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 permitted without express written permission.

Interested in learning more?
Check out the list of upcoming events offering "Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec
Vulnerability Assessments: Methodologies to Perform a Self-Assessment
Nakeva N. Corothers
GSEC v1.4a

Abstract
Vulnerability assessments are a crucial component to network security and the risk management process. Internetworks and Transmission Control Protocol/Internet Protocol (TCP/IP) networks have grown exponentially over the last decade. Along with the advent of this growth, computer vulnerabilities and malicious exploitation have increased. Operating system updates, vulnerability patches, virus databases, and security bulletins are becoming a key resource for any savvy network administrator or network security team. It is the application of the patches and use of knowledge gained from these resources that actually make the difference between a secure network system and a network used as a backdoor playground for malicious hacker attacks. Starting with a system baseline analysis, routine vulnerability assessments need to be performed and tailored to the needs of the company to maintain a network system at a relatively secure level.

There are two types of vulnerability assessments: network-based and host-based. The assessment can be carried out either internally or outsource to a third-party vendor like Foundstone (www.foundstone.com) or Vigilante (www.vigilante.com). The initial vulnerability assessment should be performed internally with collaboration between the Information Technology (IT) department and upper management using the host-based approach. The scope of this paper outlines methods and guidelines to perform a basic host-based vulnerability assessment with a review of the risk management process, performing a system baseline assessment, and finally, a basic vulnerability assessment. All examples are based on Windows NT/2000 operating system and can be applied to both the server or desktop architecture.

1.0 Risk Management Overview
Prior to conducting the assessment, consider the big picture of risk management. Risk management is the general process of taking necessary steps towards implementing a secure network production environment by providing clear policies and procedures outlining the basic needs and expectations of a corporate network security structure. The main output of interest is the working security policies and parties responsible for maintaining the network systems. The vulnerability assessment is only a part of this larger picture and is “a combination of people, policies, procedures and technologies.” [6] The System Administration, Networking and Security (SANS) outline for the risk assessment process is:

I. Threat assessment and analysis
This is a simple blueprint methodology to work towards a secure network system. Threats to network and information security exist because of common vulnerabilities and the advent of tools that exploit those weak points. Knowing the risks involved with the threat to a system and the vulnerability associated with that threat establishes goals for the vulnerability assessment. As an example of common vulnerabilities and the threat to a network environment, figure 1 shows the extent of risk if a system is not configured properly and regular assessments performed.

![Graph showing risk, threat, and vulnerability](www.trendmicro.com)

**Figure 1. Example of risk, threat, and vulnerability (www.trendmicro.com)**

\[ \text{Risk} = \text{Threat} \times \text{Vulnerability} \]
“The beauty of this thing is that it is, again, an age old vulnerability coupled with some wonderful “features” built into the product.” George Bakos [9]. If the server is running Microsoft SQL Server and storing data containing vital customer/client information such as social security numbers, credit card numbers, or medical history, then the JS_SQLSPIDA.B vulnerability represents a high risk. The threat is caused by default software installation settings that leave the ‘sa’ account password blank, running port 1433, and no regular assessment of the environment. The company security policy and a configuration control policy would be valuable in this instance by outlining acceptable network and host configuration and the expectations for regular system maintenance. The security policy would also outline acceptable risk with measures to handle possible intrusions. Knowing your systems and keeping up-to-date with software and operating system patches will make the mitigation of threats an easier process. With the security policy in hand, the process begins with the system baseline analysis.

2.0 System Baseline Analysis

“Before you can assess what you are securing or about to audit it is important to understand what it is you are protecting.” Justin Kapp [8]. A great way to begin the security cycle of Prevention, Detection, and Response is to know what needs protection, i.e. your network servers and workstations. Three security tenets to focus on when gathering information about the network are availability, confidentiality, and integrity. These tenets are explained as, “Availability requires protection of information or services to ensure support on a timely basis to meet mission requirements or to avoid substantial losses. Integrity requires protection of information from unauthorized, unanticipated, or unintentional modification (includes detection of such activities). Confidentiality requires protection from unauthorized disclosure.” [12] Answering these three questions based on the purpose of the system, services running, operating system, and data stored will present the beginning of the network ideal and considerations for possible tests needed in the vulnerability scan. Performing a host-based vulnerability assessment focuses on one system at a time and provides insight on how systems interact with the network as a whole. Accumulating data from a system will provide the foundation for a picture of “normal” activity and behavior; this is key information in the event of a compromise or for use in weeding out the “false positives” in a vulnerability assessment. Areas to consider when gathering baseline data of a system include:

