

PSP0201

Week 3

Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

Day 10 : Networking – Don't be sElfish!

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

Enter the ‘enum4linux -h’ command to display help message where they explain the option in detail.

```
(121101390㉿kali)-[~]
└─$ enum4linux -h
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Matt Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):

-U      get userlist
-M      get machine list*
-S      get sharelist
-P      get password policy information
-G      get group and member lists
-d      be verbose (-v for -U and -S)
-u user  specify username to use (default '')
-p pass   specify password to use (default '')

The following options from enum.exe aren't implemented: -l, -N, -D, -f
Additional options:
-a      All simple enumeration (-U -S -P -r -o -n -l).
        This option is enabled if you don't provide any other options.
-h      Display this help message and exit
-r      enumerate shares via RID cycling
-R range RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
-K n    Keep searching RIDs until n consecutive RIDs don't correspond to
        a username. Implies RID range ends at 999999. Useful
        against Samba 3.6+
-l      Get some (limited) info via LDAP 389/TCP (for DCs only)
-s file  brute force guessing for share names
-k user  User(s) that exists on remote system (default: administrator,guest,krbtgt,domain admins,root,bin,
one)
        Used to get sid with "lookupsid known_username"
        Use commas to try several users: "-k admin,user1,user2"
-o      Get stats
-i      Get printer information
-w wrk  Specify工作组 manually (usually found automatically)
-n      Do an nmblookup (similar to netstat)
-v      Verbose mode. All commands run (net, rpcclient, etc.)
-A      Aggressive. Do write checks on shares etc

RID cycling should extract a list of users from Windows (or samba) hosts trying to login to the shares on the Samba server ( 10.10.10.104 ). What share doesn't require a password?
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
access: Allow anonymous SID/Name translation" enabled (XP, 2003).

NB: Samba servers often seem to have RIDs in the range 3000-3050.
Dependency: You will need to have the samba package installed as this
script will basically just run around rpcclient, net, nmblookup and
smclient. Patches from http://labs.portcullis.co.uk/application/patchenum/
is required to get Password Policy info.

(121101390㉿kali)-[~]
```

Question 2

Enter the command ‘enum4linux 10.10.37.104’. The IP address was provided from the machine of the task in tryhackme.com. This command allows us to see how many users are there on the Samba server.

```
[+] Got OS info for 10.10.37.104 from srmvinfo:
TBFC-SMB   Wk Sv PrQ Unix NT SNT tbfc-smb server (Samba, Ubuntu)
platform_id : 500
os version  : 6.1
server type : 0x009203
```

(Users on 10.10.37.104)

index:	0+1 RID	0x3e8 acb: 0x00000010 Account: elmcskiday	Name: Desc:	Address
index:	0+2 RID	0x3e9 acb: 0x00000010 Account: elmcseager	Name: Desc:	10.10.37.104
index:	0+3 RID	0x3e9 acb: 0x00000010 Account: elmcselferson	Name: Desc:	10.10.37.104

user:[elmcskiday] rid:[0x3e8]
user:[elmcseager] rid:[0x3e9]
user:[elmcselferson] rid:[0x3e9]

(Share Enumeration on 10.10.37.104)

Sharename	Type	Comment
tbfc-hr	Disk	tbfc-hr
tbfc-it	Disk	tbfc-it
tbfc-santa	Disk	tbfc-santa
IPC\$	IPC	IPC Service (tbfc-smb server (Samba, Ubuntu))

Reconnecting with SMB1 for workgroup listing.

Server	Comment
TBFC-SMB-01	TBFC-SMB

Workgroup: Master

[+] Attempting to map shares on 10.10.37.104

```
//10.10.37.104/tbfc-hr Mapping: DENIED Listing: N/A Writing: N/A  
//10.10.37.104/tbfc-it Mapping: DENIED Listing: N/A Writing: N/A  
//10.10.37.104/tbfc-santa Mapping: OK Listing: OK Writing: N/A
```

[E] Can't understand response:

```
NT_STATUS_OBJECT_NAME_NOT_FOUND Listing: *  
//10.10.37.104/IPC$ Mapping: N/A Listing: N/A Writing: N/A
```

(Password Policy Information for 10.10.37.104)

[+] Attaching to 10.10.37.104 using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

- [+] TBFC-SMB
- [+] BuiltIn

[+] Password Info for Domain: TBFC-SMB

- [+] Minimum password length: 5
- [+] Password history length: None
- [+] Maximum password age: 37 days 6 hours 21 minutes
- [+] Password Complexity Flags: 000000

Question #4 Log in to this share, what directory did Elmcselferson leave for Senta?

