Hands-On Ethical Hacking and Network Defense, Edition 4

Chapter 6: Enumeration

Module Objectives

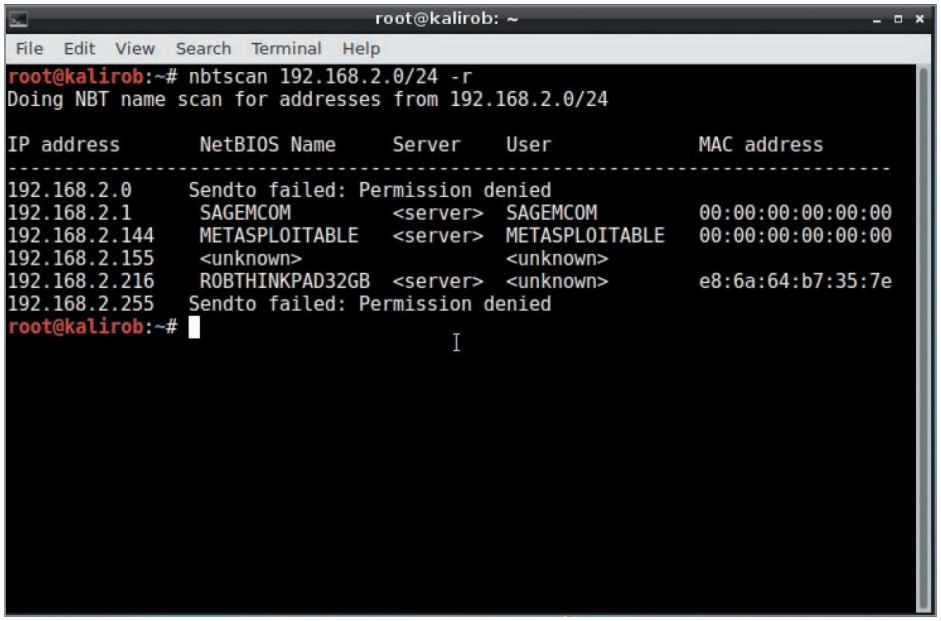
- By the end of this module, you should be able to:
  - Describe the enumeration step of security testing
  - Enumerate Windows OS targets
  - Enumerate *nix OS targets

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



Source: Kali Linux

Knowledge Check Activity 6-1

Which of the following testing processes is the most intrusive?

a. Port scanning
b. Enumeration
c. Null scanning
d. Numeration

Knowledge Check Activity 6-1: Answer

Which of the following testing processes is the most intrusive?

Answer: b. Enumeration

Enumeration is the most intrusive part of testing for security testers.

Polling Activity 6-1

Security testers conduct enumeration for which of the following reasons? (Choose all that apply.)

a. Gaining access to shares and network resources
b. Obtaining user logon names and group memberships
c. Discovering services running on computers and servers
d. Discovering open ports on computers and servers

Polling Activity 6-1: Answer

Security testers conduct enumeration for which of the following reasons? (Choose all that apply.)

Answer: a. and b. Gaining access to shares and network resources and obtaining user logon names and group memberships

Security testers conduct enumeration for gaining access to shares and network resources and obtaining user logon names and group memberships using many enumeration tools.

.

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 F A T16 file system. Version OSR2 adds support for F A T32.
Windows 98 and Me	Compared to their predecessors, these versions have an improved file system (F A T32), 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 F A T16 and F A T32 because of the difficulty in incorporating security in the earlier file systems. NTFS includes file-level security features not possible in F A T.

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	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.

Windows OS Descriptions (4 of 7)

Windows OS version	Description
Windows Server 2003	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.
Windows Vista	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 this release is Address Space Layout Randomization (ASLR), which makes exploitation of overflow-type vulnerabilities much more difficult. By default, Vista in a stand-alone environment can be difficult to enumerate without modifying its configuration.

Windows OS Descriptions (5 of 7)

Windows OS version	Description
Windows Server 2008	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.
Windows 7	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.

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 number of new features and security measures including container services, storage spaces direct, storage migration services, storage replication, shielded virtual machines, and improved Windows Defender Advanced Threat Protection (ATP).

