رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Blue Team Scenarios

Team Names:

1. **Mohamed Abdel-Moneam Mohamed**
2. **Toka Abdelgwad**
3. **Habiba Bastawe Mohamed**
4. **George Samir**
5. **Omar Mohamed Abo Elkasem**

1. Recording Network Capture on a PCAP file

Mission: Recording Network Traffics

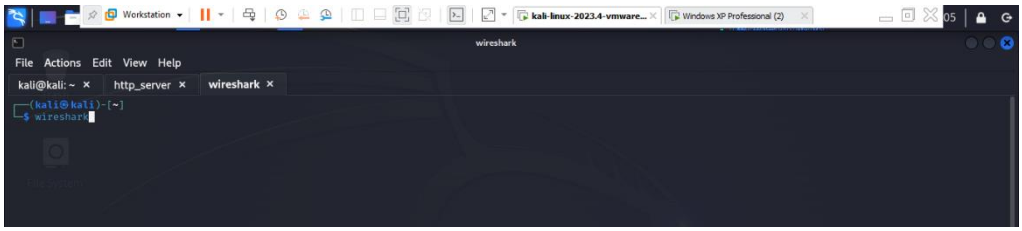
Tool: Wireshark

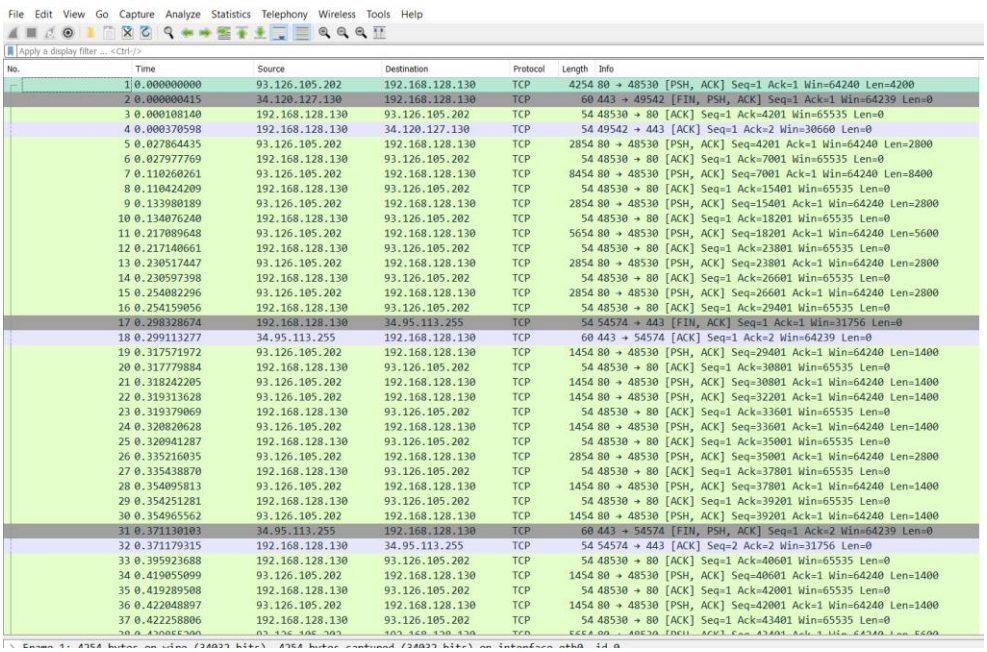
Wireshark: Wireshark is a powerful open-source network protocol analyzer used for capturing and inspecting the data traveling across a network in real-time.

Steps:

1. Open Wireshark on Linux

➢ Wireshark





PCAP File Source:
https://drive.google.com/file/d/1EnJR_Plk0BSmWuNY3YLP63pOs-gR66Ea/view?usp=sharing

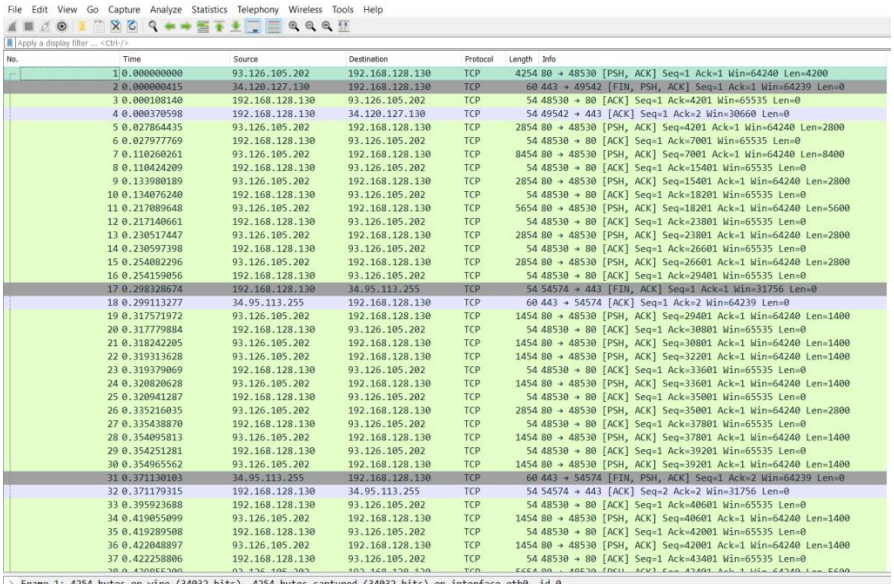
2. Investigating PCAP file to discover ongoing reconnaissance

Mission: Investigating PCAP file to discover reconnaissance on the Whole Network

Tool: Wireshark

Steps:

- Open PCAP file



- **Investigation Output**
  - Received packets :159716
  - IPV4: 159666
  - ICMP :13
  - UDP: 147
  - TCP: 159506
  - Alerts: 1111

