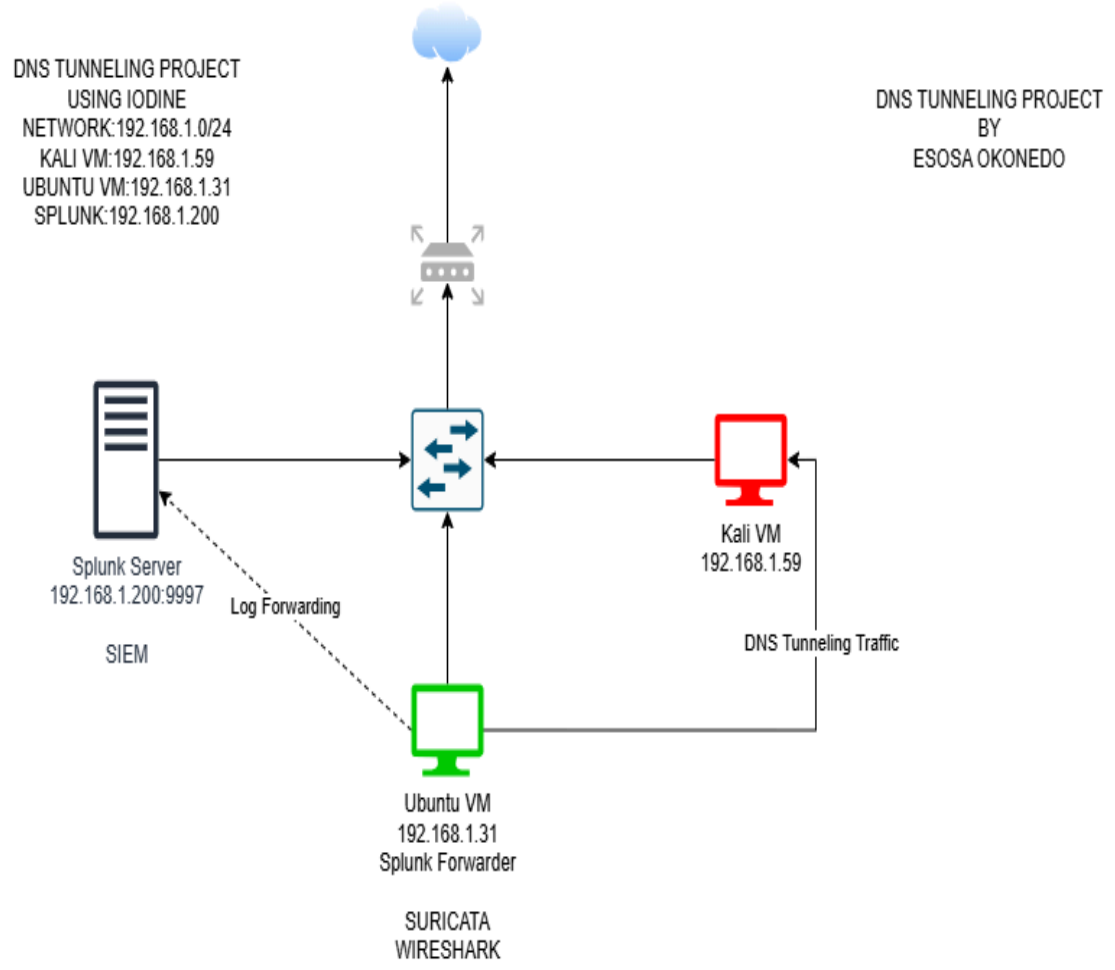
Incident Report: Detection of DNS Tunneling Attack

Author: ESOSA OKONEDO
Date Completed: May 22nd, 2025



1. Executive Summary

On May 10th, 2025, at 02:25 PM WAT, the Security Operations Center (SOC) identified a potential security incident involving DNS tunneling within a virtual lab environment. The tunneling was done by the Iodine tool, with the client located at **192.168.1.30 (Ubuntu VM**) and the server at **192.168.1.59 (Kali VM).** The activity was detected using Suricata's Intrusion Detection System (IDS) with rules **1:2029995:2** and **1:2029994:1**, and custom rules **1:000003:1** and **1:000004:1**, indicating suspicious DNS traffic.

Subsequent analysis with **Wireshark** and **Splunk** confirmed the presence of malicious tunneling, which needed an immediate response to mitigate the threat. This report details the incident, analysis, response, and lessons learned, serving as a case study for enhancing network security monitoring.

2. Incident Details

- Date and Time of Detection: May 18, 2025, 02:25 PM WAT
- Affected Systems:
    - Client: Ubuntu VM (192.168.1.31)
    - Server: Kali VM (192.168.1.59)
    - Network: Internal lab network (192.168.1.0/24),
    - Default gateway 192.168.1.1 (home router)

- Tools Used:
    - Iodine: DNS Tunneling Tool
    - Wireshark: Packet Analyzer
    - Tcpdump: Packet Analyzer
    - Suricata: Intrusion Detection System.
    - Splunk: Security Information and Events Management(SIEM)

- Detection Method: Suricata Rules
    - Custom.Rules
        - Sid:1000003
        - Sid:1000005
    - Suricata.Rules:
        - Sid:2029994
        - Sid:2029995

- Impact: No real-world data exfiltration occurred because this project was done in a controlled lab environment. However, this technique poses a significant risk for data leakage or command-and-control (C2) in large corporate networks.

3. Background

DNS Tunneling is a technique where attackers encode data within DNS queries to bypass firewalls and exfiltrate information or establish C2 channels. Iodine, an open-source tool, does this by using NULL records and long subdomains to tunnel IP traffic (e.g., SSH, ICMP) over DNS. This incident was simulated in a virtual lab to test my detection skills, mimicking a real-world attack scenario where an insider or compromised host might initiate such activity.

4. Simulation Setup with Iodine

To simulate the DNS tunneling incident, Iodine was deliberately configured on the virtual lab environment. The following steps and commands were executed to establish and test the tunnel:

Server Setup on Kali VM (192.168.1.59):

- Installed Iodine:

```
BASH
sudo apt update
sudo apt install iodine
```

- Started the Iodine server:

```
BASH
sudo iodined -f -c -P secret123 10.0.0.1 tunnel.local
```

