

Fourth Edition

# Hands-On Ethical Hacking and Network Defense

MICHAEL T. SIMPSON  
NICHOLAS D. ANTILL  
ROBERT S. WILSON

# Hands-On Ethical Hacking and Network Defense, Edition 4

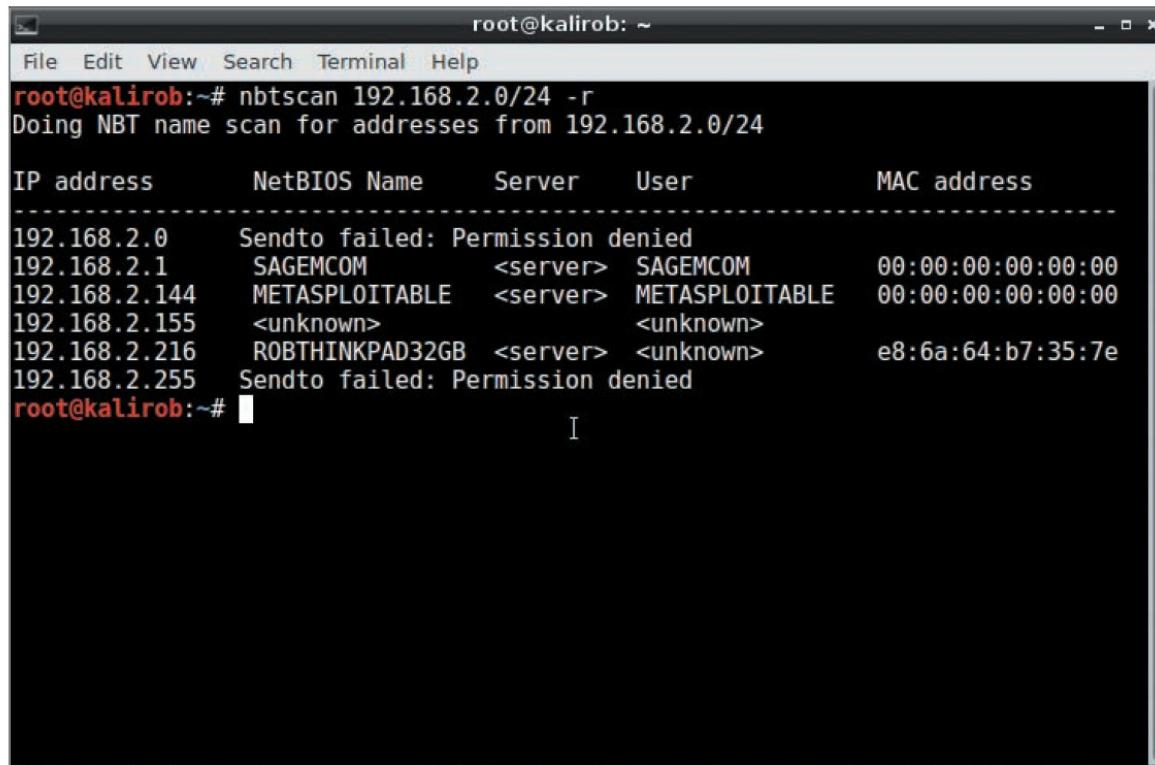
## Module 6: Enumeration

# Introduction to Enumeration (1 of 2)

- **Enumeration** refers to the process of extracting information from a network about the following:
  - Resources or shares on the network
  - Network topology and architecture
  - Usernames or groups assigned on the network
  - Information about users and recent logon times
- Port scanning and footprinting
  - Used to determine what operating system (OS) is used
- Enumeration is more intrusive
  - Attempting to access a resource, not just identifying it

# Introduction to Enumeration (2 of 2)

- NBTscan (NetBIOS over TCP/IP)
  - Tool for enumerating Windows OSs that is part of the Kali Linux suite of security tools



A terminal window titled "root@kalirob: ~" showing the output of the nbtscan command. The command "nbtscan 192.168.2.0/24 -r" is run, followed by the message "Doing NBT name scan for addresses from 192.168.2.0/24". The output lists network devices with their IP addresses, NetBIOS names, server types, users, and MAC addresses. Some entries show permission denied errors.

IP address	NetBIOS Name	Server	User	MAC address
192.168.2.0	Sendto failed: Permission denied			
192.168.2.1	SAGEMCOM	<server>	SAGEMCOM	00:00:00:00:00:00
192.168.2.144	METASPLOITABLE	<server>	METASPLOITABLE	00:00:00:00:00:00
192.168.2.155	<unknown>		<unknown>	
192.168.2.216	ROBTHINKPAD32GB	<server>	<unknown>	e8:6a:64:b7:35:7e
192.168.2.255	Sendto failed: Permission denied			

Source: Kali Linux

# Enumerating Windows Operating Systems

- Brief look at Windows OSs
  - To understand how an attacker might gain access to resources or shares on a Windows network
- This chapter focuses on Windows OS as it relates to enumeration
  - Little information can be enumerated from Windows systems after Windows 7

# Windows OS Descriptions (1 of 7)

Windows OS version	Description
Windows 95	The first Microsoft GUI product that doesn't rely on DOS, Windows 95 is the beginning of plug and play and the ActiveX standard used in all Windows versions today. A major enhancement is the Registry, a database storing information about the system's hardware and software. Previously, this information was stored in files. Windows 95 runs on stand-alone and networked computers and uses the FAT16 file system. Version OSR2 adds support for FAT32.
Windows 98 and Me	Compared to their predecessors, these versions have an improved file system (FAT32), new hardware support, and better backup and recovery tools. The enumeration process for Windows Me is the same as for Windows 98.
Windows NT 3.51 Server/Workstation	These OSs were created with security and enhancement of network functionality in mind. They emphasize domains instead of workgroups and use the client/server model instead of peer-to-peer networks; the server is responsible for authenticating users and giving them access to network resources. The client/server model also allows for having many computers in a domain instead of the limited number of computers in a workgroup. NTFS replaces FAT16 and FAT32 because of the difficulty in incorporating security in the earlier file systems.