  There are TCP syn ,UDP and Fin scanning in the target machine

3. Downloading image by Mistake and Record ongoing traffic

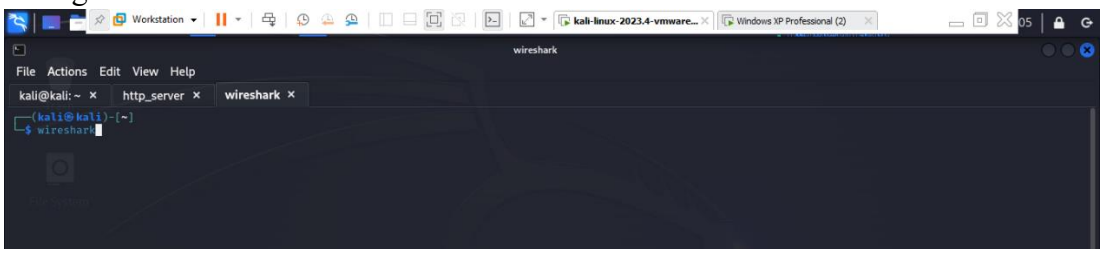
Mission: Downloading image by Mistake

Tool: Wireshark

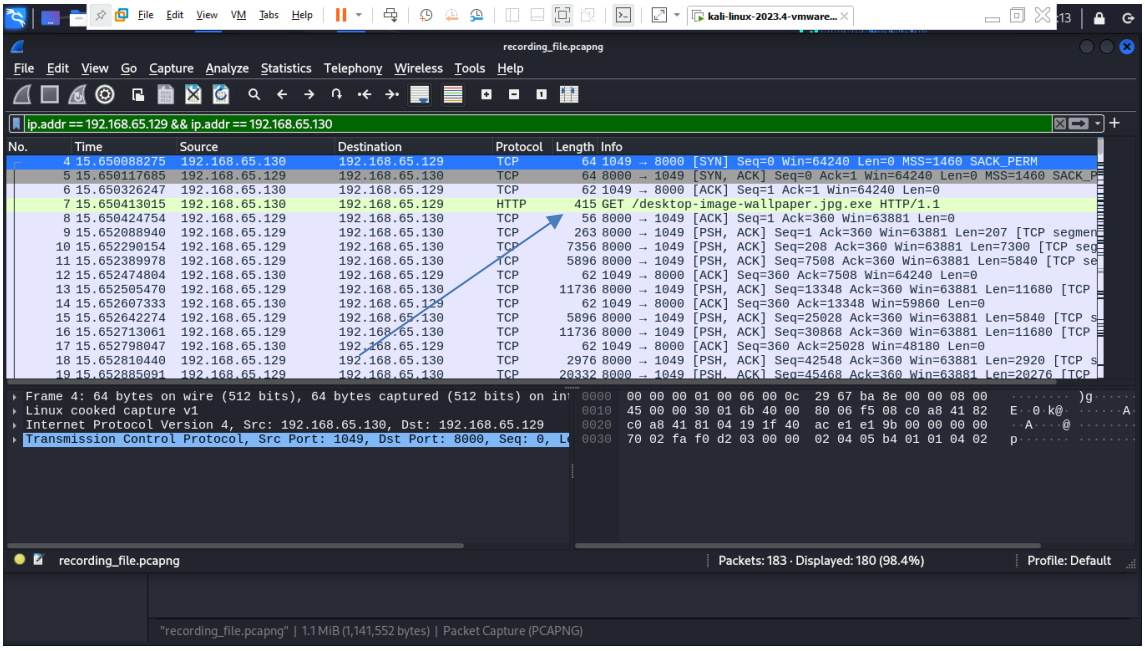
Steps:

1. Network Traffic Capture:

- During the payload delivery and execution, network traffic was captured using Wireshark. This allowed for further analysis to track the exploitation process, and any data exchanged during the attack.



- Wireshark Filters Used:
  ip.addr == 192.168.65.129 && ip.addr == 192.168.65.130



PCAP File Source:

https://drive.google.com/file/d/1GaOZr0pqx2hR8Isc3gahzeb9h2vJ7T-h/view?usp=sharing

4. Investigating the PCAP file for alert

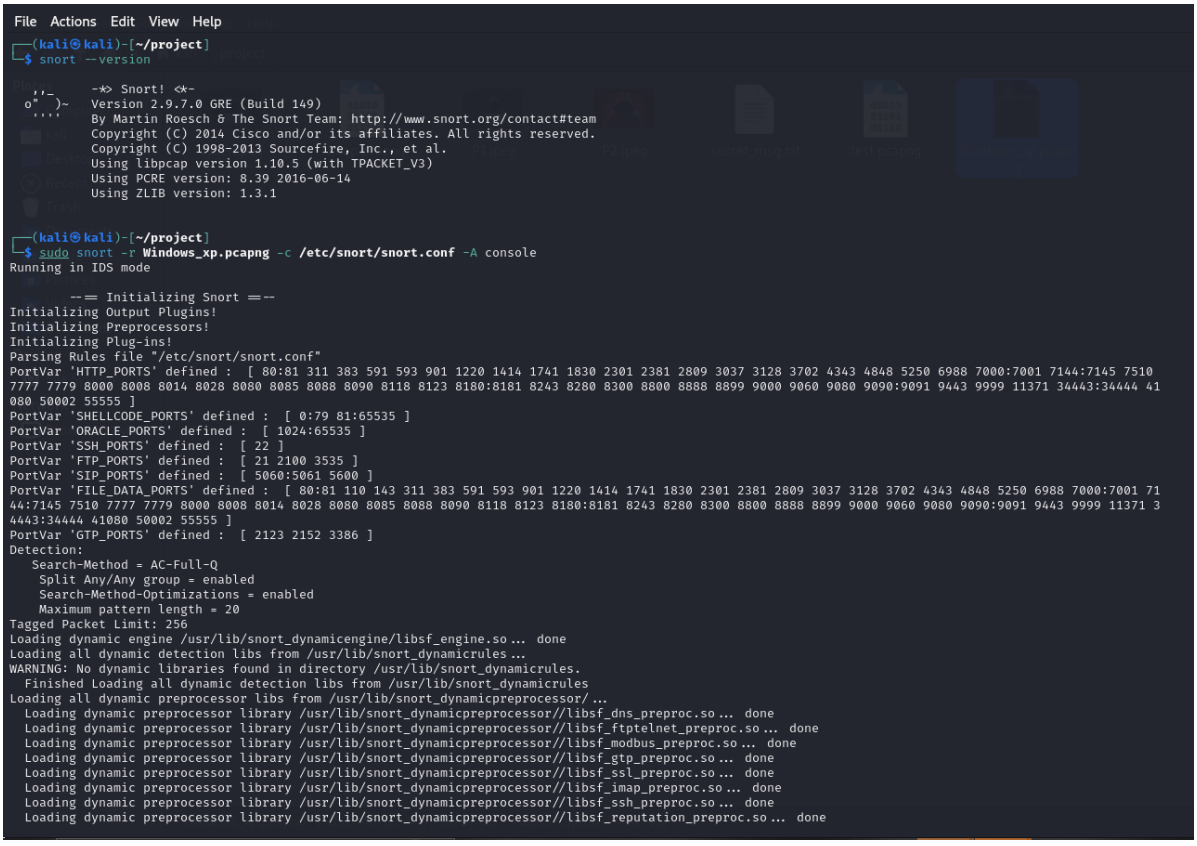
Mission: investigating PCAP file

Tool: Snort

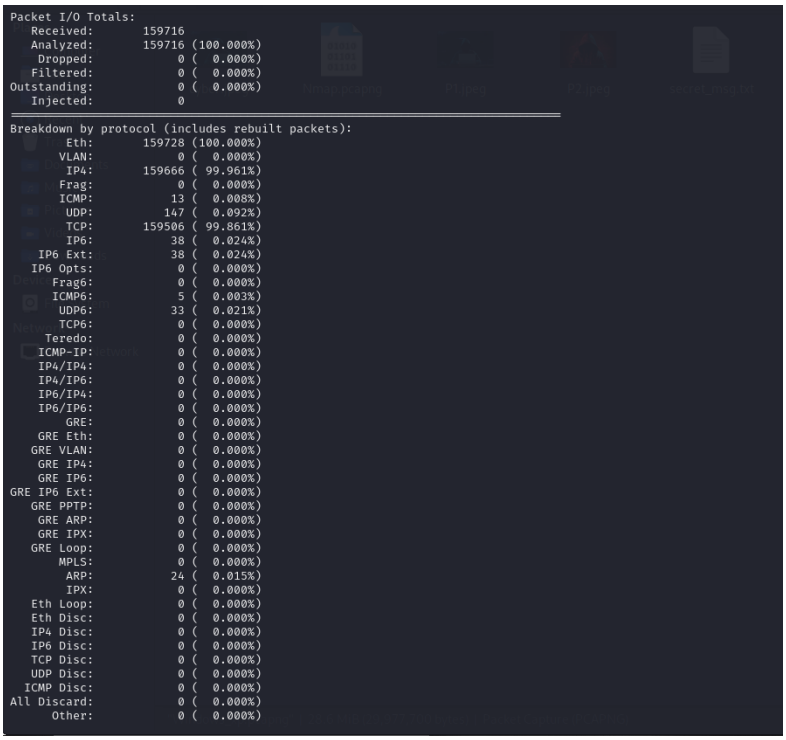
In this mission, we utilized a PCAP file recorded from a Windows XP machine, capturing reconnaissance activities conducted on that system.