1. Open ports/processes
2. Running services
3. Loaded drivers
4. User/Group information
5. Registry entries
6. Event logs
There are several tools available to aid this process. Tools on the Windows Resource Kit cd-rom include: dumpel.exe, pstat.exe, and drivers.exe. Systernals, www.systernals.com, has a package called Ptools with utilities like pslist.exe, psservice.exe, and psinfo.exe to document services, processes, drivers, and host information. Somarsoft, www.somarsoft.com, provides free tools, DumpSec, DumpEVT, and DumpReg to easily document user/group permissions, registry information, as well as policies, services, and rights. Foundstone, www.foundstone.com, also offers free tools such as Fport and Vision to provide a methodical means of mapping processes to ports for baseline documentation. G-Lock Software, www.glocksoft.com, offers Advanced Administrative Tools as an overall administration/monitoring tool. The application is provided with most features of the licensed version, $49.95 single-license, with the exception of the reporting capabilities; it remains useful even without the ability to create reports simply for viewing and comparing with similar data gathered using other tools. Another application of interest for system information and configuration management is Belarc, www.belarc.com, which can be used to document installed software, software licenses, operating system, as well as motherboard type, memory and hardrive data, and drive information. Generally, install and run Belarc as well as the Windows NT Diagnostics program before installing any of the listed programs. Listed below is a table to compare baseline data objectives with the tools needed to gather the information.

<table>
<thead>
<tr>
<th>WINDOWS TOOLS</th>
<th>THIRD-PARTY TOOLS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PORTS/PROCESSES</strong></td>
<td></td>
</tr>
<tr>
<td>Netstat.exe</td>
<td>Fport.exe</td>
</tr>
<tr>
<td>Pstat.exe</td>
<td>Vision.exe</td>
</tr>
<tr>
<td>Task manager</td>
<td>Advanced Administrative Tools</td>
</tr>
<tr>
<td></td>
<td>Pslist.exe</td>
</tr>
<tr>
<td><strong>SERVICES</strong></td>
<td></td>
</tr>
<tr>
<td>Windows NT Diagnostics</td>
<td>DumpSec</td>
</tr>
<tr>
<td></td>
<td>Advanced Administrative Tools</td>
</tr>
<tr>
<td></td>
<td>Psservice.exe</td>
</tr>
<tr>
<td><strong>DRIVERS</strong></td>
<td></td>
</tr>
<tr>
<td>Windows NT Diagnostics</td>
<td>Advanced Administrative Tools</td>
</tr>
<tr>
<td>Administrative Tools (Windows 2000)</td>
<td>DumpSec</td>
</tr>
<tr>
<td>Drivers.exe</td>
<td></td>
</tr>
<tr>
<td><strong>USER/GROUP information</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DumpSec</td>
</tr>
<tr>
<td><strong>REGISTRY information</strong></td>
<td></td>
</tr>
<tr>
<td>Regedit.exe; export and save</td>
<td>DumpReg</td>
</tr>
<tr>
<td></td>
<td>DumpSec</td>
</tr>
</tbody>
</table>
**EVENT LOGS**

<table>
<thead>
<tr>
<th>Event Viewer</th>
<th>DumpEVT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dumpel.exe</td>
<td></td>
</tr>
</tbody>
</table>

**TABLE 1. Baseline objectives and tool comparison**

### 2.1a Baseline: Ports

Gathering information on listening/open ports will show normal operation of network TCP/IP communication from the target host; this information will also present an input variable used in the vulnerability analysis by knowing what ports are identified as acceptable according to installed applications and known running services. To start simple, open a command-prompt and type: the `netstat –an` command (to print to file, type: `netstat –an >> [filename.txt]`). Identify all listening ports and verify any possible applications using the services on these ports.

![Figure 2. Netstat example](image)

The next tool to use is fport.exe, which will map processes to ports to compare listening ports with running system services or applications. Installation of Fport only requires extracting to a location, `c:\fport` for example, open a command-prompt, type: `cd fport`, then type: `fport` (to print to file, type: `fport >> [filename.txt]`). The output on screen and in the file shows the following:

FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

<table>
<thead>
<tr>
<th>Pid</th>
<th>Process</th>
<th>Port</th>
<th>Proto</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>System</td>
<td>21</td>
<td>TCP</td>
<td>C:\WINNT\System32\inetsrv\inetinfo.exe</td>
</tr>
<tr>
<td>121</td>
<td>inetinfo</td>
<td>21</td>
<td>TCP</td>
<td>C:\WINNT\System32\inetsrv\inetinfo.exe</td>
</tr>
<tr>
<td>2</td>
<td>System</td>
<td>70</td>
<td>TCP</td>
<td>C:\WINNT\System32\inetsrv\inetinfo.exe</td>
</tr>
<tr>
<td>121</td>
<td>inetinfo</td>
<td>80</td>
<td>TCP</td>
<td>C:\WINNT\System32\inetsrv\inetinfo.exe</td>
</tr>
</tbody>
</table>
The comparison of the output data from netstat and fport indicate a win32 platform using TCP/IP settings for NETBIOS services on ports 137, 138, and 139; the target host is also running the basic IIS server processes such as File Transfer Protocol (FTP) on tcp port 21, Gopher on tcp port 70, and the World Wide Web HTTP port 80. The implication here is to verify the target host has a version of IIS installed, configured and running; then search for the operating system service pack level and IIS patches. Several Trojans and worms exist, such as the infamous NIMDA, Back Orifice, or Qaz that compromise networks through these ports testing system availability, confidentiality and integrity. In a vulnerability assessment, a port scan is performed and will list all open ports, thereby pointing out how to make use of crafted TCP packets and connection attempts to these ports.

