System Security Scanning and Discovery

Chapter 14

Lecturer: Pei-yih Ting

Overview

- Security Scanning
- Important Security Web Sites
- Fingerprinting OS
- FingerPrinting IP Stacks
- Share Scans
- SNMP Vulnerabilities
- FingerPrinting TCP/IP Services
- Social Engineering

Security Scanning

- Security scanning is the process of methodically assessing a system to find known vulnerabilities
- Create a list of all known vulnerabilities for your operating system
- Check whether each vulnerability exists on your system
- Document vulnerabilities that are found
- Rank those found by severity and cost
- Take corrective actions as necessary

Security Scanning (cont'd)

- Take advantage of Web resources to help with creating a vulnerability list

Organization	Web Address	Description
SANS	**http://www.sans.org/top20**	**The SANS/FBI top 20 vulnerability list**
SecurityFocus	**http://www.securityfocus.com/bid**	**The de facto standard for finding any vulnerability for any software**
Common Vulnerabilities and Exposures	**http://www.cve.mitre.org**	**A list of standardized names for vulnerabilities and other security exposures**
CERT Coordination Center	**http://www.cert.org/nav/index_red.html**	**CERT vulnerabilities, incidents, and fixes**
Securia	**http://securia.com**	**Vulnerability lists and security advisories**

Table 14.1 Web Sites with Common Security Vulnerability Lists

Security Scanning (cont'd)

- To check for vulnerabilities on your system, you can
  - Hire an outside company (easy but costly and less flexible)
  - Use a toolset that will help you do it yourself
- There are a number of tools available that perform various activities related to security assessment
  - Some are free

Security Scanning (cont'd)

Table 14.2 Web Sites for Security Scanners

Organization	Web Address	Product Name	Cost
Nessus	http://www.nessus.org	Nessus Security Scanner	Free
Microsoft Corporation	http://www.microsoft.com/technet/security/tools/mbsahome.mspx	Microsoft Baseline Security Analyzer	Free
Foundstone	http://www.foundstone.com	Foundstone Professional	$121,000 per year
Insecure.org	http://www.insecure.org	Nmap	Free
Gfi	http://www.gfi.com	Gfi LanGuard	$499
The Center for Internet Security	http://www.cisecurity.org	CIS Security Benchmarks and Scoring Tools	Free

OS Fingerprinting Utilities

- The process of detecting the operating system of a remote computer is called operating system fingerprinting
- Most attacks are operating system specific
- Scanning tools typically communicate with a remote system and compare responses to a database in order to guess the operating system
- Scanning tools provide at least the operating system and often the version
  - Most can provide much more information

OS Fingerprinting Utilities

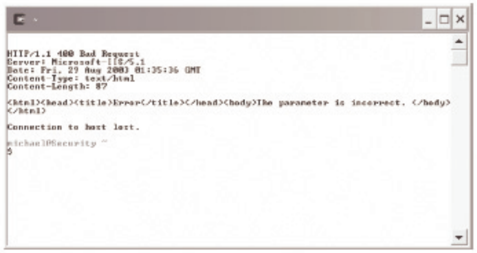
Table 14.3 Popular Operating System Fingerprint Utilities

Organization	Web Address	Product Name
Insecure.org	http://www.insecure.org	Nmap
Safemode.org	http://www.safemode.org/sprint/	Sprint
Sys-Security Group	http://www.sys-security.com/html/projects/X.html	Xprobe2

Network- and Server-Discovery Tools

- Once the OS is known, you can query open ports to discover what software is running
- When you connect to a port, many programs will respond with a welcome message called a banner
  - Banners provide information about the responding program
  - You may want to suppress or modify banner information to thwart attackers
  - Scanning programs use this information to detect programs and versions

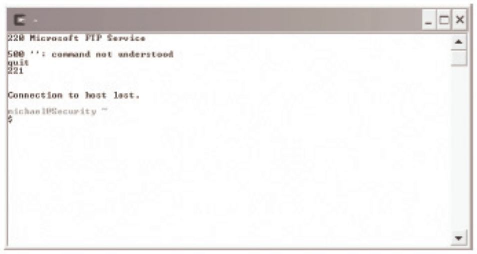
Using Telnet for Discovery



```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.1
Date: Fri, 29 Aug 2003 01:35:36 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body>
</html>

Connection to host lost.

michael@Security ~
$
```

