De La Salle University
College of Computer Studies

Ethical Hacking

Module No. 4 – Enumeration

Name : Daniel Gavrie Clemente

1.0 Objectives

- To understand the concept of enumeration
- To understand how services on a host can be exploited to gain information on target hosts

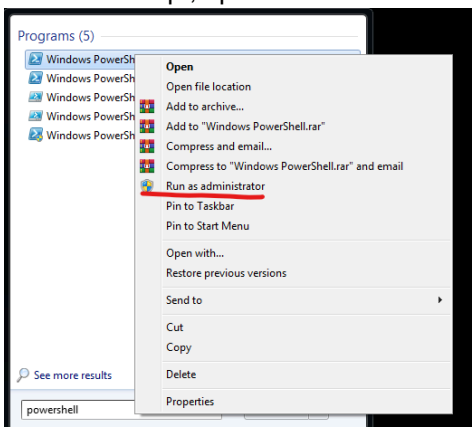
2.0 Procedure

2.1 Initial Setup

1. Set up three machines (whether physical or virtual) with the following specifications :

Machine	Operating System	IP Address/Subnet Mask
Hacker – Linux	Kali Linux	172.16.15.x/24
Victim – Windows	Windows 7	172.16.15.1x/24
Victim – Metasploitable	Metasploitable Linux Username: msfadmin Password: msfadmin	172.16.15.2x/24

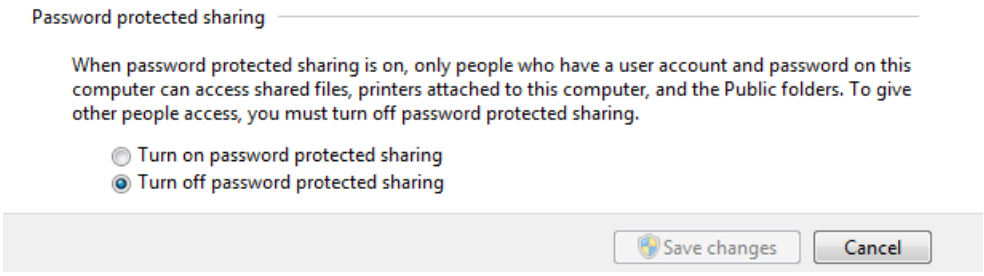
2. Take a snapshot of your Windows 7 Machine before making any changes.
3. Extract the file from script.zip to your Windows 7 Desktop with a password of "`infected`".
4. To run the script, open a PowerShell and run it as Administrator.



5. Change the directory to Desktop and run the following commands:

```
Set-ExecutionPolicy Bypass -Scope Process -Force
.\smb-enum-script.ps1
```

6. Go to Control Panel > Network and Internet > Network and Sharing Center > Advanced sharing settings. Turn off the password protected sharing and save changes.



2.2 Using nbtscan and smbclient

7. Open a terminal application in the Kali Linux system.
8. On the command prompt, type in "`nbtscan 172.16.15.0/24`".
9. What are the NETBIOS names of the computer?

WIN-AHAJBHIP7GK - Windows 7 METASPLOITABLE - Metasploitable

10. On the command prompt, type in "`smbclient -L=[Metasploitable Linux IP address]`". Enter a blank password if prompted.

11. Were you able to see the shared folders without entering a password on the Metasploitable Linux machine? Why? (Hint: Research null scan on Windows-based computers on the Internet)

Yes, because Metasploitable Linux is intentionally configured with insecure settings, including open and unprotected services like SMB (Server Message Block), which is commonly used for file sharing.

12. List down shared folders of the Metasploitable Linux machine, if there are any.

Sharename Type Comment --------- ---- ------- print$ Disk Printer Drivers tmp Disk oh noes! opt Disk IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian)) ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))

2.3 Enumerating users and shares - NMAP

13. Open a terminal application in the Kali Linux system.
14. At the command prompt, type in the command "`nmap --script=smb-enum-users [Metasploitable Linux IP address]`"
15. List down the discovered users on the Metasploitable Linux below:

Discovered Users

Enabled Users:
`msfadmin`
`user`
 	
Disabled Users:
backup
bin
bind
daemon
dhcp

distccd ftp games gnats irc klog libuuid list lp mail man mysql news nobody postfix postgres proftpd proxy root service sshd sync sys syslog telnetd tomcat55 uucp www-data

16. At the command prompt, type in the command "`nmap --script=smb-enum-shares [Metasploitable Linux IP address]`"
17. List down the discovered shares on the Metasploitable Linux below:

Discovered Shares
ADMIN$ IPC$ opt print$ tmp

18. What does a shared folder with "$" mean? (You may search for this on the Internet)

A folder or **network share name ending with a dollar sign (`$`)** is known as a **hidden share** in Windows and SMB (Server Message Block) environments.

19. At the command prompt, type in the command "`nmap --script=smb-enum-groups [Metasploitable Linux IP address]`"
20. List down the discovered groups on the Metasploitable Linux below:

Discovered Groups
There are currently no discovered groups on Metasploitable Linux.