# Windows OS Descriptions (2 of 7)

Windows OS version	Description
Windows NT 4.0 Server/Workstation	These upgrades to Windows NT 3.51 have improved GUIs and performance.
Windows 2000 Server/Professional	In this upgrade to NT, Microsoft includes Active Directory (AD) for object storage. AD is more scalable than other available solutions for managing large networks. It uses Lightweight Directory Access Protocol (LDAP), which is still in use today. Also, this update includes the first version of Microsoft Management Console (MMC) and Encrypted File System (EFS). Enumeration of these OSs includes enumerating Active Directory.

# Windows OS Descriptions (3 of 7)

Windows OS version	Description
Windows XP Professional	<p>This OS includes Windows 2000 features, such as standards-based security, improved manageability, and the MMC. In addition, Windows XP has an improved user interface and better plug-and-play support. Security improvements in the kernel data structures make them read-only to prevent rogue applications from affecting the OS core, and Windows File Protection is added to prevent overwriting core system files. With Service Pack 2 (SP2), security is improved further with features such as Data Execution Prevention (DEP) and a firewall enabled by default. DEP fixes a security exposure caused by vulnerable running services that hackers often use for buffer overflow attacks, and the firewall makes it more difficult for hackers to exploit Windows service vulnerabilities and enumerate shares and services. In fact, enumeration of Windows XP SP2 and later systems can be difficult without modifying the configuration. Disabling the Windows Firewall is common in corporate networks, but this practice gives hackers additional attack surface. In these environments, the enumeration processes used for earlier Windows versions still work much the same way in Windows XP Professional.</p>

# Windows OS Descriptions (4 of 7)

Windows OS version	Description
Windows Server 2003	<p>Windows Server 2003 includes improvements over Windows 2000 in some security areas, such as Internet Information Services (IIS), and comes in four editions. Generally, all editions include Remote Desktop, load balancing, VPN support, management services such as Windows Management Instrumentation (WMI), and .NET application services. The higher-end editions offer better support for PKI, certificate services, and Active Directory as well as enhancements to reliability, scalability, manageability, and security. Even with improvements in security and stability, enumeration techniques described for other Windows versions are effective with Windows Server 2003.</p>
Windows Vista	<p>Vista comes in several editions and is the first Windows version to introduce User Account Control (UAC) and built-in full drive encryption, called BitLocker (available in Vista Enterprise and Ultimate editions). UAC allows running Vista in nonprivileged mode to prevent unwanted code or user actions from damaging or controlling the computer (maliciously or inadvertently). However, UAC has been widely criticized because of its intrusive security prompts that force many users to disable it. In Windows 7, you can configure the frequency of these prompts. Also introduced in</p>

# Windows OS Descriptions (5 of 7)

Windows OS version	Description
Windows Server 2008	<p>This OS features security options similar to Vista, including BitLocker drive encryption and UAC. Vista and Windows Server 2008 support Network Access Protection (NAP), which reduces the possibility of rogue systems being able to access network resources. Features, services, and roles in Windows Server 2008 can be fine-tuned to meet specific needs. A command-line version that requires fewer resources, called Server Core, is available for certain server roles. This version is designed to reduce maintenance, use of resources, and the "attack surface." Hyper-V, a full-featured virtualization product, is included with Windows Server 2008 and allows installing guest OSs, such as Linux and other Windows versions.</p>
Windows 7	<p>Windows 7 builds on the security advances made in Vista with the introduction of AppLocker, which allows for control over application execution. Including the Action Center in Windows 7 allows users to view potential configurations in one simple interface. Other improvements include refinements to the UAC feature and Windows Defender, which protect the system from known spyware.</p>

# Windows OS Descriptions (6 of 7)

Windows OS version	Description
Windows 8.1	Boasting “groundbreaking malware resistance,” Windows 8.1 comes with features that make user-level infection much less dangerous by limiting the privileges of basic users. In addition, Windows 8.1 includes several heap integrity checks designed to make exploitation more difficult. Upgrades to Windows Defender make it a full anti-malware product. SmartScreen is extended to the OS to display an alert when an application is launched on a PC. For the first time, SecureBoot prevents execution of non-trusted boot content, preventing rootkits/bootkits.
Windows Server 2012	With this edition, Microsoft introduces Authentication Silos to prevent pass-the-hash attacks, a major weakness in all earlier versions of Windows servers. It also includes enhanced support for Domain Name System Security Extensions (DNSSEC), which relies on digital signatures to prove zone ownership.

# Windows OS Descriptions (7 of 7)

Windows OS version	Description
Windows 10	Designed for use on tablets, gaming consoles, and traditional PCs, Windows 10 can be found in more places than ever. Numerous security enhancements were brought to Windows 10. One of the more progressive enhancements is that it only allows trusted apps by default through Device Guard. It also adds Credential Guard, which uses virtualization to protect access tokens from theft by attackers. Originally released in 2015, Windows 10 has improved through many feature and security enhancements. Windows 10 was supposed to be the last name change for Windows, but it is rumored that the next major release of Windows in 2021 will be called Windows 11.
Windows Server 2016	Windows Server 2016 features a number of security upgrades. The most important, Windows Containers, allows for application isolation to protect applications from one another. Windows Defender (malware protection) is now enabled by default. In this version, the option for telnet server is eliminated completely (telnet client is still available). A feature named Just Enough Administration (JEA) allows for more detailed access control settings on tasks.
Windows Server 2019	Windows Server 2019 was developed concurrently with Windows 10. It contains a

