PENETRATION TESTING

ENUMERATION

RELEVANT CONCEPT

Enumeration is an important phase of the penetration test process. It consists in exploiting the characteristics of a certain service in order to obtain as much information as possible.

ENUMERATION

There are services that work well with this type of investigation, such as:

- SMTP, TCP port 25.
- DNS, UDP/TCP port 53.
- SNMP, UDP port 161.
- NETBIOS, UDP port 137,138; TCP port 139.
- ...

ENUMERATION

In this lesson, we will examine enumeration related to the following services:

- SAMBA/NETBIOS enumeration.
- SMTP enumeration.

ENUMERATION WITH NETBIOS

RELEVANT CONCEPT

NetBIOS (Network Basic IO System) uses a protocol that operates at the session layer of the ISO/OSI model. This protocol allows us to explore the network resources of computers, printers or files.

ENUMERATION

We can use Netbios to extract several information, including the following:

- Hostnames.
- Usernames.
- Domains.
- Workgroups.
- Printers.
- Shared network folders.

ENUMERATION

First of all, we should use Nmap to confirm that the TCP ports 139 and 445 are open:

```
nmap -v -p 139,445 192.168.122.137
```

ENUMERATION

```
gabriele@gabriele-XPS-13-9370: ~/Scaricati
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
gabriele@gabriele-XPS-13-9370  ~/Scaricati  sudo nmap -sV 192.168.122.137 -p 139,445

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-09 16:08 CEST
Nmap scan report for 192.168.122.137
Host is up (0.00042s latency).

PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 0C:94:7C:A7:3D:01 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.87 seconds
gabriele@gabriele-XPS-13-9370  ~/Scaricati
```

ENUMERATION

After completing this step, we can use a special command, the NBTSCAN, to investigate systems with open port 139.

```
nbtscan -vh 192.168.122.137
```

ENUMERATION

```
gabriele@gabriele-XPS-13-9370: ~
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
gabriele@gabriele-XPS-13-9370  ~  nbtscan -vh 192.168.122.137
Doing NBT name scan for addresses from 192.168.122.137


NetBIOS Name Table for Host 192.168.122.137:

Incomplete packet, 227 bytes long.
Name             Service          Type
----------------------------------------
METASPLOITABLE   Workstation Service
METASPLOITABLE   Messenger Service
METASPLOITABLE   File Server Service
__MSBROWSE__     Master Browser
WORKGROUP        Domain Name
WORKGROUP        Master Browser
WORKGROUP        Browser Service Elections

Adapter address: 00:00:00:00:00:00
----------------------------------------
gabriele@gabriele-XPS-13-9370  ~
```

ENUMERATION

The same result can be obtained by means of Nmap using the scripting engine (NSE)

```
nmap -sV -p139 192.168.122.137 --script nbstat.nse
```

ENUMERATION

gabriele@gabriele-XPS-13-9370: ~/Scaricati

File Modifica Visualizza Cerca Terminale Aiuto

```
gabriele@gabriele-XPS-13-9370  ~/Scaricati  nmap -sV -p139 192.168.122.137 --script nbstat.nse

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-09 16:21 CEST
Nmap scan report for 192.168.122.137
Host is up (0.00086s latency).

PORT    STATE SERVICE     VERSION
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.33 seconds
gabriele@gabriele-XPS-13-9370  ~/Scaricati
```

ENUMERATION

Nmap contains many scripts that can be used to enumerate NETBIOS. You can find them on the following path: /usr/share/nmap/scripts.

```
gabriele@gabriele-XPS-13-9370: /usr/share/nmap/scripts
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
gabriele@gabriele-XPS-13-9370  /usr/share/nmap/scripts  ls | grep smb-enum
smb-enum-domains.nse
smb-enum-groups.nse
smb-enum-processes.nse
smb-enum-sessions.nse
smb-enum-shares.nse
smb-enum-users.nse
gabriele@gabriele-XPS-13-9370  /usr/share/nmap/scripts
```

ENUMERATION

Exercise (~3’)

Use nmap to find a SAMBA username that is not disabled

ENUMERATION

Exercise (~3’)

Use nmap to find a SAMBA username that is not disabled

```
gabriele@gabriele-XPS-13-9370: ~
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
gabriele@gabriele-XPS-13-9370  ~  nmap --script=smb-enum-users.nse 192.168.122.137 -p139

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-09 19:09 CEST
Nmap scan report for 192.168.122.137
Host is up (0.0011s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Account disabled, Normal user account
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Account disabled, Normal user account
```

ENUMERATION

We can also use a SAMBA client to enumerate the users, e.g., **rpcclient**

```
rpcclient -U "" 192.168.122.137
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
gabriele@gabriele-XPS-13-9370  ~  rpcclient -U "" 192.168.122.137
Enter WORKGROUP\'s password:
rpcclient $> querydominfo
Domain:         WORKGROUP
Server:         METASPLOITABLE
Comment:        Metasploitable server (Samba 3.0.20-Debian)
Total Users:    35
Total Groups:   0
Total Aliases:  0
Sequence No:    1586451752
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
```

