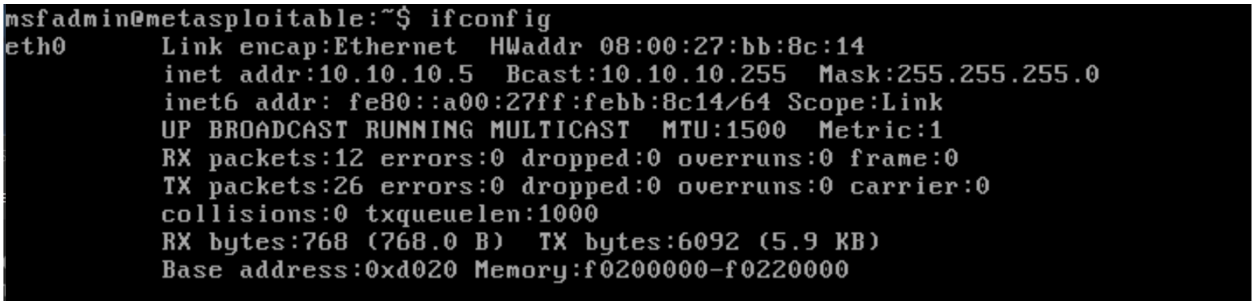
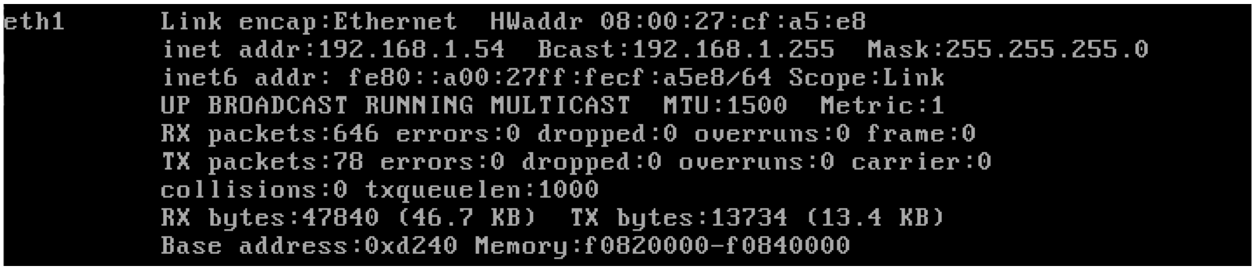
Lab Objective: To design and implement a custom Security Orchestration, Automation, and Response (SOAR) pipeline within a virtualized enterprise network environment. This project demonstrates the ability to ingest threat intelligence from a SIEM (Security Onion), parse nested Elastic Common Schema (ECS) event logs using a custom Python automation script and execute programmatic firewall containment strategies on a target asset to neutralize active cyber threats.

System Setup Details: (Oracle VirtualBox v7.2.6)
Analyst: *SecurityOnion* (IP Address: 192.168.1.50)
Network Adapter 1: Bridged, Network Adapter 2: Internal Network (inet)
Attacker: *Kali* (IP Address: 10.10.10.6)
Network Adapter 1: Internal Network (inet, promiscuous mode: Deny)
Victim: *Metasploitable* (eth0 IP Address: 10.10.10.5, eth1 IP Address: 192.168.1.54)
Network Adapter 1: Internal Network (inet, promiscuous mode: Allow All),
Network Adapter 2: Bridged (to allow the SOAR script to modify firewall rules)



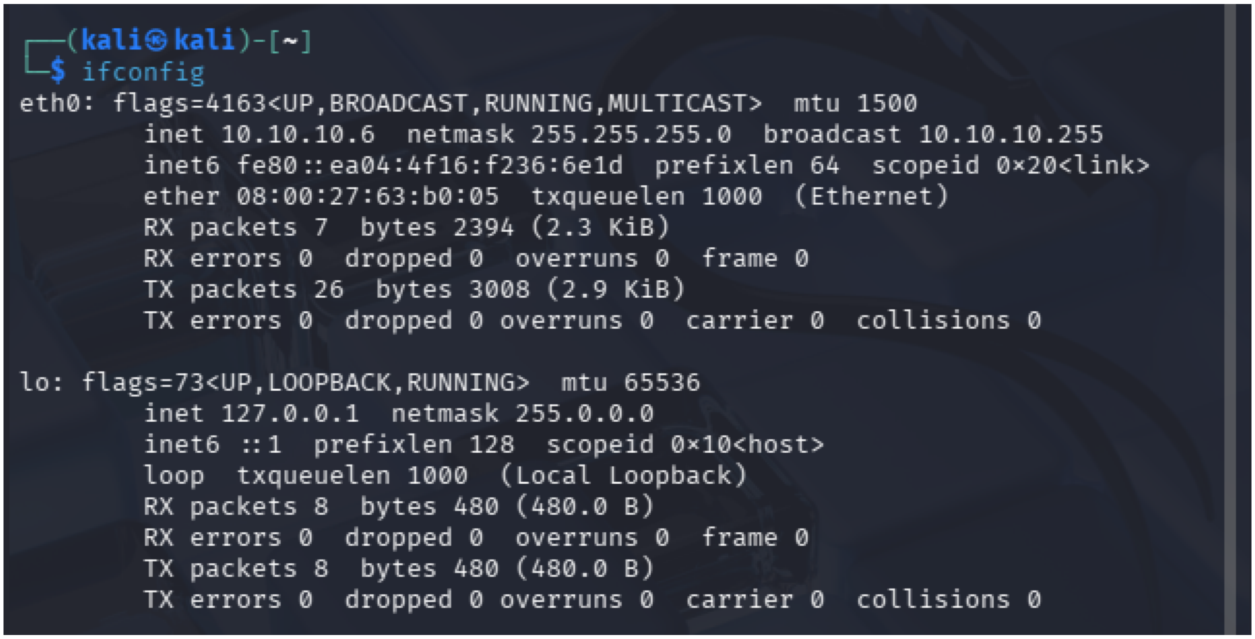
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:bb:8c:14
          inet addr:10.10.10.5  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febb:8c14/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:768 (768.0 B)  TX bytes:6092 (5.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```