# NetBIOS Basics (1 of 3)

- **Network Basic Input Output System (NetBIOS)**
  - Programming interface
  - Allows computer communication over a LAN
  - Most Windows OSs use it to share files and printers
    - Requires an upper-level service called Server Message Block (SMB)
  - Listens on UDP ports 137 and 138 and TCP port 139
- NetBIOS names
  - Computer names assigned to Windows systems
  - Have a limit of 16 characters
  - Last character is reserved for a hexadecimal number that identifies the type of service running on the computer
  - Must be unique on a network

# NetBIOS Basics (2 of 3)

NetBIOS name	Suffix	Description
<i>computer name</i>	00	The Workstation service registered the computer name (also called the NetBIOS name).
<i>computer name</i>	20	Registered by the Server service. A computer must have this service running to share printers or files.
<i>computer name</i>	22	Registered by the Microsoft Exchange Interchange service.
<i>computer name</i>	23	Registered by the Microsoft Exchange Store service. A store is where mailboxes and public folders are stored.
<i>computer name</i>	24	Registered by the Microsoft Exchange Directory service.
<i>computer name</i>	87	Signifies that Microsoft Exchange Message Transfer Agent (MTA) is running on this computer.
<i>domain name</i>	00	Indicates that Domain Name System (DNS) is running.
<i>domain name</i>	1C	Identifies the computer as a domain controller.

# NetBIOS Basics (3 of 3)

- You do not need to memorize all the NetBIOS suffixes
  - But note that some identify the computer or server being enumerated as a stand-alone computer or domain controller
  - Hackers often exert more effort to attack computers identified as domain controllers
    - These systems store more information, including logon names for user accounts and network resources

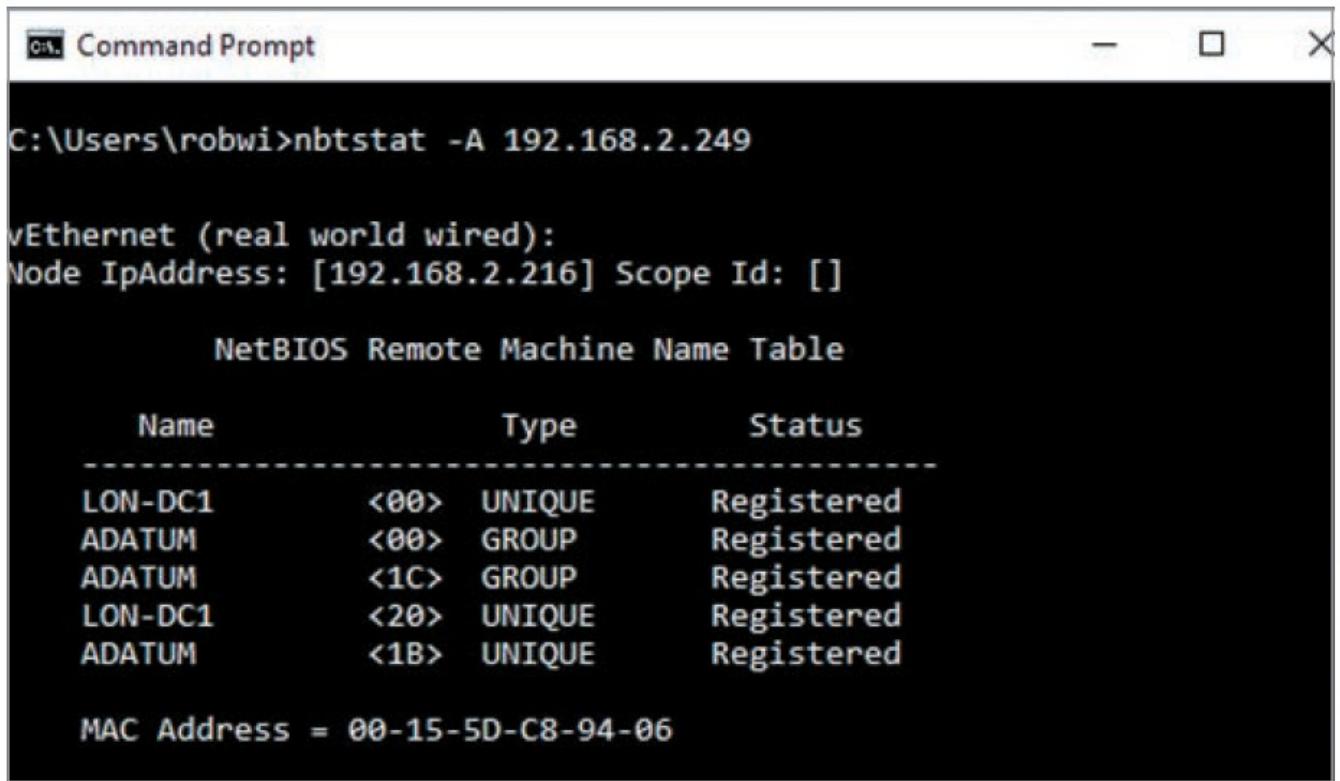
# NetBIOS Null Sessions

- **Null session**
  - Refers to an unauthenticated connection to a Windows computer
  - One of the biggest vulnerabilities of NetBIOS systems
  - Does not use logon and password values
- Many enumeration tools establish a null session to gather information such as logon accounts, group membership, and file shares from an attacked computer
- Has been around for more than a decade
  - Still present in Windows XP
  - Disabled by default in Windows Server 2003
  - Not available in Windows Vista and Server 2008

# NetBIOS Enumeration Tools (1 of 5)

- Nbtstat command
  - Powerful enumeration tool
  - Included with Windows
  - Displays the NetBIOS table
    - To display the NetBIOS table, type nbtstat -a IPaddress