Question 3

From the command we had entered earlier, we scroll down to see more information until we found the ‘Share Enumeration on 10.10.37.104’ where we can see the amount of ‘shares’ on the Samba server.

Question 4

We use ‘smbclient //10.10.37.104/*shares*’ to try logging to the shares on the Samba server. After a few trials and error, we found that the share ‘tbfc-santa’ doesn’t require password so we logged into the share with it.

Question 5

We use 'ls' command to see the directory list and found a few files. We decided to download the text file named 'note_from_mcskidy.txt' using the get command.

In another tab, we use the ‘cat’ function to display the text file that has been downloaded earlier and found mcskidys note to santa. We understood then that the directory ‘jingle-tunes’ was left for santa from mcskidys.

File Actions Edit View Help

1211101390@kali: ~ x 1211101390@kali: ~ x 1211101390@kali: ~ x

[1211101390@kali: ~]

Desktop Documents Downloads Music note_from_mcskidy.txt Pictures Public Templates Videos Address Book

note_from_mcskidy.txt note_from_mcskidy.txt 00:00:00:00 Expires 10:00:00:00 2018-03-10 2018-03-10 10:00:00:00

Hi Santa, I decided to put all of your favourite jingles onto this share - allowing you access it from anywhere you like! Regards ~ El'Mskidy

[1211101390@kali: ~]

You can use the `ls` command to list some of the commands you can run when connected to the Samba share. Here's a quick rundown of the fundamentals:

Command	Description
<code>ls</code>	List files and directories in the current directory.
<code>cd <directory></code>	Change our working directory.
<code>pwd</code>	Output the full path to our working directory.
<code>more <filename></code>	Find out more about the contents of a file. To close the open file, you press <code>q</code> .
<code>get <filename></code>	Download a file from a share.
<code>put <filename></code>	Upload a file to a share.

You can now proceed to answer Question #1 and Question #4

10.6. Conclusion, where to go from here and additional material

You've learned the fundamentals of how a very common protocol used by computing devices works, and ultimately, can be leveraged through the use of enumeration and misconfiguration. With this said, you might be surprised that even painters can use the protocols behind Samba. You've also created a Samba room on Port 445 (Kali-Lab-107).

There's no true statement in pen-testing that practice makes perfect. Not only can you test the tools within this room, why not give a few others a try and apply your knowledge in the "Kiosk" Walkthrough room or the "Anonymous" Challenge room (CTF).

Average 80% completion rate

Question #1 Using `lsnmap` is there many users are there on this Samba server [10.10.10.107]?

Question #2 How many "shares" are there on the Samba server?

Question #3 Use `msfvenom` to try to login to the shares on the Samba server [10.10.10.107]. What share doesn't require a password?

Thought Process/Methodology:

After thorough read, we open the terminal to start our work. We enter the ‘enum4linux -h’ command to display help message where they explain the option in detail. In there, we

learn more option and are able to answer the first question. Next, we enter the command ‘enum4linux 10.10.37.104’. The IP address was provided from the machine of the task in tryhackme.com so it may vary with users. This command allows us to see how many users are there on the Samba server. Under ‘Users on 10.10.37.104’, we found 3 user which are elfmcskidy, elfmcager, eldmcelerson. Then, we continue scrolling down for more information until we stumbled across the ‘Share Enumeration on 10.10.37.104’. Under it are the sharename for the Samba server. With ‘smbclient //10.10.37.104/*shares*’ command, we tried logging to the shares on the Samba server in a new tab. After a few trials and error, we found that the share ‘tbfc-santa’ doesn’t require password, so we logged into the share with it. Afterward, we use ‘ls’ command to see the directory list. We decided to download the text file named ‘note_from_mcskidy.txt’ using the get command. Once again, we open a new tab and display the text file that has been downloaded earlier with the ‘cat’ function. We read the note left for santa by mcskidy and concluded that the directory ‘jingle-tunes’ is the directory left for santa.