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
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Table of Contents

Introduction 2
Why is Vulnerability Assessment important? 2
Network-based Vulnerability Assessment 3
What is it? 3
How the tools work? 3
Retina by eEye Digital Security 3
Introduction 3
Policy 4
List of Audits 4
Functionality 5
Reports 5
Strategy 6
Pros 6
Host based Vulnerability Assessment 8
What is it? 8
How the tools work? 8
Enterprise Security Manager by Symantec 8
Introduction & Components 8
Modules 10
Security 10
Query 10
Strategy 10
Pros 11
Limitations of Vulnerability Assessment 13
Conclusion 13
References 14

© SANS Institute 2004, Author retains full rights.

Name: Sameer Mathur
Version: 1.4b GSEC Practical Assignment.
Option 1-Research on Topics in Information Security.
Date: 17th November, 2003
Title: Vulnerability Assessment-Host and Network based

Vulnerability Assessment- Network and Host based

Introduction

Security is one of the most challenging and complex issue facing corporate Information Technology (IT) today. Security breaches cost organizations millions of dollars in financial losses each year. Although 99% of all attacks result from known vulnerabilities and faulty misconfigurations, a solution is not straightforward. With a myriad of networks, operating system and application-related vulnerabilities, security professionals are becoming increasingly aware of the need to assess and manage potential security risks on their networks and systems. This necessitates a more efficient and intelligent approach to fortifying the enterprise. [1]

Vulnerability Assessment (VA) is the process of measuring and prioritizing risks associated with network and host-based systems to allow rational planning of technologies and activities that manage business risk. Vulnerability Assessment (VA) tools allow customization of security policy, automated analysis of vulnerabilities, and creation of reports that effectively communicate security vulnerability discoveries and detailed corrective actions to all levels of an organization.

Why is Vulnerability Assessment important?

Vulnerability Assessment involves design, development and review of security policies, procedures, and standards, and validation of the state of security of the information technology infrastructure. [2]

[1] www.foundstone.com
[2] www.symantec.com/region/mx/product/policy/vul_assessment.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Network Based Vulnerability Assessment

What is it?

Network based vulnerability assessment tools perform automated, distributed or event driven probes of geographically dispersed network services, operating systems, routers/switches, mail servers, web servers, firewalls and applications and display scan results and remediation information.[3]

How the tools work?

Most network vulnerability assessment tools use "stack fingerprinting". Stack Fingerprinting is the ability to identify various consistent properties of the TCP/IP stack on a remote host by matching packets sent in response to a condition initiated by the vulnerability assessment tool. [4]

Network vulnerability-scanning tools can be broken down to the following common set of elements:[5]

- Vulnerability database-This element is the brain of the vulnerability scanner. It contains a list of vulnerabilities for a variety of systems and describes how those vulnerabilities should be checked.
- User configuration tool-By interacting with this component of the vulnerability scanner, the user selects the target systems and identifies which vulnerability checks should be run.
- Scanning engine-This element is the arms and legs of the vulnerability scanner. Based on the vulnerability database and user configuration, this tool formulates packets and sends them to the target to determine whether vulnerabilities are present.
- Knowledge base of current active scan-This element acts like the short-term memory of the tool, keeping track of the current scan, remembering the discovered vulnerabilities, and feeding data to the scanning engine.
- Results repository and report generation tool-This element is the mouth of the vulnerability scanner, where it says what it found during a scan. It generates reports for the users, explaining which vulnerabilities were discovered on which target hosts.

Some of the commonly used network vulnerability scanners are:

- Nessus, by Nessus Project team
- CyberCop Scanner by Cyber Associates
- Internet Scanner by Internet Security Systems
- NetRecon by Symantec, Inc
- Retina by eEye Digital Security

Retina by eEye Digital Security is one of the top rated network vulnerability

[3] http://documents.iss.net
[4] http://www.ncircle.com/products/analysis.html
[5] Counter Hack: A Step-By-Step Guide to Computer Attacks and Effective Defenses (Prentice Hall PTR, 2001), by Ed Skoudis