2.4 Enumeration on Windows 7 Machine - NMAP

21. Open a terminal application in the Kali Linux system.
22. At the command prompt, type in the command "`nmap --script=smb-enum-users [Windows 7 IP address]`"
23. List down the discovered users on Windows 7 below:

Discovered Users
Administrator
DLSU_User
gavri
Guest
HomeGroupUser$
student

24. At the command prompt, type in the command "`nmap --script=smb-enum-shares [Windows 7 IP address]`"
25. List down the discovered shares on Windows 7 below:

Discovered Shares
ADMIN$
C$
IPC$
Users
Hackme
public

26. At the command prompt, type in the command "`nmap --script=smb-enum-groups [Windows 7 IP address]`"
27. List down the discovered groups on the Metasploitable Linux below:

Discovered Groups
Builtin\Administrators
Builtin\Users
Builtin\Guests
Builtin\Power Users
Builtin\Backup Operators
Builtin\Replicator
Builtin\Remote Desktop Users
Builtin\Network Configuration Operators
Builtin\Performance Monitor Users
Builtin\Performance Log Users
Builtin\Distributed COM Users
Builtin\IIS_IUSRS
Builtin\Cryptographic Operators
Builtin\Event Log Readers

2.5 Banner Grabbing - HTTP

28. Open a terminal application in the Kali Linux system.
29. At the command prompt, type in the command "`telnet [Metasploitable Linux IP Address] 80`". You should see a connected message.
30. When connected, type in the following :

```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.10.195 80
Trying 192.168.10.195 ...
Connected to 192.168.10.195.
Escape character is '^]'.
GET / HTTP/1.1
HOST: 192.168.10.195
```

31. What information can you gather about the web server?

This is a Metasploitable 2 web server running Apache and PHP on Ubuntu, hosting multiple intentionally vulnerable web applications that are ideal targets for SQL Injection, XSS, Command Injection, File Upload Exploits, and WebDAV attacks.

32. What is the software name and version of the web server used by the target host?

Web Server Software: Apache

Version: 2.2.8

Platform: Ubuntu Linux

Additional Modules:

- **DAV/2** (WebDAV enabled)
- **PHP/5.2.4-2ubuntu5.10** (as the backend scripting engine)

2.6 SMTP Enumeration Part 1

33. Before starting SMTP enumeration, research what the « netcat application can do on the Internet. What is the "netcat" application?

Netcat (often abbreviated as `nc`) is a **powerful networking utility** used by system administrators, network engineers, and ethical hackers. It's often referred to as the **"Swiss Army knife" of networking**.

34. Open a terminal application in the Kali Linux system.
35. At the command prompt, type in the command "`nc [Metasploitable Linux IP address] 25`". You should see a message "`[*] 192.168.25.128:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)`" when you are connected.
36. At the prompt, type in the command "`vrfy root`". What is the output? Does this indicate that the user exists?

After typing in the command "vrfy root," the output is "252 2.0.0 root." The output does indicate the user exists.

37. At the prompt, type in the command "`vrfy user1`". What is the output? Does this indicate that the user exists?

The output is
"550 5.1.1 <user1>: Recipient address rejected: User unknown in local recipient table."
The output indicates the user doesn't exist.

38. At the prompt, type in the command "`vrfy msfadmin`". What is the output? Does this indicate that the user exists?

The output is “252 2.0.0 msfadmin.” The output does indicate the user exists.

39. Is it possible to enumerate the users through the SMTP protocol?

Yes, it is possible to enumerate users through the SMTP protocol.

2.7 SMTP Enumeration Part 2

40. Open a terminal application in the Kali Linux system.
41. At the command prompt type in the command “`smtp-user-enum -M VRFY -U /usr/share/wordlists/fern-wifi/common.txt -t [Metasploitable Linux IP address]`”

42. What are the usernames discovered?

```
lp

root

service

sys

user

MAIL

Root

SERVICE

SYS

Service

User
```

43. Was the “msfadmin“ username found? Why?

No, the msfadmin username was not found in the SMTP enumeration result because `msfadmin` was not found because it probably wasn't in the wordlist.

44. Edit the file “`/usr/share/wordlists/fern-wifi/common.txt`” to include the msfadmin username. After editing, run the script again. Was it able to discover the msfadmin username? Why?

Yes, because the `msfadmin` username was added to the wordlist, allowing the enumeration tool to explicitly check for it against the SMTP server.

3.0 Guide Questions:

1. What is enumeration? How can this technique help in investigating the network?
   Enumeration is the process of actively connecting to a system and gathering detailed information, such as users, shares, services, and more, which helps in identifying potential vulnerabilities in the network.
2. What information can be gathered using Nmap SMB scripts and SMTP scripts? Why is this possible?
   Nmap SMB and SMTP scripts can gather data like shared resources, user accounts, domain information, and email server configuration because they interact with exposed service ports that respond with such details.
3. What information can be gathered from banner grabbing web servers? Why is this possible?
   Banner grabbing web servers can reveal software versions, server types, and operating systems because servers often send this information in HTTP headers during connections.
4. What information can be gathered from an SMTP server? Why is this possible?
   SMTP servers can provide user enumeration, mail relay status, and software versions because they respond with detailed messages to SMTP commands during connection attempts.
5. What other tools can you use (whether for Linux or Windows) to do enumeration?
   Other enumeration tools include Netcat, Enum4linux, SNMPwalk, RPCclient, LDAPsearch, and PowerView (for Windows), as they can query various services and protocols for detailed network and system information.

Resources:

Kali Linux - Hacker Machine
https://www.kali.org/get-kali/

Metasploitable 2 - Victim Machine
https://sourceforge.net/projects/metasploitable

Windows 7 Victim Machine
https://drive.google.com/drive/folders/16lKVVJxEVBbIIu1AspjglaZ1bLh7yZMe?usp=sharing

SMB Enum Script for Windows 7
https://drive.google.com/file/d/1Xd8A0vCq7m3pq7zFb1_dfCvaOuzy_HYl/view?usp=sharing
*Password - infected