The “Open Source Security Testing Methodology Manual” [1] suggests the following during the port scanning security test:

   This module is to enumerate live or accessible Internet services as well as penetrating the firewall to find additional live systems.

   Enumerate Systems
   • Use TCP fragments in reverse order with FIN, NULL, and XMAS scans on ports 21, 22, 25, 80, and 443 for all hosts in the network.
   • Use FTP and Proxies to bounce scans to the inside of the DMZ for ports 22, 81, 111, 132, 137, and 161 for all hosts on the network.

Clearly, having baseline information on ports is vital information for both system maintenance and vulnerability analysis.

2.1b Baseline: Processes

To obtain a nice list of running processes use pstat.exe, pslist.exe, and in Windows NT use Task Manager. To use pslist.exe, extract the executable to a location on the hardrive, c:\pslist for example, open a command-prompt and type: cd pslist, then type: pslist (to print to file, type: pslist >> [filename.txt]). The information is listed as follows:

PsList v1.2 - Process Information Lister
Copyright (C) 1999-2002 Mark Russinovich
Sysinternals - www.sysinternals.com
Pstat is a Windows 2000 utility that will list processes first as a list then details about each specific process. A list of loaded drivers can be found at the end of the report. Listed below is example output including details for the first two listed processes.

Pstat version 0.3: memory: 523568 kb uptime: 5:11:24:52.403
### Two great GUI applications to list processes, drivers, and services are

- Vision.exe will work like fport.exe with added features of a graphical user interface listing running applications in real-time, running services, loaded drivers and the ability to log the TCP/IP port and process mappings. Advanced Administrative Tools Process Monitor module will do all the above with the beneficial feature of creating reports in several formats such as HTML, MS Excel, MS Access, etc.; however, this report feature is only available in the licensed version. Listed below are screenshots of both applications.

<table>
<thead>
<tr>
<th>Process ID</th>
<th>PID</th>
<th>Priority</th>
<th>Start Time</th>
<th>User Time</th>
<th>Kernel Time</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
<td>0</td>
<td>00:00:00</td>
<td>00:00:30</td>
<td>00:00:00</td>
<td>Waiting</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>0</td>
<td>00:00:00</td>
<td>00:00:30</td>
<td>00:00:00</td>
<td>Waiting</td>
</tr>
</tbody>
</table>

Two great GUI applications to list processes, drivers, and services are Foundstone's Vision.exe and G-Lock Software's Advanced Administrative Tools. Vision.exe will work like fport.exe with added features of a graphical user interface listing running applications in real-time, running services, loaded drivers and the ability to log the TCP/IP port and process mappings. Advanced Administrative Tools Process Monitor module will do all the above with the beneficial feature of creating reports in several formats such as HTML, MS Excel, MS Access, etc.; however, this report feature is only available in the licensed version. Listed below are screenshots of both applications.
Figure 3. Foundstone’s Vision.exe Process List Example

Figure 4. G-Lock Software’s Advanced Administrative Tools Process Monitor Example
Figure 5. Example HTML report output from Advanced Administrative Tools

Knowledge of processes running on a system will help understand a normal state of system activity and regular patterns of network interaction. Process information can also give clues to company supported software installed and verification of rouge processes from illegal, or non-company supported programs that would potentially increase network security risk.

2.2 Baseline: Services and Drivers
When an operating system is installed, several default services are also started to assure minimum functionality. However, if, for example, the system objective is to act as an internal file server with internal addressing schemes, then using a default installation of Windows NT would install services to run an IIS web server with remote login capability and use of FTP and Gopher. To verify the function of a system gather information of all services present on a host. This information can be compared to the ports and processes baseline data for a clear picture of what a system is setup to do and how vulnerable it is based on the latest hacker exploits targeting specific services.

In Windows NT use the Windows NT Diagnostics program to create a report of services and drivers running on the system. There are options to print a summary or a complete report; choose the option for a complete report additionally choose to print to a file and add this data with the other reports gathered for future reference.