# NetBIOS Enumeration Tools (2 of 5)



```
C:\Users\robwi>nbtstat -A 192.168.2.249

vEthernet (real world wired):
NodeIpAddress: [192.168.2.216] Scope Id: []

      NetBIOS Remote Machine Name Table

      Name          Type        Status
      -----
LON-DC1        <00>    UNIQUE    Registered
ADATUM         <00>    GROUP     Registered
ADATUM         <1C>    GROUP     Registered
LON-DC1        <20>    UNIQUE    Registered
ADATUM         <1B>    UNIQUE    Registered

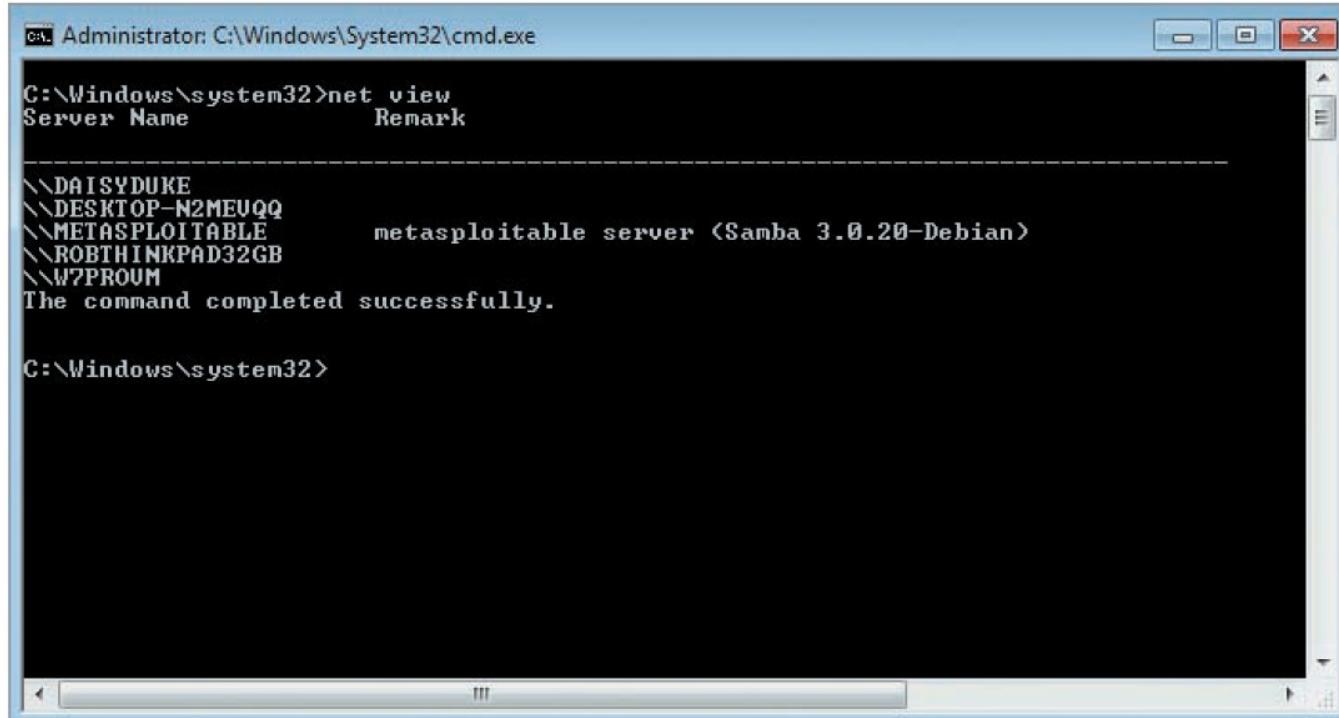
MAC Address = 00-15-5D-C8-94-06
```

Source: Kali Linux

**Figure 6-2** Using the Nbtstat command

# NetBIOS Enumeration Tools (3 of 5)

- Another built-in Windows tool is the net view command
  - Shows shared resources on a computer or server
  - To display syntax for this command, type net view ?



The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\System32\cmd.exe". The command "net view" has been run, displaying a list of shared resources. The output is as follows:

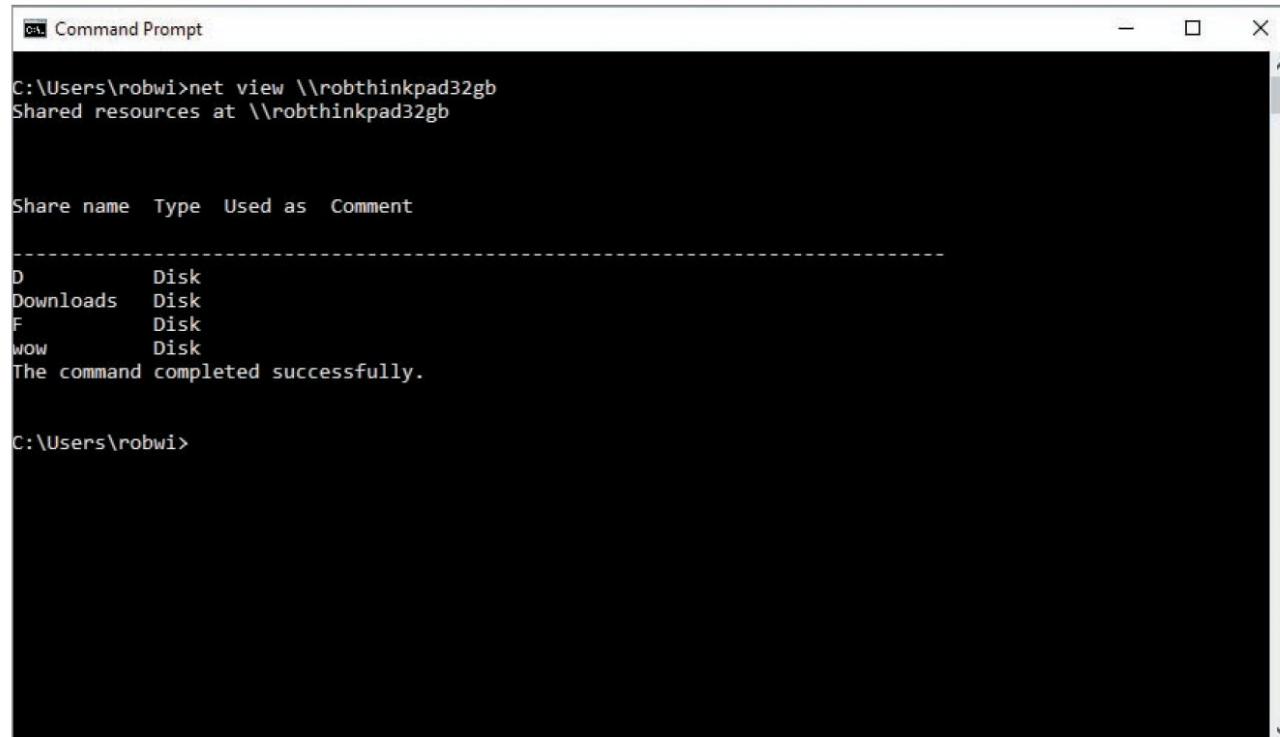
```
C:\>Administrator: C:\Windows\System32\cmd.exe
C:\>Windows\system32>net view
Server Name          Remark
-----
\\DAISYDUKE
\\DESKTOP-N2MEUQQ
\\METASPLOITABLE      metasploitable server (Samba 3.0.20-Debian)
\\ROBTHINKPAD32GB
\\W7PROUM
The command completed successfully.

C:\>Windows\system32>
```