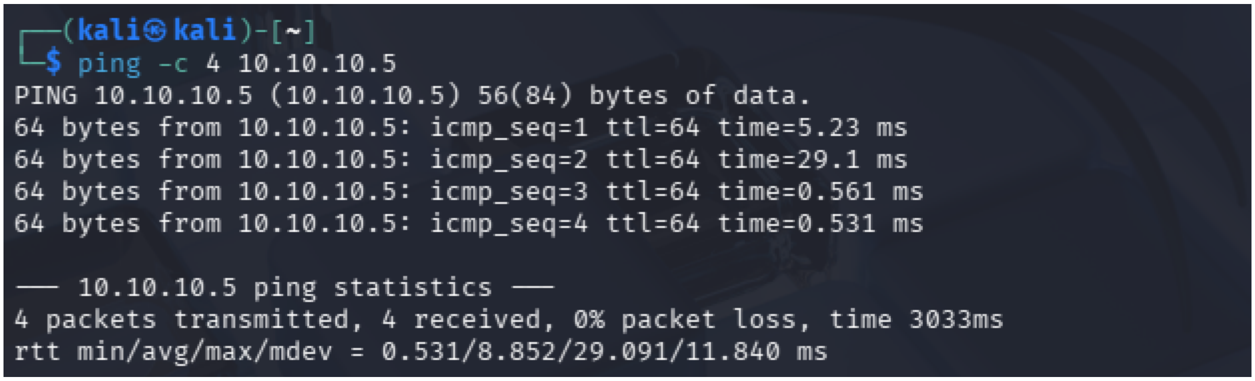
```
eth1      Link encap:Ethernet  HWaddr 08:00:27:cf:a5:e8
          inet addr:192.168.1.54  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fecf:a5e8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:646 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:47840 (46.7 KB)  TX bytes:13734 (13.4 KB)
          Base address:0xd240 Memory:f0820000-f0840000
```

Target System Configuration (Metasploitable):

- **IP Address:** eth0: *10.10.10.5* and eth1: 192.168.1.54 confirmed via *ifconfig*.
- **Status:** Interface *eth0* is UP and reachable on the internal *10.10.10.0/24* subnet.
- **Role:** This asset hosts intentionally vulnerable services (FTP, HTTP, MySQL) to serve as the target for Red Team operations.