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

assessment scanners in the industry. With Retina's unique, artificial intelligence technology called Common Hacker Attack Methods or CHAM, Retina is able to think like a hacker or network security analyst attempting to penetrate your network. CHAM Modules are a feature in Retina that attempt to exploit or overflow RFC compliant commands on various services such as SMTP, HTTP, FTP and POP3. CHAM Modules can be used to find unknown vulnerabilities in the following services: HTTP, FTP, SMTP, and POP3. In this way, Retina can actually detect previously unknown or hidden vulnerabilities, giving the knowledge needed to better secure your networks. Since eEye is a recognized digital security research powerhouse, Retina incorporates the most comprehensive and up-to-date vulnerabilities database. Along with constantly monitoring security advisories, eEye frequently has advanced knowledge of security issues due to discoveries made by its own team of security experts. Retina incorporates the Nmap (Network Mapper) Fingerprint Database, an open-source utility for network exploration and the most complete database of OS TCP/IP stack fingerprints available. Nmap uses raw IP packets in novel ways to determine which hosts are available on the network, services or ports they are offering, operating system they are running and what type of packet filters/firewalls are in use. Retina uses smart protocol scanning, not making any assumptions about typical protocols running behind specific ports. It analyzes the input/output data on each port to determine which protocol and service is actually running. It has remote repair capability, allowing automatically to correct common system security issues such as registry settings and file permissions. Retina can function remotely across any size network, giving freedom and flexibility of operating from a single location. It also detects rogue wireless access points, which may have been established on the network.[6]

A Retina "Policy" contains the scan (force or normal) along with ports and audit settings used to perform a scan. In a normal scan, Retina will wait for a response from the target computer before beginning a scan. With the force scan setting enabled, Retina will not ping the target machine at all. Retina will scan the target machine regardless if it responds to pings or not. A Retina audit is a single security check, or a single security audit for particular security vulnerability. Retina contains a database of audits that the scanner module uses to search a computer for security flaws.

Following are the list of Audits performed by Retina:[7]

- •Accounts
- CGI scripts
- CHAM (Common Hacker Attack Methods)
- Database
- DNS services
- DOS (Denial of service)

[6] http://www.eeye.com/html/Products/Retina
[7] http://www.eeye.com/html/Products/Retina/RTHs/index.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- FTP servers
- IP Services
- Mail Servers

From a functionality perspective, Retina has 4 modules i.e. Scanner, Miner, Tracer and Browser.[8]

- The Scanner Module is the starting point for a network audit; it scans for all known open ports and services on the specified target IP address. Based on its findings, the scanner module will search available services or open ports for security vulnerabilities. The scanner module also has the feature to determine what protocol is running on a port using protocol detection.
- The Miner Module is the first of many agents to be released for the Retina AI (Artificial Intelligence) Engine. It is an HTTP mining application that runs using the AI rules defined in a brain file supplied by the Retina modules. The Miner Module reports any findings based on the web server's response.
- The Tracer module executes a trace route between the computer running Retina, and the target computer. Retina will then show the results in a graphical format in the Content view window. The tracer module is also responsible for collecting any IP addresses of possible gateways, routers and/or proxies that can be found along the network path to the specified IP address.
- The Browser module allows you to browse the Internet from the Retina interface. The Content view contains an embedded version of Internet Explorer. The Details view contains information about the current web page, including the file size, the creation date, the last modification date, and a text dump of the text on the page. The outline section of the Retina interface will list all relevant links including external servers from the pages being viewed.

Retina provides the following customization of reports:[9]

- General
  The General section provides the target computer's IP, the date of the Retina scan, and the domain name of the target computer.
- Audits
  The Audits section provides a list of security vulnerabilities that have been discovered during the scan as well as fixes for vulnerabilities found.
- Machine
  The Machine section gives information about the scanned computer, such as OS name and version.
- Ports
  The Ports section lists all active ports discovered that are specified to be searched for in the policy.
- Services
  The Services section details services installed/active on the remote machine.

[8] Retina 4.9.137. Help Topics->Introduction->Components
[9] Retina 4.9.137. Help Topics->Reports

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Shares
  The Shares section lists all network shares available on the remote machine.
- Users
  The Users section provides specific information on all user accounts discovered on the remote machine.

In addition, Retina can be tuned to send alerts (pop-up, email & messenger) to a security analyst incase a vulnerability of a specified severity is found on a computer that is being scanned. Customized Retina Audits can also be created using the Retina Audit Wizard. It also supports auditing wireless networks.

