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

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

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

II. Asset identification and analysis
III. Vulnerability analysis
IV. Risk evaluation
V. Interim report
VI. Establish risk acceptance criteria
VII. Selection of countermeasures
VIII. Cost/Benefit analysis
IX. Final report

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.

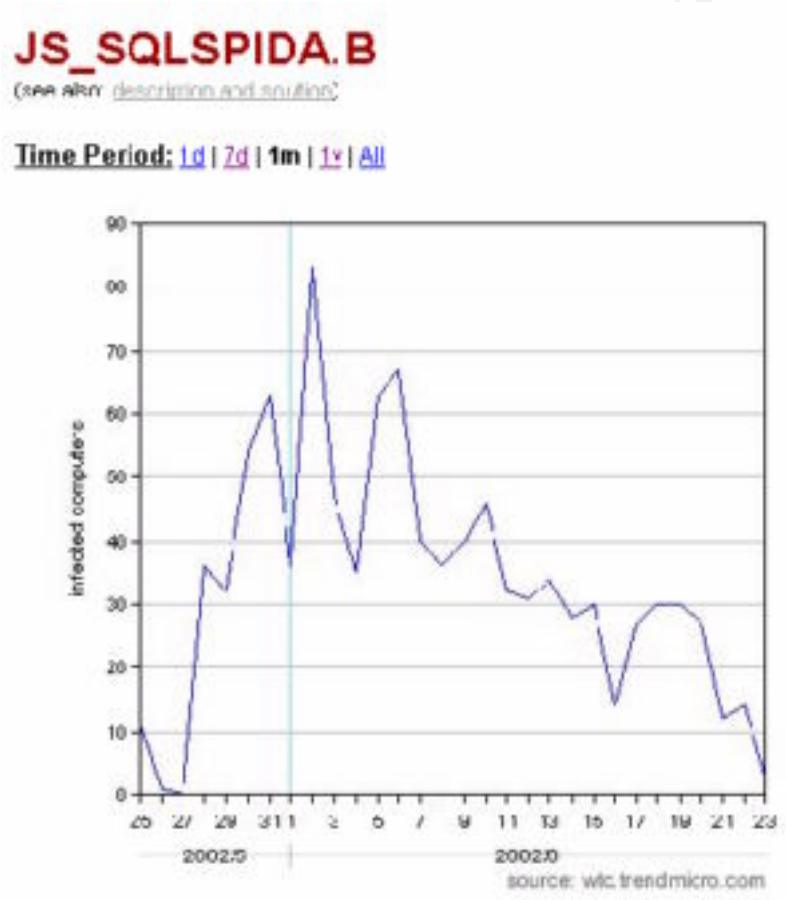


Figure 1. Example of risk, threat, and vulnerability (www.trendmicro.com)
Risk = Threat x Vulnerability

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

"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

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

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 Pstools 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.

WINDOWS TOOLS	THIRD-PARTY TOOLS
PORTS/PROCESSES	
Netstat.exe	Fport.exe
Pstat.exe	Vision.exe
Task manager	Advanced Administrative Tools
	Pslist.exe
SERVICES	
Windows NT Diagnostics	DumpSec
	Advanced Administrative Tools
	Psservice.exe
DRIVERS	
Windows NT Diagnostics	Advanced Administrative Tools
Administrative Tools (Windows 2000)	DumpSec
Drivers.exe	
USER/GROUP information	
	DumpSec
REGISTRY information	
Regedit.exe; export and save	DumpReg
	DumpSec

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

EVENT LOGS	
Event Viewer	DumpEVT
Dumpel.exe	

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.

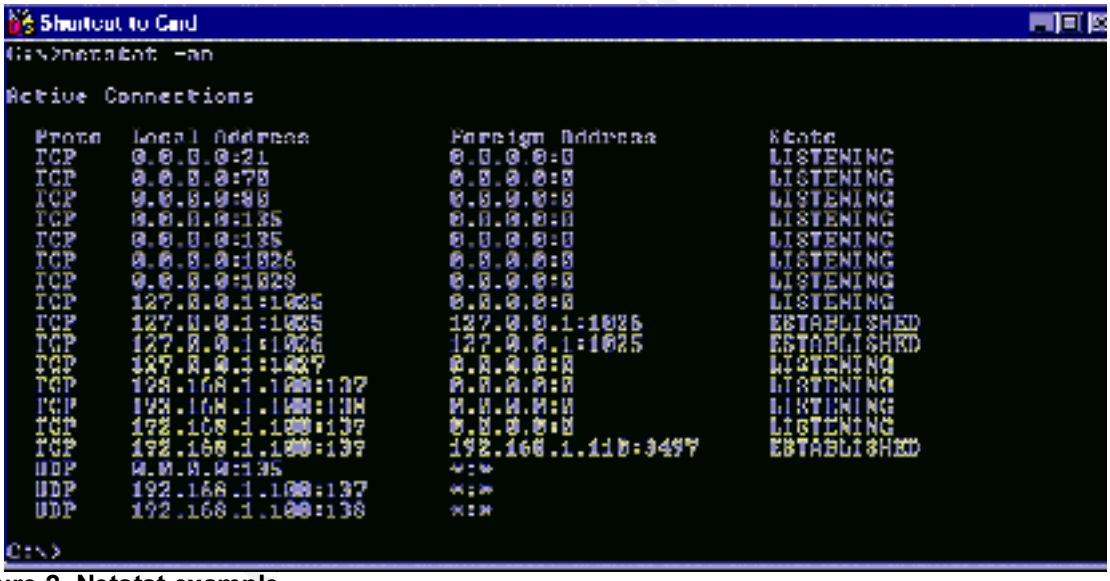


Figure 2. Netstat example

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

Pid   Process            Port  Proto Path
2     System         ->  21    TCP
121   inetinfo       ->  21    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
2     System         ->  70    TCP
121   inetinfo       ->  70    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
2     System         ->  80    TCP
121   inetinfo       ->  80    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
```

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

```
107   RpcSs          ->  135   TCP   C:\WINNT\system32\RpcSs.exe
2     System         ->  135   TCP
2     System         ->  139   TCP
107   RpcSs          ->  1025  TCP   C:\WINNT\system32\RpcSs.exe
2     System         ->  1025  TCP
107   RpcSs          ->  1026  TCP   C:\WINNT\system32\RpcSs.exe
2     System         ->  1026  TCP
2     System         ->  1027  TCP
121   inetinfo       ->  1027  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
2     System         ->  1028  TCP
121   inetinfo       ->  1028  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe107   RpcSs
->  135   UDP   C:\WINNT\system32\RpcSs.exe
2     System         ->  135   UDP
2     System         ->  137   UDP
2     System         ->  138   UDP
```

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
```