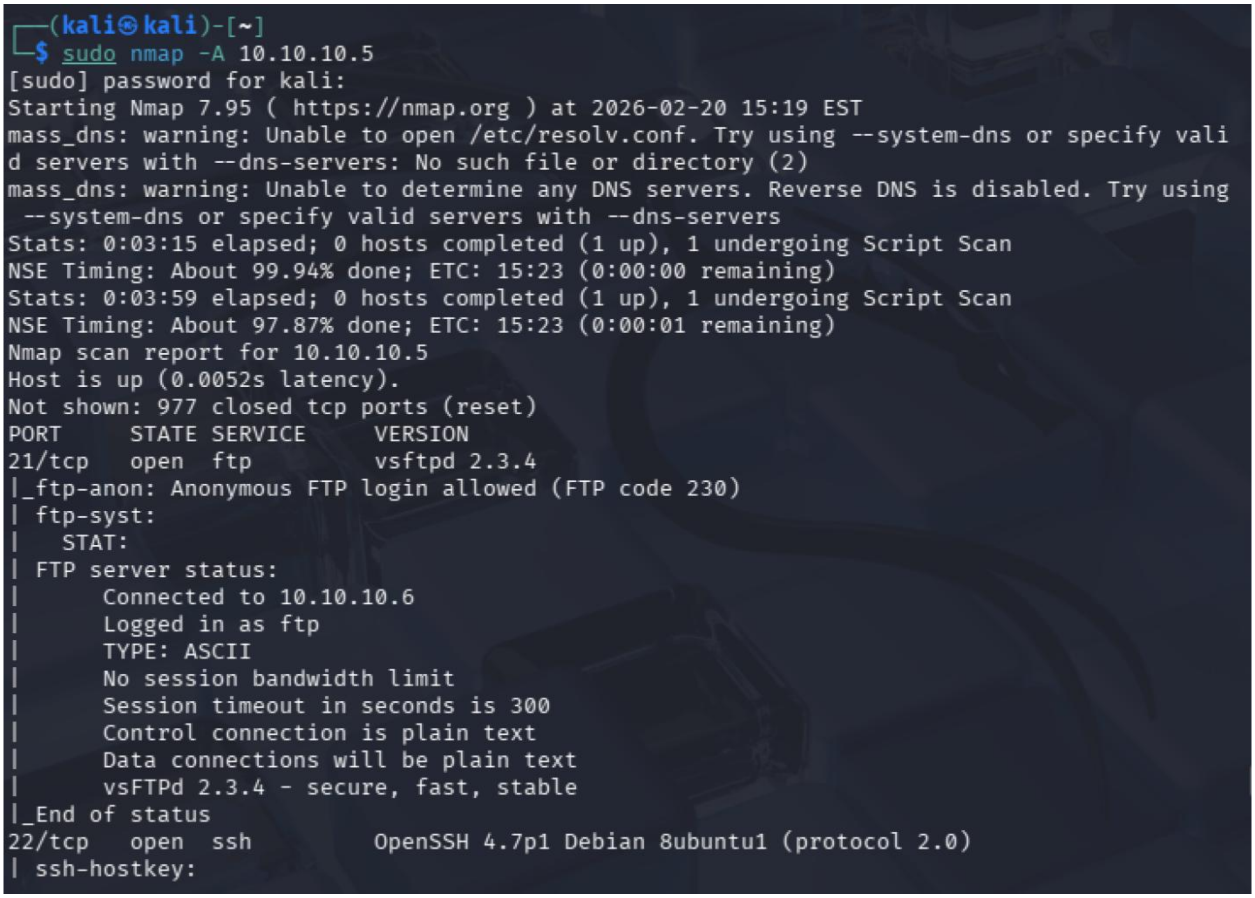
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.6  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::ea04:4f16:f236:6e1d  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:63:b0:05  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 2394 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26  bytes 3008 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



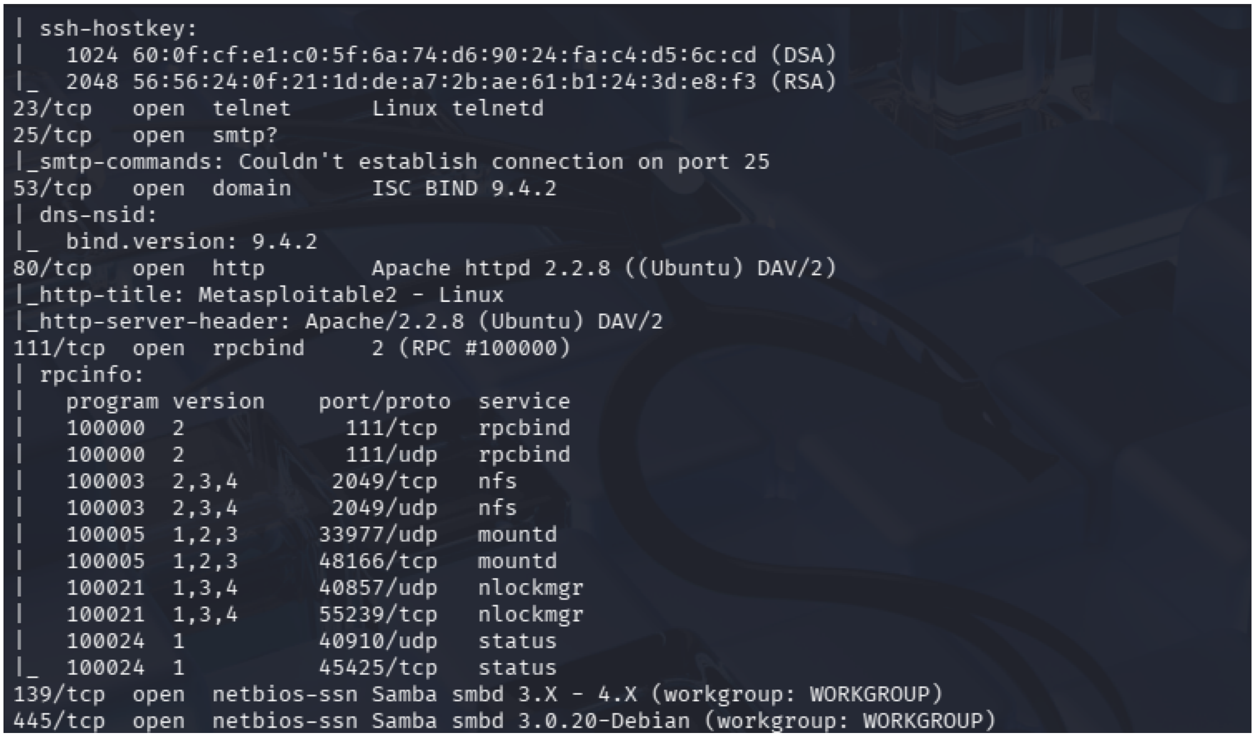
```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 10.10.10.5
PING 10.10.10.5 (10.10.10.5) 56(84) bytes of data.
64 bytes from 10.10.10.5: icmp_seq=1 ttl=64 time=5.23 ms
64 bytes from 10.10.10.5: icmp_seq=2 ttl=64 time=29.1 ms
64 bytes from 10.10.10.5: icmp_seq=3 ttl=64 time=0.561 ms
64 bytes from 10.10.10.5: icmp_seq=4 ttl=64 time=0.531 ms

── 10.10.10.5 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3033ms
rtt min/avg/max/mdev = 0.531/8.852/29.091/11.840 ms
```