Network Vulnerability Assessment Strategy

A network vulnerability scan can be approached in two ways: Internal and External. An internal scan is performed from inside the network, to get a full picture of the status of all machines on it. An external scan is performed from a host outside the network, thus outside the router and firewall. This allows the administrator to see his network the way an outside attacker might. The downside of performing only external scans is that it only protects the administrator's network from an outside attacker. It provides no protection from a malicious employee, or from an attacker who has already gained access to the network. Internal scans provide more information, and allow the security administrator to protect against or remedy security flaws more thoroughly.[10] The external IP space in a corporation should be divided into subnets and each subnet scanned (externally) periodically for security vulnerabilities. Also critical parts of the network should be scanned internally to check for configuration errors and application related vulnerabilities. For e.g. In a 3-tier architecture, an external scan can check connections accepted by web servers in the DMZ other than on ports 443(https) and 80(http). An internal scan on the other hand can be used to make sure that there is no direct communication channel back from the web tier to the database tier/internal network (used for system administration). This would ensure that even if the web-tier is comprised the hacker cannot directly get into the database tier or internal network without breaking an additional layer of security.

Pros of Network Vulnerability Assessment [11]

The first tool used in the vulnerability assessment process should be a network scanner. It provides a quick snapshot of the highest risk vulnerabilities like misconfigured firewalls or vulnerable web servers in a DMZ that could provide a stepping-stone to an intruder and allow them to quickly compromise an organization's security. Network-based scanning performs quick, detailed analyses of an enterprise's critical network and system infrastructure from the

[10] http://www.itworld.com/nl/unix_sec/03142002
[11] Network Scanning Strengths in
http://www.isskk.co.jp/customer_care/resource_center/whitepapers/nva.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

perspective of an external or internal intruder trying to use the network to break into systems. They evaluate security risks associated with vendor supplied software and network and systems administration.

There are two main advantages of using a network-based scanner:

- Centralized access to enterprise security information.
  Network-based scanners discover unknown or unauthorized devices and systems on a network, helping determine if there are unknown perimeter points on the network, such as unauthorized remote access servers or connections to insecure networks of business partners. In addition network scanners provide a comprehensive view of all operating systems and services running and available on the network, as well as detailed listings of all system user accounts that can be discovered from standard network resources. This data and corresponding reports give administrators a clear picture of what types of services are actually being used on their network. This information can be used by a network scanner for further vulnerability evaluation, such as using user accounts to test for password strength, or services detected to check for vulnerable services.

- Unique "Network-centric" view of an organization's security risks.
  Network-based scanners assess network-based vulnerabilities by replicating techniques that intruders use to exploit remote systems over the network. These include vulnerable operating system services and daemons, DNS servers, "denial of service" exploits (i.e., "teardrop" and "land"), and low-level protocol weaknesses. Advanced network-based attacks such as protocol spoofing can only be tested thoroughly from the network. They also test vulnerabilities of critical network devices that don't support host-scanning software, including routers, switches, printers, remote access servers and firewalls. Network scanners by using features like stealth scanning for firewalls, specific router vulnerability checks and "brute force" check default user ID and password back doors built in by network device manufacturers.

  Network-based scanners provide "real-world" testing of systems that have already been locked down with host-based assessment tools, such as critical file, database, web and application servers, and firewalls.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Host based Vulnerability Assessment

What is it?

Host-Based vulnerability assessment tools perform policy compliance and report security vulnerabilities, based on standard security practices across the enterprise.

How the tools work?

Most tools use manager/agent architecture, where agents perform scans on workstations/servers and report system conformance to the manager based on the security standards.

Some of the commonly used Host-Based Vulnerability Assessment (VA) tools are:

- Systems Scanner by ISS
- Enterprise Security Manager by Symantec, Inc
- SecurityExpressions by Pedestal Software
- Enterprise Configuration Manager by Configuresoft
- Security Manager by NetIQ

ISS System Scanner and Symantec's Enterprise Security Manager require an agent to be installed on all target systems to provide the system-level access needed to perform the vulnerability assessment. On the other hand, Pedestal Software's SecurityExpressions is agentless though it requires administrator account to perform scans.