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

```
Process information for VENONA:

Name          Pid Pri Thd  Hnd     Mem      User Time   Kernel Time   Elapsed Time
Idle            0   0   1    0      16   0:00:00.000 513:55:26.170    0:00:00.000
System          2   8  26  461     120   0:00:00.000   0:01:18.853    0:00:00.000
SMSS           21  11   6   30      36   0:00:00.150   0:00:00.290  514:00:28.737
CSRSS          24  13   7  197     896   0:00:00.660   0:00:03.044  514:00:21.457
WINLOGON       35  13   2   42     132   0:00:00.130   0:00:00.711  514:00:19.965
SERVICES       41   9  20  230    3384   0:00:11.416   0:00:13.940  514:00:18.483
LSASS          44   9  13  109    2648   0:00:00.320   0:00:00.460  514:00:17.471
SPOOLSS        70   8   6   55     108   0:00:00.030   0:00:00.090  514:00:03.201
LLSSRV         84   9   9   75     784   0:00:00.120   0:00:00.931  513:59:18.767
LOCATOR        98   8   5   37      44   0:00:00.030   0:00:00.020  513:59:18.586
RPCSS         107   8   7   84     848   0:00:00.090   0:00:00.100  513:59:18.176
inetinfo      121   8  22  351     856   0:00:00.130   0:00:00.310  513:59:15.552
PSTORES       125   8   4   37     124   0:00:00.040   0:00:00.110  513:59:15.492
NDDEAGNT      117   8   1   16     156   0:00:00.010   0:00:00.010  513:57:32.844
EXPLORER      157   8   5   66    4136   0:00:08.472   0:00:22.882  513:57:32.294
NTVDM          90   8   2   54    3248   0:00:01.842   0:00:00.450   19:44:41.149
CMD           152   8   1   22    1168   0:00:00.020   0:00:00.020    0:00:46.787
pslist        169   8   1   46    2116   0:00:00.090   0:00:00.190    0:00:00.280
```

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

PageFile: \??\C:\pagefile.sys
        Current Size: 1536000 kb  Total Used:  49756 kb   Peak Used  67368 kb

 Memory: 523568K Avail: 256816K  TotalWs: 308848K InRam Kernel: 5968K P:42712K
 Commit: 237752K/ 159488K Limit:2027268K Peak: 280868K  Pool N:17056K P:43756K

    User Time   Kernel Time     Ws   Faults  Commit Pri Hnd Thd Pid Name
                               95340 56085227                      File Cache
  0:00:00.000   4:04:43.699    16        1       0   0    0   1   0 Idle Process
  0:00:00.000   0:03:12.486   216    34736      32   8  204  39   8 System
  0:00:00.010   0:00:00.861   372      643     148  11   33   6 144 SMSS.EXE
  0:00:00.680   0:02:47.110  2284    31500    1344  13  520  10 172 CSRSS.EXE
  0:00:01.211   0:00:04.796  2312    30765    6572  13  417  17 192 WINLOGON.EXE
  0:00:32.867   0:01:08.919  7812    30077    3544   9  616  38 220 SERVICES.EXE
  0:00:10.645   0:00:13.279   568    28545    2604   9  301  15 232 LSASS.EXE
  0:00:00.861   0:00:20.439  4316     3638    1788   8  376   9 404 svchost.exe
  0:00:05.908   0:00:21.961  7284    12985    4804   8  209  19 448 spoolsv.exe
  0:00:00.640   0:00:22.272  6488     1809    3288   8  186  20 480 msdtc.exe
  0:00:00.010   0:00:00.460  1032      260     340   8   32   2 612 Ctsvccda.exe
  0:00:00.610   0:00:01.011  6216    11164    2072   8  264  17 628 svchost.exe
  0:00:00.080   0:00:03.134  4128     1137   10160   8  150   9 664 mysqld-nt.exe
  0:00:00.020   0:00:00.320  1692      689     744   8   45   3 692 nalntsrv.exe
  0:00:00.540   0:00:02.423  1188      623     564   8   60   9 788 METHWNT.EXE
  0:00:11.666   0:00:16.103  4080     1308    1920   8  183  13 804 BRAD32.EXE
  0:00:00.030   0:00:00.360  1648      415     604   8   44   5 812 NPSSVC.EXE
  0:00:00.010   0:00:00.380   868      224     260   8   30   2 888 regsvc.exe
  0:00:00.050   0:00:01.822  4124     1149    1376   8  156   6 916 mstask.exe
  0:00:04.636   0:00:00.540   416     8925    1728   8  162   4 1012 WinMgmt.exe
  0:00:00.090   0:00:00.500  1952      753     712   8   72   9 1032 wm.exe
  0:00:00.020   0:00:00.380  1456      368     468   8   48   2 1048 mspmspsv.exe
  0:01:02.940   0:02:27.552  4728   810531   13280   8  845  27 1492 explorer.exe
  0:00:00.030   0:00:00.490  2360      660     776   8   71   2 1288 atiptaxx.exe
  0:00:00.020   0:00:02.093  4128     1153    1936   8  138   4 1396 dpmw32.exe
  0:00:36.592   0:00:09.333 14160    22707   10008   8  309   6 2312 WINWORD.EXE
  0:00:10.304   0:00:32.636  2708    22801    8344   8  158   5 4640 AAtools.exe
  0:00:00.610   0:00:01.532  2416   263880     760   8   97   6 4868 MDM.EXE
  0:00:00.270   0:00:00.400  2452     3876    6524   8  142   5 3432 mmc.exe
  0:00:01.792   0:00:00.971   436     1018    1212   8   70   1 5020 DUMPSEC.exe
  0:00:03.254   0:00:03.244 21012     8220   11092   8  110   3 4984 Acrobat.exe
  0:00:00.090   0:00:00.140  4452     2002    1072   8   95   4 4916 msiexec.exe
  0:00:00.030   0:00:00.010  1004      282     312   8   24   1 4952 CMD.EXE
 0:00:00.010   0:00:00.000   696      172     256   8   18   1 4944 pstat.exe


pid:  0 pri: 0 Hnd:    0 Pf:      1 Ws:     16K Idle Process
 tid pri Ctx Swtch StrtAddr    User Time  Kernel Time  State
```

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