Attacker Connectivity & Reachability Check:

- **IP Address:** *10.10.10.6* (Static Assignment).
- **Connectivity Test:** Successful ICMP Echo (Ping) requests to the target (*10.10.10.5*) confirm network path availability and low latency (<1ms), verifying the virtual switch configuration for the **internal network** (inet).

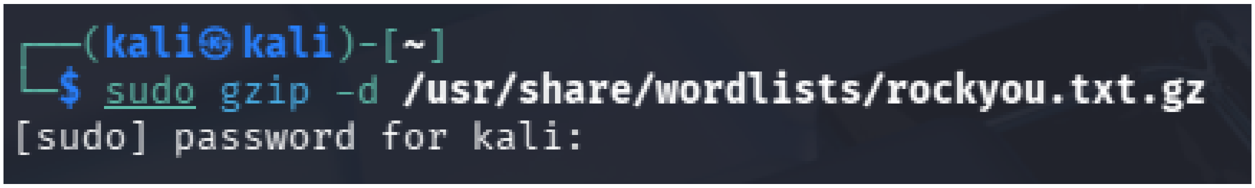


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 10.10.10.5
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-20 15:19 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify vali
d servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using
 --system-dns or specify valid servers with --dns-servers
Stats: 0:03:15 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.94% done; ETC: 15:23 (0:00:00 remaining)
Stats: 0:03:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.87% done; ETC: 15:23 (0:00:01 remaining)
Nmap scan report for 10.10.10.5
Host is up (0.0052s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.10.6
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
```

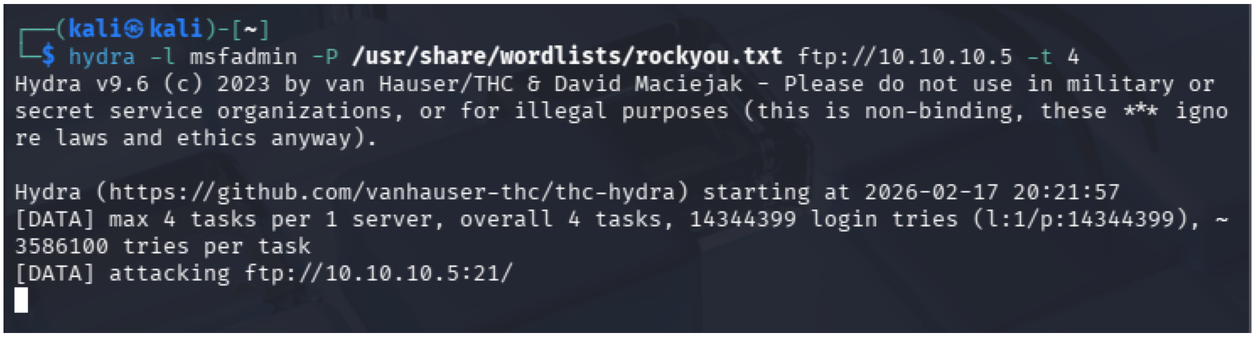


```
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      33977/udp   mountd
|   100005  1,2,3      48166/tcp   mountd
|   100021  1,3,4      40857/udp   nlockmgr
|   100021  1,3,4      55239/tcp   nlockmgr
|   100024  1          40910/udp   status
|_  100024  1          45425/tcp   status
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)
```

Execution of Aggressive Reconnaissance Scan (Cyberattack 1/2):



```
┌──(kali㉿kali)-[~]
└─$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:
```