Figure 14.1

Results of using Telnet to attach to port 80



```
220 Microsoft FTP Service

500 '': command not understood
quit
221

Connection to host lost.

michael@Security ~
$
```

Figure 14.2

Results of using Telnet to attach to port 21

Fingerprinting IP Stacks

- Most scanning tools use IP Stack fingerprints to identify operating systems
- The tools send carefully designed test packets to the remote system and analyze the responses
  - Each IP stack implementation has a slightly different response pattern
  - Once an IP stack implementation is known, the operating system can be guessed

Fingerprinting IP Stacks

- Nmap
  - Sends normal and malformed TCP and UDP packets to the target computer in 9 separate tests to 3 ports
  - Responses are compared to a database of known IP stack versions
- Sprint
  - Can be run in active or passive mode
    - In active mode, sends and receives packets
    - In passive mode, only listens for packets from the target machine
  - Also provides basic uptime information
  - Has an option to do banner grabbing to obtain more information

Fingerprinting IP Stacks

- Xprobe2
  - Sends primarily ICMP packets
  - Does not do a preliminary scan on ports
    - The absence of a port scan and the use of ICMP packets make this utility less noticeable to the target machine
  - Uses a fingerprint matrix approach that allows for “near matches” with the result that it is more likely to be able to make an operating system guess

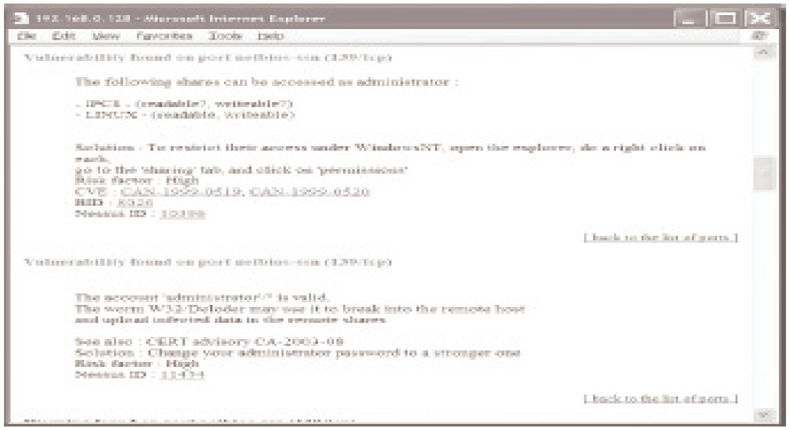
Share Scans

- Shared network resources such as files and printers are called shares on Windows machines
  - Windows uses the SMB (Server Message Block) protocol to provide network access
  - UNIX uses Samba (provides cross-platform accessibility)
- Using shares presents several security weaknesses
  - Increase the likelihood that an unauthorized user will gain access to the resource
  - SMB/Samba are software implementations, S/W flaws
  - Antivirus packages are configured to ignore shared folders and mapped drives by default
- Use shares sparingly and keep them secure

Share Scans (cont’d)

- Share scanner tools can detect shares
  - Nessus is an example tool
  - Shares are easy for both administrators and attackers to find

Share Scans (cont’d)



```
Vulnerability found on port netbios-ssn (139/tcp)

        The following shares can be accessed as administrator :

        - IPC$ - (readable?, writeable?)
        - LINUX - (readable, writeable)

        Solution : To restrict their access under WindowsNT, open the explorer, do a right click on
        each,
        go to the 'sharing' tab, and click on 'permissions'
        Risk factor : High
        CVE : CAN-1999-0519, CAN-1999-0520
        BID : 8026
        Nessus ID : 10396

                                                                [ back to the list of ports ]

Vulnerability found on port netbios-ssn (139/tcp)

        The account 'administrator'/'' is valid.
        The worm W32/Deloder may use it to break into the remote host
        and upload infected data in the remote shares.

        See also : CERT advisory CA-2003-08
        Solution : Change your administrator password to a stronger one
        Risk factor : High
        Nessus ID : 11454

                                                                [ back to the list of ports ]
```