![Figure 6. Example of Windows NT Diagnostics](image)

Systernals psservice.exe is a tool that will list all services with descriptive information on the service usage and other system values. To use psservice.exe, extract the executable to a location on the hardrive, c:\psservice for example, open a command-prompt and type: cd psservice, then type: psservice (to print to file, type: psservice >> [filename.txt]). The information is listed as follows:
DumpSec is also an excellent application that will list both services and drivers running on a system along with the status of the service and the account under which the service will run. After installing and opening the program, go to the Report menu, scroll down and choose Dump Services. The second pop-up window allows choices of services to display, click the OK button and the list of services will be displayed.
You can save the report as comma-delimited text and the output file shows the following information:

6/25/02 7:48 PM - Somarsoft DumpSec (formerly DumpAcl) - \VENONA (local)
FriendlyName,Name,Status ,Type ,Account
3Com Etherlink 10 ISA Adapter Driver,Elnk3,Running,Kernel,,
3Com TCAITDI Diagnostic TDI,TCAITDI,Running,Kernel,
2.3 Baseline: Users and Groups

User accounts on a network represent portals of access to company information and applications. Groups are used to organize user account privileges and access rights to the network and information. Keeping track of user accounts and access policies is an important aspect of regular network administration. If an attacker, internal or external, could enumerate a network gathering information on open ports, services running, and determine the operating system, knowing user account information and the group structure could prove a deadly confidentiality compromise. Baseline data gathered for user account structure and groups will help verify known accounts and the settings then differentiate any accounts that may have been modified or replaced in an attempt to subvert normal system activity.

Although use of the `net` command or the Resource Kit tool `addusers.exe` will suffice in gathering user and groups data, the DumpSec program is an excellent GUI tool that offers several options to view and report user and group information. Permissions can be reviewed for users and groups that would take more time than necessary to sift through within the modules of the built-in Administrative Tools of Windows NT and Windows 2000. The ability to gather the information and export the data in .csv format puts the administrator in control of regular assessment documentation and analysis. Below are examples of the .csv reports from DumpSec list of user and group information.

User:

6/25/02 8:13 PM - Somarsoft DumpSec (formerly DumpAcl) - \VENONA (local)
**Administrator**

Groups, Administrators (Local, Members can fully administer the computer/domain)
Groups, Domain Admins (Global, Designated administrators of the domain)
Groups, Domain Users (Global, All domain users)

**FullName**

**AccountType**, **User**

**Comment**, Built-in account for administering the computer/domain

**HomeDrive**

**Profile**

**LogonScript**

**Workstations**

PswdCanBeChanged, Yes
PswdLastSetTime, 10/15/01 9:03 AM
PswdRequired, Yes
PswdExpire, No
PswdExpiresTime, Never
AcctDisabled, No
AcctLockedOut, No
AcctExpiresTime, Never
LastLogonTime, 7/5/02 7:23 PM
LastLogonServer, VENONA
LogonHours, All
Sid, S-1-5-21-592014603-2105167985-1190612905-500
RasDialin, No
RasCallback, None
RasCallbackNumber

**Guest**

Groups, Domain Guests (Global, All domain guests)

**FullName**

**AccountType**, **User**

**Comment**, Built-in account for guest access to the computer/domain

**HomeDrive**

**Profile**

**LogonScript**

**Workstations**

PswdCanBeChanged, No
PswdLastSetTime, Never
PswdRequired, Yes
PswdExpire, No
PswdExpiresTime, ?Unknown
AcctDisabled, Yes
AcctLockedOut, No
AcctExpiresTime, Never
LastLogonTime, Never
LastLogonServer, VENONA
LogonHours, All
Sid, S-1-5-21-592014603-2105167985-1190612905-501
RasDialin, No
RasCallback, None
RasCallbackNumber

**IUSR_VENONA**

Groups, Domain Users (Global, All domain users)

Groups, Guests (Local, Users granted guest access to the computer/domain)

**FullName**, Internet Guest Account

**AccountType**, **User**

**Comment**, Internet Server Anonymous Access

**HomeDrive**

**Profile**

**LogonScript**

**Workstations**

PswdCanBeChanged, No
PswdLastSetTime, 10/15/01 9:06 AM
PswdRequired, Yes
PswdExpire, No
PswdExpiresTime, Never
AcctDisabled, No
AcctLockedOut, No
AcctExpiresTime, Never
LastLogonTime, 6/12/02 8:27 AM
LastLogonServer, VENONA
LogonHours, All
Sid, S-1-5-21-592014603-2105167985-1190612905-1001
RasDialin, No
RasCallback, None
RasCallbackNumber

---

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.
Groups:

- Domain Admins, Designated administrators of the domain, Global
  - Administrator,, User
- Domain Guests, All domain guests, Global
  - User
- Domain Users, All domain users, Global
  - Administrator,, User
- IUSR_VENONA,, User
- Account Operators, Members can administer domain user and group accounts, Local
  - Administrator,, User
- Backup Operators, Members can bypass file security to back up files, Local
  - Guests, Users granted guest access to the computer/domain, Local
  - Domain Guests,, Global
- IUSR_VENONA,, User
- Print Operators, Members can administer domain printers, Local
  - Replicator, Supports file replication in a domain, Local
- Server Operators, Members can administer domain servers, Local
- Users, Ordinary users, Local
  - Domain Users,, Global

2.4 Baseline: Registry Entries

The Windows registry is like the “Godfather” of the operating system. How the operating system is configured, from desktop icons and software interaction with critical system files to TCP/IP properties and user account settings, stems from entries in the registry. Regular backups and review of the registry can verify placement of unacceptable programs and processes usually attributed to Trojan programs and worms. Both DumpSec and DumpReg are tools to facilitate viewing and reporting of registry information for the baseline assessment and regular systems assessment.

Figure 9. Example using DumpReg to display registry
2.5 Baseline: Event Logs

A key resource to network security is the ability to log information and compare that data for any suspicious activity. Event logs are a good way to see how a system functions in the normal networking environment. The three log types include: application, security, and system. These logs will record application errors, logon attempts, or system-specific errors. Windows NT and Windows 2000 Event Viewer allows quick access to logs as well as options to export the information for baseline data and regular review. The Resource Kit tool dumpel.exe is a command-line utility that can be used to dump event log
information for documentation. Somarsoft's DumpEVT is another tool that will gather event log data for baseline analysis.

![Figure 12. Using dumpel.exe](image-url)

6/13/02 8:33:54 AM 8 6 612 Security DOMAIN1\Administrator VENONA +
+ + + + + + + + + Administrator DOMAIN1 (0x0,0x29C7)
6/13/02 8:34:06 AM 8 3 560 Security DOMAIN1\Administrator VENONA

Security Account Manager SAM_USER DOMAINS\Account\Users\000003E9 1422704 0 47483 2154113888 SYSTEM NT AUTHORITY (0x0,0x3E7) Administrator DOMAIN1 (0x0,0x29C7) %51538 %5440

%5441 %5443 %5444 %5448
6/13/02 8:34:06 AM 8 3 562 Security NT AUTHORITY\SYSTEM VENONA

Security Account Manager 1422704 2154113888 VENONA
6/13/02 8:34:43 AM 8 5 593 Security DOMAIN1\Administrator VENONA

2152688544 Administrator DOMAIN1 (0x0,0x29C7)
6/13/02 8:34:52 AM 8 5 592 Security DOMAIN1\Administrator VENONA

2152688544 IEXPLORE.EXE 2152797440 Administrator DOMAIN1 (0x0,0x29C7)
6/13/02 8:35:23 AM 8 5 593 Security DOMAIN1\Administrator VENONA

2152688544 Administrator DOMAIN1 (0x0,0x29C7)
6/13/02 8:35:42 AM 8 5 592 Security DOMAIN1\Administrator VENONA

2152688544 SETUP.EXE 2152797440 Administrator DOMAIN1 (0x0,0x29C7)
6/13/02 8:35:57 AM 8 5 593 Security DOMAIN1\Administrator VENONA

2152688544 Administrator DOMAIN1 (0x0,0x29C7)
6/13/02 8:36:46 AM 8 5 592 Security DOMAIN1\Administrator VENONA

2152688544 rundl132.exe 2152797440 Administrator DOMAIN1 (0x0,0x29C7)
All the baseline data collected coupled with company policies and network security policies form the outline for a risk and security posture. A method for the actual security assessment can be constructed from the baseline analysis and provide specific tests to perform and expected output for the final vulnerability assessment report. The process of vulnerability assessment and regular testing of the network systems at risk can provide a more thorough insight to the systems vulnerability and lead to actions in securing the network, thereby mitigating the threat of attacks, compromise, and loss of profit.

3.0 The Vulnerability Assessment Overview

A vulnerability assessment aims to identify threats to a network or specific system. A vulnerability can be defined as any flaw or “hole” in a system that presents the opportunity for malicious exploitation, thereby posing a threat against network resources and information. An assessment of system vulnerabilities requires goals, methods to achieve those goals and tools to provide information and analysis. The goals of the assessment are determined by the security requirements of the company and target system, what will be assessed, and the depth of the assessment [9]. A methodology for performing the assessment should be outlined to maximize the information used in determining the security posture. One method suggested in an article aimed at penetration testing suggests the following: discovery, enumeration, vulnerability mapping, and exploitation [10]. A more exhaustive methodology posed by Foundstone, whose founders also co-authored the book, “Hacking Exposed”, suggests the following steps: host discovery, service discovery, operating system identification, service enumeration, network mapping, vulnerability assessment, e-commerce application assessment [11]. To determine which tools to use, consider the points of attack, or threat vectors, to include: outsider attack from network, outsider attack from telephone, insider attack from local network, insider attack from local system, attack from malicious code. These threat vectors as outlined by SANS help determine the perspective needed for the vulnerability assessment.