```
┌──(kali㉿kali)-[~]
└─$ hydra -l msfadmin -P /usr/share/wordlists/rockyou.txt ftp://10.10.10.5 -t 4
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these *** igno
re laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-17 20:21:57
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~
3586100 tries per task
[DATA] attacking ftp://10.10.10.5:21/
█
```

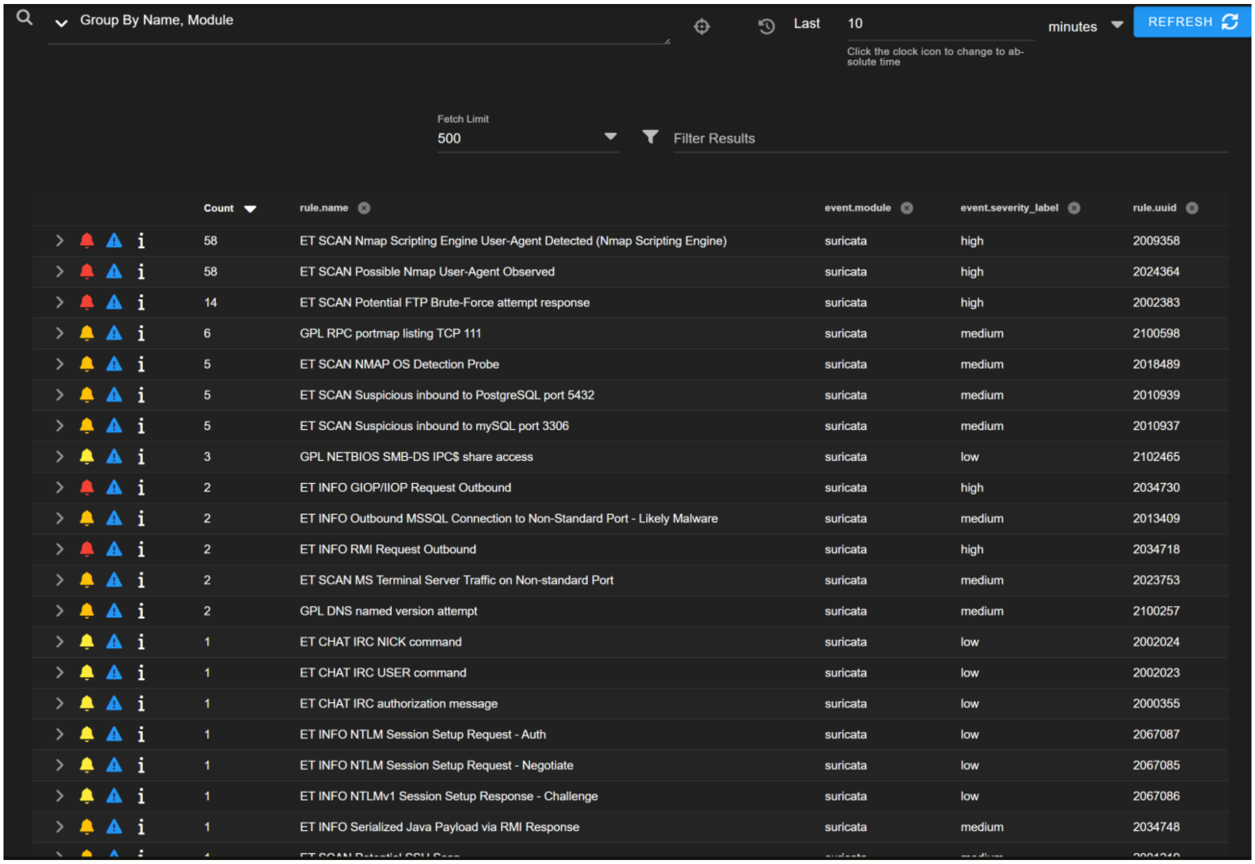
Execution of Brute Force Attack via Hydra through FTP (Cyberattack 2/2)

As seen above, two different types of cyberattacks were performed on the victim machine and can be seen on the Security Onion Alerts web interface.

The Need for Automation (SOAR Implementation):

While the Security Onion dashboard successfully detected and indexed the attacks, relying on manual human intervention creates an unacceptable delay in incident response. To modernize this workflow, a custom Python-based SOAR pipeline was developed to achieve the following:

- **Drastic Reduction in MTTR**: Reduces the Mean Time to Respond (MTTR) from minutes or hours down to milliseconds by eliminating the need for an analyst to manually review the alert and log into the firewall.
- **Automated Log Parsing**: Programmatically queries the Elasticsearch API to parse complex ECS data, extracting actionable IOCs (Indicators of Compromise) such as the attacker's IP address and the specific threat signature.
- **Proactive Containment**: Utilizes the paramiko SSH library to securely bridge the management network and the victim network, automatically injecting iptables drop rules directly onto the compromised asset.



Group By Name, Module

Last 10 minutes

Click the clock icon to change to absolute time

REFRESH

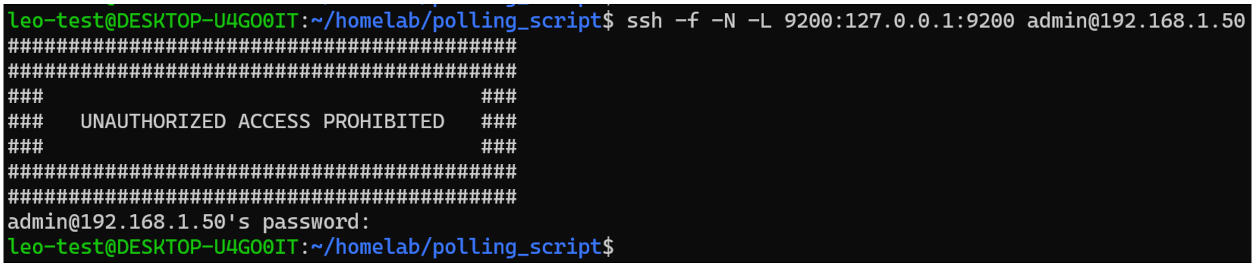
Fetch Limit 500

Filter Results