Steps:

- sudo snort -r Windows_xp.pcapng -c /etc/snort/snort.conf -A console



- **The output:**



```
Packet I/O Totals:
   Received:       159716
   Analyzed:       159716 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
═══════════════════════════════════════════════════════════════════════════
Breakdown by protocol (includes rebuilt packets):
        Eth:       159728 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:       159666 ( 99.961%)
       Frag:            0 (  0.000%)
       ICMP:           13 (  0.008%)
        UDP:          147 (  0.092%)
        TCP:       159506 ( 99.861%)
        IP6:           38 (  0.024%)
    IP6 Ext:           38 (  0.024%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
     ICMP6:             5 (  0.003%)
      UDP6:           33 (  0.021%)
      TCP6:            0 (  0.000%)
    Teredo:            0 (  0.000%)
   ICMP-IP:            0 (  0.000%)
    IP4/IP4:           0 (  0.000%)
    IP4/IP6:           0 (  0.000%)
    IP6/IP4:           0 (  0.000%)
    IP6/IP6:           0 (  0.000%)
        GRE:           0 (  0.000%)
    GRE Eth:           0 (  0.000%)
   GRE VLAN:           0 (  0.000%)
    GRE IP4:           0 (  0.000%)
    GRE IP6:           0 (  0.000%)
GRE IP6 Ext:           0 (  0.000%)
   GRE PPTP:           0 (  0.000%)
    GRE ARP:           0 (  0.000%)
    GRE IPX:           0 (  0.000%)
   GRE Loop:           0 (  0.000%)
       MPLS:           0 (  0.000%)
        ARP:          24 (  0.015%)
        IPX:           0 (  0.000%)
   Eth Loop:           0 (  0.000%)
   Eth Disc:           0 (  0.000%)
   IP4 Disc:           0 (  0.000%)
   IP6 Disc:           0 (  0.000%)
   TCP Disc:           0 (  0.000%)
   UDP Disc:           0 (  0.000%)
  ICMP Disc:           0 (  0.000%)
All Discard:           0 (  0.000%)
      Other:           0 (  0.000%)
═══════════════════════════════════════════════════════════════════════════
Action Stats:
     Alerts:         1111 (  0.696%)
     Logged:         1111 (  0.696%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
Verdicts:
      Allow:       159703 ( 99.992%)
      Block:            0 (  0.000%)
    Replace:            0 (  0.000%)
  Whitelist:           13 (  0.008%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
      Retry:            0 (  0.000%)
═══════════════════════════════════════════════════════════════════════════
Frag3 statistics:
       Total Fragments: 0
    Frags Reassembled: 0
             Discards: 0
       Memory Faults: 0
            Timeouts: 0
            Overlaps: 0
           Anomalies: 0
              Alerts: 0
               Drops: 0
   FragTrackers Added: 0
  FragTrackers Dumped: 0
FragTrackers Auto Freed: 0
  Frag Nodes Inserted: 0
   Frag Nodes Deleted: 0
═══════════════════════════════════════════════════════════════════════════
═══════════════════════════════════════════════════════════════════════════
Stream statistics:
          Total sessions: 73375
            TCP sessions: 73334
            UDP sessions: 41
           ICMP sessions: 0
             IP sessions: 0
              TCP Prunes: 0
              UDP Prunes: 0
             ICMP Prunes: 0
               IP Prunes: 0
TCP StreamTrackers Created: 73334
TCP StreamTrackers Deleted: 73334
           TCP Timeouts: 0
           TCP Overlaps: 0
     TCP Segments Queued: 1177
```

```
===============================================================================
HTTP Inspect - encodings (Note: stream-reassembled packets included):
    POST methods:                         0
    GET methods:                          0
    HTTP Request Headers extracted:       0
    HTTP Request Cookies extracted:       0
    Post parameters extracted:            0
    HTTP response Headers extracted:      1
    HTTP Response Cookies extracted:      0
    Unicode:                              0
    Double unicode:                       0
    Non-ASCII representable:              0
    Directory traversals:                 0
    Extra slashes ("//"):                 0
    Self-referencing paths ("./"):        0
    HTTP Response Gzip packets extracted: 0
    Gzip Compressed Data Processed:       n/a
    Gzip Decompressed Data Processed:     n/a
    Total packets processed:              4759
===============================================================================
SMTP Preprocessor Statistics
  Total sessions                                   : 0
  Max concurrent sessions                          : 0
===============================================================================
dcerpc2 Preprocessor Statistics
  Total sessions: 0
===============================================================================
SSL Preprocessor:
   SSL packets decoded: 11
          Client Hello: 0
          Server Hello: 2
           Certificate: 0
           Server Done: 0
   Client Key Exchange: 0
   Server Key Exchange: 0
         Change Cipher: 4
              Finished: 0
    Client Application: 6
    Server Application: 3
                 Alert: 0
  Unrecognized records: 2
  Completed handshakes: 0
       Bad handshakes: 0
     Sessions ignored: 1
    Detection disabled: 1
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
Snort exiting
```