Source: Microsoft Windows

# NetBIOS Enumeration Tools (4 of 5)

- You can also use the IP address or hostname of computers you discovered with port-scanning tools



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is "net view \\robthinkpad32gb". The output displays shared resources at the specified location, listing four disk shares: D, Downloads, F, and wow. The command concludes with a success message. The source of the image is Microsoft Windows.

```
C:\Users\robwi>net view \\robthinkpad32gb
Shared resources at \\robthinkpad32gb

Share name  Type  Used as  Comment
-----
D           Disk
Downloads   Disk
F           Disk
wow         Disk
The command completed successfully.

C:\Users\robwi>
```

source: Microsoft Windows

# NetBIOS Enumeration Tools (5 of 5)

- Although you can download or buy enumeration tools, you should learn how to take advantage of the tools available in Windows
  - A simple command-line utility can give you the name of a logged-on user
  - User's password can then be guessed in order to gain access to a system

# Additional Enumeration Tools (1 of 9)

- **enum4linux**
  - Enumeration tool for Windows and Samba systems
  - Written in Perl and uses the Samba tools smbclient, rpclient, net, and nmblookup
  - Must run it on a system that supports Perl, such as Kali Linux

# Additional Enumeration Tools (2 of 9)

- DumpSec
  - Enumeration tool for Windows NT, 2000, and XP systems
  - Does not work well on newer versions of Windows
  - Produced by Foundstone, Inc.
  - Allows user to connect to a server and “dump” the following information:
    - Permissions for shares
    - Permissions for printers
    - Permissions for the Registry
    - Users in column or table format
    - Policies
    - Rights
    - Services

# Additional Enumeration Tools (3 of 9)

- Hyena
  - Excellent GUI tool for managing and securing Windows OSs
  - Easy to use interface
  - Gives security professionals a wealth of information
  - Paid-for tool but has a free trial you can experiment with
  - 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

# Additional Enumeration Tools (4 of 9)

- OpenVAS (known as Greenbone Security Assistant)
  - Operates in client/server mode
  - Open-source descendant of Nessus
    - Popular tool for identifying vulnerabilities
- Nessus Server and OpenVAS
  - Compatible with, and easy to install on, Kali Linux
  - Can use these tools interchangeably for most purposes when enumerating systems
- Nessus Essentials
  - Latest version can run on Windows, macOS, and Linux distributions
  - Handy tool when enumerating different OSs on a large network

# Additional Enumeration Tools (5 of 9)

The screenshot shows a web browser window for the Greenbone Security Manager. The URL is 192.168.2.253/omp?cmd=get\_res... . The page title is "Result: SSH Brute Force Logins With Default Credentials Reporting". The main content area displays a table with one row:

Vulnerability	Severity	QoD	Host	Location	Actions
SSH Brute Force Logins With Default Credentials Reporting	7.5 (High)	95%	192.168.2.144	22/tcp	

**Summary**  
It was possible to login into the remote SSH server using default credentials.  
As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

**Vulnerability Detection Result**  
It was possible to login with the following credentials <User>:<Password>  
msfadmin:msfadmin  
user:user