Enterprise Security Manager architecture consists of three main components: [12]

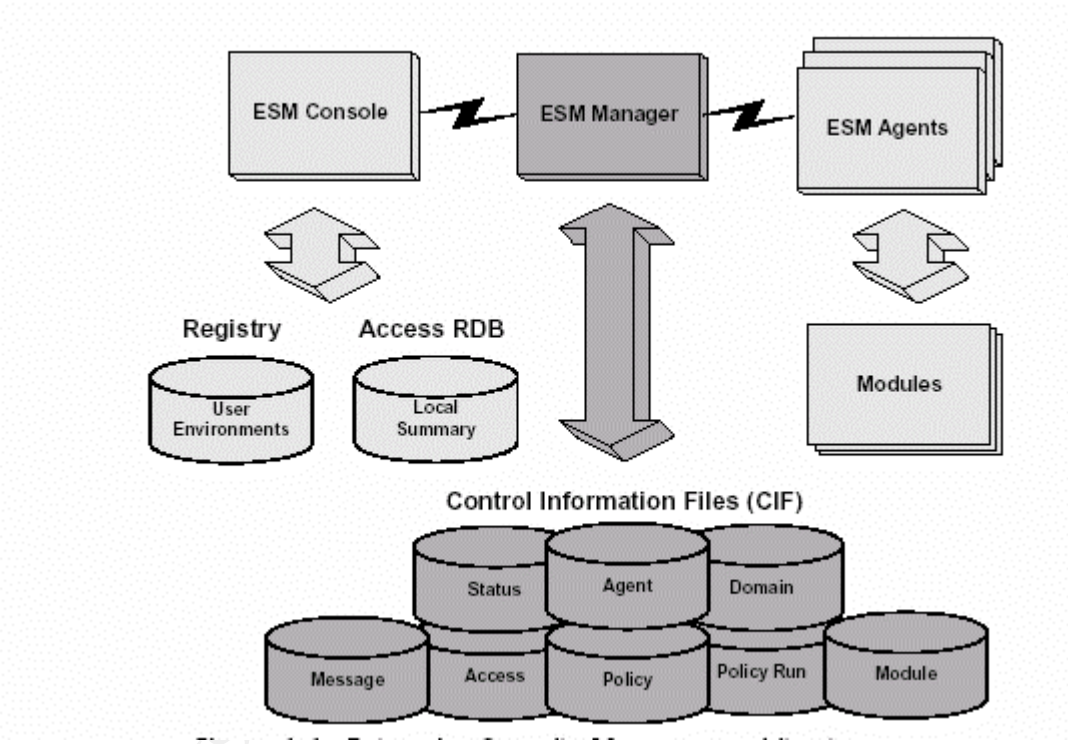
- ESM Agent
  ESM agent is the workhorse of the ESM system. It gathers and interprets the data that pertains to system's security in response to a policy run request from an ESM manager. Security modules in the policy analyze the configuration of the workstation, server, or machine node where the agent resides, or the system where the agent acts as a proxy. The agent server gathers the resulting data and returns it to the manager that initiated the request. The manager responds by updating the appropriate files in its database.
- ESM Manager
  ESM manager controls and stores policy data, passing the data to ESM agents or ESM consoles as needed. It also gathers and stores security data from ESM agents, passing the data to ESM consoles. The manger contains CIF (Control Information files) which store data about manager access, domains, agents, policies, policy runs, templates, suppressions, and the messages output by the security modules in CIF files.

[12] Enterprise Security Manager, Agent/Manager Architecture
ftp://ftp.symantec.com/public/english_us_canada/products/esm/6.0/manuals/esmuser60.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- ESM console (GUI)
  It organizes agents into “Domains” and stores policy information per manager. One instance of the console can manage multiple ESM managers. To initiate a scan, ESM console receives input from the manager and sends scan requests to the agents. After completion of a system scan ESM console formats the information for display, creating spreadsheet reports, pie charts, bar charts, and other visual objects.

In addition, ESM provides the command line interface (CLI) as an alternate way to run security functions.



ESM Host-Based Vulnerability Assessment Architecture from Symantec[13]

ESM uses policies, templates, and modules to identify and evaluate the vulnerabilities of system resources (i.e. servers, clients). These policies form the standard by which ESM measures the security of agent systems. Modules are the most important part of an agent. They are the executables that do the checking at the server or workstation level. ESM agents contain security and query modules.

[13] ESM 6.0 User Guide in http://www.symantec.com/techsupp/enterprise/products/sym_esm/esm_6.0/manuals.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Security modules assess a particular area or aspect of system security. Each module relates to an area of a computing environment that can present a security problem. The following are the main checks in the security modules: 13

- User Accounts and Authorizations
  - Account Information
  - Account Integrity
  - Login Parameters
  - Password Strength
- Network and Server Settings
  - Network Vulnerabilities
  - OS Patches
  - System Auditing
  - Services
- File System and Directories
  - File Attributes
  - File Access
  - Registry Permissions

Query Modules gather general information that relates to security policies along with being useful for system administration. For example, a query module may list all users in a particular group or all users with administrator privileges.

