

THOMSON



COURSE TECHNOLOGY

Hands-On Ethical Hacking and Network Defense



Chapter 6 *Enumeration*

Modified 1-11-17

Objectives

- Describe the enumeration step of security testing
- Enumerate Microsoft OS targets
- Enumerate *NIX OS targets

Introduction to Enumeration

- Enumeration extracts information about:
 - Resources or shares on the network
 - Network topology and architecture
 - Usernames or groups assigned on the network
 - Information about users and recent logon times
- Before enumeration, you use Port scanning and footprinting
 - To Determine OS being used
- Intrusive process

NBTscan

- NBT (NetBIOS over TCP/IP)
 - is the Windows networking protocol
 - used for shared folders and printers
- NBTscan
 - Tool for enumerating Microsoft OSs

```
yourname@S214-01u:~$ nbtscan 192.168.2.1-254
Doing NBT name scan for addresses from 192.168.2.1-254
```

IP address	NetBIOS Name	Server	User	MAC address
192.168.2.30	RICKHP	<server>	<unknown>	00:40:2b:66:78:80
192.168.2.14	SAMP4	<server>	<unknown>	00:10:b5:0e:5c:8a
192.168.2.22	SAM_LAPTOP		SAM_LAPTOP	00:10:60:03:b6:bf
192.168.2.222	SAM2G	<server>	<unknown>	00:30:48:82:11:bd

Enumerating Microsoft Operating Systems

- Study OS history
 - Knowing your target makes your job easier
- Many attacks that work for older Windows OSs still work with newer versions

Windows 95

- The first Windows version that did not start with DOS
- Still used the DOS kernel to some extent
- Introduced the Registry database to replace Win.ini, Autoexec.bat, and other text files
- Introduced Plug and Play and ActiveX
- Used FAT16 file system

Windows 98 and ME

- More Stable than Win 95
- Used FAT32 file system
- Win ME introduced System Restore
- Win 95, 98, and ME are collectively called "Win 9x"



TSA Carry-On Baggage Scanners Easy To Hack

- They run Windows 98
- Use plaintext passwords
 - Research from Billy K Rios, published 2-11-14

Windows NT 3.51 Server/Workstation

- No dependence on DOS kernel
- Domains and Domain Controllers
- NTFS File System to replace FAT16 and FAT32
- Much more secure and stable than Win9x
- Many companies still use Win NT Server Domain Controllers
- Win NT 4.0 was an upgrade

Windows 2000 Server/Professional

- Upgrade of Win NT

- Active Directory

- Powerful database storing information about all objects in a network

- Users, printers, servers, etc.

- Based on Novell's Novell Directory Services

- Enumerating this system would include enumerating Active Directory

Windows XP Professional

- Much more secure, especially after Service Pack 2
 - Windows File Protection
 - Data Execution Prevention
 - Windows Firewall

Bill Gates: Trustworthy Computing

Bill Gates  01.17.02

This is the e-mail Bill Gates sent to every full-time employee at Microsoft, in which he describes the company's new strategy emphasizing security in its products.

From: Bill Gates

Sent: Tuesday, January 15, 2002 5:22 PM

To: Microsoft and Subsidiaries: All FTE

Subject: Trustworthy computing

Every few years I have sent out a memo talking about the highest priority for Microsoft. Two years ago, it was the kickoff of our .NET strategy. Before that, it was several memos about the importance of the Internet to our future and the ways we could make the Internet truly useful for people. Over the last year it has become clear that ensuring .NET is a platform for Trustworthy Computing is more important than any other part of our work. If we don't do this, people simply won't be willing - or able -- to take advantage of all the other great work we do. Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing.

 Link Ch 6n

Windows Server 2003

- Much more secure, especially after Service Pack 1
 - Network services are closed by default
 - Internet Explorer security set higher