5. Conclude a malicious activity and scan the device network

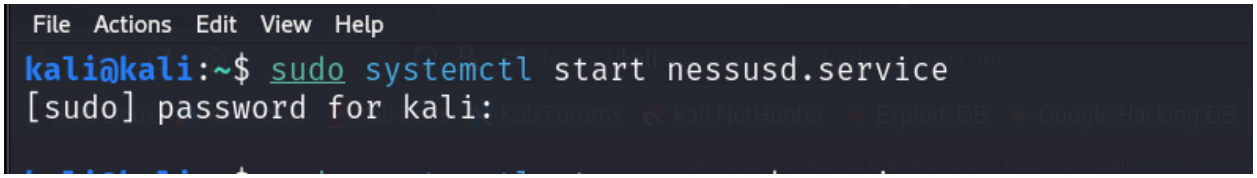
Mission :make scanning on machine

Tool: Nessus

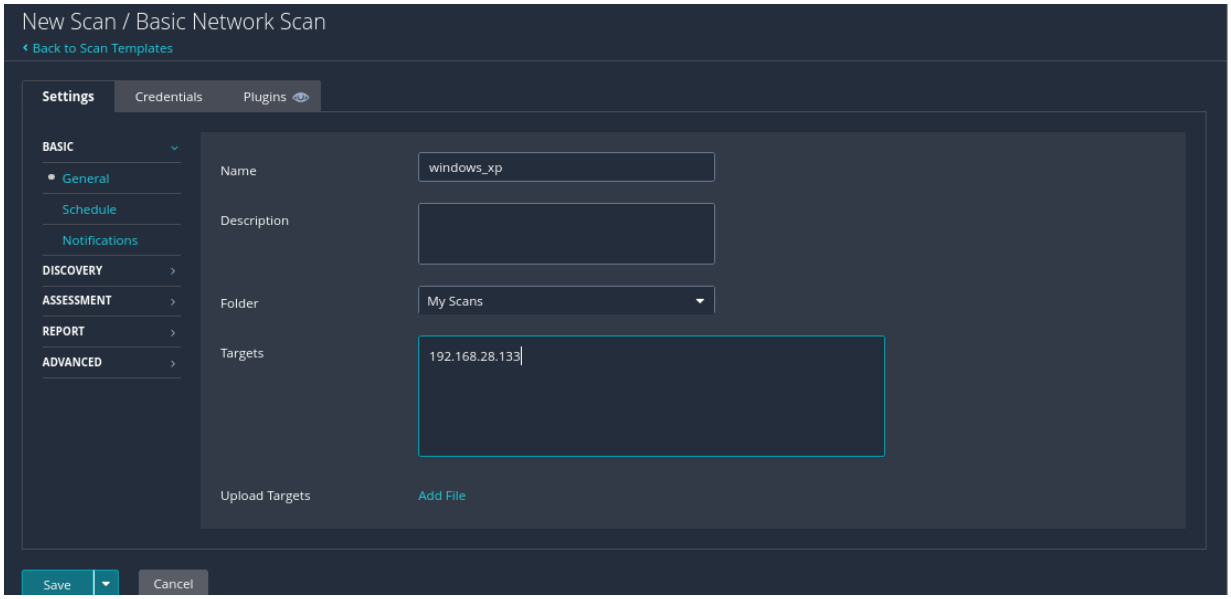
Nessus: is a popular vulnerability scanning tool used to identify security weaknesses in systems

Steps:

1. Open Nessus from terminal



2. **Set target Ip and start scanning**



192.168.128.133

4	2	1	1	23
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 31

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	34477	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)
CRITICAL	10.0	-	73182	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	-	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
HIGH	8.1	-	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.3	-	26920	SMB NULL Session Authentication
MEDIUM	5.3	-	57608	SMB Signing not required
LOW	2.1*	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type

Nessus file:
https://drive.google.com/file/d/1vZ5jlPdXSlBMWbZOze8VjcHnIciqUnys/view?usp=sharing

6. After finding vulnerabilities, Launching an IPS to prevent the attack

Mission : after finding vulnerabilities and port scanning in network ,launching rules to prevent the attack

Tool: snort

Snort: Snort is an open-source network intrusion detection and prevention system (IDPS) . It is designed to monitor network traffic in real-time and analyze it for suspicious activities and potential threats.

Steps to prevent suspicious activity:

After analyzing the PCAP file using Snort and Wireshark, we observed TCP and UDP scanning activities on unknown ports, which may indicate potential malicious behavior. Additionally, we detected numerous packets associated with ping scans, suggesting reconnaissance efforts across the entire network. To address these security concerns, we will implement rules to alert and drop these suspicious packets.

ip.addr==192.168.128.133&&tcp

No.	Time	Source	Destination	Protocol	Length	Info
1027	18.388810009	192.168.128.130	192.168.128.133	TCP	58	47590 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1028	18.388914754	192.168.128.130	192.168.128.133	TCP	58	47590 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1029	18.388978343	192.168.128.130	192.168.128.133	TCP	58	47590 → 587 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1030	18.389024025	192.168.128.130	192.168.128.133	TCP	58	47590 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1031	18.389115952	192.168.128.130	192.168.128.133	TCP	58	47590 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1032	18.389169532	192.168.128.130	192.168.128.133	TCP	58	47590 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1033	18.389212838	192.168.128.133	192.168.128.130	TCP	60	25 → 47590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1034	18.389234680	192.168.128.130	192.168.128.133	TCP	58	47590 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1035	18.389283045	192.168.128.133	192.168.128.130	TCP	60	53 → 47590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1036	18.389283067	192.168.128.130	192.168.128.133	TCP	58	47590 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1037	18.389283171	192.168.128.133	192.168.128.130	TCP	60	587 → 47590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1038	18.389331291	192.168.128.130	192.168.128.133	TCP	58	47590 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1039	18.389431100	192.168.128.130	192.168.128.133	TCP	58	47590 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1040	18.389480555	192.168.128.133	192.168.128.130	TCP	60	445 → 47590 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1041	18.389480793	192.168.128.133	192.168.128.130	TCP	60	995 → 47590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1042	18.389507727	192.168.128.130	192.168.128.133	TCP	54	47590 → 445 [RST] Seq=1 Win=0 Len=0
1043	18.389622772	192.168.128.133	192.168.128.130	TCP	60	139 → 47590 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
1044	18.389674598	192.168.128.130	192.168.128.133	TCP	54	47590 → 139 [RST] Seq=1 Win=0 Len=0
1045	18.389748934	192.168.128.133	192.168.128.130	TCP	60	1720 → 47590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1046	18.389876498	192.168.128.133	192.168.128.130	TCP	60	199 → 47590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1047	18.389876685	192.168.128.133	192.168.128.130	TCP	60	1723 → 47590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1048	18.389941680	192.168.128.133	192.168.128.130	TCP	60	80 → 47590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1049	18.390058123	192.168.128.130	192.168.128.133	TCP	58	47590 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1050	18.390152411	192.168.128.130	192.168.128.133	TCP	58	47590 → 8888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1051	18.390189781	192.168.128.130	192.168.128.133	TCP	58	47590 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1052	18.390225729	192.168.128.130	192.168.128.133	TCP	58	47590 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1053	18.390265889	192.168.128.130	192.168.128.133	TCP	58	47590 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1054	18.390295274	192.168.128.133	192.168.128.130	TCP	60	23 → 47590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1055	18.390305597	192.168.128.130	192.168.128.133	TCP	58	47590 → 111 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1056	18.390374522	192.168.128.130	192.168.128.133	TCP	58	47590 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1057	18.390398476	192.168.128.133	192.168.128.130	TCP	60	8888 → 47590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1058	18.390406448	192.168.128.130	192.168.128.133	TCP	58	47590 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1059	18.390435054	192.168.128.130	192.168.128.133	TCP	58	47590 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1060	18.390458599	192.168.128.133	192.168.128.130	TCP	60	113 → 47590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1061	18.390467766	192.168.128.130	192.168.128.133	TCP	58	47590 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1062	18.390496749	192.168.128.133	192.168.128.130	TCP	60	8080 → 47590 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1063	18.390499887	192.168.128.130	192.168.128.133	TCP	58	47590 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