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

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

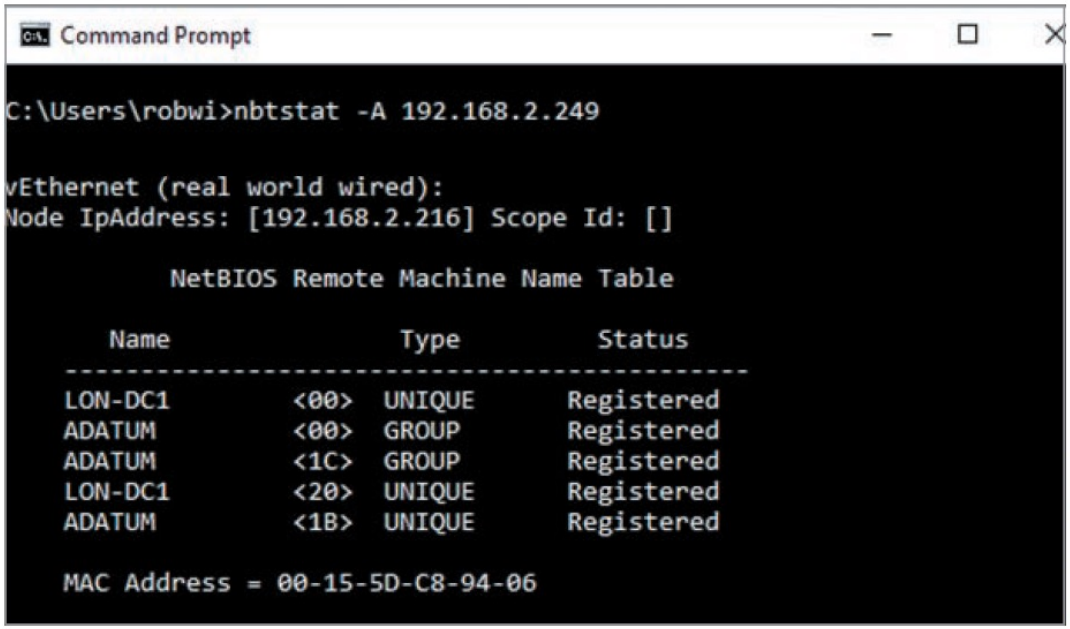
NetBIOS Null Sessions

- **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)

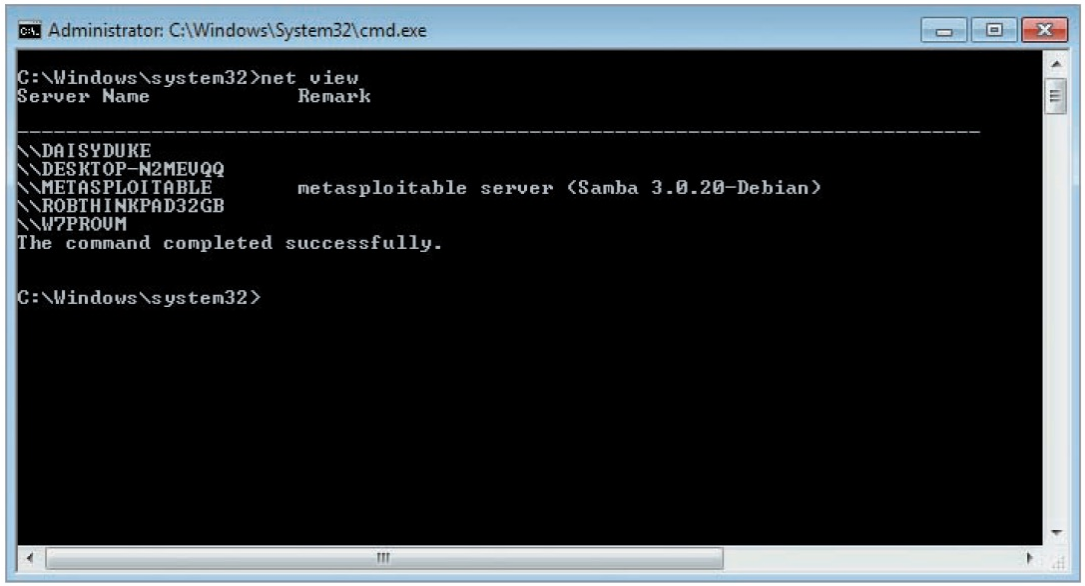


Source: Kali Linux

Figure 6-2 Using the Nbtstat command

NetBIOS Enumeration Tools (3 of 5)