```
   0   0  52659418 00000000  0:00:00.000  4:04:43.699 Running

pid:  8 pri: 8 Hnd:  204 Pf:  34736 Ws:    216K System
 tid pri Ctx Swtch StrtAddr    User Time  Kernel Time  State
   4   0   2365012 8054E3B8  0:00:00.000  0:00:38.014 Wait:FreePage
   c  13         1 80418B84  0:00:00.000  0:00:00.000 Wait:EventPairLow
  10  13    358476 80418B84  0:00:00.000  0:00:05.638 Wait:EventPairLow
  14  13    386082 80418B84  0:00:00.000  0:00:09.944 Wait:EventPairLow
  18  14    667922 80418B84  0:00:00.000  0:00:08.882 Wait:EventPairLow
  1c  13    537535 80418B84  0:00:00.000  0:00:06.218 Wait:EventPairLow
  20  12    700389 80418B84  0:00:00.000  0:00:27.509 Wait:EventPairLow
  24  13    238290 80418B84  0:00:00.000  0:00:01.792 Wait:EventPairLow
  28  12    375090 80418B84  0:00:00.000  0:00:01.712 Wait:EventPairLow
  2c  15     45141 80418B84  0:00:00.000  0:00:00.250 Wait:EventPairLow
  30  15    472452 804CA812  0:00:00.000  0:00:00.000 Wait:Executive
  34  18     75017 804392EE  0:00:00.000  0:00:05.157 Wait:VirtualMemory
  38  17     26778 804F0C80  0:00:00.000  0:00:00.230 Wait:FreePage
  3c  16   9461063 804634E0  0:00:00.000  0:00:00.180 Wait:Executive
  40  23  51554010 804635DF  0:00:00.000  0:00:59.846 Wait:Executive
  44  16         1 8041E123  0:00:00.000  0:00:00.000 Wait:EventPairLow
  48  17         1 8041E123  0:00:00.000  0:00:00.000 Wait:EventPairLow
  4c   8       337 BFFE5868  0:00:00.000  0:00:00.010 Wait:Executive
  50  17      3710 8043CC62  0:00:00.000  0:00:00.040 Wait:VirtualMemory
  54   8         1 BFFA0C4C  0:00:00.000  0:00:00.000 Wait:Executive
  58   8        25 BFECB1B8  0:00:00.000  0:00:00.000 Wait:EventPairLow
  5c   8       107 EB4A02E0  0:00:00.000  0:00:00.010 Wait:Executive
  68   8         6 EB4C1AF1  0:00:00.000  0:00:00.000 Wait:Executive
  6c   8         1 EB4C1B76  0:00:00.000  0:00:00.000 Wait:Executive
  70   8         1 EB91AD8E  0:00:00.000  0:00:00.000 Wait:Executive
  74   9      6101 BCB81C74  0:00:00.000  0:00:00.010 Wait:EventPairLow
  7c   9       806 BCB81C74  0:00:00.000  0:00:00.000 Wait:EventPairLow
  80   8     12436 BCB799E0  0:00:00.000  0:00:00.010 Wait:Executive
  88   9     83914 8051217B  0:00:00.000  0:00:00.570 Wait:LpcReceive
 2a4  10        59 BA6DC040  0:00:00.000  0:00:00.010 Wait:EventPairLow
 2a8  10       208 BA6DC040  0:00:00.000  0:00:00.020 Wait:EventPairLow
 300   8     15869 BA5DC584  0:00:00.000  0:00:00.010 Wait:DelayExecution
 358   8         2 BA6A8F08  0:00:00.000  0:00:00.000 Wait:Executive