Figure 14.3 Results of a Nessus scan for Windows shared network resources

Telnet Inquiries

- Telnet is a good discovery tool
- Telnet uses port 23 by default but will connect to another port if one is specified
  - Many services will respond to any TCP connection with information that could be useful to an attacker
- Telnet messages are sent in the clear (not encrypted)
  - They are easy to intercept and read
  - They should not be used for sensitive information
    - Use an alternative like Secure Shell (ssh)

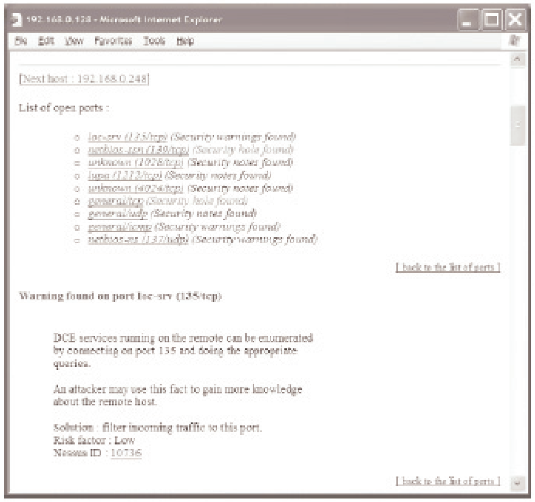
SNMP Vulnerabilities

- Simple Network Management Protocol (SNMP) has been in use for many years
- It is a standard management communication protocol for network hardware and software devices
- Several vulnerabilities were found in SNMP after many years of use
  - Remember that even existing software can have undiscovered vulnerabilities
- When assessing your system, scan network devices such as routers and firewalls
  - Using multiple scanners gives you greater coverage and protection

TCP/IP Service Vulnerabilities

- Most services use TCP/IP as a standard to improve compatibility
- Many TCP/IP services have known vulnerabilities
  - Unneeded or outdated services running on a machine are often targets for attackers
- Disable services that are not being used
- Before using a scanning tool, be sure it is up-to-date
  - Nessus and other tools can perform self-updates automatically by running an update command
- Educate yourself and stay up-to-date on services through newsletters, mailing lists, and security Web sites

TCP/IP Service Vulnerabilities (cont'd)



[Next host : 192.168.0.248]

List of open ports :

- loc-srv (135/tcp) (Security warnings found)
- netbios-ssn (139/tcp) (Security hole found)
- unknown (1026/tcp) (Security notes found)
- lupa (1212/tcp) (Security notes found)
- unknown (4024/tcp) (Security notes found)
- general/tcp (Security hole found)
- general/udp (Security notes found)
- general/icmp (Security warnings found)
- netbios-ns (137/udp) (Security warnings found)

[back to the list of ports]

Warning found on port loc-srv (135/tcp)

DCE services running on the remote can be enumerated by connecting on port 135 and doing the appropriate queries.

An attacker may use this fact to gain more knowledge about the remote host.

Solution : filter incoming traffic to this port.
Risk factor : Low
Nessus ID : 10736

[back to the list of ports]

Figure 14.4
Results of a Nessus scan for running network services

Vulnerability Mailing Lists and Newsletters

Table 14.4 Security Vulnerability Mailing Lists and Newsletters

Organization	Web Address	Description
Security Focus	http://www.securityfocus.com/subscribe?listname=1	Configurable mailing list of new and significant vulnerabilities
SANS Institute	http://www.sans.org/newsletters/	SANS newsletters and mailing list digest subscriptions
Sintelli	http://www.sintelli.com	SINTRAQ Security Vulnerability mailing list

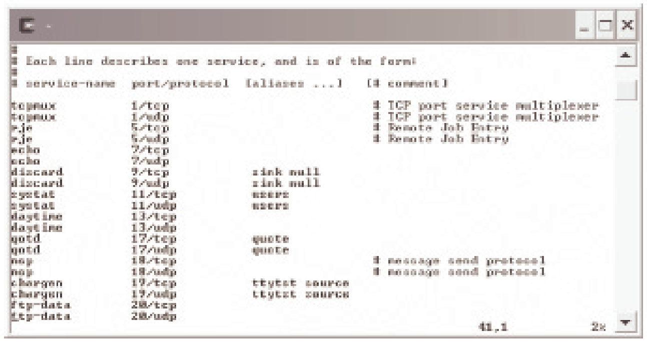
Simple TCP/IP Services

- To access a network service, a remote client needs to know the host name, the port, and the protocol
- Ports from 0 to 1023 are the well-known ports and are reserved for standard services
- A list of services and their ports and protocols are maintained in a file called services
- Windows defines 5 services as Simple TCP/IP Services
  - Designed for testing purposes
  - Can often be disabled