3.1 Assessment Guides

Many organizations and Information Security professionals conduct security tests and assess risk using numerous methods; there is not just one industry-identified standard to encompass every need of every business network. A good practice would be to review different methods and standards applied in the realm of security audits and assessments before actually conducting your own. Several documents are available as outlines, guidelines, manuals, or checklists to help any IT department complete a security self-assessment. These documents cover various methods for assessing risk, cost-benefit analysis, types of threats to consider, how to perform security tests, and common testing tools. Each of these
guides provides a defense-in-depth style approach to prepare for the vulnerability security self-assessment.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>assessment Guide</td>
<td>for Information Technology</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Questionnaire</td>
<td>Self-directed risk evaluation</td>
<td></td>
<td>Tool usage</td>
<td>Testing techniques</td>
</tr>
<tr>
<td>Outline of standards and point system for questionnaire; Samples provided</td>
<td>General process of long-term risk assessment, threat management, and vulnerability assessment</td>
<td>Sample tool usage; tables of tools; table of testing cycles</td>
<td>Outline of testing; list of tools to use; description of testing technique; sample forms</td>
<td>Outline process of complete risk assessment; good for qualitative and quantitative analysis</td>
</tr>
<tr>
<td>August 2001</td>
<td>December 2001</td>
<td>February 2002</td>
<td>February 2002</td>
<td>October 1999</td>
</tr>
</tbody>
</table>

TABLE 2. Vulnerability Assessment Guides

There exists a basic process between all the assessment guides: plan, organize, gather information, test, analyze, and report. The “Open Source Testing Methodology Manual” (OSSTMM) provides an excellent starting point for anyone, at any level, offering a scientific approach to the art of the vulnerability assessment. For example, descriptions and purpose for each test are given along with expected output or results, and sample templates. With this working knowledge, a tester can perform a variety of tests tailored to a specific system need. This manual is meant to provide a certain level of bias so the security testing team can function within the scope of their particular set of policies and criteria. Another great source to use in comparison, or as a second test, is the National Institute of Standards and Technology (NIST) special publication 800-42, “DRAFT Guideline on Network Security Testing.” The software and system planning cycle is where the focus begins in this document. A good security plan should be implemented from the start when choosing hardware, operating systems, and software. An interesting feature of the publication is the outline of the basic security testing metrics such as network mapping, penetration testing, vulnerability scanning, as well as war dialing. An outline of well-known tools and testing objectives provides a concise understanding of testing techniques and possible testing cycles to implement regular security management. For the enthusiastic security analysis team or network administrator, the “Threat and Risk Assessment Working Guide” (TRAWG) will take an overall risk management perspective providing tables and a point system based on risk, asset value and vulnerability ratings. The process is broken down into nine task areas covering the complete spectrum of risk assessment to include the vulnerability analysis. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method provided by CERT (CERT®/CC) is a self-directed information risk assessment with network and information security at the center of interest. An evaluation is performed in three phases: threat profiles, identification of vulnerabilities, and strategic planning based on the output of the evaluation.
OCTAVE is comprised of several volumes outlining the process, procedures, and methods for a risk assessment; the complete program can be purchased as an IT department training tool. Finally, the NIST special publication 800-26, “Security Self-Assessment Guide for Information Technology Systems” is a government-based security testing and evaluation system. Control objectives and various techniques to carry out specific testing and result analysis are realized through a questionnaire format. The evaluation output can also be a useful input from the business perspective of budget analysis. These guides and manuals offer a spectrum of measures and techniques an organization can employ towards an information security management process and lead to regular, productive, risk analysis through vulnerability assessments.

4.0 The Vulnerability Assessment

Now armed with the security policies, target host baseline analysis, goals, methods, and various guides used to approach the assessment, it is time to actually put the information to use. The combination of assessment guides point out areas to consider during the actual testing. For the purposes of this paper the two documents of interest are the OSSTMM and the NIST sp800-42. These guides offer the quickest route to perform a vulnerability self-assessment using the following core areas:

<table>
<thead>
<tr>
<th>Network Mapping</th>
<th>Vulnerability Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penetration testing</td>
<td>File Integrity checks</td>
</tr>
<tr>
<td>Password cracking</td>
<td>Virus detection</td>
</tr>
<tr>
<td>IDS/Firewall/Log review</td>
<td>War dialing</td>
</tr>
<tr>
<td>Wireless/802.11 Leak checks</td>
<td>Analysis and Report</td>
</tr>
</tbody>
</table>

TABLE 2. Core Areas of Vulnerability Assessment

There are two ways to perform a security test; passive or intrusive [1]. A passive attack will merely gather information that would be available to the general public or easily obtained without illegal implications. The intrusive attack, usually a penetration test, will sometimes actually attempt to thwart security of a system by gaining access, executing Denial of Service (DoS) attacks, password cracking, etc. Considering the broad scope of different testing schemes, this paper will focus on two tests that combine the passive and intrusive attack such as network mapping and vulnerability scanning. The goal here is to get to know a system or network through insight from the security baseline assessment of a target host, then comparing the data with a limited vulnerability assessment.