ip.addr==192.168.128.133&&udp

No.	Time	Source	Destination	Protocol	Length	Info
10296	66.036962367	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB DELL-C03BD99FD1<00>
12933	67.536306433	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB DELL-C03BD99FD1<00>
22475	69.037128918	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB WORKGROUP<1d>
28805	70.536813503	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB WORKGROUP<1d>
40975	72.037153227	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB WORKGROUP<1d>
53078	73.536644922	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB WORKGROUP<1e>
63894	75.036931260	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB WORKGROUP<1e>
75619	76.536792785	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB WORKGROUP<1e>
87095	78.037433750	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB WORKGROUP<00>
99366	79.536891030	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB WORKGROUP<00>
111872	81.036649771	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB WORKGROUP<00>
148492	119.880908852	192.168.128.133	192.168.128.255	BROWSER	243	Local Master Announcement DELL-C03BD99FD1, Workstation, Serve…
159024	175.537452383	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB <01><02>__MSBROWSE__<02><01>
159172	177.037584845	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB <01><02>__MSBROWSE__<02><01>
159203	177.227190685	192.168.128.130	192.168.128.133	UDP	342	38562 → 41623 Len=300
159204	177.227819473	192.168.128.133	192.168.128.130	ICMP	190	Destination unreachable (Port unreachable)
159262	178.264596114	192.168.128.130	192.168.128.133	UDP	43	34594 → 1434 Len=1
159263	178.264788703	192.168.128.130	192.168.128.133	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><0…
159264	178.264958828	192.168.128.130	192.168.128.133	NBNS	92	Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><0…
159265	178.265056826	192.168.128.133	192.168.128.130	ICMP	71	Destination unreachable (Port unreachable)
159266	178.265119337	192.168.128.133	192.168.128.130	NBNS	271	Name query response NBSTAT
159267	178.265150140	192.168.128.133	192.168.128.130	NBNS	271	Name query response NBSTAT
159299	178.422552846	192.168.128.130	192.168.128.133	UDP	56	60806 → 64042 Len=14
159302	178.422814253	192.168.128.133	192.168.128.130	ICMP	84	Destination unreachable (Port unreachable)
159309	178.537728382	192.168.128.133	192.168.128.2	NBNS	110	Refresh NB <01><02>__MSBROWSE__<02><01>
159333	178.931091018	192.168.128.130	192.168.128.133	UDP	56	47768 → 43471 Len=14
159334	178.931478616	192.168.128.133	192.168.128.130	ICMP	84	Destination unreachable (Port unreachable)

Rules :

```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
#------------------
# LOCAL RULES
#------------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
# TCP Full Scan Detectio# TCP SYN Scan Detection
alert tcp any any -> 192.168.128.133 any (msg:"TCP SYN Scan Detected"; flags:S; threshold:type threshold, track by_src, count 5, seconds 10; sid:1000001; re
v:1;)
drop tcp any any -> 192.168.128.133 any (msg:"TCP SYN Scan Detected and Dropped"; flags:S; threshold:type threshold, track by_src, count 5, seconds 10; sid:
1000002; rev:1;)
# UDP Scan Detection
alert udp any any -> 192.168.128.133 any (msg:"UDP Scan Detected"; threshold:type threshold, track by_src, count 5, seconds 10; sid:1000003; rev:1;)
drop udp any any -> 192.168.128.133 any (msg:"UDP Scan Detected and Dropped"; threshold:type threshold, track by_src, count 5, seconds 10; sid:1000004; rev:
1;)

# ICMP Ping Scan Detection
alert icmp any any -> 192.168.128.133 any (msg:"ICMP Ping Scan Detected"; sid:1000005; rev:1;)
drop icmp any any -> 192.168.128.133 any (msg:"ICMP Ping Scan Detected and Dropped"; sid:1000006; rev:1;)
~
~
~
~
~
```

We will test these rules in real-time; however, we encountered some issues with (IPS) functionality in Snort, as it is not operating effectively on our machine. The required packages are incompatible, and despite our efforts to resolve these issues, we were unable to do so. As a result, we have opted to operate in (IDS) mode to identify and analyze the threats effectively.

1. Test TCP SYN Scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.128.133
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 16:07 EDT
Nmap scan report for 192.168.128.133 (192.168.128.133)
Host is up (0.00041s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:61:FD:09 (VMware)
```

- **Snort detected that activity and give us alert**

```
10/21-16:07:59.139904  [**] [1:1000001:1] TCP SYN Scan Detected [**] [Priori
ty: 0] {TCP} 192.168.128.130:34678 → 192.168.128.133:1723
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:07:59.140031  [**] [1:1000001:1] TCP SYN Scan Detected [**] [Priori
ty: 0] {TCP} 192.168.128.130:34678 → 192.168.128.133:22
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:07:59.140158  [**] [1:1000001:1] TCP SYN Scan Detected [**] [Priori
ty: 0] {TCP} 192.168.128.130:34678 → 192.168.128.133:1720
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:07:59.140276  [**] [1:1000001:1] TCP SYN Scan Detected [**] [Priori
ty: 0] {TCP} 192.168.128.130:34678 → 192.168.128.133:12345
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
```

2. Test UDP scan

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU 192.168.128.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-21 16:15 EDT
Nmap scan report for 192.168.128.133 (192.168.128.133)
Host is up (0.00040s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
123/udp  open          ntp
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
445/udp  open|filtered microsoft-ds
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
MAC Address: 00:0C:29:61:FD:09 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```

- **Snort Detection**

```
10/21-16:15:32.551316  [**] [1:1000003:1] UDP Scan Detected [**] [Priority: 0] {UDP} 192.168.128.130:42103 → 192.168.128.133:9876
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:15:32.551605  [**] [1:1000003:1] UDP Scan Detected [**] [Priority: 0] {UDP} 192.168.128.130:42103 → 192.168.128.133:434
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:15:32.551866  [**] [1:1000003:1] UDP Scan Detected [**] [Priority: 0] {UDP} 192.168.128.130:42103 → 192.168.128.133:3401
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:15:32.552112  [**] [1:1000003:1] UDP Scan Detected [**] [Priority: 0] {UDP} 192.168.128.130:42103 → 192.168.128.133:19956
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
```

3. Test Ping Scan

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.128.133
PING 192.168.128.133 (192.168.128.133) 56(84) bytes of data.
64 bytes from 192.168.128.133: icmp_seq=1 ttl=128 time=1.26 ms
64 bytes from 192.168.128.133: icmp_seq=2 ttl=128 time=0.671 ms
64 bytes from 192.168.128.133: icmp_seq=3 ttl=128 time=0.770 ms
64 bytes from 192.168.128.133: icmp_seq=4 ttl=128 time=1.01 ms
```

- **Snort Detection**

```
10/21-16:20:42.514074  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:43.538275  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:44.562464  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:45.586016  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:46.610358  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:47.634227  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:48.635405  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:49.650961  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:50.674166  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:51.697959  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:52.722156  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:53.746153  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:54.769920  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/21-16:20:55.770891  [**] [1:1000005:1] ICMP Ping Scan Detected [**] [Priority: 0] {ICMP} 192.168.128.130 → 192.168.128.133
WARNING: No preprocessors configured for policy 0.
```

9. Forensic Investigation Report on Backdoor Discovery

Mission: Perform Forensic Investigation on the Image and Get the Backdoor

Tool: Autopsy

Autopsy: Autopsy is the premier open-source forensics platform which is fast, easy-to-use, and capable of analyzing all types of mobile devices and digital media. Its plug-in architecture enables extensibility from community-developed or custom-built modules. Autopsy evolves to meet the needs of hundreds of thousands of professionals in law enforcement, national security, litigation support, and corporate investigation