Count	rule.name	event.module	event.severity_label	rule.uuid
58	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	suricata	high	2009358
58	ET SCAN Possible Nmap User-Agent Observed	suricata	high	2024364
14	ET SCAN Potential FTP Brute-Force attempt response	suricata	high	2002383
6	GPL RPC portmap listing TCP 111	suricata	medium	2100598
5	ET SCAN NMAP OS Detection Probe	suricata	medium	2018489
5	ET SCAN Suspicious inbound to PostgreSQL port 5432	suricata	medium	2010939
5	ET SCAN Suspicious inbound to mySQL port 3306	suricata	medium	2010937
3	GPL NETBIOS SMB-DS IPC$ share access	suricata	low	2102465
2	ET INFO GIOP/IIOP Request Outbound	suricata	high	2034730
2	ET INFO Outbound MSSQL Connection to Non-Standard Port - Likely Malware	suricata	medium	2013409
2	ET INFO RMI Request Outbound	suricata	high	2034718
2	ET SCAN MS Terminal Server Traffic on Non-standard Port	suricata	medium	2023753
2	GPL DNS named version attempt	suricata	medium	2100257
1	ET CHAT IRC NICK command	suricata	low	2002024
1	ET CHAT IRC USER command	suricata	low	2002023
1	ET CHAT IRC authorization message	suricata	low	2000355
1	ET INFO NTLM Session Setup Request - Auth	suricata	low	2067087
1	ET INFO NTLM Session Setup Request - Negotiate	suricata	low	2067085
1	ET INFO NTLMv1 Session Setup Response - Challenge	suricata	low	2067086
1	ET INFO Serialized Java Payload via RMI Response	suricata	medium	2034748
1	ET SCAN Potential SSH Scan	suricata	medium	2001219

Subtitle:

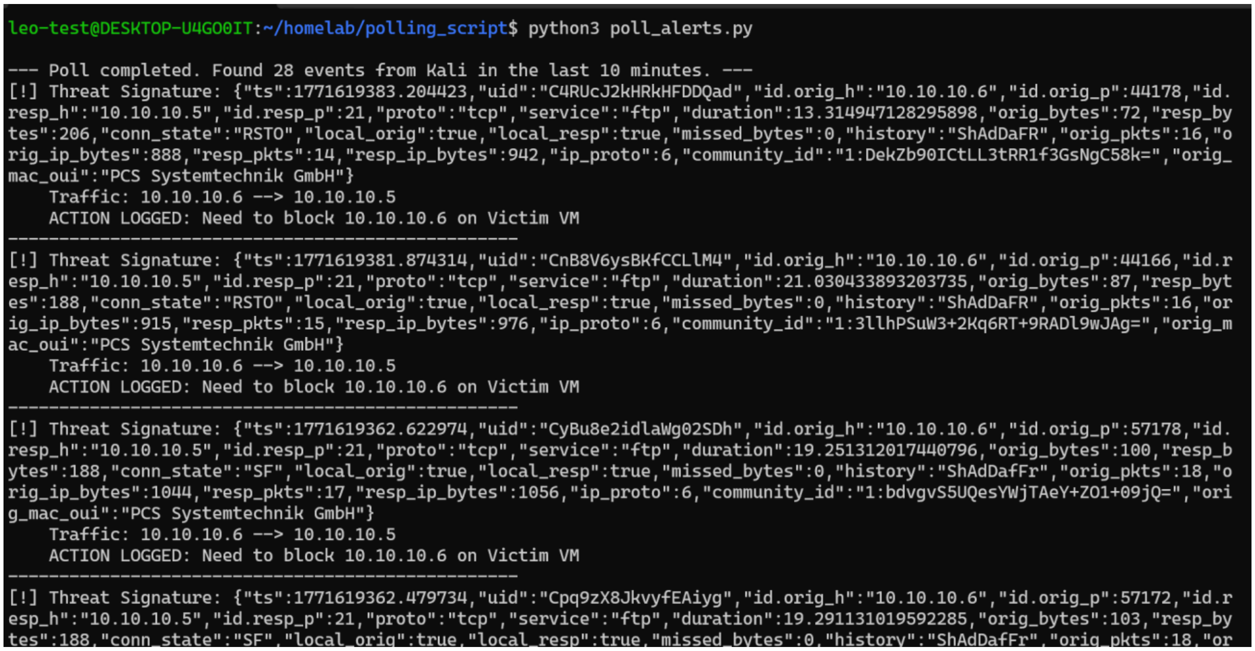
- **Dashboard View**: The Security Onion "Alerts" console successfully ingested and indexed the attack traffic.
- We can connect the Security Onion API with a custom SOAR python script that will automate the workflow for handling these issues much more effectively.