Host Vulnerability Assessment Strategy

Based on the above-mentioned checks, customized polices can be created. These policies can then be used as baselines and systems can be scanned and deviations reported. A good practice would be to come up with security settings (hardened OS policies) for every platform (Windows NT/2000/2003, AIX, Solaris) in the enterprise, create ESM polices/templates based on the security settings and then check compliance of machines to the security policy. In addition, ESM can also be used to check the compliance of a machine to the latest vendor patches. For e.g. Using ESM we can find out that a machine is running IIS but does not have the latest cumulative patch for IIS, therefore is vulnerable and could be compromised by a hacker.

A domain consists of an agent or several agents grouped together for the purpose of running ESM policies. These domains can group agents by function, location, organizational structure such as finance, development, sales or according to any other classification. Depending how agents are organized into domains, separate policies can be created for each domain. Then these domains can be scanned periodically to ensure that they all meet desired security standards. 13

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Pros of Host-based Vulnerability Assessment[14]

Host-based scanning provides insight into potential user activity risks. Their strength lies in direct access to low-level details of a host's operating system, specific services, and configuration details. While a network-based scanner emulates the perspective that a network-based intruder would have, a host-based scanner can view a system from the security perspective of a user who has a local account on the system. They are excellent tools in evaluating security risk associated with all types of user risks.

There are three main advantages of using a host-based scanner:

- Identifies Risky User Activities.

A risky user activity can range from user ignorance to behavior that intentionally violates an organization's security policy for the convenience of the individual user. All types of risky user behavior within this spectrum can potentially compromise the security of all systems in the organization. Users selecting easily guessed passwords or using no passwords, sharing of entire hard drive over the network, either because it is easier than learning the secure method of sharing information, or accidentally, through a default setting for a Windows 95/98 or Windows NT system all fall under risky user activity.

Host-based scanners also have the ability to detect installed devices such as modems and determine if that modem is connected to an active phone line. This type of hardware setup could indicate an unauthorized remote access server that circumvents the organizations firewall and secure dial-in procedures.

- Hacker identification and intrusion recovery (internal or external intruders).

Host-based scanners detect signs that an intruder has already infiltrated a system. These hacker traces include suspicious file names, unexpected new files, device files found in unexpected places and unexpected SUID/SGID privileged programs that have potentially gained "root" privilege. Host-based scanners create cryptographically secure MD5 baselines of critical files, allowing security analysts to compare the current files on a system to a previously known secure state. This process allows detection of any unauthorized changes in these critical system files, such as a "login" program that may have been replaced by a "Trojan horse" back-door. In addition, host-based scanners on Windows NT systems can use baselining to notify administrators of unauthorized changes to registry entries, which contain critical security settings.

By locating "sniffer" programs actively looking for passwords and other critical information, or unauthorized services popular with hackers currently running on the system, such as IRC chat and FSP file transfer servers, Host-based scanners detect signs that an intruder is still currently active on a system.

- Security checks that are impossible or difficult for a network scanner, or are extremely time consuming over a network.

Security checks including password guessing and policy checks, searching for

[14] Host Scanning Strengths in http://www.isskk.co.jp/customer_care/resource_center/whitepapers/nva.pdf

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Windows password hash files (.PWL), and active file share detection are performed significantly faster and more reliably by a host-based scanner. Host-based scanners are ideal for performing resource-intensive baseline and file system checks, which are impractical with network-based scanners and would require that entire contents of hard drives be transferred over the network to the scanning system. They can also check network services to ensure they been correctly configured and implemented, including NFS, HTTPD, and FTP. For example, an incorrectly configured trust relationship under NFS could allow an intruder that has broken into one system to have an open door to all other NFS systems on the entire network.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Limitations of Vulnerability Assessment [15]

Vulnerability scanners are better at detecting well-known vulnerabilities than they are at finding more esoteric ones because it is impossible for any one product to incorporate all known vulnerabilities In addition, manufacturers may elect to exclude some vulnerability detection in order to keep the speed of their scanners high (more vulnerabilities detected require more tests, which slows the overall scanning process).

Vulnerability scanners especially network based scanning can generate significant amounts of network traffic. This traffic may have a negative impact on the hosts and the network being scanned.