ENUMERATION

With rpcclient we can list the users (enumdomusers) and even get some details (queryuser)

```
rpcclient -U "" 192.168.122.137
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
```

```
rpcclient -U "" 192.168.122.137
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
gabriele@gabriele-XPS-13-9370  ~  rpcclient -U "" 192.168.122.137
Enter WORKGROUP\'s password:
rpcclient $> queryuser user
        User Name   :   user
        Full Name   :   just a user,111,,
        Home Drive  :   \\metasploitable\user
        Dir Drive   :
        Profile Path:   \\metasploitable\user\profile
        Logon Script:
        Description :
        Workstations:
        Comment     :   (null)
        Remote Dial :
        Logon Time               :      gio, 01 gen 1970 01:00:00 CET
        Logoff Time              :      gio, 14 set 30828 03:48:05 CET
        Kickoff Time             :      gio, 14 set 30828 03:48:05 CET
        Password last set Time   :      mar, 18 mag 2010 03:39:25 CEST
        Password can change Time :      mar, 18 mag 2010 03:39:25 CEST
        Password must change Time:      gio, 14 set 30828 03:48:05 CET
        unknown_2[0..31]...
        user_rid :      0xbba
        group_rid:      0xbbb
        acb_info :      0x00000010
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $>
```

ENUMERATION

An even faster and powerful tool is **enum4linux (or enum4linux-ng)**

We can use it to enumerate users, shares, printers and more in a single scan

We can also accurately detect the SAMBA version we are interacting with

```
 ==========================================
|    OS information on 192.168.122.137    |
 ==========================================
Use of uninitialized value $os_info in concatenation (.) or string at /usr/bin/enum4linux line 464.
[+] Got OS info for 192.168.122.137 from smbclient:
[+] Got OS info for 192.168.122.137 from srvinfo:
        METASPLOITABLE Wk Sv PrQ Unx NT SNT Metasploitable server (Samba 3.0.20-Debian)
        platform_id     :       500
        os version      :       4.9
        server type     :       0x9a03
```

ENUMERATION WITH SMTP

ENUMERATION

Simple Mail Transfer Protocol is used to send emails from a client to a (SMTP) server

SMTP typically runs on port 25 and it allows to submit few commands that we can test via telnet

- HELO: used by clients to identify themselves
- QUIT: used to close a connection
- DATA: used to start data transfer
- VRFY: used to check whether a certain user/mailbox exists

ENUMERATION

```
gabriele@gabriele-XPS-13-9370: ~
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
gabriele@gabriele-XPS-13-9370  ~  telnet 192.168.122.137 25
Trying 192.168.122.137...
Connected to 192.168.122.137.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
vrfy user
252 2.0.0 user
vrfy root
252 2.0.0 root
vrfy doesnotexist
550 5.1.1 <doesnotexist>: Recipient address rejected: User unknown in local recipient table
quit
221 2.0.0 Bye
Connection closed by foreign host.
✘ gabriele@gabriele-XPS-13-9370  ~
```

ENUMERATION

If we have a list of usernames we can quickly check them through the SMTP methods

For instance we can create a list through OSINT and other enumeration techniques

Also, we can retrieve lists of frequent usernames online

ENUMERATION

Metasploit has a module for SMTP enumeration

```
msfconsole
File  Modifica  Visualizza  Cerca  Terminale  Aiuto

msf5 > use auxiliary/scanner/smtp/smtp_enum
msf5 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting                                                    Required
   ----       ---------------                                                    --------
   RHOSTS                                                                        yes
   RPORT      25                                                                 yes
   THREADS    1                                                                  yes
   UNIXONLY   true                                                               yes
   USER_FILE  /opt/metasploit-framework/embedded/framework/data/wordlists/unix_users.txt  yes

msf5 auxiliary(scanner/smtp/smtp_enum) >
```

ENUMERATION

msfconsole

File Modifica Visualizza Cerca Terminale Aiuto

```
msf5 auxiliary(scanner/smtp/smtp_enum) > set rhosts 192.168.122.137
rhosts => 192.168.122.137
msf5 auxiliary(scanner/smtp/smtp_enum) > set user_file /home/gabriele/usernames-shortlist.txt
user_file => /home/gabriele/usernames-shortlist.txt
msf5 auxiliary(scanner/smtp/smtp_enum) > exploit

[*] 192.168.122.137:25    - 192.168.122.137:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.122.137:25    - 192.168.122.137:25 Users found: ftp, mysql, user
[*] 192.168.122.137:25    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smtp/smtp_enum) >
```

ENUMERATION VIA USERDIR

ENUMERATION

Apache has a module called **mod_userdir** that allows for the creation of user directories (UserDir)

A UserDir always has a certain path syntax, e.g., www.site.com/~user

UserDir can be automatically checked by asking the server to access them

The server answer tells us whether the user exists (e.g., 403) or not (e.g., 404)

Nmap has a script for testing this: http-userdir-enum

ENUMERATION WITH DEFAULT CREDENTIALS

ENUMERATION

Network devices – such as routers and switches – very often have a default password.

These passwords are defined directly by the device manufacturer.

They obviously suggest to change them as soon as possible, but sometimes this does not happen.

ENUMERATION

DefaultPassword is one of the many sites where default device passwords are stored (https://default-password.info/).

This website is very easy to use. You just need to select the device model and manufacturer:

ENUMERATION

Cisco - CallManager

Default username, password, ip...

	User name	Password	Description
☹	admin	show me!	- nabil ouchn\n- Admin access (HTTP)

ENUMERATION

The very same approach was used by Mirai, a botnet that infected thousands of devices.

The list of credentials used for Mirai in https://github.com/danielmiessler/SecLists/blob/master/Passwords/Malware/mirai-botnet.txt

Mirai infected IoT devices by using a list of 60 credential pairs

ENUMERATION WITH VULNERABILITIES

RELEVANT CONCEPT

What we have seen so far is based on the specific behavior of some services, but information may leak through vulnerabilities.

ENUMERATION

Usernames as well as other critical data is typically stored in a database

Vulnerabilities that allow us to tamper with the database can also leak information

Soon we will see, for instance, SQL injection vulnerabilities and we will reason about their implications

Again, the phases of penetration testing are not in linear sequence