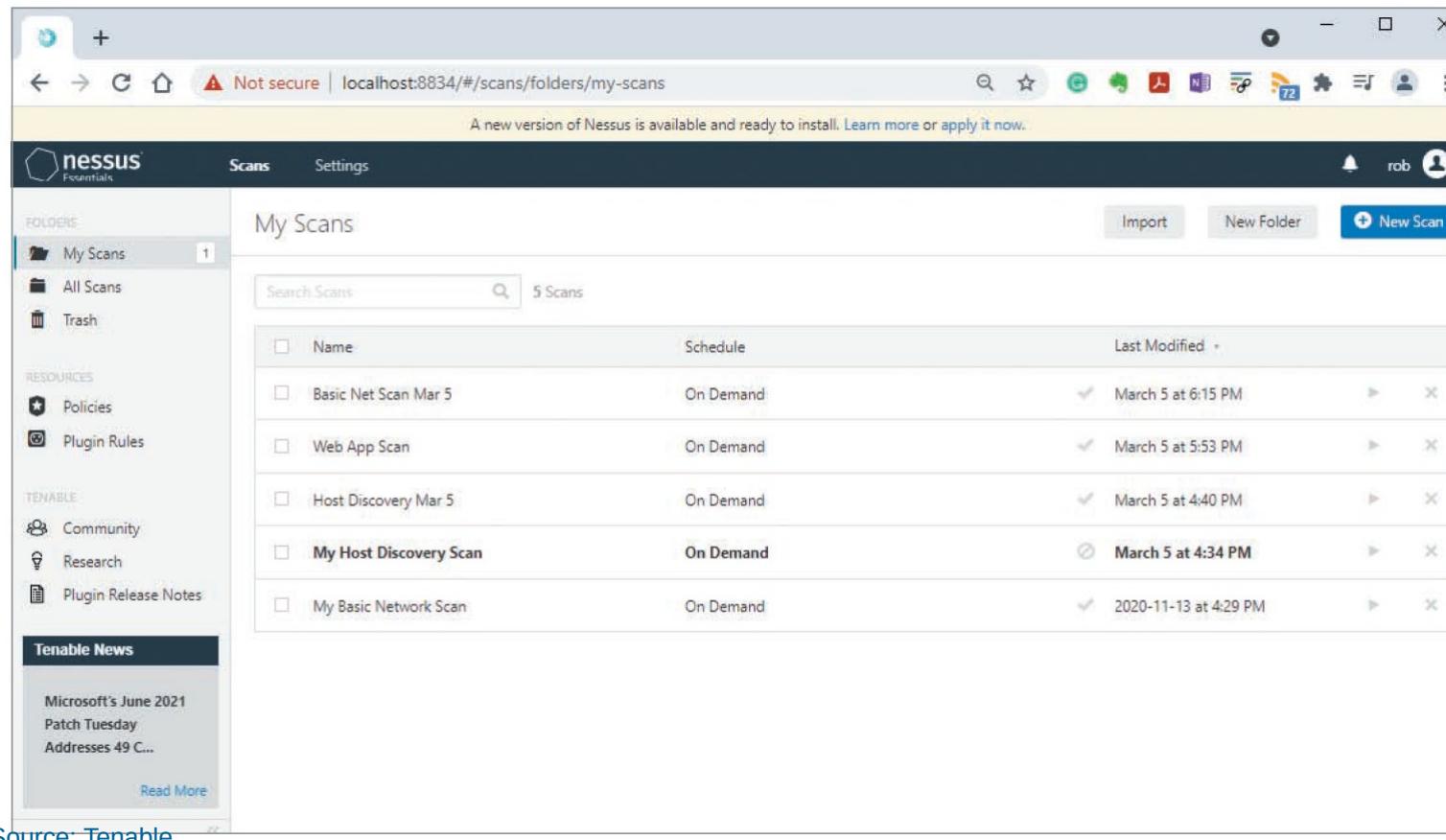
**Solution**  
Solution type: Mitigation  
Change the password as soon as possible.

**Vulnerability Detection Method**  
Try to login with a number of known default credentials via the SSH protocol.

Details: SSH Brute Force Logins With Default Credentials Reporting (OID: 1.3.6.1.4.1.25623.1.0.103239)  
Version used: \$Revision: 13568 \$

**Figure 6-9** OpenVAS enumerating a SSH Brute Force Logins With Default Credentials Vulnerability

# Additional Enumeration Tools (6 of 9)



The screenshot shows the Nessus interface on a web browser. The title bar indicates the URL is [localhost:8834/#/scans/folders/my-scans](http://localhost:8834/#/scans/folders/my-scans). A message at the top says, "A new version of Nessus is available and ready to install. [Learn more or apply it now.](#)" The main content area is titled "My Scans" and displays a table of five scan entries:

<input type="checkbox"/>	Name	Schedule	Last Modified	Actions
<input type="checkbox"/>	Basic Net Scan Mar 5	On Demand	March 5 at 6:15 PM	<a href="#">View</a> <a href="#">Delete</a>
<input type="checkbox"/>	Web App Scan	On Demand	March 5 at 5:53 PM	<a href="#">View</a> <a href="#">Delete</a>
<input type="checkbox"/>	Host Discovery Mar 5	On Demand	March 5 at 4:40 PM	<a href="#">View</a> <a href="#">Delete</a>
<input type="checkbox"/>	My Host Discovery Scan	On Demand	March 5 at 4:34 PM	<a href="#">View</a> <a href="#">Delete</a>
<input type="checkbox"/>	My Basic Network Scan	On Demand	2020-11-13 at 4:29 PM	<a href="#">View</a> <a href="#">Delete</a>

The left sidebar includes sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules), and TENABLE (Community, Research, Plugin Release Notes). A "Tenable News" box highlights "Microsoft's June 2021 Patch Tuesday Addresses 49 C..." with a "Read More" link. The bottom left corner credits "Source: Tenable".

Figure 6-10 Nessus Scans page

# Additional Enumeration Tools (7 of 9)

- The next several figures show Nessus in action
- This figure shows information Nessus has discovered using NetBIOS

The screenshot shows the Nessus web interface. The URL is `localhost:8834/#/scans/reports/27/vulnerabilities/group/11011/10150`. The main content area displays a report titled "SMB Scan / Plugin #10150". The report details a "Windows NetBIOS / SMB Remote Host Information Disclosure" vulnerability. It includes a "Description" section stating that the host is listening on UDP port 137 or TCP port 445 and replies to NetBIOS nbtscan or SMB requests. A note indicates that the plugin gathers information for other plugins but does not generate a report itself. The "Output" section shows gathered NetBIOS names:

W7PROV	= Computer name
WORKGROUP	= Workgroup / Domain name
W7PROV	= File Server Service
WORKGROUP	= Browser Service Elections

It also lists the MAC address of the remote host's adapter: 00:1E:5d:c8:94:00. A "Port - Hosts" table shows the connection 137/udp/nmbios-ns to 192.168.2.250. To the right, the "Plugin Details" panel provides the following information:

Severity:	Info
ID:	10150
Version:	1.91
Type:	remote
Family:	Windows
Published:	October 12, 1999
Modified:	February 10, 2021

The "Risk Information" section notes a "Risk Factor: None". A vertical "Source: Tenable" watermark is visible on the right side of the report.