```
leo-test@DESKTOP-U4GO0IT:~/homelab/polling_script$ ssh -f -N -L 9200:127.0.0.1:9200 admin@192.168.1.50
##########################################
##########################################
###                                    ###
###    UNAUTHORIZED ACCESS PROHIBITED  ###
###                                    ###
##########################################
##########################################
admin@192.168.1.50's password:
leo-test@DESKTOP-U4GO0IT:~/homelab/polling_script$
```

Establishing the SSH Tunnel:

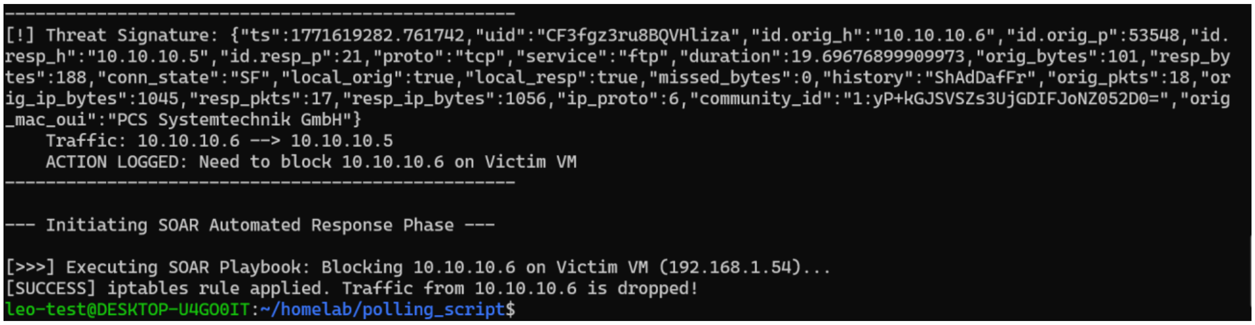
This for ensuring Local Port Forwarding is enabled for SSH to Security Onion's API.