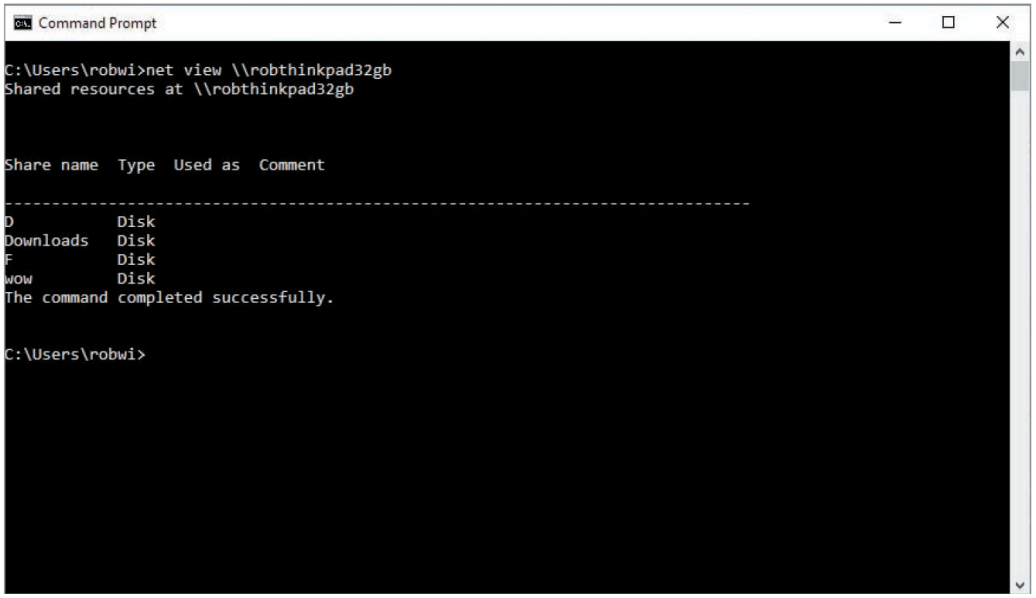
- Another built-in Windows tool is the `net view` command
  - Shows shared resources on a computer or server
  - To display syntax for this command, type `net view ?`



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



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

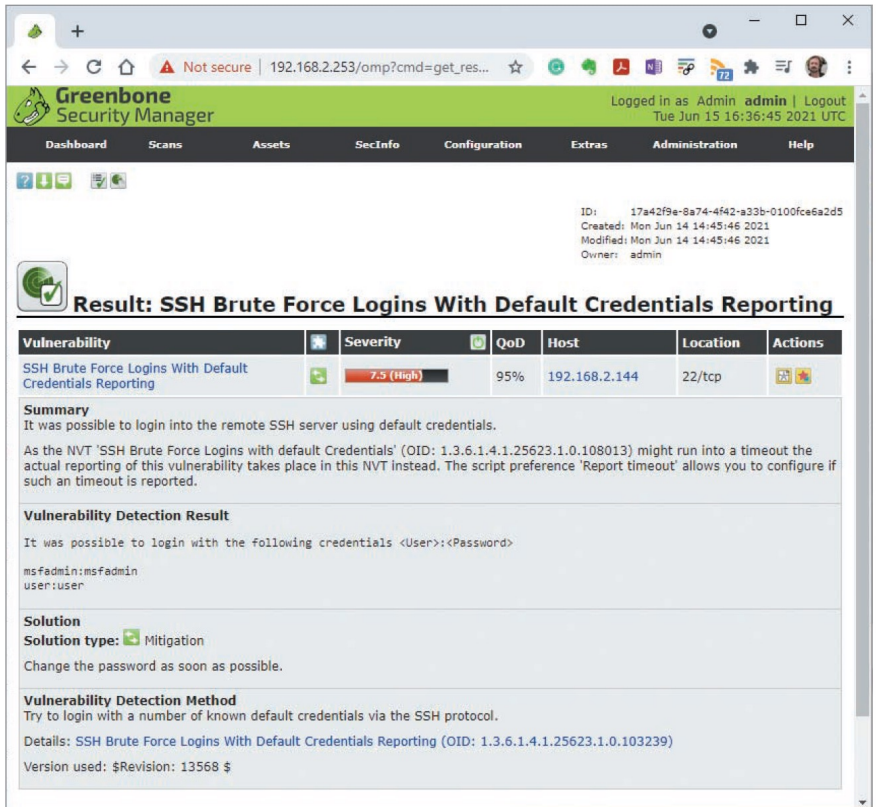
Additional Enumeration Tools (3 of 9)