 3c4  15      9066 BA42A622  0:00:00.000  0:00:00.000 Wait:Executive
 498   8   2358160 EB7F9542  0:00:00.000  0:00:00.741 Wait:DelayExecution
 5d8   8   2030724 EB4DB60C  0:00:00.000  0:00:00.120 Wait:UserRequest
 138c  24         1 B97BB346  0:00:00.000  0:00:00.000 Wait:Executive
 1390  24       149 B97BB346  0:00:00.000  0:00:00.000 Wait:Executive
 e4c   8       150 BCB8657F  0:00:00.000  0:00:00.000 Wait:EventPairLow
```

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.

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

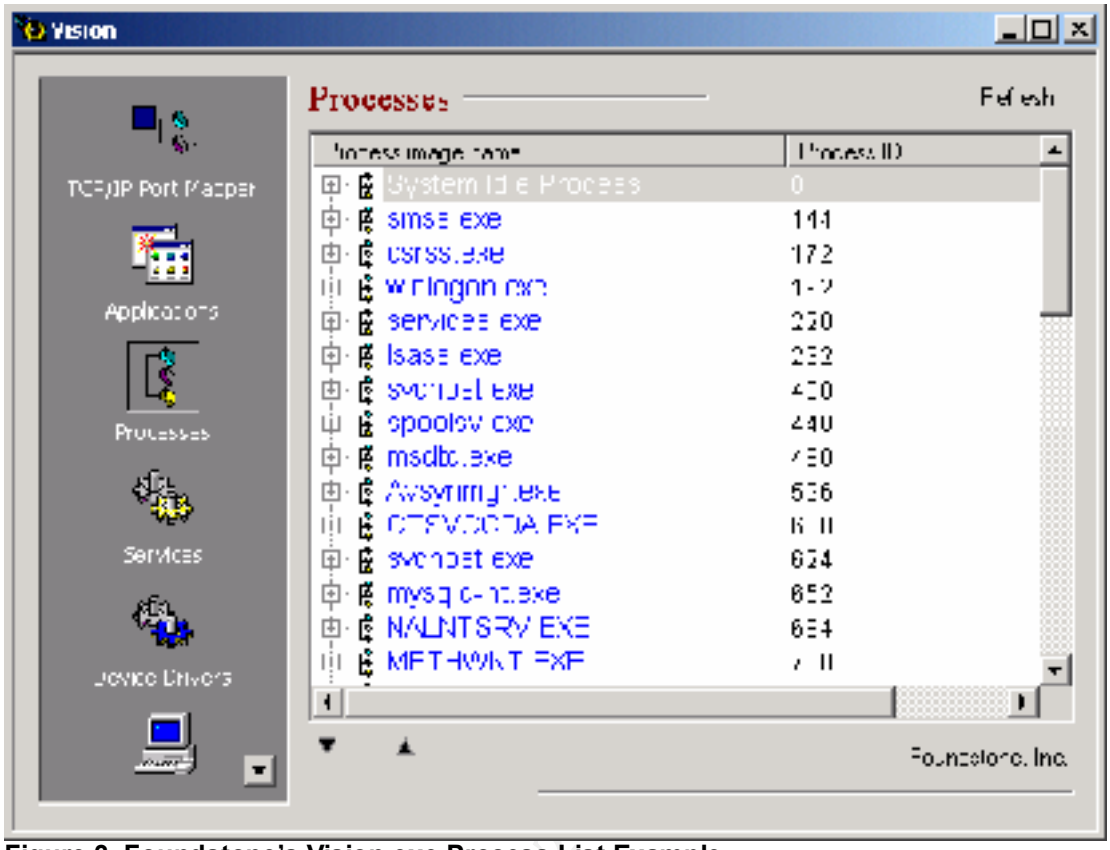


Figure 3. Foundstone's Vision.exe Process List Example

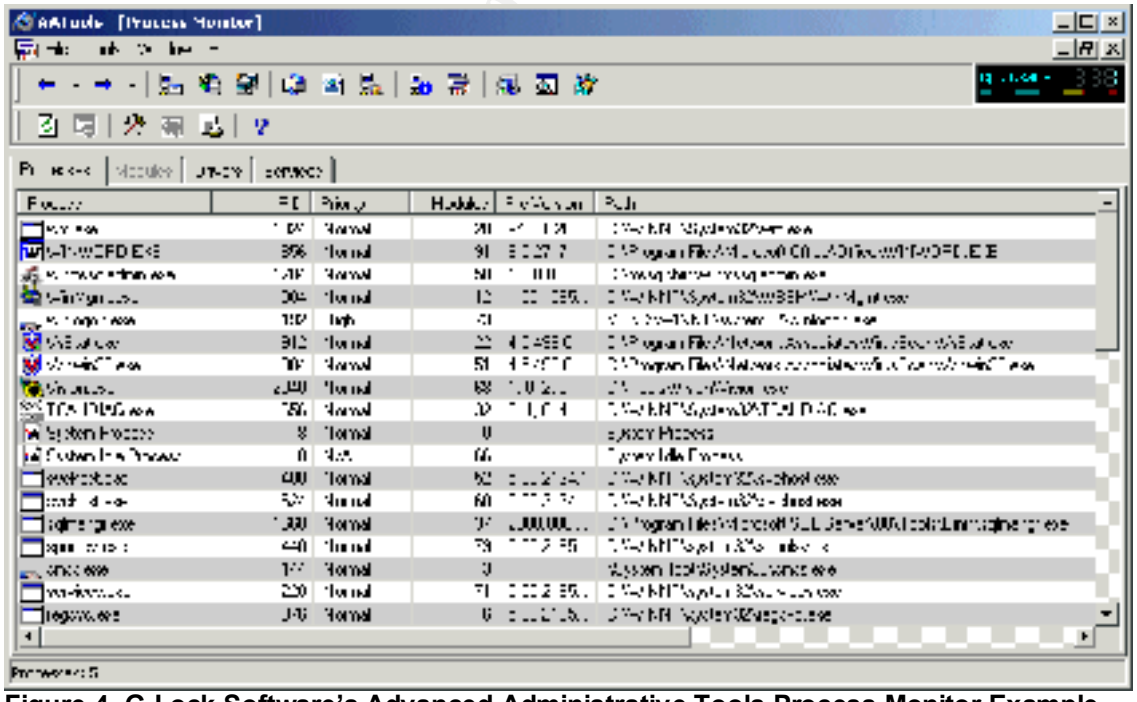


Figure 4. G-Lock Software's Advanced Administrative Tools Process Monitor Example

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

Process: System Process	
Process Info	PID: 8 Priority: Normal Modules: 0 Path: System Process
Modules List	

Process: smss.exe	
Process Info	PID: 144 Priority: Normal Modules: 2 Path: \SystemRoot\System32\smss.exe
Modules List	smss.exe, ntdll.dll

Process: winlogon.exe	
Process Info	PID: 192 Priority: High Modules: 73 Path: \??\C:\WINNT\system32\winlogon.exe
Modules List	winlogon.exe, ntdll.dll, MSVCRT.DLL, KERNEL32.dll, ADVAPI32.DLL, RPCRT4.DLL, GDI32.DLL, USER32.DLL, USERENV.DLL, NDDEAPI.DLL, SFC.DLL, sfcfiles.dll, SECUR32.DLL, PROFMAP.DLL, NETAPI32.dll, NETRAP.DLL, SAMLIB.DLL, WS2_32.DLL, WS2HELP.DLL, WLDAP32.DLL, DNSAPI.DLL, WSOCK32.DLL, NWGINA.DLL, MPR.dll, CALWIN32.DLL, CLNWIN32.DLL, LOCWIN32.DLL, NCPWIN32.dll, NETWIN32.DLL, CLXWIN32.DLL, NWGINAR.DLL, PSAPI.DLL, WINMM.dll, setupapi.dll, COMCTL32.dll, wintrust.dll, CRYPT32.dll, MSASN1.DLL, IMAGEHLP.dll, ole32.dll, mscat32.dll, rsaenh.dll, shell32.dll, SHLWAPI.dll, VERSION.dll, LZ32.DLL, wdmaud.drv, cscdll.dll, WINotify.dll, WINSCARD.DLL, WINSPOOL.DRV, msacm32.drv, MSACM32.dll, CLBCATQ.DLL, OLEAUT32.dll, OLEPRO32.DLL, WMSCHAPI.DLL, WMNTAPI.DLL, cscui.dll, NOVNPNT.DLL, MAPBASE.dll, NWSHLXNT.dll, MAPBASER.DLL, NWSHLXNR.DLL, NOVNPNTR.DLL, ntlanman.dll, NETUI0.DLL, NETUI1.DLL, MPRUI.DLL, NETUI2.dll, comdlg32.dll, netmsg.dll, msv1_0.dll

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

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

When an operating system is installed, several default services are also started to insure 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.

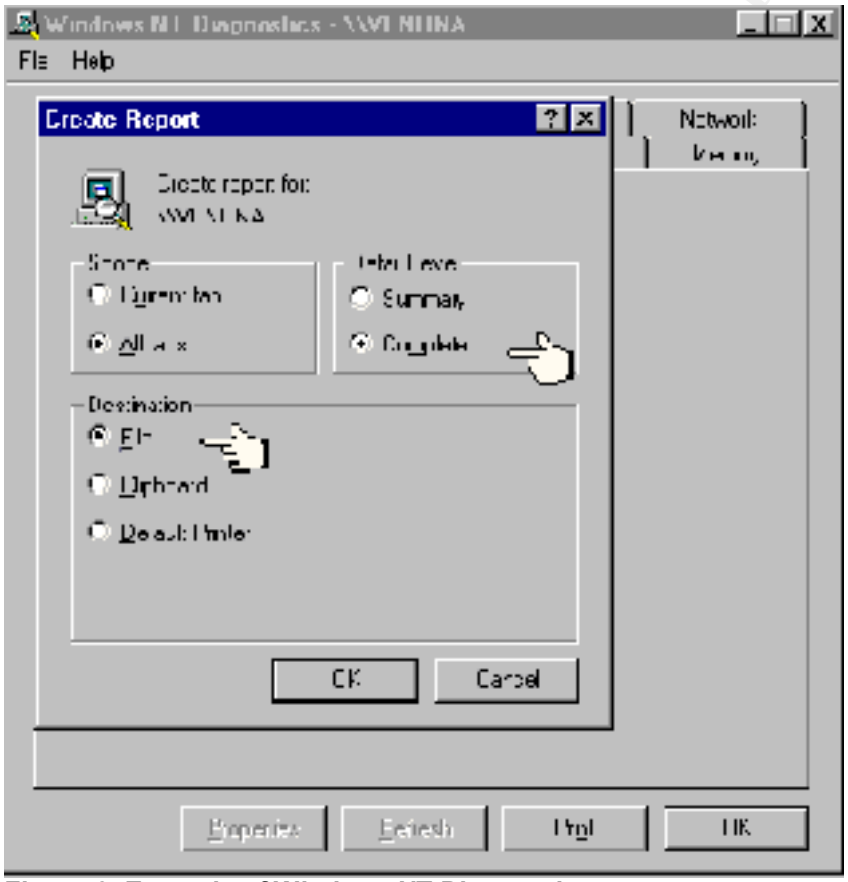


Figure 6. Example of Windows NT Diagnostics

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:

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