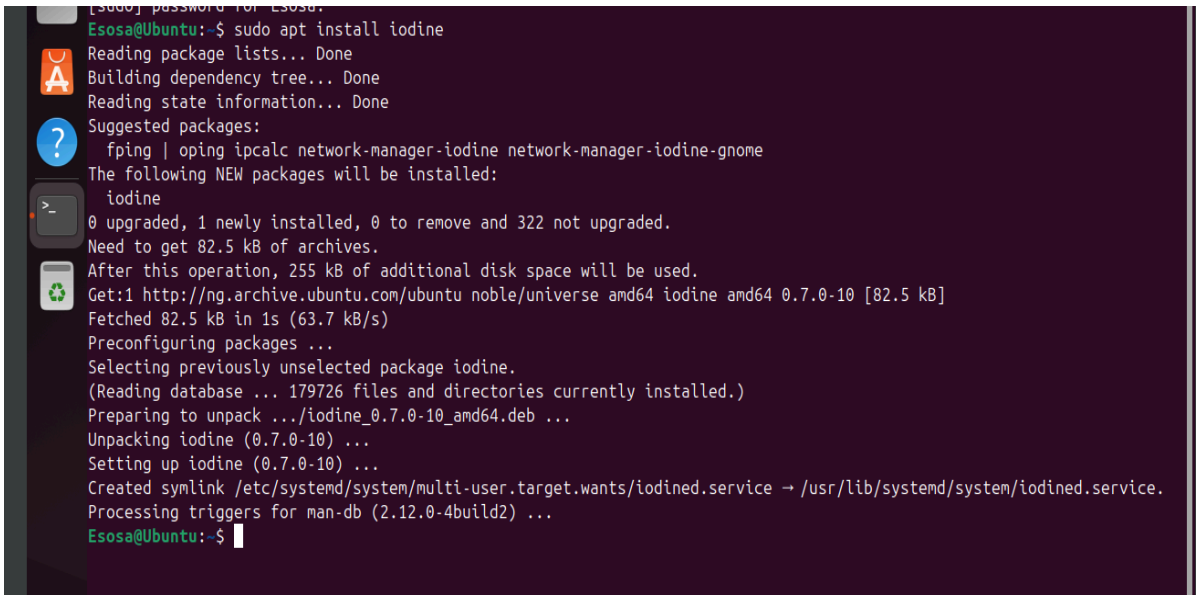
- -f: Runs in foreground for monitoring.
- -c: Ignores case in DNS queries.
- -P secret123: Sets the shared password.
- 10.0.0.1: IP for the server.
- Tunnel.local: The fake domain name.

Running iodine

Client setup in Ubuntu VM(192.168.1.31)

- Installed Iodine:

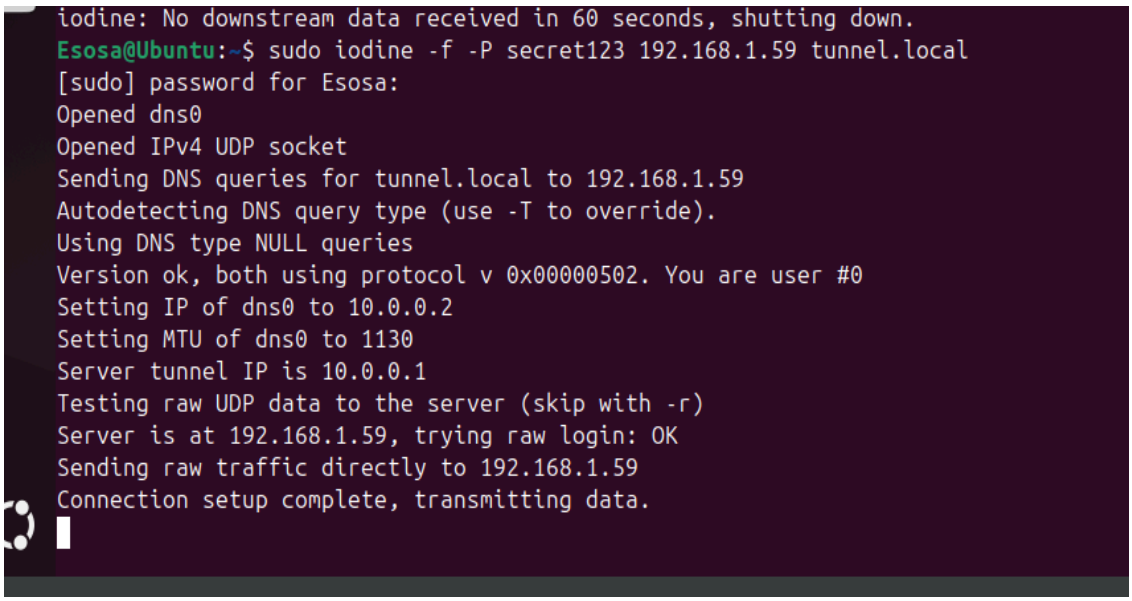
BASH
sudo apt update sudo apt install iodine



Iodine Installation

- Connected the Iodine client to the server:

```
BASH
sudo iodine -f -P secret123 192.168.1.59 tunnel.local
```

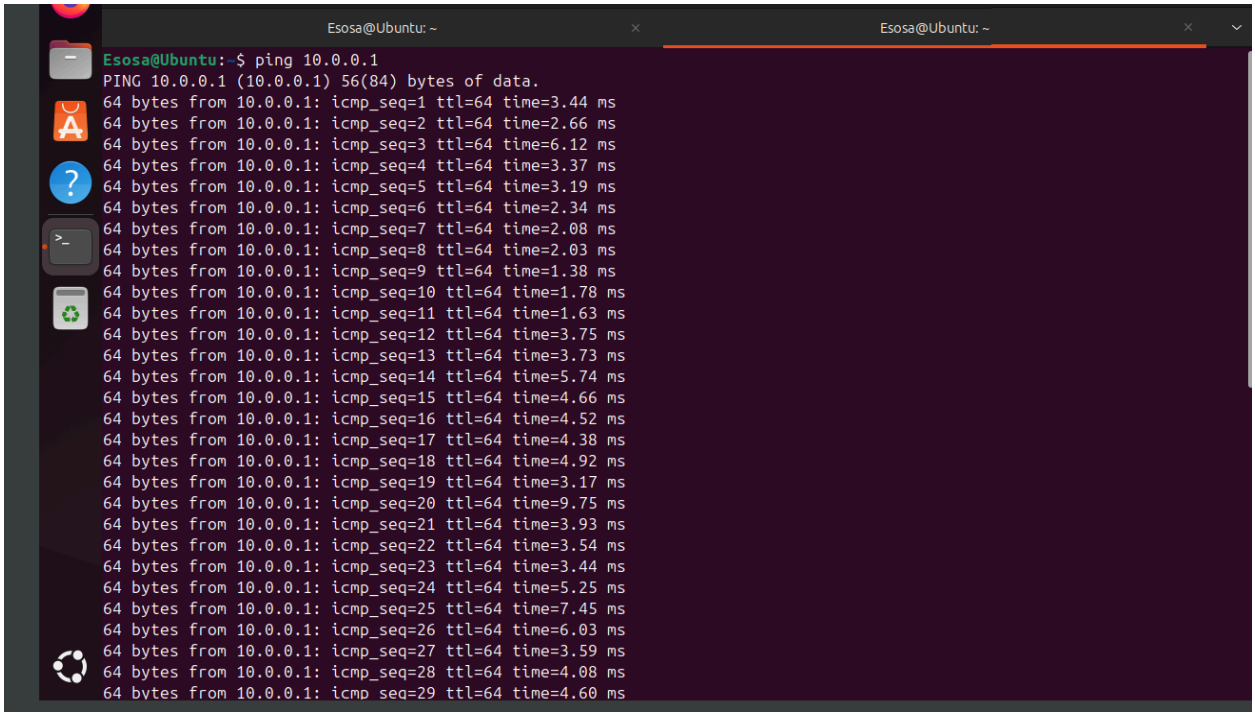


Running Iodine Client

By doing this, the client automatically received IP: 10.0.0.2.