Simple TCP/IP Services (cont'd)

Table 14.5 Location of Services File in Windows and UNIX

Operating System	Services File Location
Windows	%windir%\System32\Drivers\Etc\Services
UNIX	/etc/services



```
#
# Each line describes one service, and is of the form:
#
# service-name  port/protocol  [aliases ...]   [# comment]

tcpmux          1/tcp                           # TCP port service multiplexer
tcpmux          1/udp                           # TCP port service multiplexer
rje             5/tcp                           # Remote Job Entry
rje             5/udp                           # Remote Job Entry
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
systat          11/udp          users
daytime         13/tcp
daytime         13/udp
qotd            17/tcp          quote
qotd            17/udp          quote
msp             18/tcp                          # message send protocol
msp             18/udp                          # message send protocol
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp-data        20/udp
                                                   41,1          2%
```

Figure 14.5

Portion of the services file on Red Hat Linux

Location of Simple TCP/IP Services

Table 14.6 Location of Simple TCP/IP Services

Service	Port	Description
CHARGEN (Character Generator) Service	19	Listens to port 19, waits for a connection, and then dumps characters across the connection
Daytime Server	13	Provides the system date and time to anyone who asks
Discard Server	9	Discards everything it receives
Echo Server	7	Echoes everything it receives
Quote of the Day	17	When prompted, returns a quote for the current day

Social Engineering

- Social engineering is an attack that depends on convincing an authorized user to disclose information or perform an unauthorized act
- Social engineering depends on human nature
  - People don’t like to challenge other people (especially those acts like they know what they are doing)
  - People usually want to be helpful
- Deterrence requires user education (security awareness training) and depends on making security policies explicit and known to all employees

Social Engineering (cont’d)

Fred was performing a penetration test for his client.

- Fred found that the company’s FTP site had an upload directory anyone could write to.
- Fred uploaded a keystroke-logging program. He called the program *fixvirus.exe*.
- Fred called the CEO’s secretary, posed as a network administrator, and told her he had received a notice that her PC was infected with a virus.
- Fred instructed her to go to the company FTP site and download the fix program – *fixvirus.exe*.
- Within two days, Fred had CEO’s secretary’s password and the CEO’s password.

Obtaining Security-Related Information Fraudulently

- Before you scan a system, get written permission from the owner
- When you scan a system, you have access to potentially sensitive information
  - Adhere to a high standard of ethics and professionalism
- Any use of confidential or sensitive data outside the scope of your agreement is fraudulent and could result in legal action

The Footprinting and Fingerprinting Drill (System Profiling)

- The five Ps of scanning
  - Purpose, permission, process, patience, and persistence
- Purpose will focus your efforts and aid in the selection of tools
- Permission is needed
- A methodical and well-planned process will make your efforts effective and efficient
- Patience and persistence are required because system assessment is detailed and time-consuming

Summary

- Security scanning is a process that involves methodically eliciting information about a system and its software and hardware
- Vulnerabilities are usually operating system specific
  - Sometimes even version specific
- Scanning enables you to determine what operating system is running on a machine
  - This is called operating system fingerprinting
- Operating system fingerprinting is typically dependent on IP stack fingerprinting

Summary (cont'd)

- There are many tools available to aid in scanning
  - Including Nmap, Sprint, Xprobe2, Nessus
- Telnet is useful for discovering running services
  - Many programs respond to a telnet connection with banners containing useful information
- Shares, SNMP, and TCP/IP services are very vulnerable
  - Be sure to include them in your scanning assessment
- Social engineering is an attack method in which the attacker gets an authorized person to disclose information or perform unauthorized activity

Assignments

- Reading: Chapter 14
- Practice 14.14 Challenge Questions

- Turn in Challenge Exercise 14.1 next week
- Tell me a vivid social engineering example