Steps:

1. Introduction

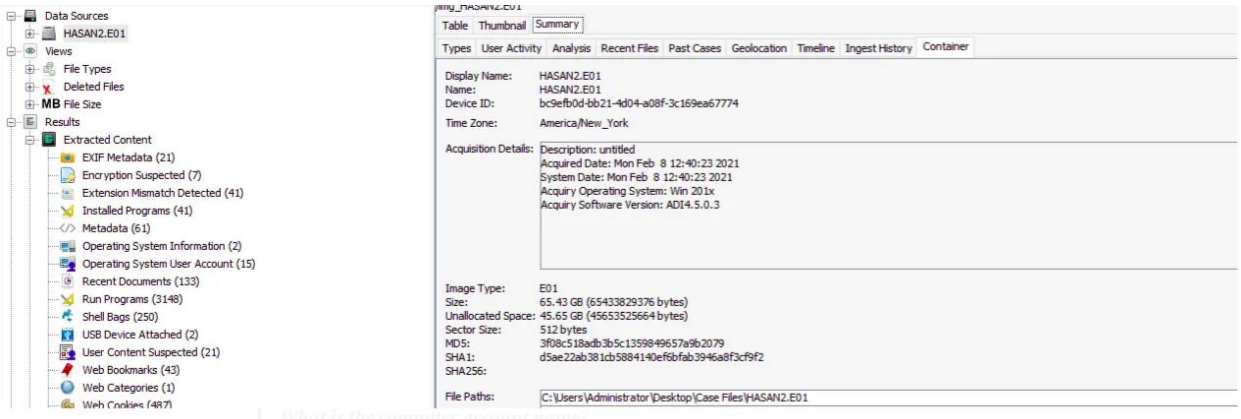
- **Purpose of the Investigation:**
  - To analyze the disk image for malicious activity and identify any backdoors present.
- **Scope of the Report:**
  - This report details the methodology used, findings, and conclusions drawn from the investigation.

2. Initial Findings

- **MD5 Hash of The Image**

We can find the hash of the image by selecting the appropriate data source in Autopsy and navigating to the Container tab under Summary.

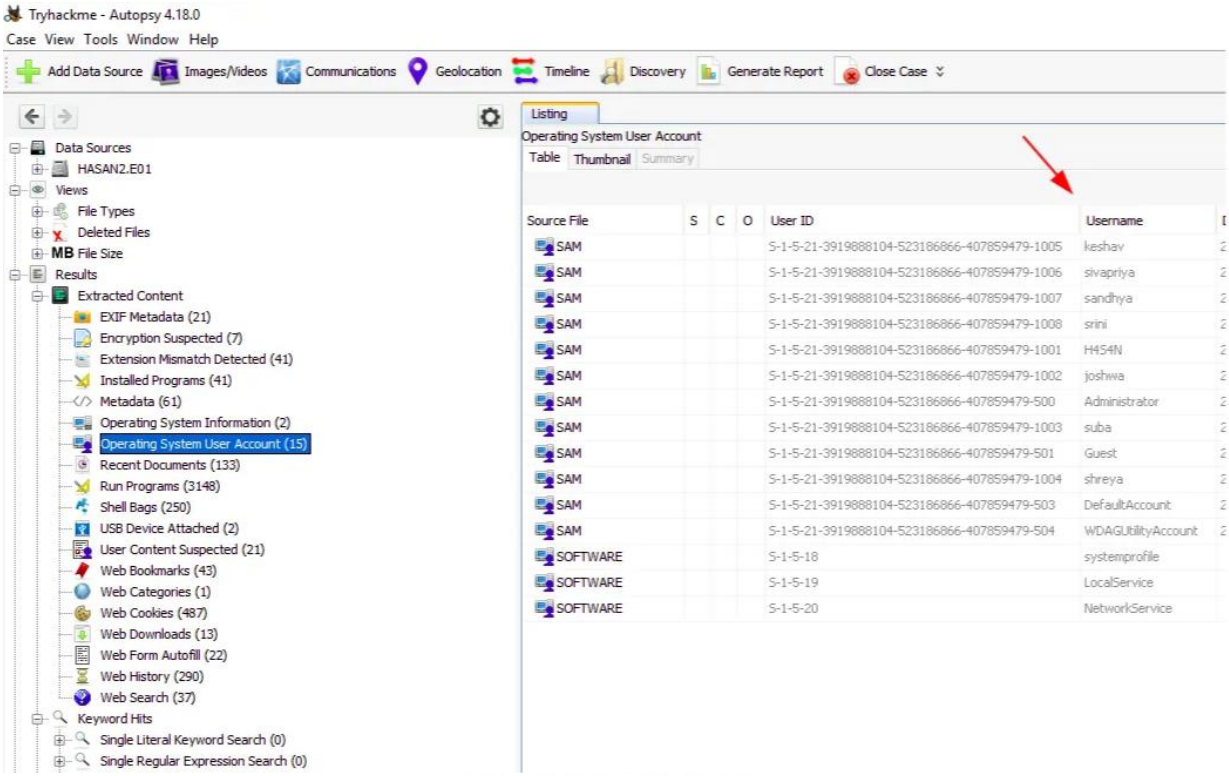
3f08c518adb3b5c1359849657a9b2079



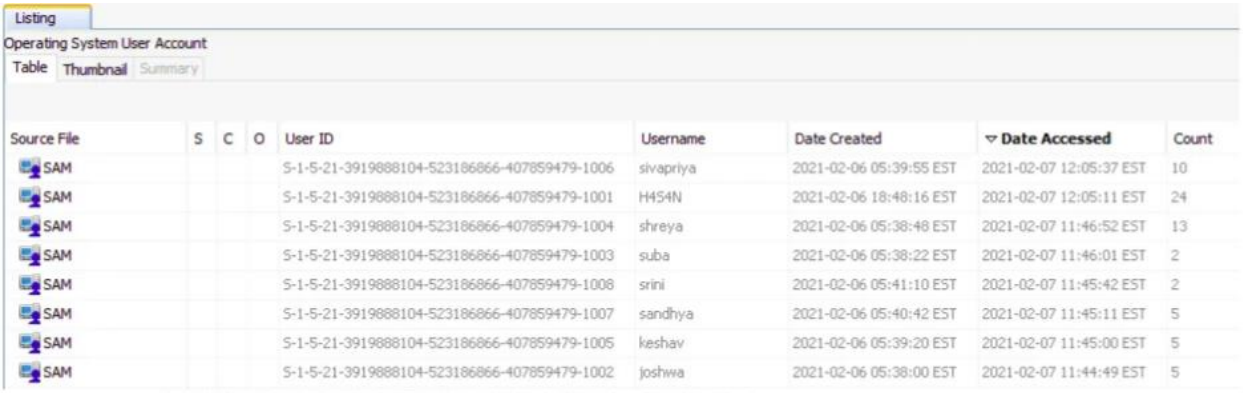
- **User Accounts Identified**

Just below the *Operating System Information* results, we see an option for *Operating System User Accounts,* we can get our answer from there.