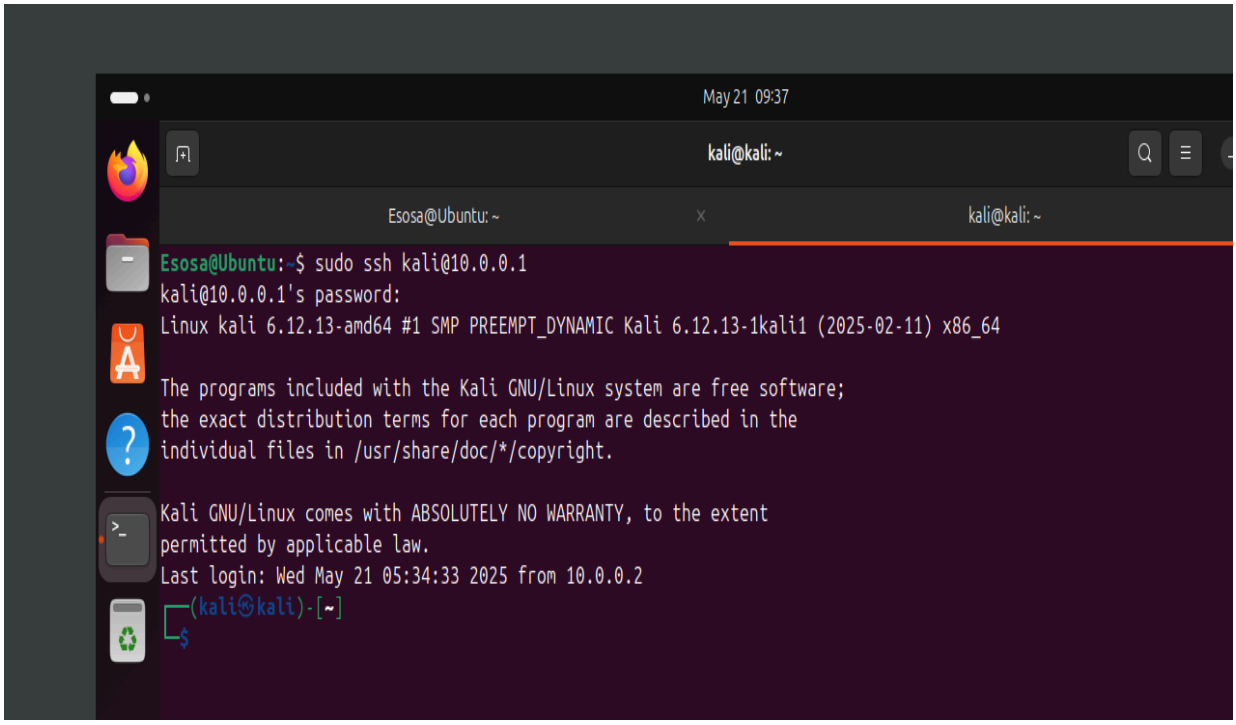
- Traffic was generated with ping and SSH.

```
BASH
ping 10.0.0.1
```



Generating ICMP traffic

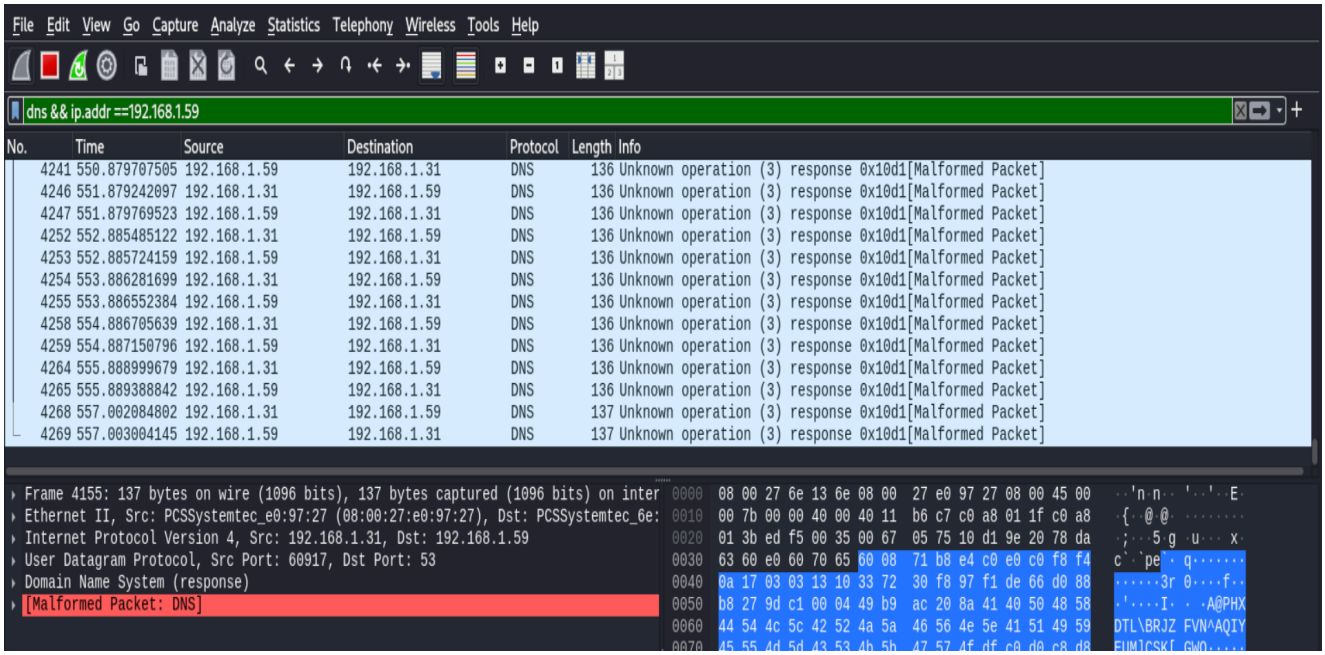
BASH
`sudo ssh kali@10.0.0.1`



Generating SSH Traffic

- Pinging and SSH connections produced sufficient DNS query traffic to trigger the detection mechanism(Suricata).

With this setup, I was able to successfully simulate a DNS Tunneling attack, where ICMP and SSH traffic were encoded in DNS queries, generating malformed packets.