```
PsService v1.01 - local and remote services viewer/controller
Copyright (C) 2001 Mark Russinovich
Sysinternals - www.sysinternals.com

SERVICE_NAME: Alerter
DISPLAY_NAME: Alerter
        TYPE              : 20 WIN32_SHARE_PROCESS
        STATE             : 4  RUNNING
                               (STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE         : 0  (0x0)
        SERVICE_EXIT_CODE : 0  (0x0)
        CHECKPOINT        : 0x0
        WAIT_HINT         : 0x0

SERVICE_NAME: Browser
DISPLAY_NAME: Computer Browser
        TYPE              : 20 WIN32_SHARE_PROCESS
        STATE             : 4  RUNNING
                               (STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE         : 0  (0x0)
        SERVICE_EXIT_CODE : 0  (0x0)
        CHECKPOINT        : 0x0
        WAIT_HINT         : 0x0

SERVICE_NAME: ClipSrv
DISPLAY_NAME: ClipBook Server
        TYPE              : 10 WIN32_OWN_PROCESS
        STATE             : 1  STOPPED
                               (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE         : 1077 (0x435)
        SERVICE_EXIT_CODE : 0  (0x0)
        CHECKPOINT        : 0x0
        WAIT_HINT         : 0x0
. . .
```

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.

© SANS Institute 2000 - 2002, Author retains full rights.

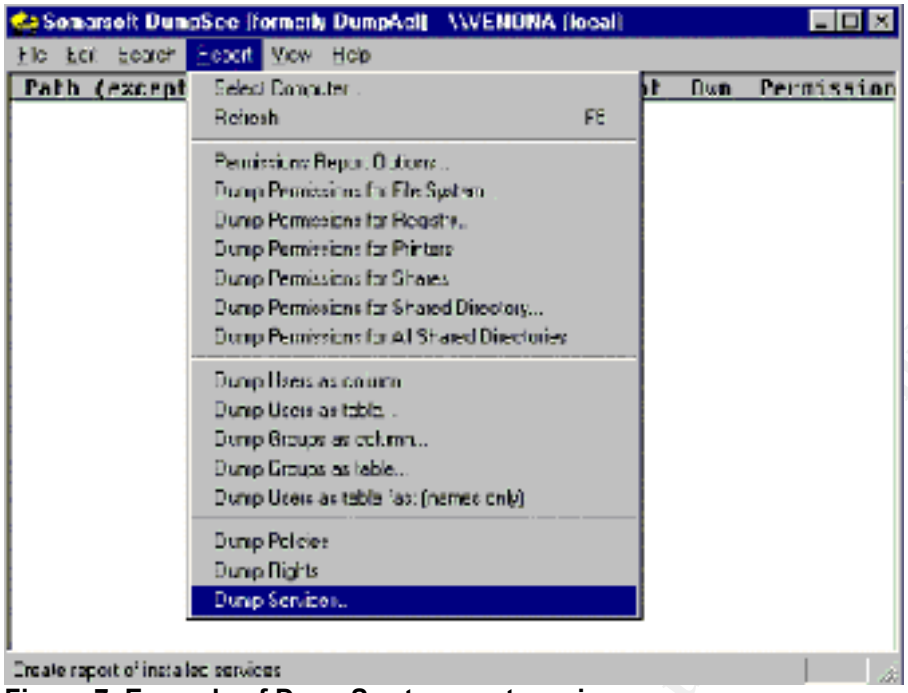


Figure 7. Example of DumpSec to report services

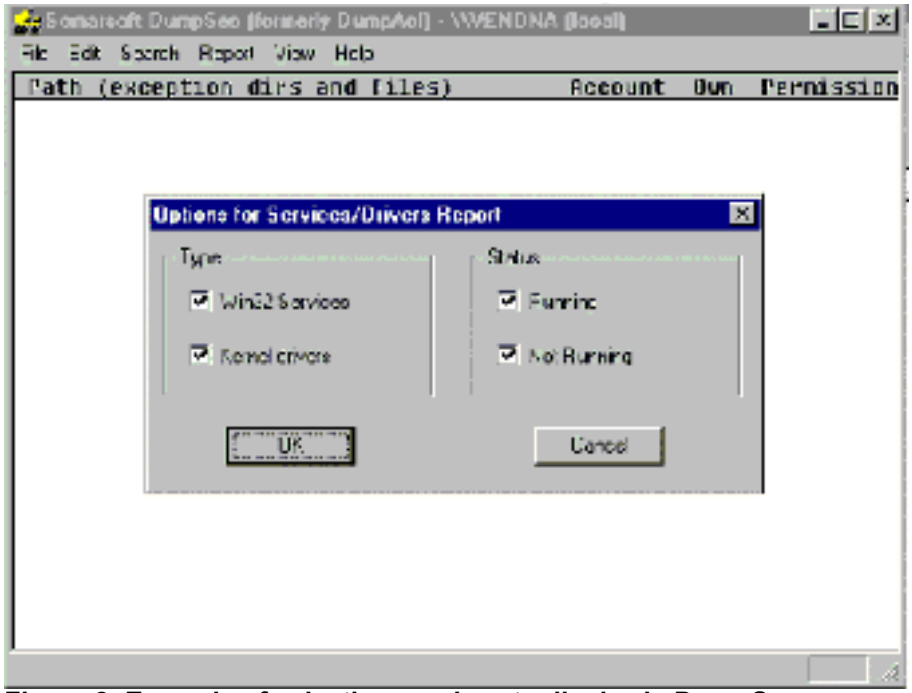


Figure 8. Example of selecting services to display in DumpSec

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,,
```

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

```
Abiosdsk,Abiosdsk,Stopped,Kernel,,
AFD Networking Support Environment,Afd,Running,Kernel,,
Aha154x,Aha154x,Stopped,Kernel,,
Aha174x,Aha174x,Stopped,Kernel,,
aic78xx,aic78xx,Stopped,Kernel,,
Alerter,Alerter,Running,Win32 ,LocalSystem,
Always,Always,Stopped,Kernel,,
amiOnt,amiOnt,Stopped,Kernel,,
amsint,amsint,Stopped,Kernel,,
Arrow,Arrow,Stopped,Kernel,,
atapi,atapi,Running,Kernel,,
Atdisk,Atdisk,Stopped,Kernel,,
ati,ati,Stopped,Kernel,,
Beep,Beep,Running,Kernel,,
Belarc SMBios Access,BANTExt,Running,Kernel,,
bp32drv4,bp32drv4,Running,Kernel,,
BusLogic,BusLogic,Stopped,Kernel,,
Busmouse,Busmouse,Stopped,Kernel,,
Cdaudio,Cdaudio,Stopped,Kernel,,
Cdfs,Cdfs,Running,Kernel,,
Cdrom,Cdrom,Running,Kernel,,
Changer,Changer,Stopped,Kernel,,
cirrus,cirrus,Stopped,Kernel,,
ClipBook Server,ClipSrv,Stopped,Win32 ,LocalSystem,
cnratapi-seagate,cnratapi-seagate,Stopped,Kernel,,
Computer Browser,Browser,Running,Win32 ,LocalSystem,
Cpqarray,Cpqarray,Stopped,Kernel,,
cpqfws2e,cpqfws2e,Stopped,Kernel,,
dac960nt,dac960nt,Stopped,Kernel,,
dce376nt,dce376nt,Stopped,Kernel,,
Dell_DGX,Dell_DGX,Stopped,Kernel,,
Delldsa,Delldsa,Stopped,Kernel,,
DHCP Client,DHCP,Stopped,Win32 ,LocalSystem,
. . .
```

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)
UserName
```

© SANS Institute 2000 - 2002, Author retains full rights.