# Additional Enumeration Tools (8 of 9)

- Additional Nessus scan to enumerate Server Message Block (SMB) shares has provided a list of folders that are accessible via SMB in this figure

The screenshot shows the Nessus interface with a report titled "SMB Scan / Plugin #10395". The report details "Microsoft Windows SMB Shares Enumeration". It states that Nessus was able to enumerate network share names. The output section lists shares available on the remote host when logged in as robwilson, including ADMIN\$, C\$, exploit, IPC\$, and Users. A table shows a single host entry: Port 445 / tcp / off, Host 192.168.2.250. The report includes sections for Plugin Details, Risk Information, and Vulnerability Information. The "Plugin Details" section provides the following information:

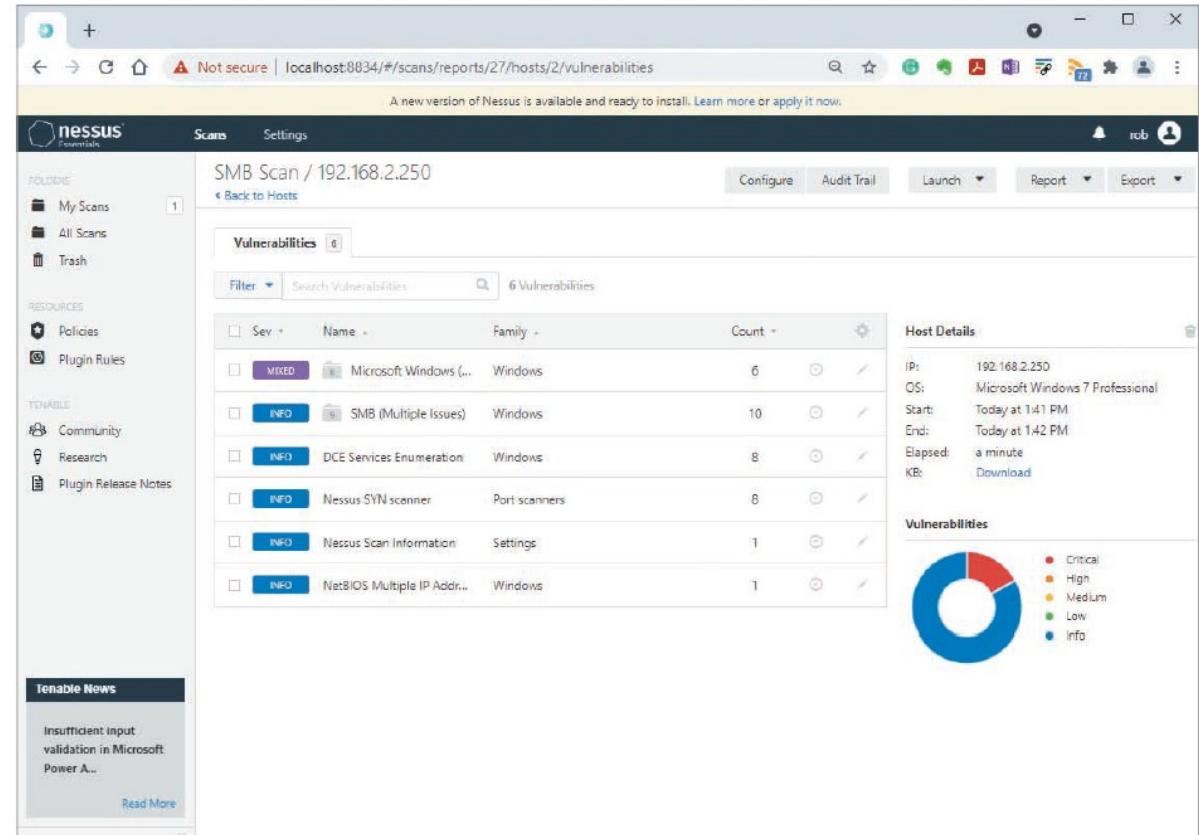
Severity:	Info
ID:	10395
Version:	1.47
Type:	local
Family:	Windows
Published:	May 9, 2000
Modified:	March 9, 2020

The "Risk Information" section notes that the Risk Factor is None. The "Vulnerability Information" section indicates Asset Inventory: True.

Source: Tenable

# Additional Enumeration Tools (9 of 9)

- Nessus is helpful in identifying the OS and service pack running on a computer



# Enumerating \*nix Operating System

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

# \*nix Enumeration (1 of 6)

- **Simple Network Management Protocol (SNMP)**
  - An old but still popular network management service for network administrators that enables remote administration
  - Can run on both Windows and \*nix
    - This section focuses on \*nix
- SNMP is useful for administrators who want to see:
  - System statistics
  - Version numbers
  - Other detailed host information remotely
- SNMP is also useful for hackers

# \*nix Enumeration (2 of 6)

- SNMPWalk
  - A tool useful in enumerating hosts running SNMP with the default configuration
  - If attackers know the processor architecture and the detailed version number of the remote operating system, they will have an easier time finding exploits that will be successful
  - The SNMP daemon (snmpd) listens on UDP port 161
  - SNMP often runs on network hardware such as routers, switches, and firewalls

# \*nix Enumeration (3 of 6)

```
root@kali:~# snmpwalk -c public 192.168.56.110 -v1
iso.3.6.1.2.1.1.1.0 = STRING: "Vyatta VyOS 1.1.6"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.30803
iso.3.6.1.2.1.1.3.0 = Timeticks: (1816453) 5:02:44.53
iso.3.6.1.2.1.1.4.0 = STRING: "root"
iso.3.6.1.2.1.1.5.0 = STRING: "vyos"
iso.3.6.1.2.1.1.6.0 = STRING: "Unknown"
iso.3.6.1.2.1.1.7.0 = INTEGER: 14
iso.3.6.1.2.1.1.8.0 = Timeticks: (14) 0:00:00.14
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.2.1.10.131
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.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
```