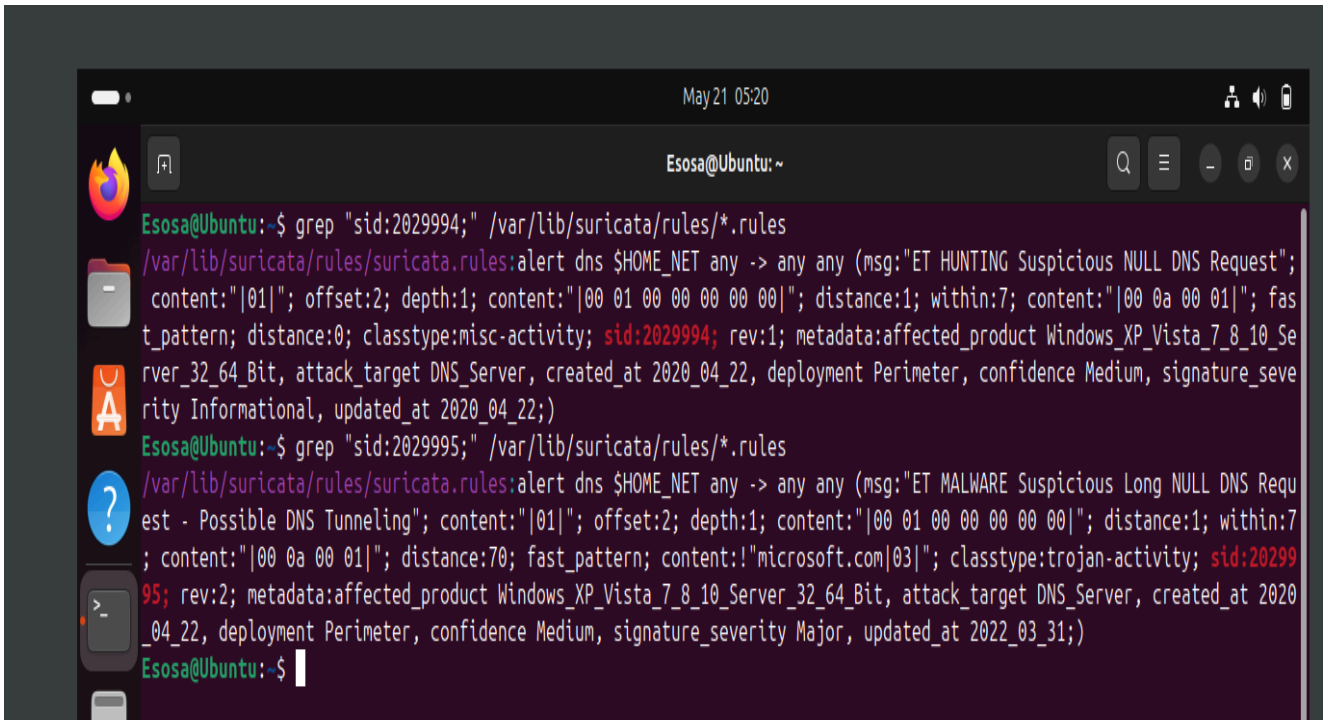
Malformed Packets in Wireshark

5. Investigation and Analysis

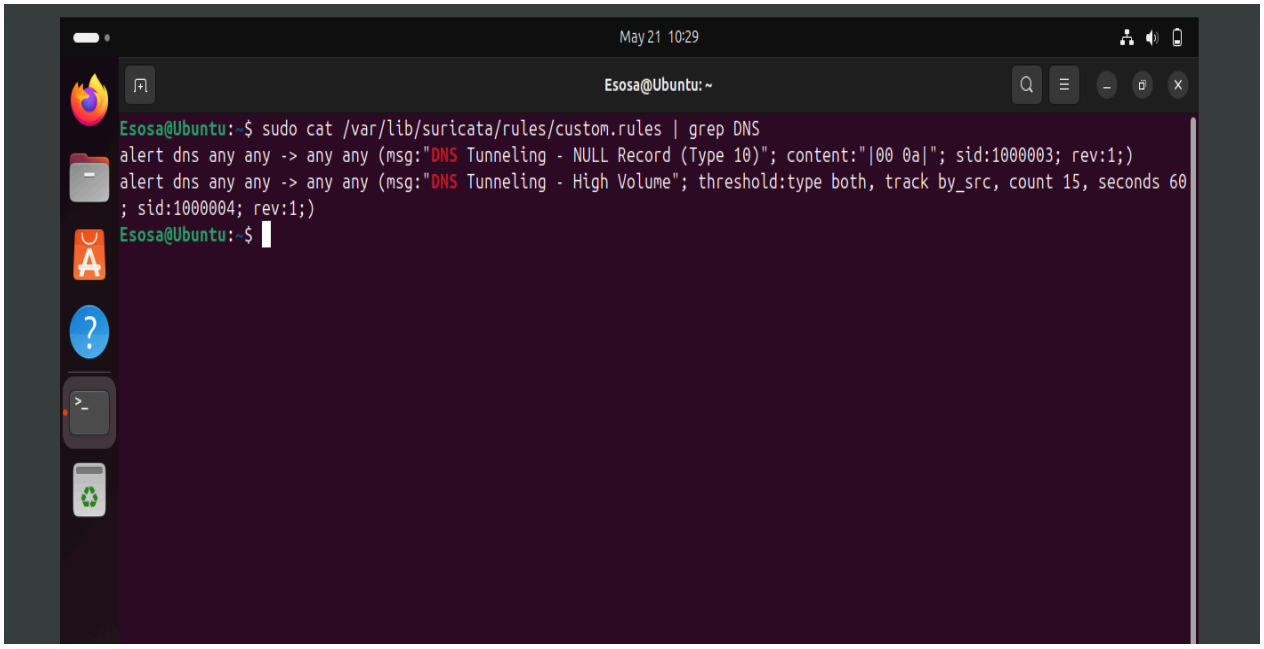
5.1 Initial Detection:

The incident was detected by Suricata on the Ubuntu VM (192.168.1.31), which monitors network traffic on interface enp0s3. The IDS triggered alerts based on the following rules:

- Rule 1:2029994:1: Detects Suspicious NULL DNS requests (dns.qry.type == 10).
- Rule 1:2029995:2: Detects Suspicious **Long** NULL DNS query names (e.g., exceeding 30 characters), a common Iodine signature.
- Rule 1: 1000003:1: Detects DNS NULL Records
- Rule 1: 1000005:1: Detects DNS Tunneling, High Volume.