- 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

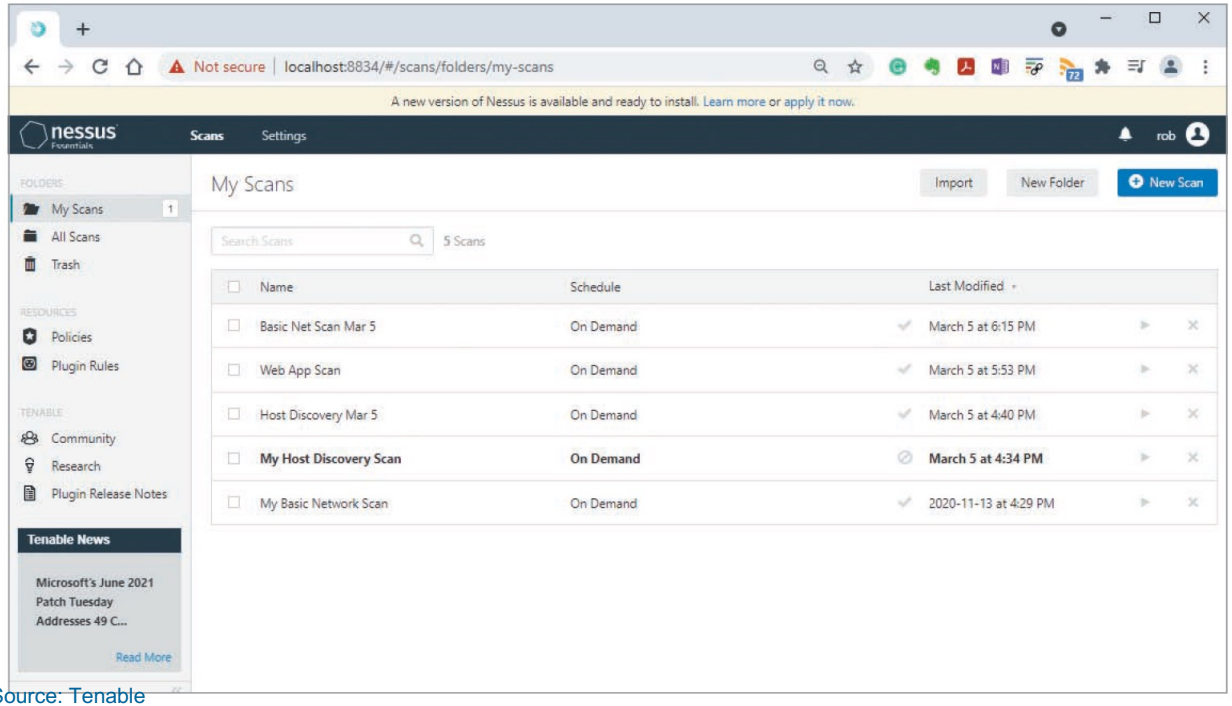
Additional Enumeration Tools (5 of 9)



Source: Greenbone Security

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

Additional Enumeration Tools (6 of 9)