Conclusion

While both network and host-based scanning technologies have their unique strengths, using both tools in a coordinated fashion provides the best vulnerability assessment for measuring an organization's security risks. Network-based scanners allow security professionals to assess and correct network-based vulnerabilities, secure network perimeter points on an ongoing basis and strengthen initial lines of defense against intrusion. Host-based scanners provide an additional level of security by locking down individual hosts to prevent critical resources from being accessed by internal misuse or external intruders using compromised accounts.

The key to getting the most out of vulnerability scanning tools is to run scans on a regular basis and/or at critical project milestones i.e. installation or upgrade of system software, modification of user privileges or suspected attack on a system. Scanning a network for vulnerabilities once, fixing those vulnerabilities, and then never scanning it again buys very little in the way of security since new vulnerabilities are found in software every day.

Human factor is truly security's weakest link. Gurpreet Dhillon says in Information Security Management: Global Challenges in the New Millennium "A focus on developing a security culture in the organization goes a long way in developing and sustaining a secure environment." Security is partly a technology problem-more a people and management problem. As better security technologies are invented, it becomes increasingly difficult to exploit technical vulnerabilities, and attackers will turn more to exploiting the human element. Cracking the human firewall is easy, requires no investment beyond the cost of a phone call, and involves minimal risk. [16]

[15] http://www.csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf
[16] The Art of Deception: Controlling the Human Element of Security by Kevin D. Mitnick and William L. Simon

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

1. Foundstone, Inc. “Products Overview”. Products. www.foundstone.com. 2003

2. VA Managed Security Services, Symantec Inc. “Executive Summary”, Symantec Vulnerability Assessment Guide .page 3 http://www.symantec.com/region/mx/product/policy/vul_assessment.pdf

3. Internet Security Systems. “Datasheet”, Internet Scanner 7.0 Documentation. page 1. http://documents.iss.net/literature/InternetScanner/IS7.0_Datasheet.pdf

4. nCircle Network Security, Inc. Products->Features and Benefits-> Discriminant Analysis->Stack Fingerprinting. http://www.ncircle.com/products/analysis.html

5. Skoudis, Ed. “Vulnerability-Scanning Tools”. Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses (Prentice Hall PTR, 2001). September 28,2001. www.informit.com

6. eEye Digital Security.” Superior Vulnerability Assessment & Remediation Management.” Retina® Network Security Scanner. http://www.eeye.com/html/Products/Retina

7. eEye Digital Security.” Home->Products->Retina -> RTH’s.” Retina® Network Security Scanner. http://www.eeye.com/html/Products/Retina/RTHs/index.html

8. eEye Digital Security. “Help->Help Topics->Introduction->Components.” Retina v4.9.137. Retina® Network Security Scanner.

9. eEye Digital Security. “Help->Help Topics->Reports-> The Retina Reporting Interface.” Retina v4.9.137. Retina® Network Security Scanner.

9. Zaborav, Dev. “Know Your Network: How Vulnerable Are You?” Unix Security. 14 March, 2002 http://www.itworld.com/nl/unix_sec/03142002

11. Internet Security Systems. “Network Scanning Strengths”. Network and Host Based Vulnerability Assessment. page 3 http://www.isskk.co.jp/customer_care/resource_center/whitepapers/nva.pdf

12. Symantec, Inc.” ESM Agent/Manager Architecture”. ESM 6.0 User’s Guide. page 16-30. September 16, 2003.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

http://www.symantec.com/techsupp/enterprise/products/sym_esm/esm_6.0/manuals.tml

13. Symantec, Inc.” ESM Agent/Manager Architecture”. ESM 6.0 User’s Guide. page 19. September 16, 2003. http://www.symantec.com/techsupp/enterprise/products/sym_esm/esm_6.0/manuals.html

14. Internet Security Systems. “Host Scanning Strengths”. Network and Host Based Vulnerability Assessment. page 5 http://www.isskk.co.jp/customer_care/resource_center/whitepapers/nva.pdf

15. Peter Mell & Miles C Tracy, National Institute of Standards and Technology. “Vulnerability Scanners”. Procedures for Handling Security Patches. page 21. http://www.csrc.nist.gov/publications/nistpubs/800-40/sp800-40.pdf

16. Kevin D. Mitnick and William L. Simon. “The Human Factor - Security's Weakest Link**”.** The Art of Deception: Controlling the Human Element of Security. page 2, Chapter 1. 2002.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.