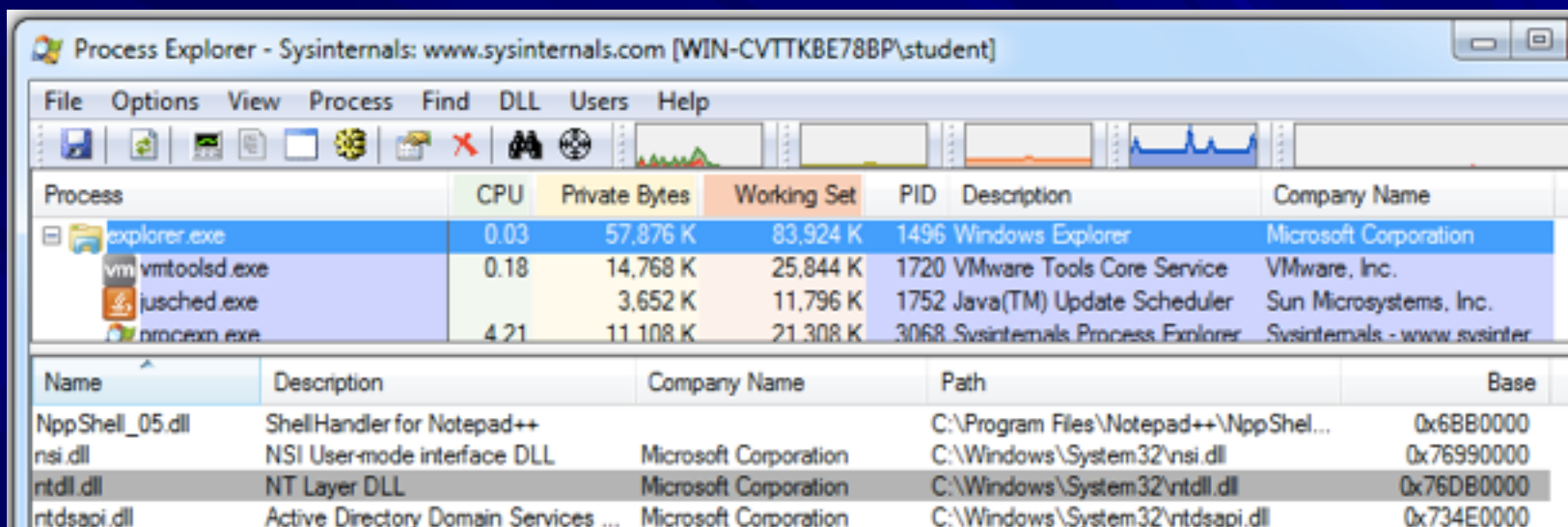
Windows Vista

- User Account Control
 - Users log in with low privileges for most tasks
- BitLocker Drive Encryption
- Address Space Layout Randomization (ASLR)

ASLR Demo

- Download Process Explorer (link Ch 3e)
- View, Show Lower Pane
- View, Lower Pane View, DLLS
- View, Select Columns, DLL tab, Base Address
- Select explorer.exe and find ntdll.dll
- Reboot to see base address change

