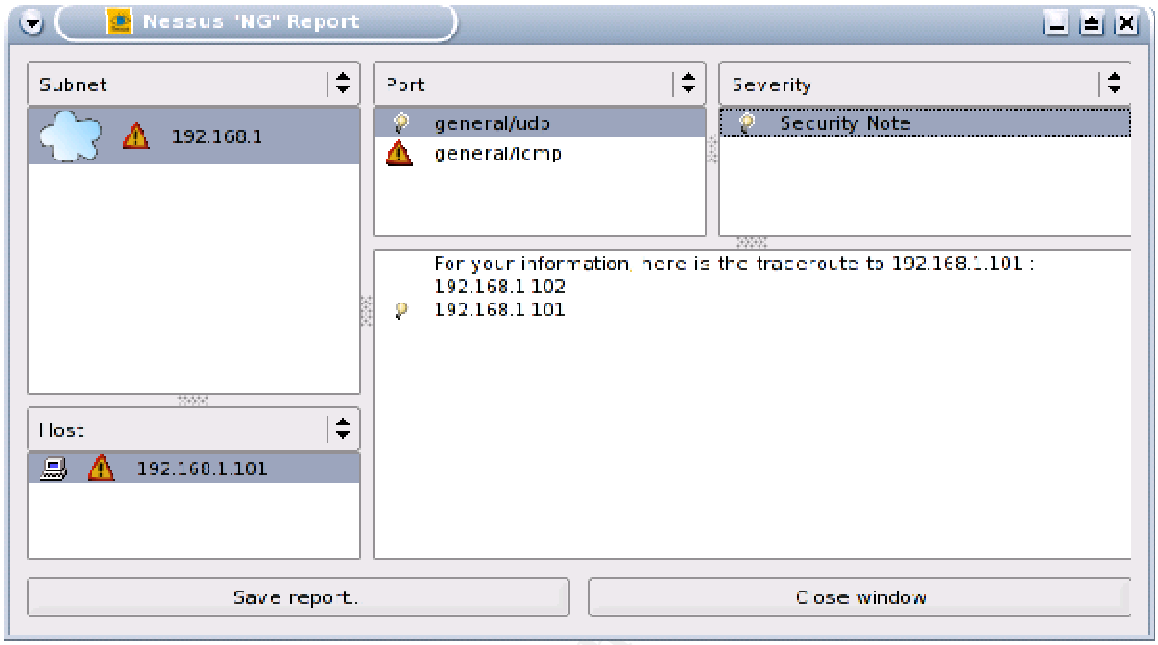


Figure 27 No vulnerability noted on UDP

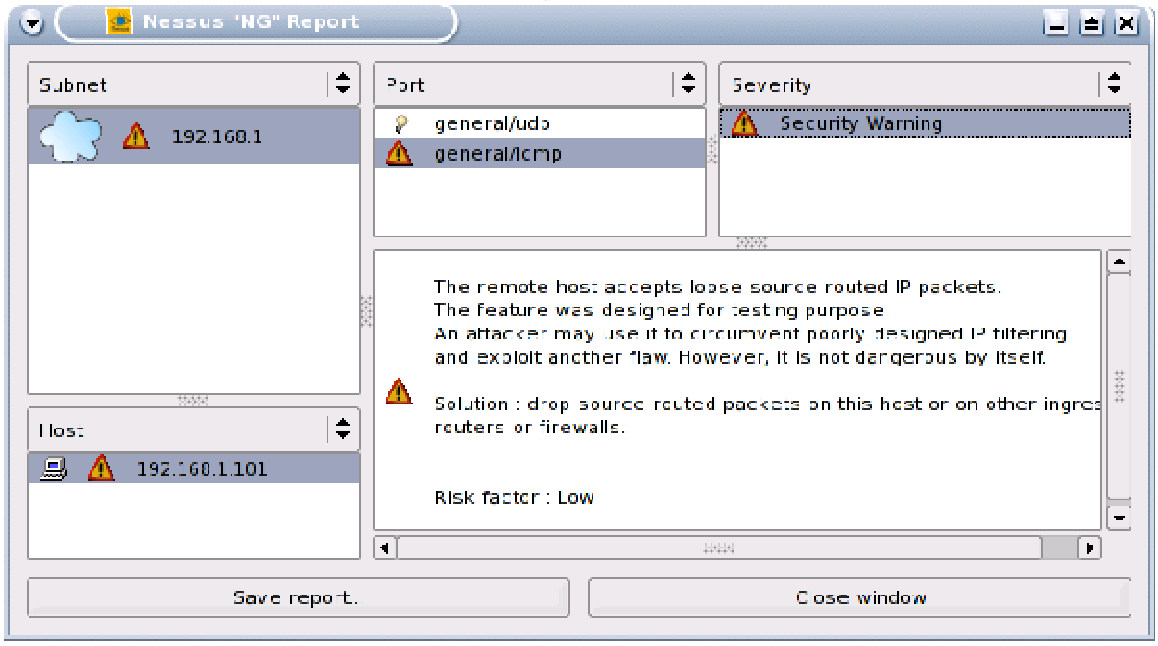


Figure 28 Low risk on ICMP

© SANS Institute 2005 Author retains full rights.