```
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
   HomeDir
   Profile
   LogonScript
   Workstations
   PswdCanBeChanged,Yes
   PswdLastSetTime,10/15/01 9:03 AM
   PswdRequired,Yes
   PswdExpires,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
   HomeDir
   Profile
   LogonScript
   Workstations
   PswdCanBeChanged,No
   PswdLastSetTime,Never
   PswdRequired,Yes
   PswdExpires,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
   HomeDir
   Profile
   LogonScript
   Workstations
   PswdCanBeChanged,No
   PswdLastSetTime,10/15/01 9:06 AM
   PswdRequired,Yes
   PswdExpires,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, Author retains full rights.

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

Groups:

```
6/25/02 8:14 PM - Somarsoft DumpSec (formerly DumpAcl) - \\VENONA (local)
Group,Comment,Type

Domain Admins,Designated administrators of the domain,Global
   Administrator,,User
Domain Guests,All domain guests,Global
   Guest,,User
Domain Users,All domain users,Global
   Administrator,,User
   IUSR_VENONA,,User
Account Operators,Members can administer domain user and group accounts,Local
Administrators,Members can fully administer the computer/domain,Local
   Domain Admins,,Global
   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 ineraction 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.

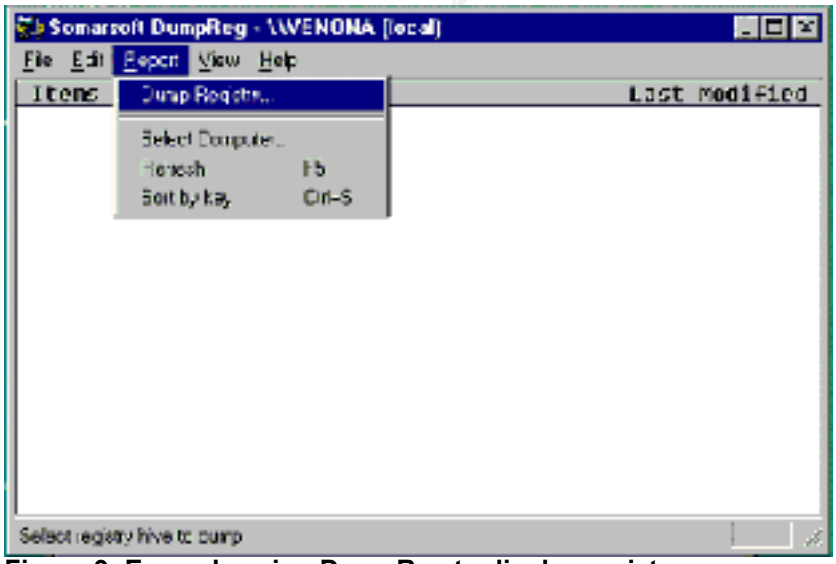


Figure 9. Example using DumpReg to display registry

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

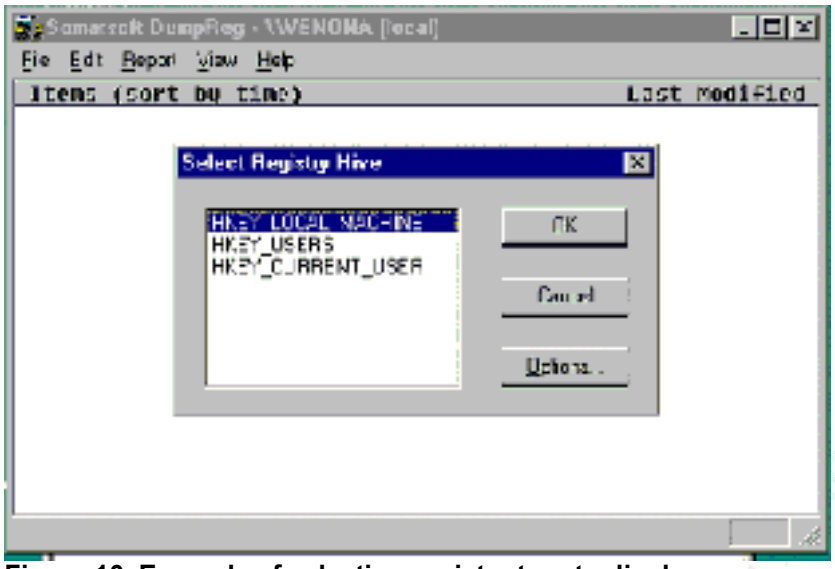


Figure 10. Example of selecting registry tree to display

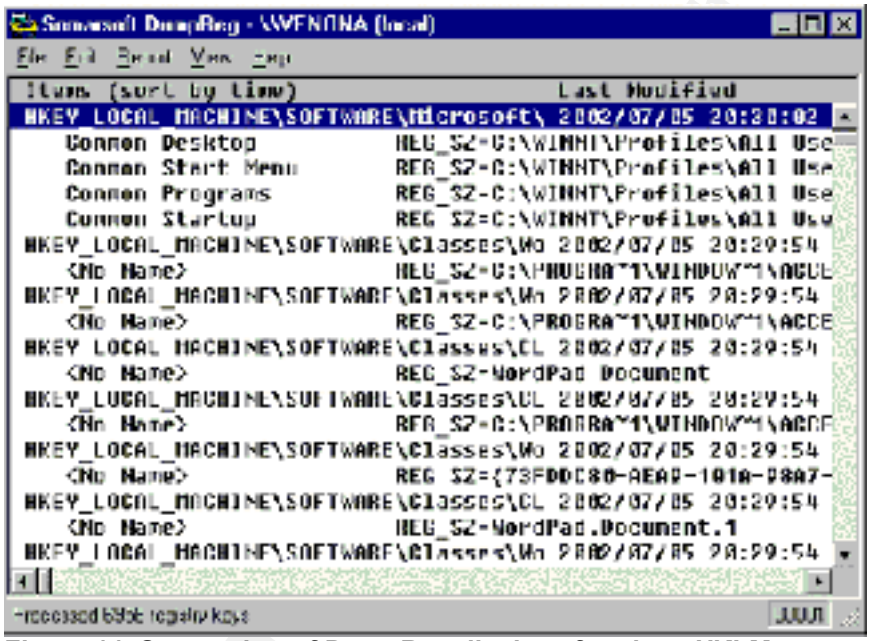


Figure 11. Screenshot of DumpReg display of registry HKLM

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 lod 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

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

information for documentation. Somarsoft's DumpEVT is another tool that will gather event log data for baseline analysis.

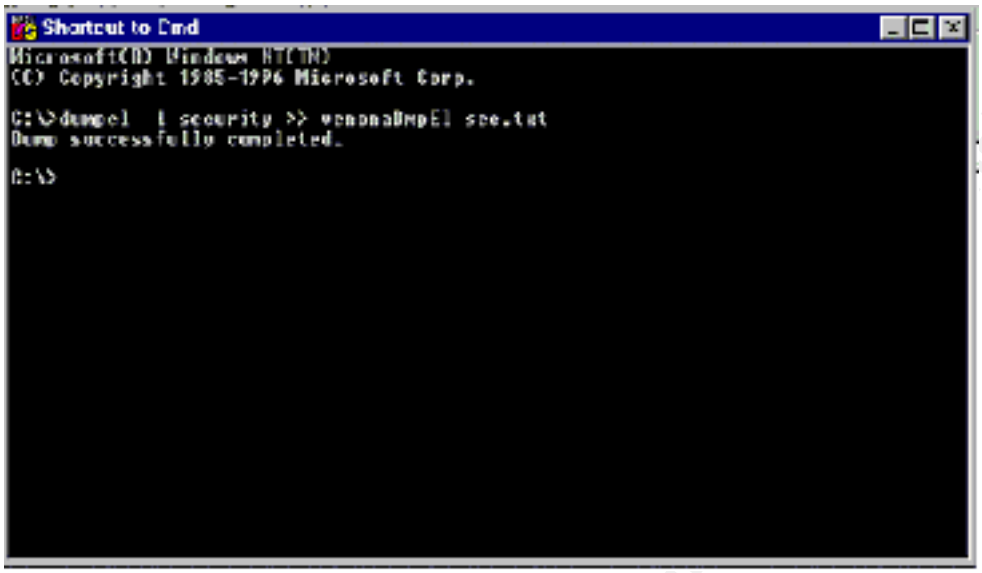


Figure 12. Using dumpel.exe