4.1 Network Mapping

Network mapping is a technique to identify hosts on a network segment. This is the first step to enumerate host names, IP addresses, services running, and possibly operating system fingerprinting. Typically, the information gathered presents both a software picture and an actual map of the network in testing. Common programs used include: Nmap (www.nmap.org), a network port
scanner and security auditing utility; Superscan (www.founstone.com), a full-featured port scanner; LANguard Network Security Scanner (www.gfi.com), a network port scanner, service and share enumerator, OS fingerprinting, service pack level, and vulnerability tests, discussed later. Research of the latest exploits and port probes should be conducted and compared to the information gathered in the security baseline analysis. Websites such as www.securityfocus.com and www.incidents.org are excellent resources to check the top ten attacked ports, current security alerts, and searchable databases of vulnerabilities.

There are three basic steps to network and host mapping: ping, port scan, and reporting. SuperScan is a tool that will cover both the ping and port scan with capabilities to verify open ports and services running. When using SuperScan for the first time, the program opens using the loopback address, 127.0.0.1, in the hostname lookup box. Click the Me button to lookup the local machine name and IP address of the interface. Under the scan type, choose the Ping Only option to ping the host. After the host is listed in the lower screen and shown as active, click the Port list setup button, then under Port list file, click the Load button and choose the hensss.lst file, then click the OK button. Go back to the scan type and choose to scan All selected ports in list, and then click the Start button. SuperScan will perform a ping and port scan of the target host with a listing in the lower window of all open ports. You can save this information to a text file for reference.
The results show four open ports and should be compared to the baseline port data to verify any differences. The information listed in SuperScan for ports 21 and 80 give away banner information of the target host. Knowing the version of the FTP server and the web server, IIS 3.0 in this case, gives an attacker the choice of exploits to use and a guess at the operating system. FTP exploits generally allow anonymous connections and the ability to upload or download files. Countless vulnerabilities exist for all versions of IIS, the most notable being NIMDA and Code Red.

The analysis here shows the security cycle step of Prevention, since the system is not compromised, would be to close ports 21 and 80 and remove the associated services bases on the classification of the server, i.e., web server, file server, application server, etc. The security tenets involved if the system were hacked would be availability, through DoS attacks, and integrity, by using an ftp exploit to upload backdoor Trojan programs or delete files. The threat vectors of concern would be an outside attack from a network or use of malicious code. The Security policy and goals for the vulnerability assessment will determine the next tasks to perform in the vulnerability scan. All baseline data and necessary documentation should be reviewed and possible vulnerabilities researched.

4.2 Vulnerability Scan
The vulnerability scan of a system, whether network-based or host-based, will identify hosts, open ports, and “can help identify out-of-date software version, vulnerabilities, applicable patches or system upgrades, and validate compliance with, or deviation from, the organization’s security policy.” [2] Vulnerability scanners will provide several options in one package allowing automated scanning of a single host or a range of hosts, usually based on an IP address range.

Output from the scan could reveal unnecessary open ports such as TCP port 27374 and 1243, ports used for the popular SubSeven Trojan and Denial of Service (DoS) attacks. The patch level of the operating system or running applications identified in the scan point out the reality of what information is presented to the world either intentionally or in stealth. Additionally, the vulnerability analysis will show exactly where to begin implementing security standards, configuration management, and compliance with security and company policies. The LANguard Network Security Scanner is a simple tool to use as a lightweight vulnerability scanner that uses both passive and intrusive techniques for a vulnerability self-assessment.

Install the scanner and configure it to scan the current target host. Scanning the network can be covered in a network-based analysis, but for the purpose of this paper, focus on the host. After configuration, make no changes to the default options and click the Start Scanning arrow. LANguard has two panes in the application window; the left pane will show a list of all information discovered on the target host, the right pane will show active debug information which proves useful as a real-time view of the tests being performed and how the host responds. When the scan is complete choose to save the report as an HTML file and the browser will open the file for immediate review. An excellent feature of the HTML file is the detailed listing of alerts for open ports, services, shares, or registry settings and hyperlinks to research the information.
Figure 14. Screenshot of LANguard Network Scanner

Figure 15. Screenshot of LANguard HTML report of alert details
The results of the scan reveal interesting information. LANguard detected a host, found four open ports, fingerprinted the operating system and service pack level, found the name of the user logged on to the system, and determined the system to be a domain controller. This information alone allows a potential attacker keys to the kingdom of your information. The listing of NETBIOS names, shares, users, groups, services, password policy, drive listing, and registry entries offer the full view of the system configuration and what vulnerabilities could escalate to a high security risk posture if the system were compromised.