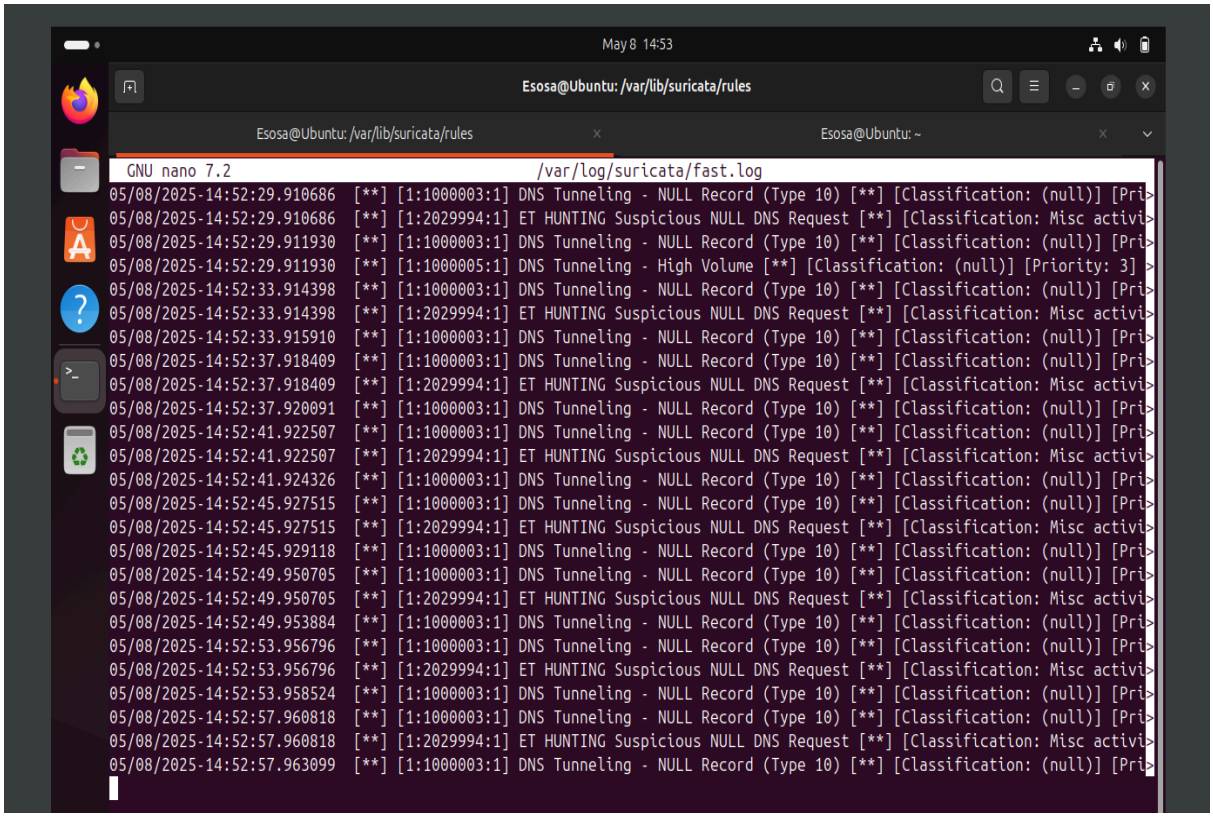


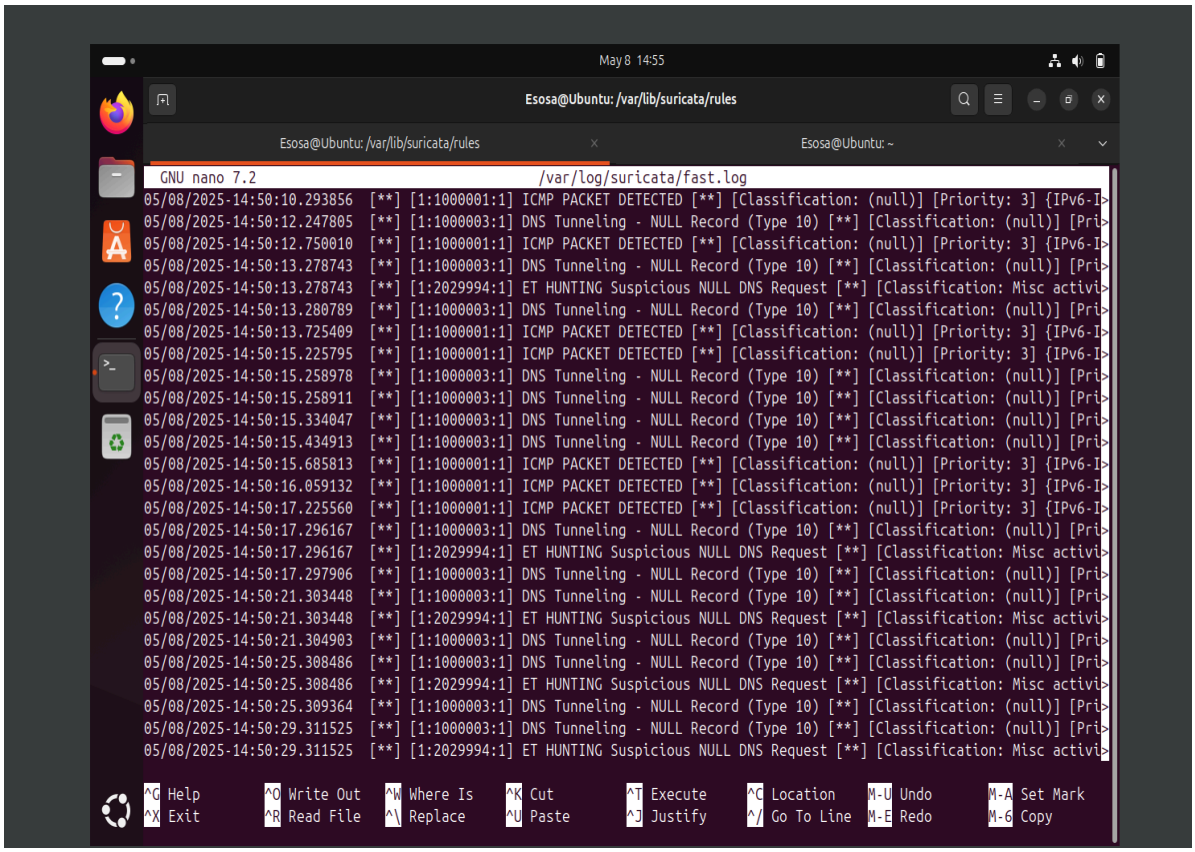
Default DNS SURICATA Rules.

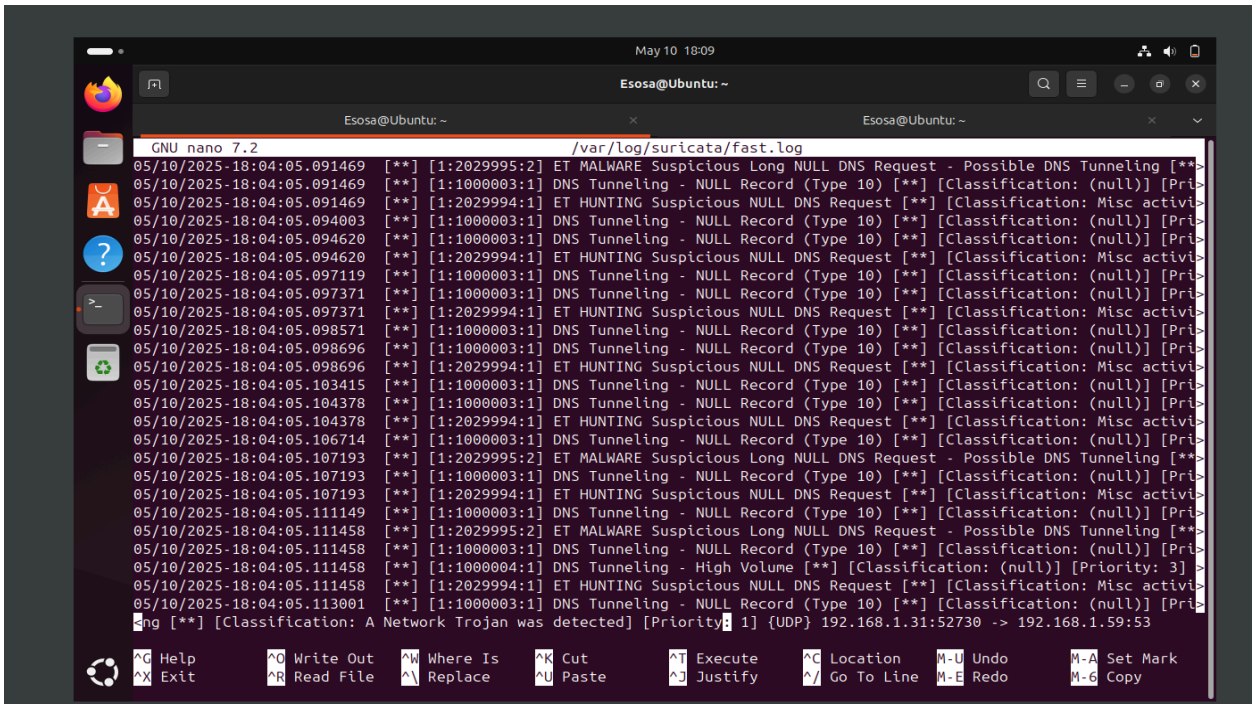


Custom SURICATA Rules.