ASLR on Windows 7

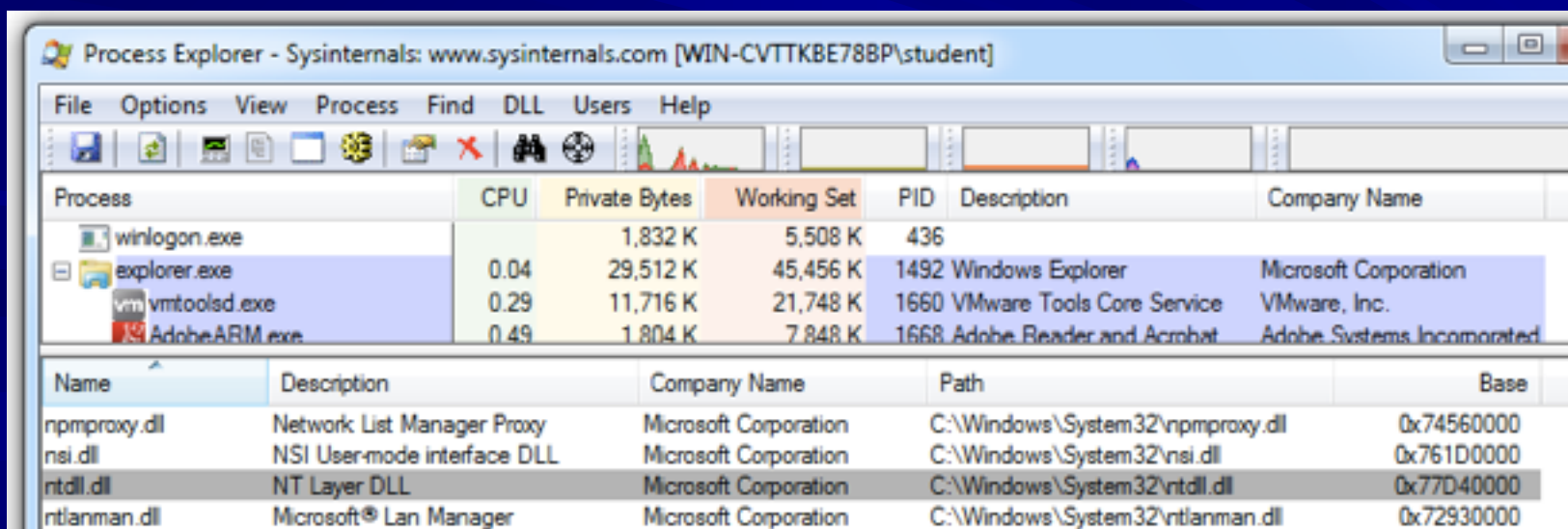


Process Explorer - Sysinternals: www.sysinternals.com [WIN-CVTTKBE78BP\student]

File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
explorer.exe	0.03	57,876 K	83,924 K	1496	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.18	14,768 K	25,844 K	1720	VMware Tools Core Service	VMware, Inc.
jusched.exe		3,652 K	11,796 K	1752	Java(TM) Update Scheduler	Sun Microsystems, Inc.
procexpn.exe	4.21	11,108 K	21,308 K	3068	Sysinternals Process Explorer	Sysinternals - www.sysinter

Name	Description	Company Name	Path	Base
NppShell_05.dll	ShellHandler for Notepad++		C:\Program Files\Notepad++\NppShel...	0x6BB0000
nsi.dll	NSI User-mode interface DLL	Microsoft Corporation	C:\Windows\System32\nsi.dll	0x76990000
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll	0x76DB0000
ntdsapi.dll	Active Directory Domain Services ...	Microsoft Corporation	C:\Windows\System32\ntdsapi.dll	0x734E0000



Process Explorer - Sysinternals: www.sysinternals.com [WIN-CVTTKBE78BP\student]

File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
winlogon.exe		1,832 K	5,508 K	436		
explorer.exe	0.04	29,512 K	45,456 K	1492	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.29	11,716 K	21,748 K	1660	VMware Tools Core Service	VMware, Inc.
AdobeARM.exe	0.49	1,804 K	7,848 K	1668	Adobe Reader and Acrobat	Adobe Systems Incorporated

Name	Description	Company Name	Path	Base
npmproxy.dll	Network List Manager Proxy	Microsoft Corporation	C:\Windows\System32\npmproxy.dll	0x74560000
nsi.dll	NSI User-mode interface DLL	Microsoft Corporation	C:\Windows\System32\nsi.dll	0x761D0000
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll	0x77D40000
ntlanman.dll	Microsoft® Lan Manager	Microsoft Corporation	C:\Windows\System32\ntlanman.dll	0x72930000

Windows Server 2008

- User Account Control
- BitLocker Drive Encryption
- ASLR
- Network Access Protection
 - Granular levels of network access based on a clients level of compliance with policy
- Server Core
 - Small, stripped-down server, like Linux
- Hyper-V
 - Virtual Machines

Windows 7

- XP Mode
 - A virtual machine running Win XP
- User Account Control was refined and made easier to use

Windows 8

- Built-in antivirus
- SmartScreen protects against phishing and social engineering by using a URL and application reputation system
- Windows 8 secure boot using EFI on ARM prevents rootkits

Windows Server 2012

- Authentication Silos to reduce the risk of pass-the-hash attacks
- DNSSEC which will someday make DNS resolutions more secure

Windows 10

- Brings back the Start button
- Forced automatic updates
- Device Guard allows only trusted apps to run
- Credential Guard uses virtualization to protect access tokens from theft
 - Reducing the risk of pass-the-hash attacks

Windows Server 2016

- Windows Containers
 - Like little virtual machines
 - Can isolate services from one another

NetBIOS Basics

- Network Basic Input Output System (NetBIOS)
 - Programming interface
 - Allows computer communication over a LAN
 - Used to share files and printers

NetBIOS names

- Computer names on Windows systems
- Limit of 16 characters
- Last character identifies type of service running
- Must be unique on a network

NetBIOS Suffixes

Table 6-2 NetBIOS names and suffixes

NetBIOS Name	Suffix	Description
<computer name>	00	The Workstation service registered the computer name (also referred to as the NetBIOS name).
<_MSBROWSE_>	01	Signifies that the computer is the master browser on the network. The master browser is responsible for notifying all computers on the network of any NetBIOS name changes or additions.
<computer name>	03	The computer is registered by the Messenger service, which the client uses when sending and receiving messages.
<computer name>	06	Registered by Routing and Remote Access Service (RRAS).
<computer name>	1F	Network Dynamic Data Exchange (NetDDE) services have been started on the computer. NetDDE is a system process that runs on Microsoft OSs to facilitate the exchange of network data.
<computer name>	20	Registered by the Server service. A computer must have this service running to share printers or files.