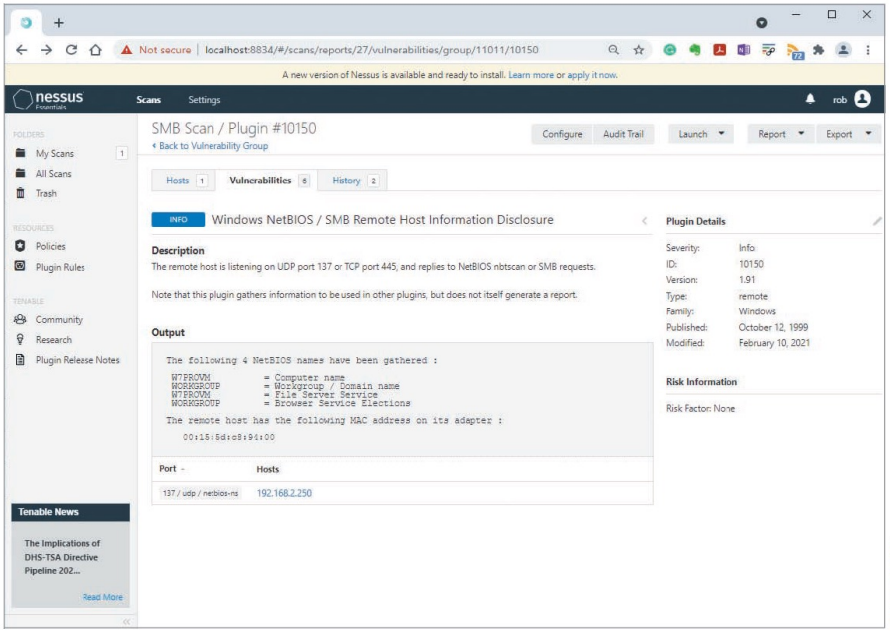


Source: Tenable

Figure 6-10 Nessus Scans page

Additional Enumeration Tools (7 of 9)

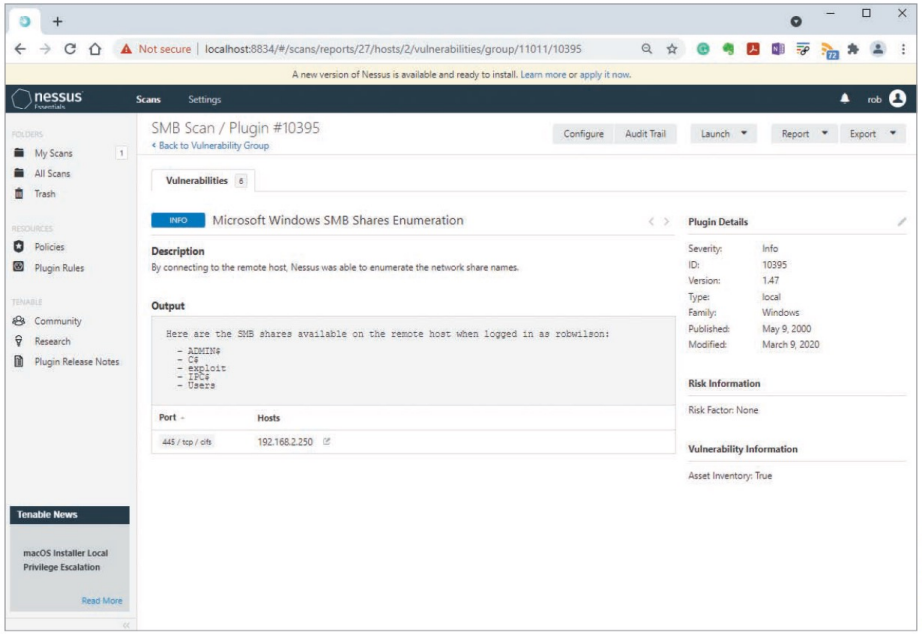
- The next several figures show Nessus in action
- This figure shows information Nessus has discovered using NetBIOS



Source: Tenable

Additional Enumeration Tools (8 of 9)

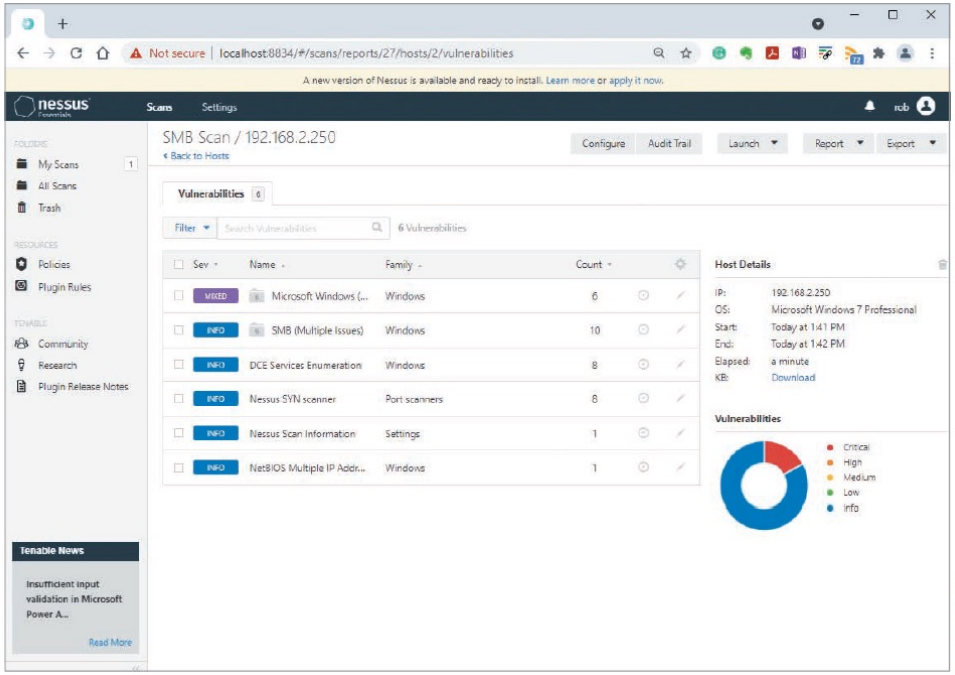
- Additional Nessus scan to enumerate Server Message Block (SMB) shares has provided a list of folders that are accessible via SMB in this figure