Accounts are: H4S4N,joshwa,keshav,sandhya,shreya,sivapriya,srini,suba

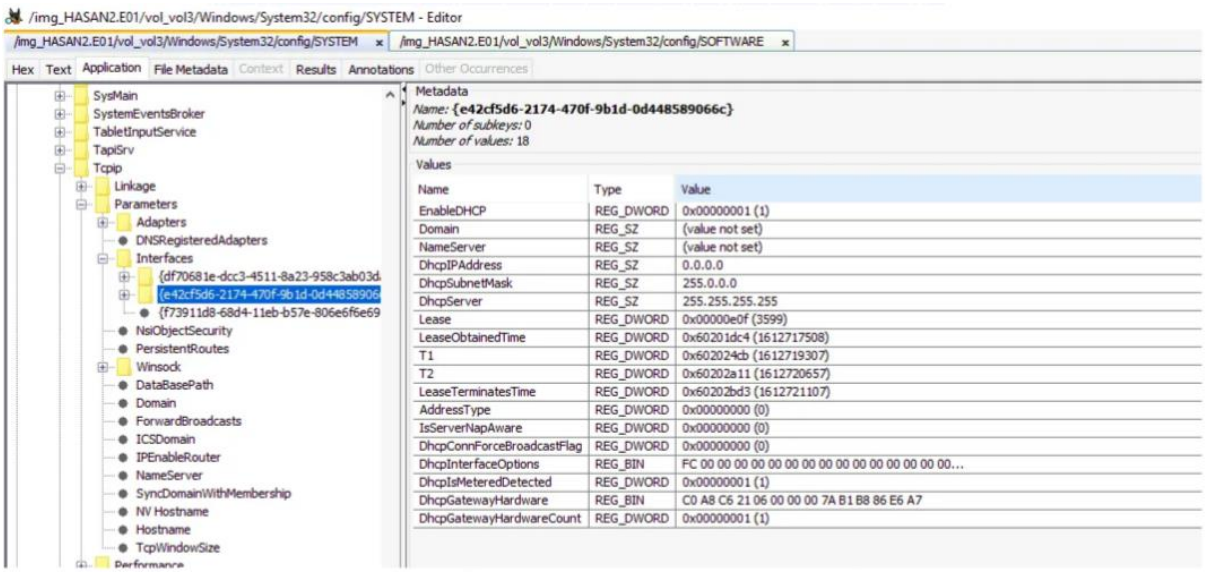


- **Last Logged Use** We can sort the User Accounts by "Date Accessed" and we see **sivapriya** was the last user who logged to the device

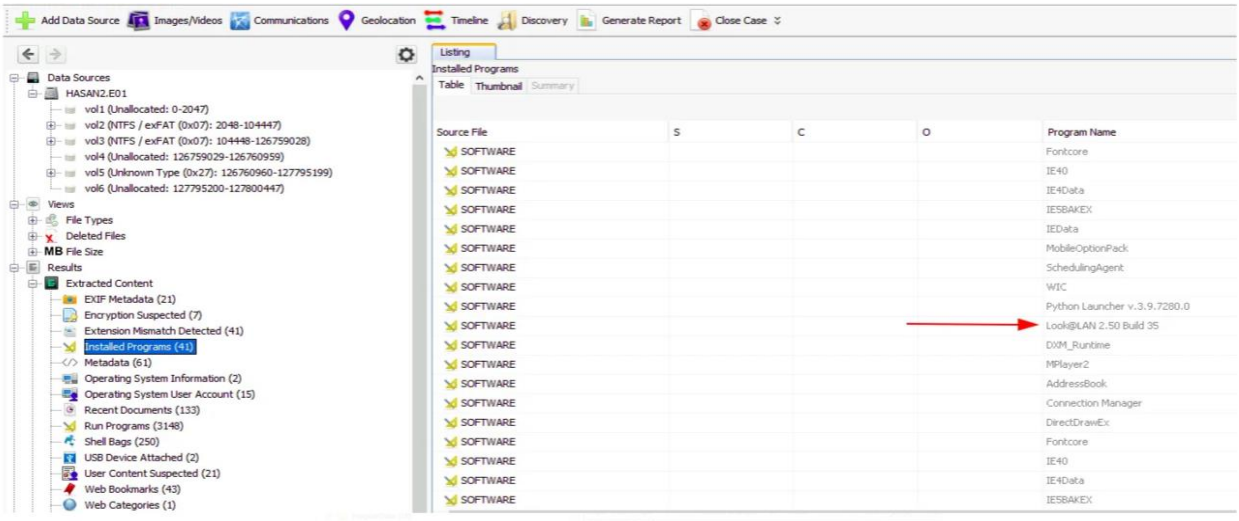


- **IP Address for the computer**

Since we're working with an image of a Windows machine, we can find the IP address associated with network adapters in the Windows Registry. We can even access the registry from within Autopsy.

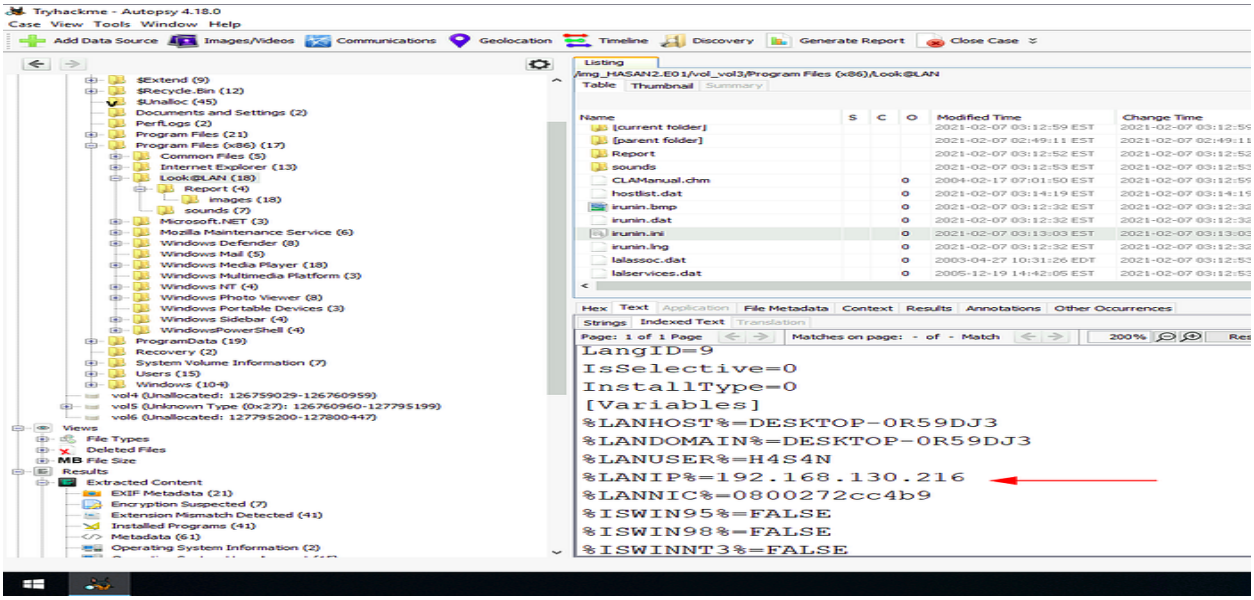


No such luck, the IP address is listed as 0.0.0.0. We'll have to find it elsewhere, and while looking through Autopsy's findings, we notice an unusual application installed on the device.