```
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) %%1538            %%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
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 rundll32.exe 2152797440 Administrator DOMAIN1 (0x0,0x29C7)
```

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

```
6/13/02 8:37:13 AM      8       5       593     Security        DOMAIN1\Administrator
        VENONA
```

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

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

guides provides a defense-in-depth style approach to prepare for the vulnerability security self-assessment.

NIST sp800-26 [5]	OCTAVE [4]	NIST sp800-42 [2]	OSSTMM [1]	TRAWG [3]
Security Self-assessment Guide for Information Technology	Operationally Critical Threat, Asset, and Vulnerability Evaluation Criteria v2.0	Security-testing draft	Open Source Testing Methodology Manual, v2.0	Threat and Risk Assessment Working Guide
PDF	PDF	PDF	PDF/HTML	PDF
Questionnaire	Self-directed risk evaluation	Tool usage	Testing techniques	Overall Risk assessment
Outline of standards and point system for questionnaire; Samples provided	General process of long-term risk assessment, threat management, and vulnerability assessment	Sample tool usage; tables of tools; table of testing cycles	Outline of testing; list of tools to use; description of testing technique; sample forms	Outline process of complete risk assessment; good for qualitative and quantitative analysis
August 2001	December 2001	February 2002	February 2002	October 1999

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.

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

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:

Network Mapping	**Vulnerability Scan**
Penetration testing	**File Integrity checks**
Password cracking	**Virus detection**
IDS/Firewall/Log review	**War dialing**
Wireless/802.11 Leak checks	**Analysis and Report**

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

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

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.

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

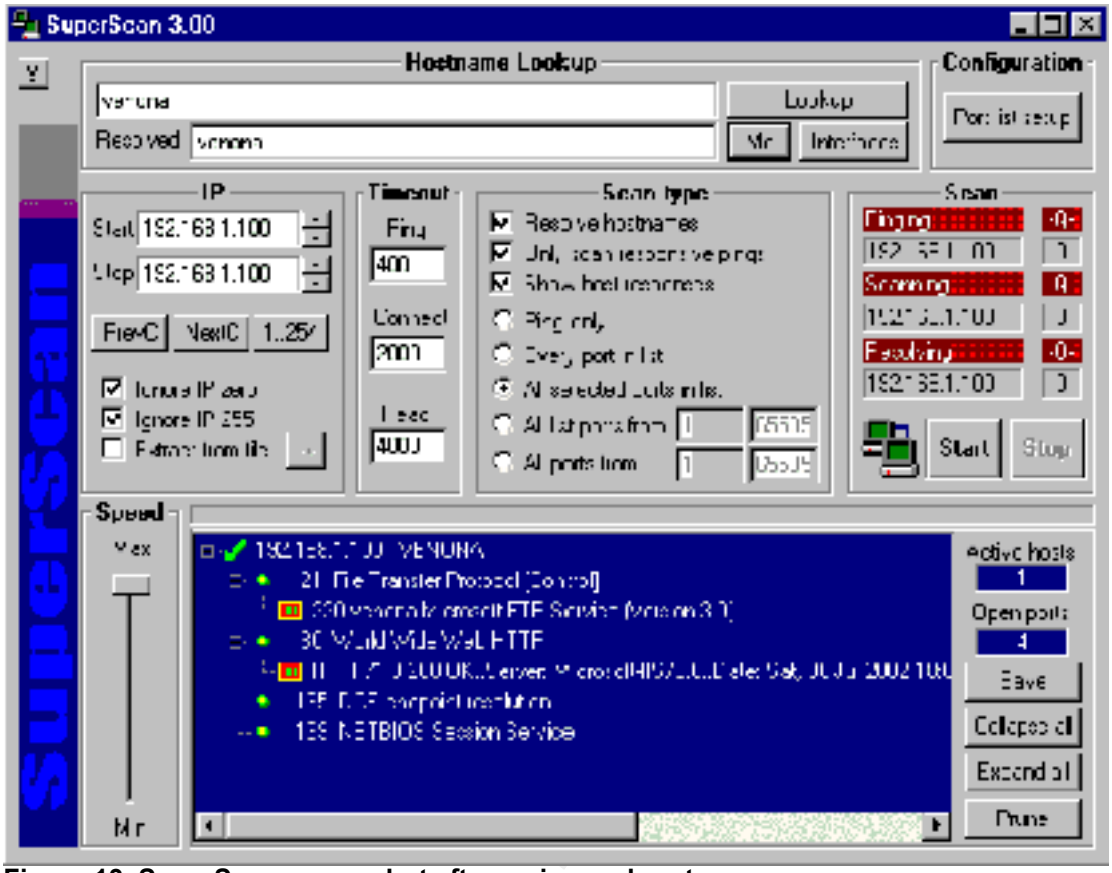


Figure 13. SuperScan screenshot after a ping and port scan

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

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

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.

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

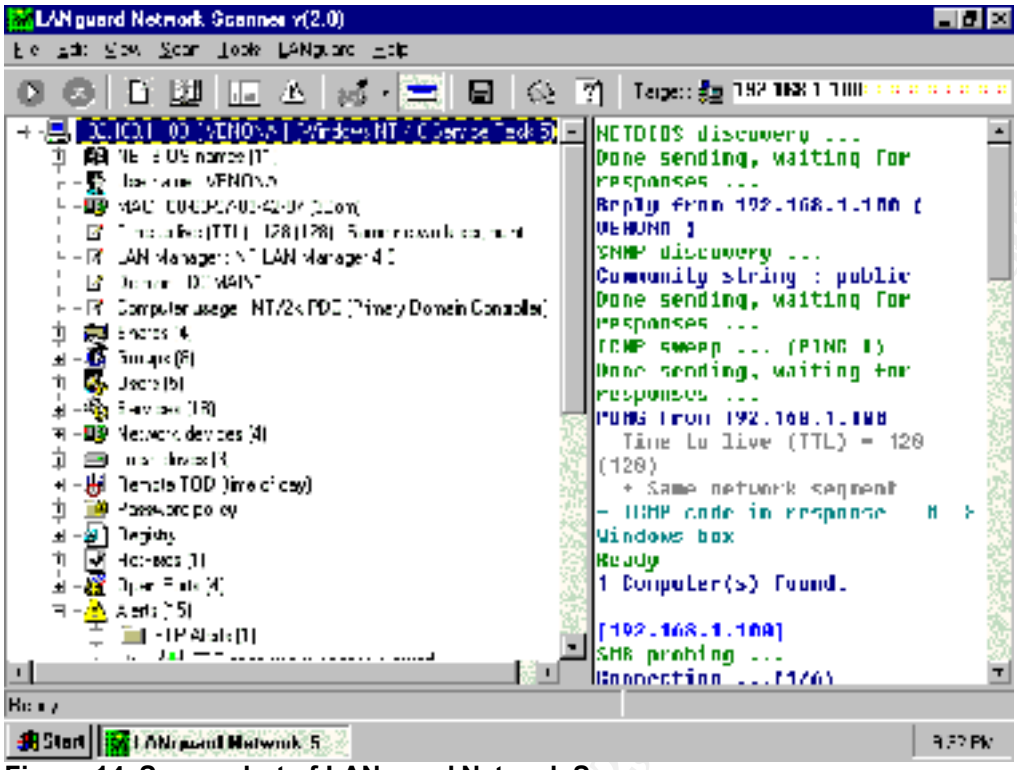


Figure 14. Screenshot of LANguard Network Scanner