 For complete list, see link Ch 6h

NetBIOS Null Sessions

■ Null session

- Unauthenticated connection to a Windows computer
- Does not use logon and passwords values

■ Around for over a decade

- Still present on Windows XP
- Disabled on Server 2003
- Absent entirely in Vista and later versions

■ A large vulnerability

- See links Ch 6a-f

Null Session Information

- Using these NULL connections allows you to gather the following information from the host:
 - List of users and groups
 - List of machines
 - List of shares
 - Users and host SIDs (Security Identifiers)
 - From brown.edu (link Ch 6b)

NetBIOS Enumeration Tools

■ Nbtstat command

- Powerful enumeration tool included with the Microsoft OS
- Displays NetBIOS table

```
F:\Install\hacking>nbtstat -a 192.168.2.15
```

```
SAMCO:
```

```
Node IpAddress: [192.168.2.14] Scope Id: []
```

NetBIOS Remote Machine Name Table

Name		Type	Status
S214-17-SAM2	<00>	UNIQUE	Registered
WORKGROUP	<00>	GROUP	Registered
S214-17-SAM2	<20>	UNIQUE	Registered
S214-17-SAM2	<03>	UNIQUE	Registered
WORKGROUP	<1E>	GROUP	Registered

```
MAC Address = 00-0C-29-3B-D9-BE
```

NetBIOS Enumeration Tools

- Net view command
 - Shows whether there are any shared resources on a network host

```
F:\Install\hacking>net view
Server Name          Remark
-----
\\RICKHP
\\S214-00
\\S214-17-SAM2
\\SAM2G
\\SAMP4
The command completed successfully.
```

```
F:\Install\hacking>net view 192.168.2.15
Shared resources at 192.168.2.15

Share name          Type  Used as  Comment
-----
My Documents        Disk
The command completed successfully.
```

NetBIOS Enumeration Tools (continued)

- Net use command
 - Used to connect to a computer with shared folders or files

Additional Enumeration Tools

- Windows tools included with BackTrack
 - Smb4K tool
- DumpSec
- Hyena
- Nessus and OpenVAS

Using Windows Enumeration Tools

■ In Kali: enum4linux

- Used to enumerate Windows computers in a network

– Image from <https://i0.wp.com/hackercool.com/wp-content/uploads/2016/07/enum4linux1.png>

```
root@kali:~# enum4linux -U 192.168.25.129
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4l
/ ) on Mon Jul 18 05:50:24 2016

=====
|   Target Information   |
=====
Target ..... 192.168.25.129
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, n

=====
| Enumerating Workgroup/Domain on 192.168.25.129 |
=====
[+] Got domain/workgroup name: WORKGROUP ←
=====
|   Session Check on 192.168.25.129   |
=====
[+] Server 192.168.25.129 allows sessions using username '', password ''
```


DumpSec

- Enumeration tool for Windows systems
 - Produced by Foundstone, Inc.
- Allows user to connect to a server and “dump”:
 - Permissions for shares
 - Permissions for printers
 - Permissions for the Registry
 - Users in column or table format
 - Policies
 - Rights
 - Services

Hyena

- Excellent GUI product for managing and securing Windows OSs
 - Shows shares and user logon names for Windows servers and domain controllers
 - Displays graphical representation of:
 - Microsoft Terminal Services
 - Microsoft Windows Network
 - Web Client Network
 - Find User/Group