Source: Tenable

Additional Enumeration Tools (9 of 9)

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



Source: Tenable

Polling Activity 6-2

Which of the following tools can be used to enumerate Windows systems? (Choose all that apply.)

a. OpenVAS or Nessus
b. Reddit
c. DumpIt
d. Hyena

Polling Activity 6-2: Answer

Which of the following tools can be used to enumerate Windows systems?

Answer: a. and d. OpenVAS or Nessus and Hyena

Hyena is an excellent GUI tool for managing and securing Windows OSs. Nessus and OpenVAS are also both compatible with Windows OS systems.

Knowledge Check Activity 6-2

Which of the following is a Windows command-line utility for seeing NetBIOS shares on a network?

a. `Net use`

b. `Net user`

c. `Net view`

d. `Nbtuser`

Knowledge Check Activity 6-2: Answer

Which of the following is a Windows command-line utility for seeing NetBIOS shares on a network?

Answer: c. `Net view`

The `net view` command is a simple command-line utility that allows an attacker to view remote NetBIOS shares on a network.

Discussion Activity 6-1

Perform a Net view scan of your own computer. Write a brief report (three paragraphs) of your findings. Were you surprised by any of the shares you discovered? Discuss the shares you discovered and why they are there with your classmates.

Discussion Activity 6-1: Answer

Perform a Net view scan of your own computer. Write a brief report (three paragraphs) of your findings. Were you surprised by any of the shares you discovered? Discuss the shares you discovered and why they are there with your classmates.

Answer: The student should at least find the administrative shares that are automatically made for each drive letter—C$ and D$—and admin$ and IPC$. These shares may be a surprise to the student. The report should mention these shares and any other shares that are found, the name or IP address of the computer, and a description of what these shares are.

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)