```
leo-test@DESKTOP-U4GO0IT:~/homelab/polling_script$ python3 poll_alerts.py

--- Poll completed. Found 28 events from Kali in the last 10 minutes. ---
[!] Threat Signature: {"ts":1771619383.204423,"uid":"C4RUcJ2kHRkHFDDQad","id.orig_h":"10.10.10.6","id.orig_p":44178,"id.
resp_h":"10.10.10.5","id.resp_p":21,"proto":"tcp","service":"ftp","duration":13.314947128295898,"orig_bytes":72,"resp_by
tes":206,"conn_state":"RSTO","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"ShAdDaFR","orig_pkts":16,"o
rig_ip_bytes":888,"resp_pkts":14,"resp_ip_bytes":942,"ip_proto":6,"community_id":"1:DekZb90ICtLL3tRR1f3GsNgC58k=","orig_
mac_oui":"PCS Systemtechnik GmbH"}
    Traffic: 10.10.10.6 --> 10.10.10.5
    ACTION LOGGED: Need to block 10.10.10.6 on Victim VM
--------------------------------------------------
[!] Threat Signature: {"ts":1771619381.874314,"uid":"CnB8V6ysBKfCCLlM4","id.orig_h":"10.10.10.6","id.orig_p":44166,"id.r
esp_h":"10.10.10.5","id.resp_p":21,"proto":"tcp","service":"ftp","duration":21.030433893203735,"orig_bytes":87,"resp_byt
es":188,"conn_state":"RSTO","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"ShAdDaFR","orig_pkts":16,"or
ig_ip_bytes":915,"resp_pkts":15,"resp_ip_bytes":976,"ip_proto":6,"community_id":"1:3llhPSuW3+2Kq6RT+9RADl9wJAg=","orig_m
ac_oui":"PCS Systemtechnik GmbH"}
    Traffic: 10.10.10.6 --> 10.10.10.5
    ACTION LOGGED: Need to block 10.10.10.6 on Victim VM
--------------------------------------------------
[!] Threat Signature: {"ts":1771619362.622974,"uid":"CyBu8e2idlaWg02SDh","id.orig_h":"10.10.10.6","id.orig_p":57178,"id.
resp_h":"10.10.10.5","id.resp_p":21,"proto":"tcp","service":"ftp","duration":19.251312017440796,"orig_bytes":100,"resp_b
ytes":188,"conn_state":"SF","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"ShAdDafFr","orig_pkts":18,"o
rig_ip_bytes":1044,"resp_pkts":17,"resp_ip_bytes":1056,"ip_proto":6,"community_id":"1:bdvgvS5UQesYWjTAeY+ZO1+09jQ=","ori
g_mac_oui":"PCS Systemtechnik GmbH"}
    Traffic: 10.10.10.6 --> 10.10.10.5
    ACTION LOGGED: Need to block 10.10.10.6 on Victim VM
--------------------------------------------------
[!] Threat Signature: {"ts":1771619362.479734,"uid":"Cpq9zX8JkvyfEAiyg","id.orig_h":"10.10.10.6","id.orig_p":57172,"id.r
esp_h":"10.10.10.5","id.resp_p":21,"proto":"tcp","service":"ftp","duration":19.291131019592285,"orig_bytes":103,"resp_by
tes":188,"conn_state":"SF","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"ShAdDafFr","orig_pkts":18,"or
```

Automated Threat Polling & Parsing:

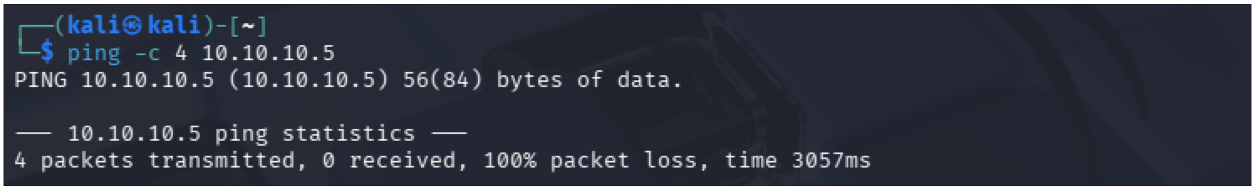
The SOAR script successfully authenticates with the Security Onion API via an encrypted SSH tunnel. It polls for events from the last 10 minutes, parses the nested JSON data to identify the malicious source IP (10.10.10.6), and logs the specific Suricata threat signatures (e.g., FTP Brute Force, Nmap Scans).



```
--------------------------------------------------
[!] Threat Signature: {"ts":1771619282.761742,"uid":"CF3fgz3ru8BQVHliza","id.orig_h":"10.10.10.6","id.orig_p":53548,"id.
resp_h":"10.10.10.5","id.resp_p":21,"proto":"tcp","service":"ftp","duration":19.69676899909973,"orig_bytes":101,"resp_by
tes":188,"conn_state":"SF","local_orig":true,"local_resp":true,"missed_bytes":0,"history":"ShAdDafFr","orig_pkts":18,"or
ig_ip_bytes":1045,"resp_pkts":17,"resp_ip_bytes":1056,"ip_proto":6,"community_id":"1:yP+kGJSVSZs3UjGDIFJoNZ052D0=","orig
_mac_oui":"PCS Systemtechnik GmbH"}
    Traffic: 10.10.10.6 --> 10.10.10.5
    ACTION LOGGED: Need to block 10.10.10.6 on Victim VM
--------------------------------------------------

--- Initiating SOAR Automated Response Phase ---

[>>>] Executing SOAR Playbook: Blocking 10.10.10.6 on Victim VM (192.168.1.54)...
[SUCCESS] iptables rule applied. Traffic from 10.10.10.6 is dropped!
leo-test@DESKTOP-U4GO0IT:~/homelab/polling_script$
```

Automated Containment Execution:

After extracting and deduplicating the attacker's IP address, the script initiates the Orchestration phase. It establishes a secure SSH connection to the Victim VM (192.168.1.54) and automatically deploys a targeted iptables firewall rule (-A INPUT -s 10.10.10.6 -j DROP) without requiring human interaction.



```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 10.10.10.5
PING 10.10.10.5 (10.10.10.5) 56(84) bytes of data.

── 10.10.10.5 ping statistics ──
4 packets transmitted, 0 received, 100% packet loss, time 3057ms
```

Verification of Mitigation:

To verify the efficacy of the SOAR pipeline, continuous ICMP Echo requests were sent from the Attacker machine. The exact moment the Python script applied the automated rule, the connectivity was severed, resulting in 100% packet loss and confirming the complete neutralization of the threat.

Future Improvements:

- In a production environment, you would typically pull credentials securely from a .env file rather than hardcoding them and utilize SSH keys instead of passwords for the paramiko connection.
- Additionally, the SOAR script can be modified to be more flexible and/or have more verbose output for analysts to review.