Log samples from /var/log/suricata/fast.log:




May 8 14:55
Esosa@Ubuntu: /var/lib/suricata/rules
Esosa@Ubuntu: /var/lib/suricata/rules
Esosa@Ubuntu: ~
GNU nano 7.2 /var/log/suricata/fast.log
05/08/2025-14:50:10.293856 [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I
05/08/2025-14:50:12.247805 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:12.750010 [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I
05/08/2025-14:50:13.278743 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:13.278743 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi
05/08/2025-14:50:13.280789 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:13.725409 [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I
05/08/2025-14:50:15.225795 [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I
05/08/2025-14:50:15.258978 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:15.258911 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:15.334047 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:15.434913 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:15.685813 [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I
05/08/2025-14:50:16.059132 [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I
05/08/2025-14:50:17.225560 [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] {IPv6-I
05/08/2025-14:50:17.296167 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:17.296167 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi
05/08/2025-14:50:17.297906 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:21.303448 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:21.303448 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi
05/08/2025-14:50:21.304903 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:25.308486 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:25.308486 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi
05/08/2025-14:50:25.309364 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:29.311525 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/08/2025-14:50:29.311525 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy


May 10 18:09
Esosa@Ubuntu: ~
Esosa@Ubuntu: ~
Esosa@Ubuntu: ~
GNU nano 7.2 /var/log/suricata/fast.log
05/10/2025-18:04:05.091469 [**] [1:2029995:2] ET MALWARE Suspicious Long NULL DNS Request - Possible DNS Tunneling [**
05/10/2025-18:04:05.091469 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.091469 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi
05/10/2025-18:04:05.094003 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.094620 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.094620 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi
05/10/2025-18:04:05.097119 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.097371 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.097371 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi
05/10/2025-18:04:05.098571 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.098696 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.098696 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi
05/10/2025-18:04:05.103415 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.104378 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.104378 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi
05/10/2025-18:04:05.106714 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.107193 [**] [1:2029995:2] ET MALWARE Suspicious Long NULL DNS Request - Possible DNS Tunneling [**
05/10/2025-18:04:05.107193 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.107193 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi
05/10/2025-18:04:05.111149 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.111458 [**] [1:2029995:2] ET MALWARE Suspicious Long NULL DNS Request - Possible DNS Tunneling [**
05/10/2025-18:04:05.111458 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
05/10/2025-18:04:05.111458 [**] [1:1000004:1] DNS Tunneling - High Volume [**] [Classification: (null)] [Priority: 3]
05/10/2025-18:04:05.111458 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi
05/10/2025-18:04:05.113001 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Pri
ng [**] [Classification: A Network Trojan was detected] [Priority: 1] {UDP} 192.168.1.31:52730 -> 192.168.1.59:53
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy

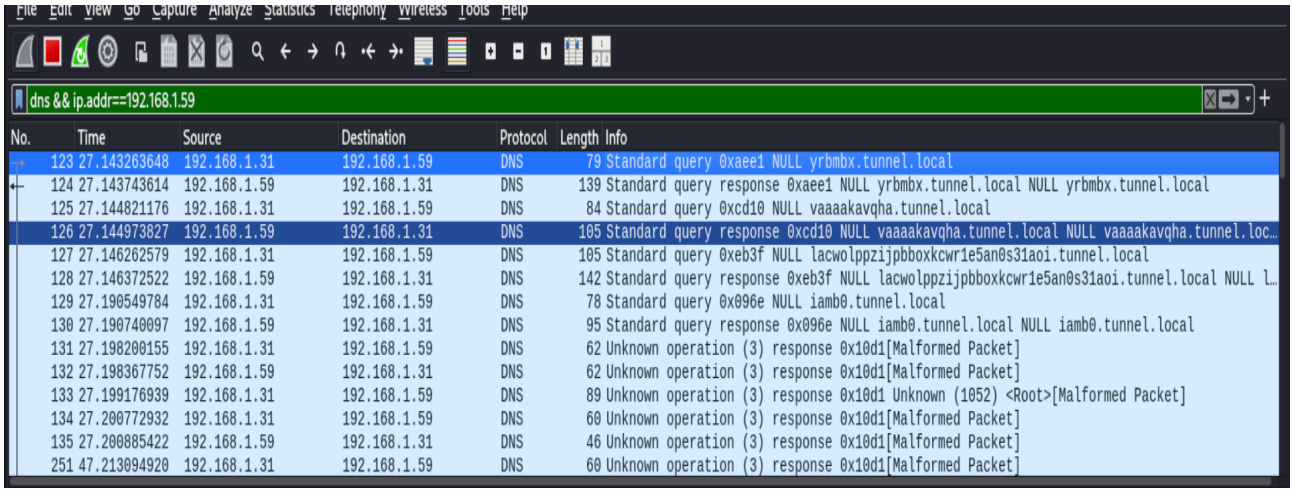
5.2 Packet Analysis with Wireshark

Wireshark was used to capture and analyze traffic on eth0 using the capture filter:

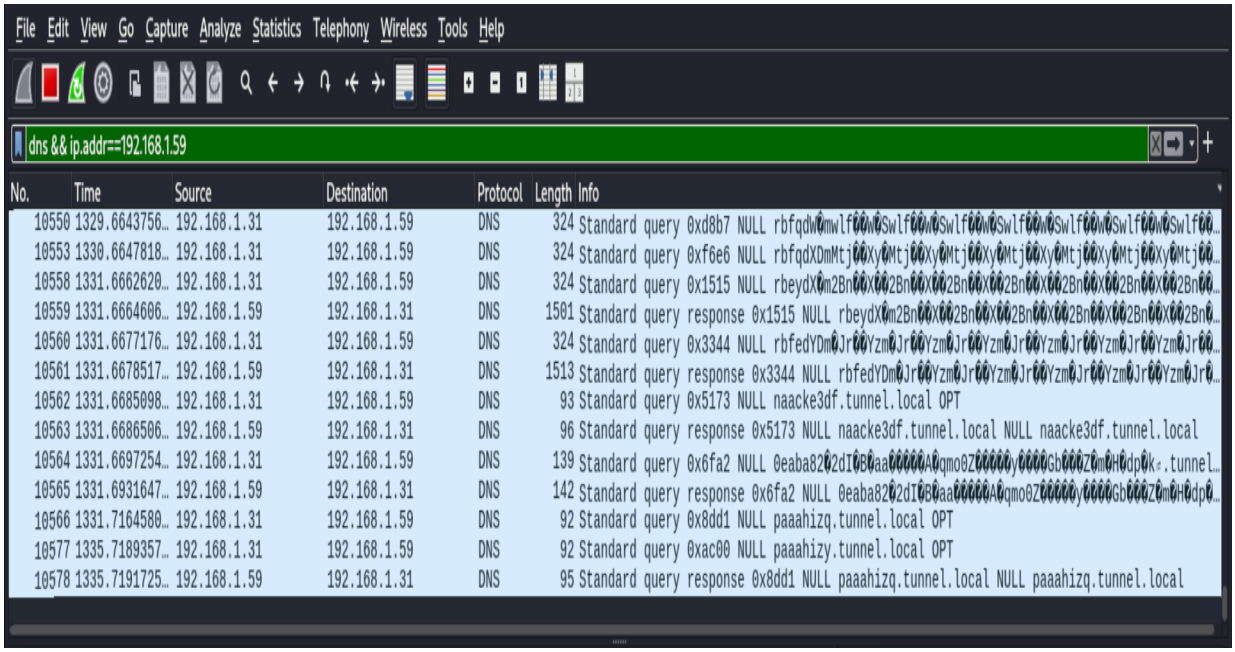
WIREHSARK
dns && Ip.addr==192.168.1.59

Key findings:

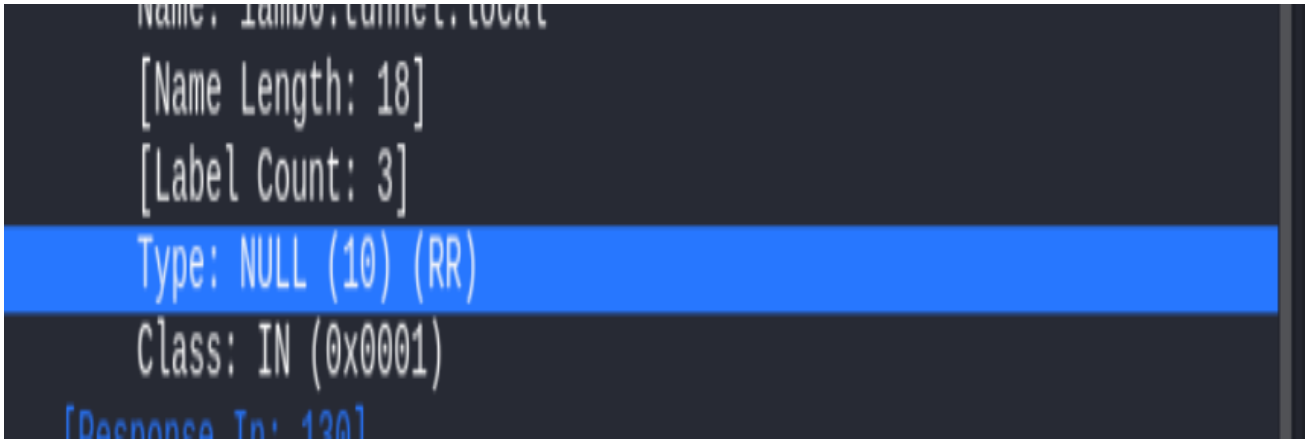
- Malformed Packets: Approximately 50 packets were flagged as **“[Malformed Packet: DNS]”** due to Iodine’s non-standard encoding.
- Traffic Patterns:
    - Source: **192.168.1.31**, Destination: **192.168.1.59**.
    - NULL records (**dns.qry.type == 10**) observed in packet details.
    - Long subdomains (e.g.,xyz123abc.tunnel.local).
    - High query volume: ~60 queries in 60 seconds (Statistics > Conversations > UDP).
    - Capture Saved: iodine_tunneling.pcap preserved for evidence



Malformed DNS traffic



Malformed DNS Traffic



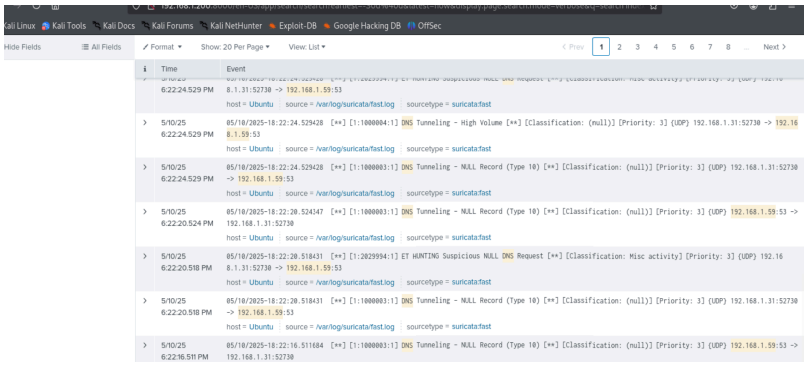
NULL DNS Record: type 10

5.3 SIEM Correlation with Splunk:

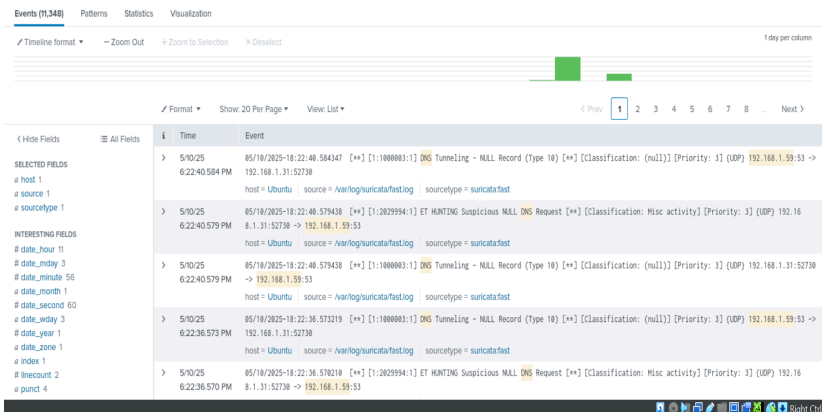
Suricata logs were forwarded to Splunk (192.168.1.200) via the Universal Forwarder.

SPL
index=’suricata’ sourcetype=’suricata:fast’

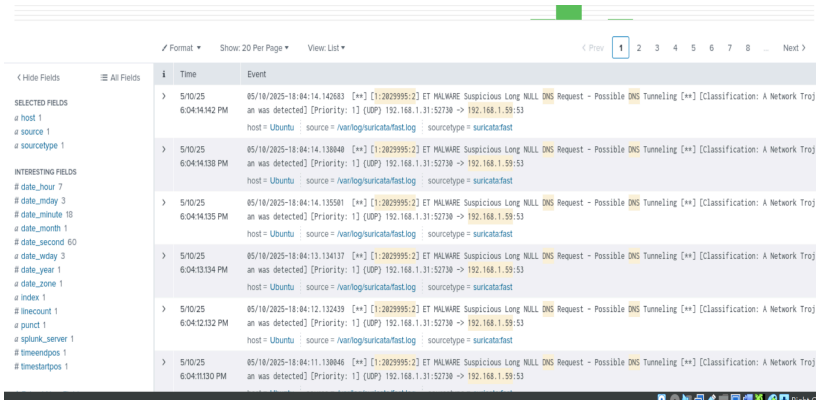
Results confirmed SIDs 2029994, 2029995, 1000003,1000005 alerts, with source IP 192.168.1.31 generating suspicious traffic.