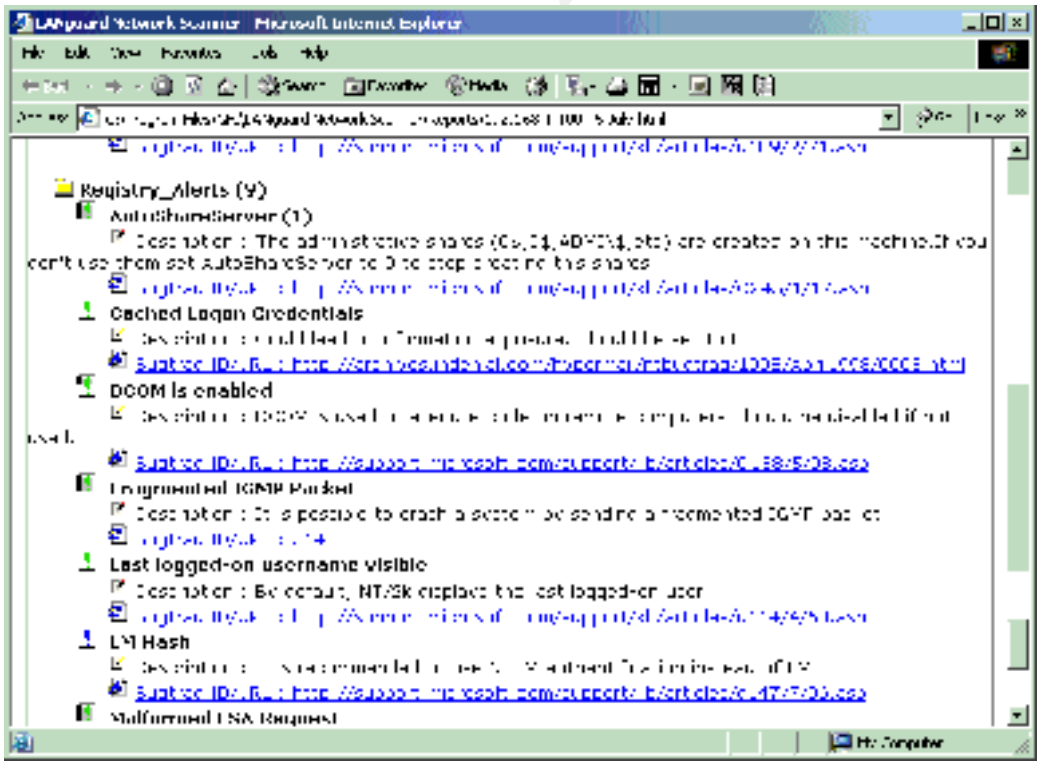


Figure 15. Screenshot of LANguard HTML report of alert details

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

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:

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

[1] Herzog, Peter. "Open-Source Security Testing Methodology Manual." Version 2.0. February 2002. URL: http://ideahamster.gnutec.com/osstmm.en.2.0.zip (June 13, 2002)

[2] Wack, Jack; Tracey, Miles. NIST special publication 800-42. "DRAFT Guideline on Network Security Testing." February 2001. URL: http://csrc.nist.gov/publications/drafts/security-testing.pdf (June 13, 2002)

[3] Canadian Communications Security Establishment. "Threat and Risk Assessment Working Guide." November 18 1999. URL: http://www.csest.gc.ca/en/documents/knowledge_centre/publications/manuals/ITSG-04e.pdf (June 13, 2002)

[4] Alberts, Christopher J.; Dorofee, Audrey J. CERT technical report. "OCTAVE Criteria Version 2.0." December 2001. URL: http://www.cert.org/archive/pdf/01tr016.pdf (June 15, 2002)

[5] Swanson, Marianne. NIST special publication 800-26. "Security Self Assessment Guide for Information Technology systems." August 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf (June 15, 2002)

[6] Symantec. "Vulnerability Assessment Guide." URL: http://enterprisesecurity.symantec.com/PDF/167100088_SymVAGuide_WP.pdf (June 15, 2002)

[7] Bakos, George. "SQLsnake Code Analysis." May 21, 2002. URL: http://www.incidents.org/diary/diary.html?id=157 (June 23, 2002)

[8] Kapp, Justin. PC network Advisor. Issue 20 (July 2000). "How To Conduct A Security Audit." URL: http://www.itp-journals.com/nasample/t04123.pdf (June 23, 2002)

[9] Winkler, Ira. "Audits, Assessments & Tests (Oh, My)." July 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/july00/features4.shtml (June 23, 2002)

[10] Kurtz, George; Chris Prosise. "Penetration Testing Exposed." September 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/september00/features3.shtml (June 23, 2002)

[11] "100% Foundstone." URL: http://www.foundstone.com/services/100_percent.html (July 6, 2002)

[12] "NIH Network Risk Assessment Users Manual". March 1995. URL: http://irm.cit.nih.gov/security/raword/ (July 7, 2002)

SANS Institute. SANS Security Essentials I: Information Security, The Big Picture. 2002.

Resources:

www.foundstone.com

www.vigilante.com

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

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.nesus.org

© SANS Institute 2000 - 2002, Author retains full rights.