Searching for the executable name tells us it is a network monitoring tool, so let's look for any logs it may have generated. We find its directory under *Program Files (x86).* Among the files in the folder, only one stands out, a .ini file. We can view the file within Autopsy by selecting it.

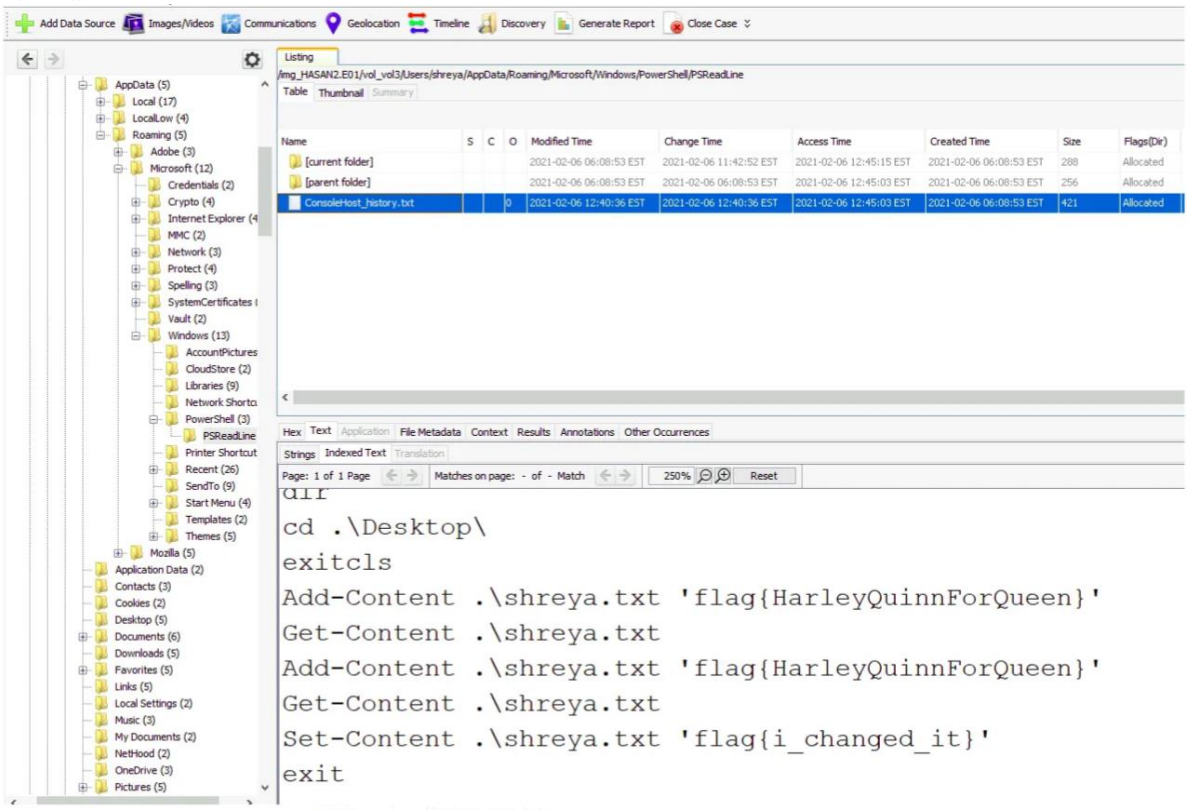
so the **IP Address** would be 192.168.130.216 and **MAC Address** would be 08-00-27-2c-c4-b9



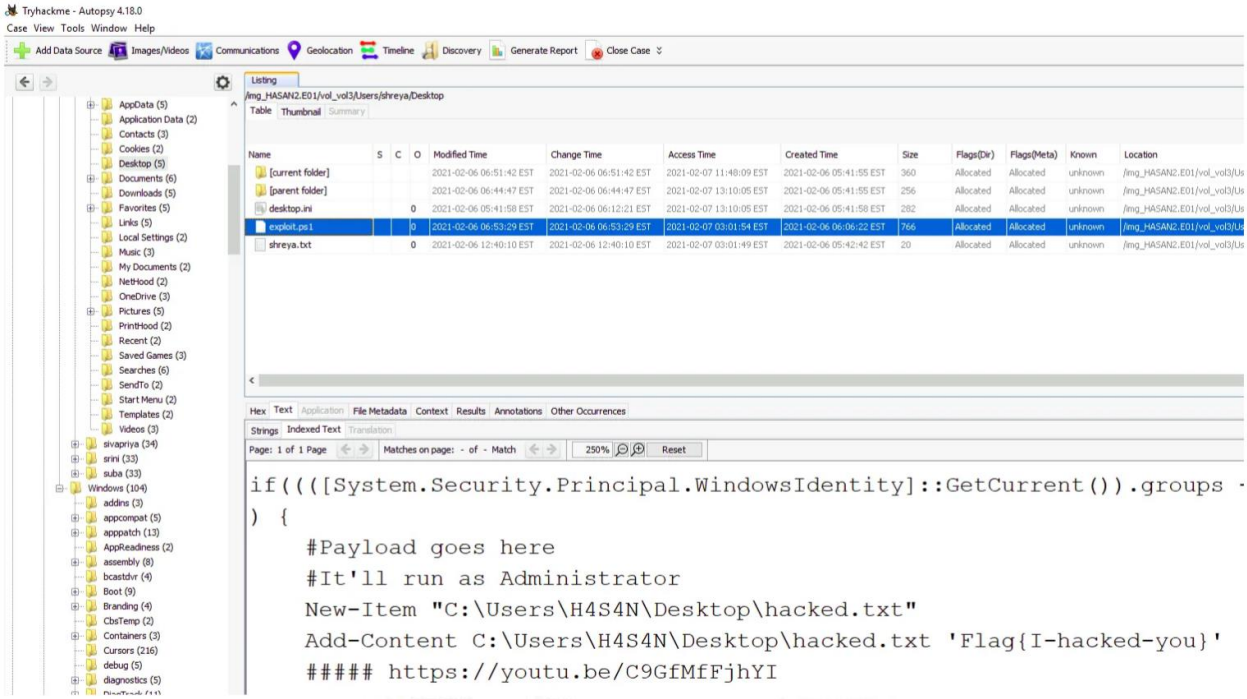
3. File System Analysis

First, we Identify unusual file names or extensions that may indicate malicious activity.
After checking some of the user's Desktops, we locate a flag within the shreya user's Desktop directory. Now that we know the user, we'll check the PowerShell history for the account. There is also a PowerShell script on the user's desktop named exploit.

PowerShell command history is stored in
APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
As expected, we find the PowerShell history with a **flag{HarleyQuinnForQueen}**



We noted a PowerShell script named exploit, so we'll go back and look at its contents now.



10. Analysis of the Backdoor By Ghidra

Using Ghidra to analyze putty.exe allows you to reverse-engineer the executable and gain insights into its structure, functions, and potential behavior. Once you've loaded putty.exe into Ghidra and completed the analysis