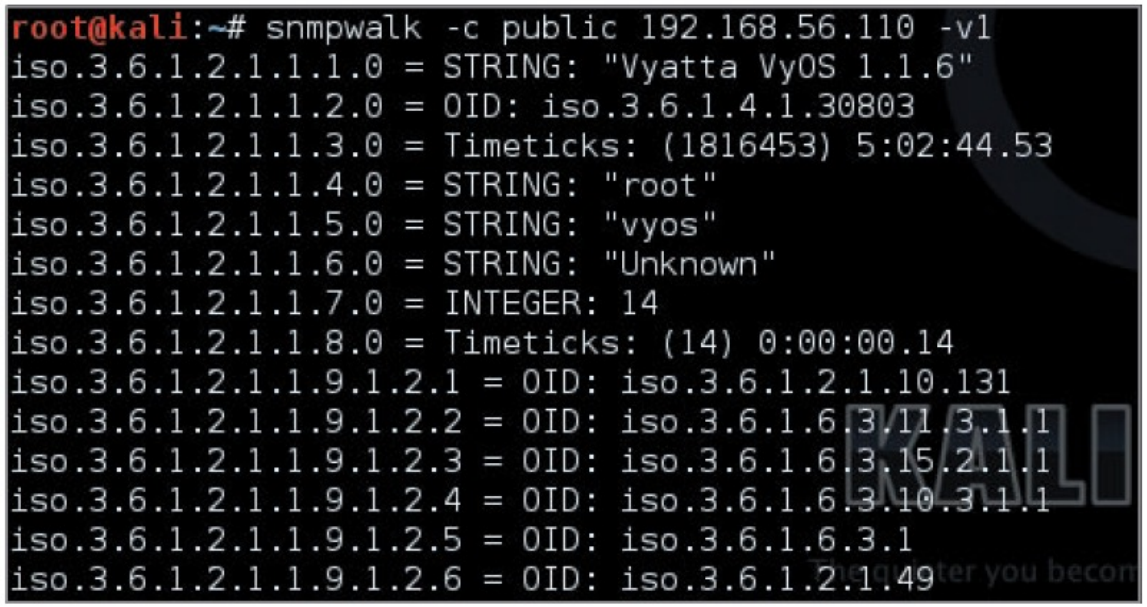
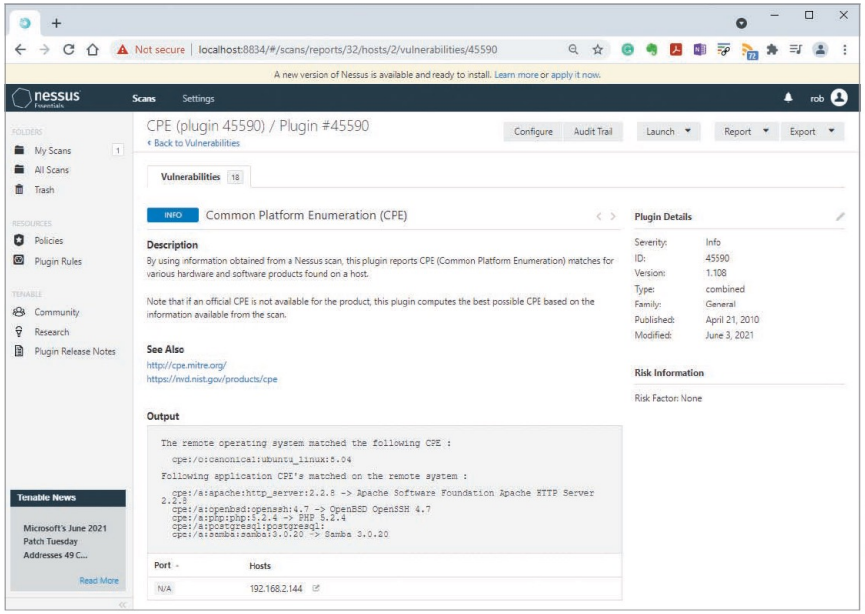


Figure 6-14 Using the SNMPWalk command

*nix Enumeration (4 of 6)

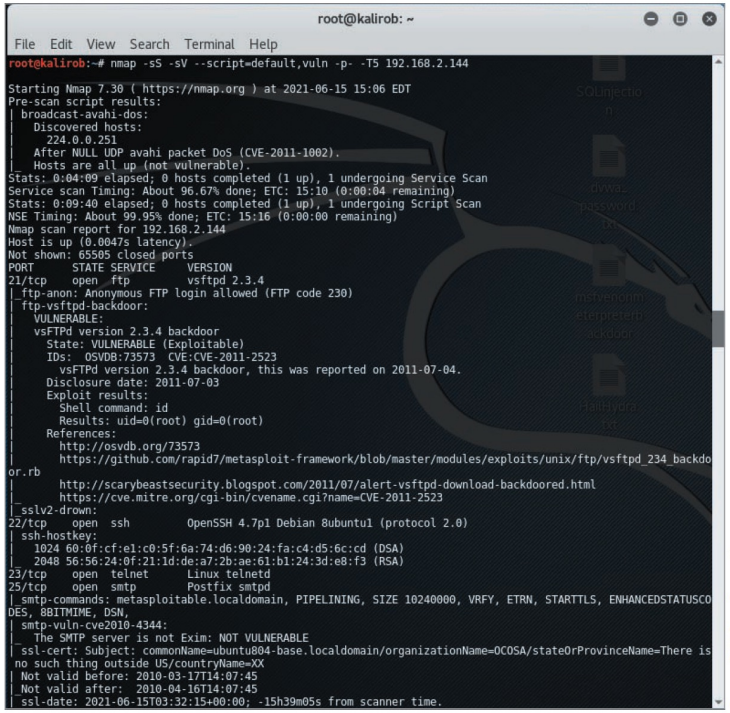
- Nessus is helpful in *nix enumeration
- This figure shows what Nessus found when scanning a Ubuntu 15.10 system



Source: Tenable

*nix Enumeration (5 of 6)

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



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

Self-Assessment

Recall the kinds of information that can be gathered with the help of enumeration.

Summary

- Now that the lesson has ended, you should be able to:
  - Describe the enumeration step of security testing
  - Enumerate Windows OS targets
  - Enumerate *nix OS targets