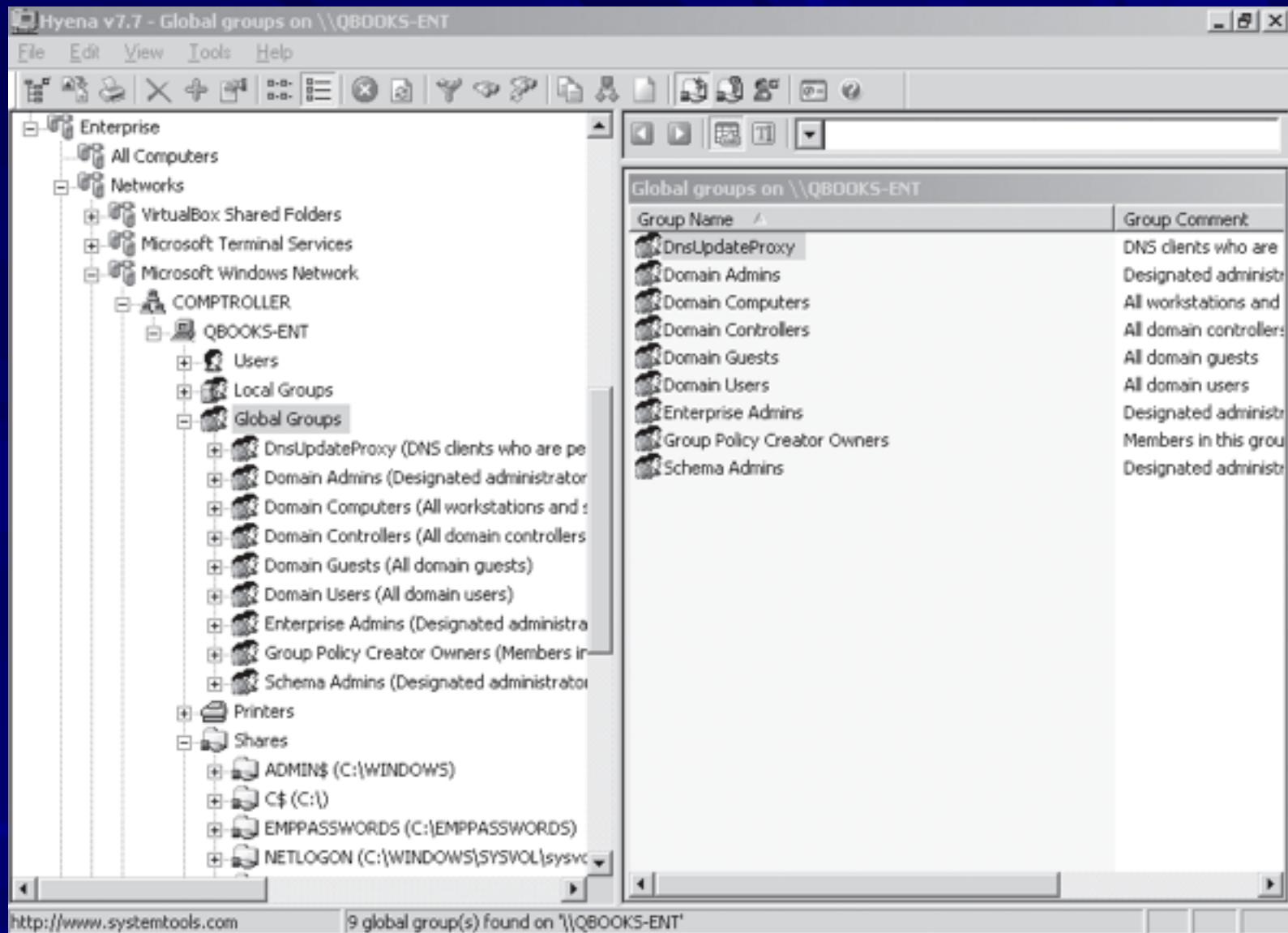


Figure 6-8 The Hyena interface

Nessus and OpenVAS

■ OpenVAS

- Operates in client/server mode
- Open-source descendent of Nessus
 - Popular tool for identifying vulnerabilities

■ Nessus Server and Client

- Latest version can run on Windows, Mac OS X, FreeBSD, and most Linux distributions
- Handy when enumerating different OSs on a large network
 - Many servers in different locations

Enumerating the *nix Operating System

- Several variations
 - Solaris and OpenSolaris
 - HP-UX
 - Mac OS X and OpenDarwin
 - AIX
 - BSD UNIX
 - FreeBSD
 - OpenBSD
 - NetBSD
 - Linux, including several distributions

Enumerating the *nix Operating System

- Simple Network Management Protocol (SNMP)
 - Enables remote administration of servers, routers, switches, firewalls, and other devices
 - Can be used on Windows and Linux