The analysis of comparing the baseline data, network mapping and vulnerability scan presents the security cycle step of Detection. The vulnerability scanner used both passive and intrusive tests to gather information on the target host. The next steps would be to review the security policy, re-evaluate risk and threat, then deploy any necessary countermeasures. After doing so, a post-scan can be conducted using the same vulnerability scanner to detect any differences, then use a more feature-rich scanner such as Internet Security Systems Inc., Internet Scanner, www.iss.net, or Nessus, the free vulnerability scanner provided by The Nessus Project, www.nessus.org. Internet Scanner is a commercial product, but is available as a limited trial version that will only scan the local host. Nessus is available to work on Windows NT/2000, however, the server portion requires access to a Linux operating system and plenty of patience for the installation.

Summary

In conclusion, a vulnerability assessment is a necessary component to network security. New vulnerabilities are detected daily and dynamically changing the risk of any system connected to the Internet. In the big picture of risk management, the vulnerability assessment is one measure to maintaining established baselines, policies, standards, and concise security management objectives. Consistency is key when deploying new systems on an established network infrastructure and gathering security baseline data will incorporate this fact. Regularly review security manuals, guides, checklists, and tools to carry out a security self-assessment. As vulnerabilities increase and threats follow, plan cycles of risk and vulnerability assessments and be persistent in securing your network from the host-level to the enterprise.

Bibliography:


Resources:
www.foundstone.com
www.vigilante.com
www.systernals.com
www.somarsoft.com
www.glocksoft.com
www.belarc.com
www.nmap.com
www.gfi.com
www.securityfocus.com
www.incidents.org
www.iss.net
www.nessus.org
# Upcoming Training

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Rocky Mountain 2019</td>
<td>Denver, CO</td>
<td>Jul 15, 2019 - Jul 20, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Boston Summer 2019</td>
<td>Boston, MA</td>
<td>Jul 29, 2019 - Aug 03, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Jose 2019</td>
<td>San Jose, CA</td>
<td>Aug 12, 2019 - Aug 17, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Minneapolis 2019</td>
<td>Minneapolis, MN</td>
<td>Aug 12, 2019 - Aug 17, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virginia Beach 2019</td>
<td>Virginia Beach, VA</td>
<td>Aug 19, 2019 - Aug 30, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Chicago 2019</td>
<td>Chicago, IL</td>
<td>Aug 19, 2019 - Aug 24, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Copenhagen August 2019</td>
<td>Copenhagen, Denmark</td>
<td>Aug 26, 2019 - Aug 31, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Brussels September 2019</td>
<td>Brussels, Belgium</td>
<td>Sep 02, 2019 - Sep 07, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Canberra Spring 2019</td>
<td>Canberra, Australia</td>
<td>Sep 02, 2019 - Sep 21, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich September 2019</td>
<td>Munich, Germany</td>
<td>Sep 02, 2019 - Sep 07, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>Mentor Session - SEC401</td>
<td>Charleston, SC</td>
<td>Sep 03, 2019 - Nov 05, 2019</td>
<td>Mentor</td>
</tr>
<tr>
<td>SANS Network Security 2019</td>
<td>Las Vegas, NV</td>
<td>Sep 09, 2019 - Sep 16, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>Mentor Session - SEC401</td>
<td>Tysons, VA</td>
<td>Sep 14, 2019 - Oct 12, 2019</td>
<td>Mentor</td>
</tr>
<tr>
<td>SANS Raleigh 2019</td>
<td>Raleigh, NC</td>
<td>Sep 16, 2019 - Sep 21, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain September 2019</td>
<td>Manama, Bahrain</td>
<td>Sep 21, 2019 - Sep 26, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>Community SANS Vancouver SEC401</td>
<td>Vancouver, BC</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Community SANS</td>
</tr>
<tr>
<td>SANS London September 2019</td>
<td>London, United Kingdom</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Francisco Fall 2019</td>
<td>San Francisco, CA</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas Fall 2019</td>
<td>Dallas, TX</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Tokyo Autumn 2019</td>
<td>Tokyo, Japan</td>
<td>Sep 30, 2019 - Oct 12, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA Fall- Reston 2019</td>
<td>Reston, VA</td>
<td>Sep 30, 2019 - Oct 05, 2019</td>
<td>Live Event</td>
</tr>
</tbody>
</table>