Source: GNU Open Source License

**Figure 6-14** Using the SNMPWalk command

# \*nix Enumeration (4 of 6)

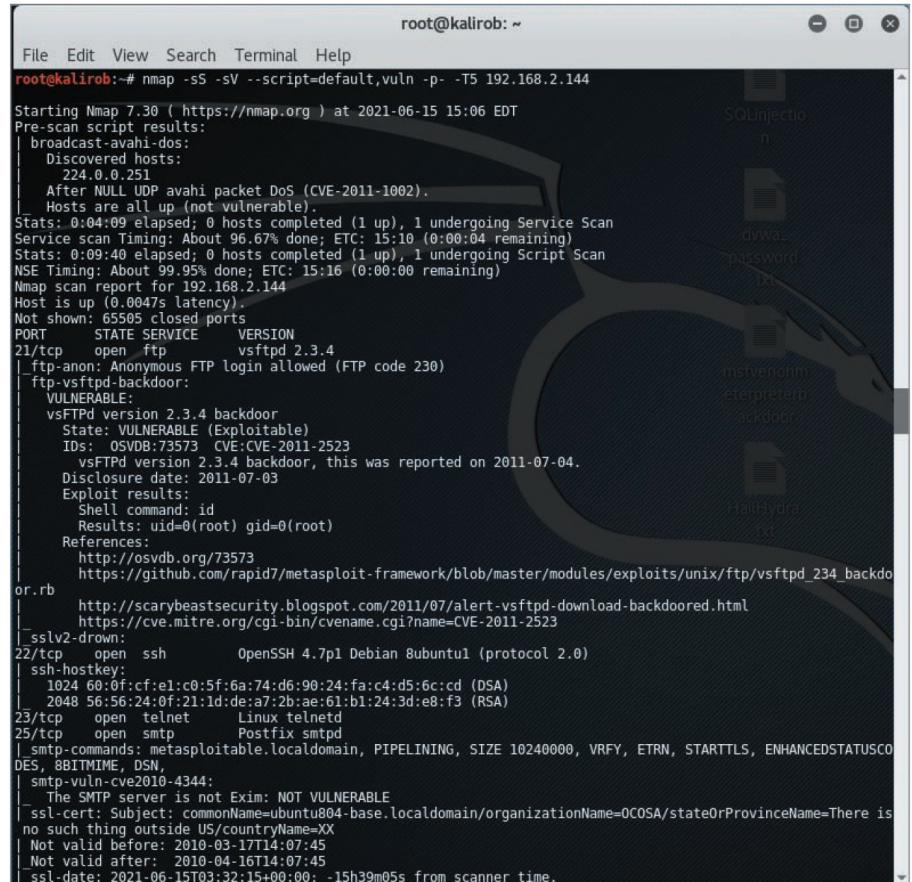
- Nessus is helpful in \*nix enumeration
- This figure shows what Nessus found when scanning a Ubuntu 15.10 system

The screenshot shows the Nessus web interface. The left sidebar has sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules), and TENABLE (Community, Research, Plugin Release Notes). A news banner at the bottom left says "Microsoft's June 2021 Patch Tuesday Addresses 49..." with a "Read More" link. The main content area shows a scan report for "CPE (plugin 45590) / Plugin #45590". It includes tabs for "Vulnerabilities" (18), "INFO" (Common Platform Enumeration (CPE)), and "Plugin Details". The "INFO" tab shows the description: "By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host." It also lists "See Also" links to cpe.mitre.org and nvd.nist.gov. The "Output" section displays the matched CPE strings: "cpe:/o:canonical:ubuntu\_linux:0.4", "cpe:/a:apache:http\_server:2.2.8", "cpe:/a:openbsd:openssh:4.7", "cpe:/a:php:php:5.6.14", "cpe:/a:postgresql:postgresql:9.1", and "cpe:/a:samba:samba:3.0.20". The "Port" and "Hosts" table shows one host at port N/A with IP 192.168.2.144. At the top right, there are buttons for Configure, Audit Trail, Launch, Report, and Export. A message at the top says "A new version of Nessus is available and ready to install. Learn more or apply it now." The URL in the address bar is localhost:8834/#/scans/reports/32/hosts/2/vulnerabilities/45590.

Source: Tenable

# \*nix Enumeration (5 of 6)

- NMap script scanning can also help an attacker gain information about remote \*nix hosts



```
root@kalirob:~# nmap -sS -sV --script=default,vuln -p- -T5 192.168.2.144
Starting Nmap 7.30 ( https://nmap.org ) at 2021-06-15 15:06 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|       After NULL UDP avahi packet DoS (CVE-2011-1002).
|       Hosts are all up (not vulnerable).
Stats: 0:04:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 15:10 (0:00:04 remaining)
Stats: 0:09:40 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.95% done; ETC: 15:16 (0:00:00 remaining)
Nmap scan report for 192.168.2.144
Host is up (0.0047s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: OSVDB:73573  CVE: CVE-2011-2523
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|           Results: uid=0(root) gid=0(root)
|       References:
|         http://osvdb.org/73573
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdo
or.rb
|           http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|           https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_sslv2-drown:
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_smtp-vuln-cve2010-4344:
|   The SMTP server is not Exim: NOT VULNERABLE
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is
no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| ssl-date: 2021-06-15T03:32:15+00:00; -15h39m05s from scanner time.
```

Source: GNU Open Source License

# \*nix Enumeration (6 of 6)

- Finger utility
  - An older but sometimes useful enumeration tool for security testers and hackers
  - Enables you to use a single command to find out who is logged on to a \*nix system
  - The Finger daemon (fingerd) listens on TCP port 79