snmpwalk in Kali

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# snmpwalk -v 2c -c public 192.168.0.17  
iso.3.6.1.2.1.1.1.0 = STRING: "Linux metasploitable 2.6.24-16-server #1 SMP Thu  
Apr 10 13:58:00 UTC 2008 i686"  
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10  
iso.3.6.1.2.1.1.3.0 = Timeticks: (245081) 0:40:50.81  
iso.3.6.1.2.1.1.4.0 = STRING: "msfdev@metasploit.com"  
iso.3.6.1.2.1.1.5.0 = STRING: "metasploitable"  
iso.3.6.1.2.1.1.6.0 = STRING: "Metasploit Lab"  
iso.3.6.1.2.1.1.8.0 = Timeticks: (1) 0:00:00.01  
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1  
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1  
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1  
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1  
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.2.1.49  
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.4  
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50  
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.6.3.16.2.2.1  
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."  
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatchin  
g."  
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for th  
e SNMP User-based Security Model."  
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"  
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "The MIB module for managing TCP implementatio
```

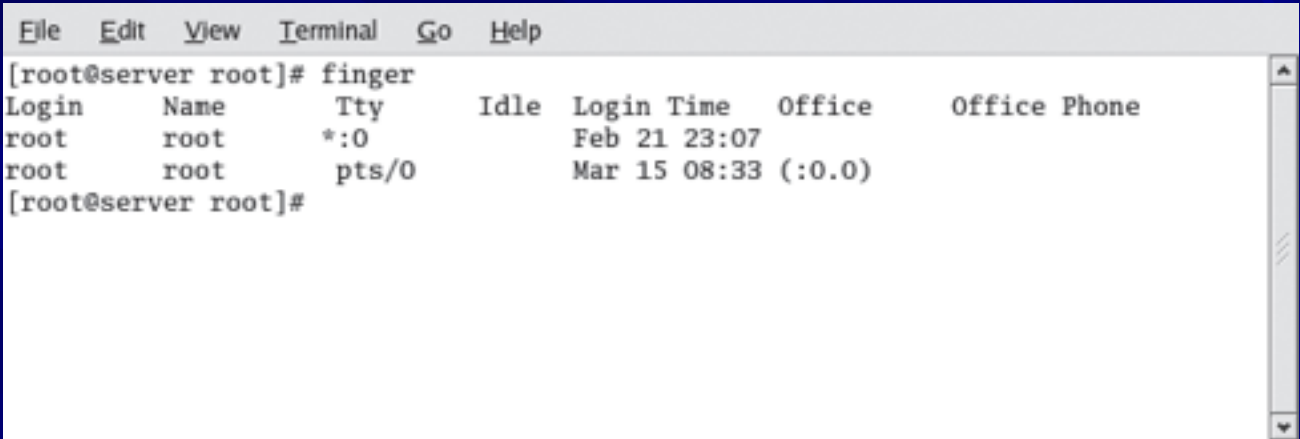
UNIX Enumeration

■ Finger utility

- Most popular enumeration tool for security testers
- Finds out who is logged in to a *nix system
- Determines who was running a process

■ Nessus

- Another important *nix enumeration tool

A terminal window with a menu bar containing 'File', 'Edit', 'View', 'Terminal', 'Go', and 'Help'. The prompt is '[root@server root]#'. The command 'finger' has been executed, resulting in a table of user information. The table has columns for Login, Name, Tty, Idle, Login Time, Office, and Office Phone. Two entries are shown for the user 'root'.

```
[root@server root]# finger
Login   Name    Tty      Idle   Login Time   Office   Office Phone
root    root    *:0      Idle   Feb 21 23:07
root    root    pts/0    Mar 15 08:33 (:0.0)
[root@server root]#
```

Figure 6-25 Using the Finger command

Nessus Scanning Linux

The screenshot shows the Nessus interface for a 'Thorough Linux Server Scan'. The main section is titled 'Vulnerability Summary' and displays a list of critical vulnerabilities. The interface includes a sidebar with 'Hosts' (1), 'Vulnerabilities' (174), and 'Export Results'. The top navigation bar contains 'Filter Options' (0), 'Audit Trail', and 'Delete All Results'. The vulnerability list includes:

Severity	Vulnerability Description	Category	Count
critical	ProFTPD < 1.3.3c Multiple Vulnerabilities	FTP	1
critical	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 / 10.04 LTS / 10.10...	Ubuntu Local Security Checks	1
critical	Unsupported Unix Operating System	General	1
critical	Default Password (toor) for 'root' Account	Default Unix Accounts	1
critical	ProFTPD < 1.3.0a Multiple Vulnerabilities	FTP	1
critical	Apache 2.2 < 2.2.15 Multiple Vulnerabilities	Web Servers	1
critical	ProFTPD < 1.3.3d 'mod_sql' Buffer Overflow	FTP	1
critical	Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow	Web Servers	1
critical	Ubuntu 6.06 LTS / 8.04 LTS / 9.04 / 9.10 : krb5 vulnerabilit...	Ubuntu Local Security Checks	1

Image from tenable.com