Splunk



Splunk



Splunk

6. Response Actions

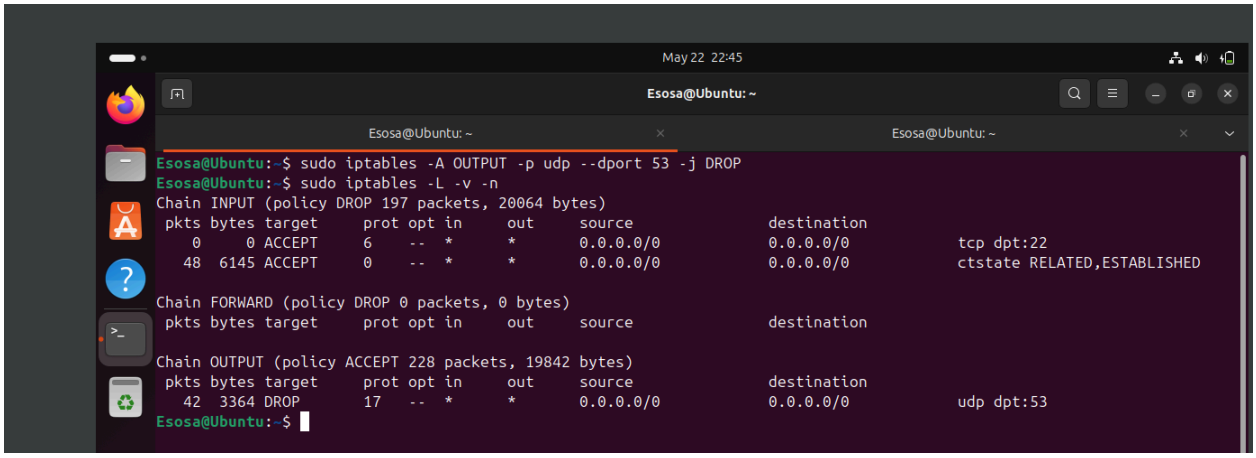
6.1. Containment

- To stop the DNS tunneling activity immediately, outbound DNS traffic from the Ubuntu VM(192.168.1.31) was blocked using iptables. A rule was added to drop all outbound traffic on port 53(DNS).

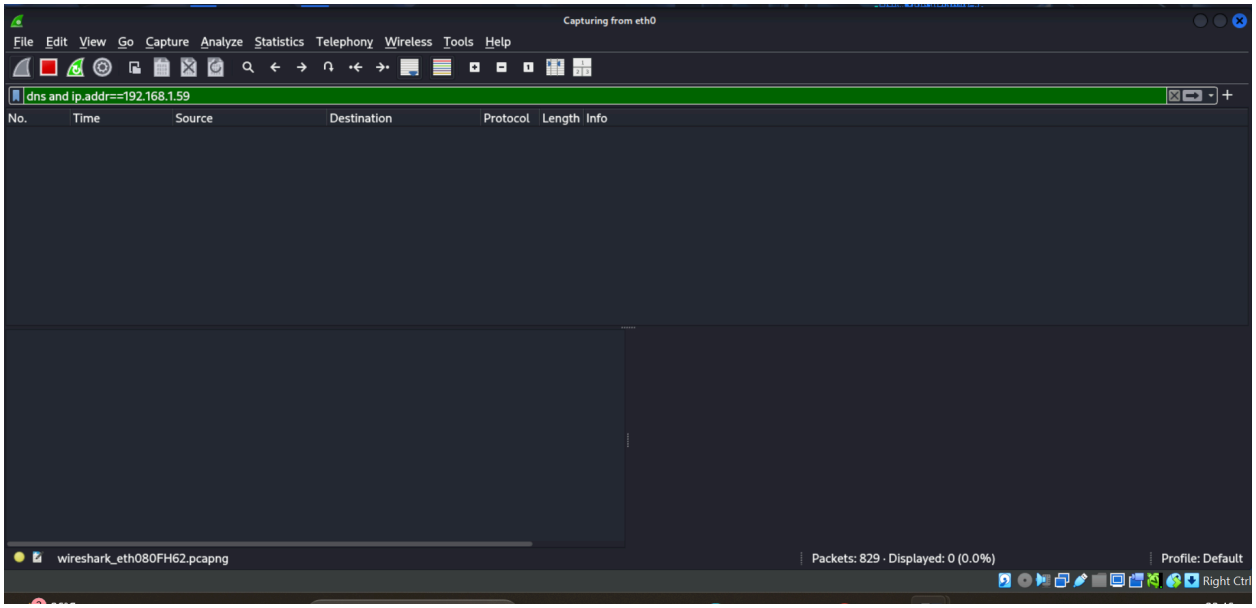
- This action prevented the client from resolving domain names temporarily, halting Iodine's functionality and containing the threat within the lab environment.

- Command used:

BASH
`sudo iptables -A OUTPUT -p udp - -dport 53 -j DROP`



Iptables



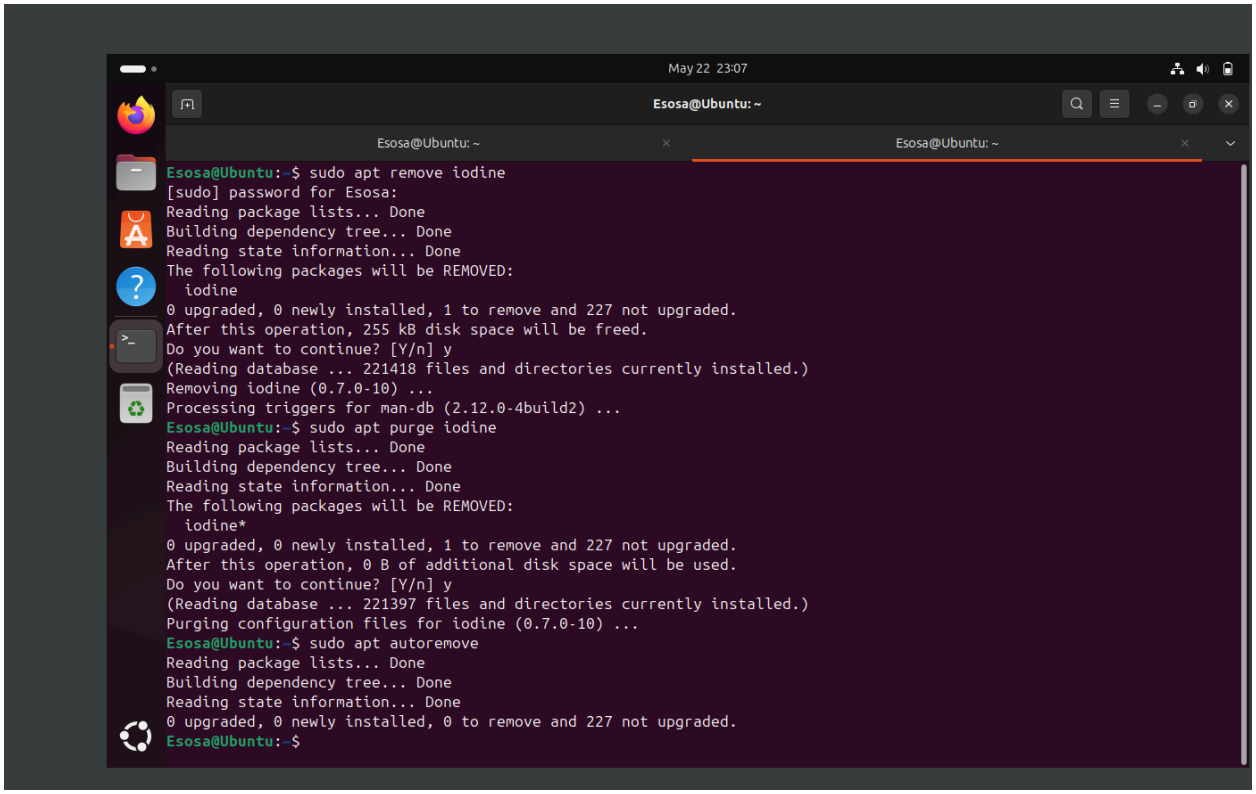
No DNS Traffic

6.2 Eradication and Recovery

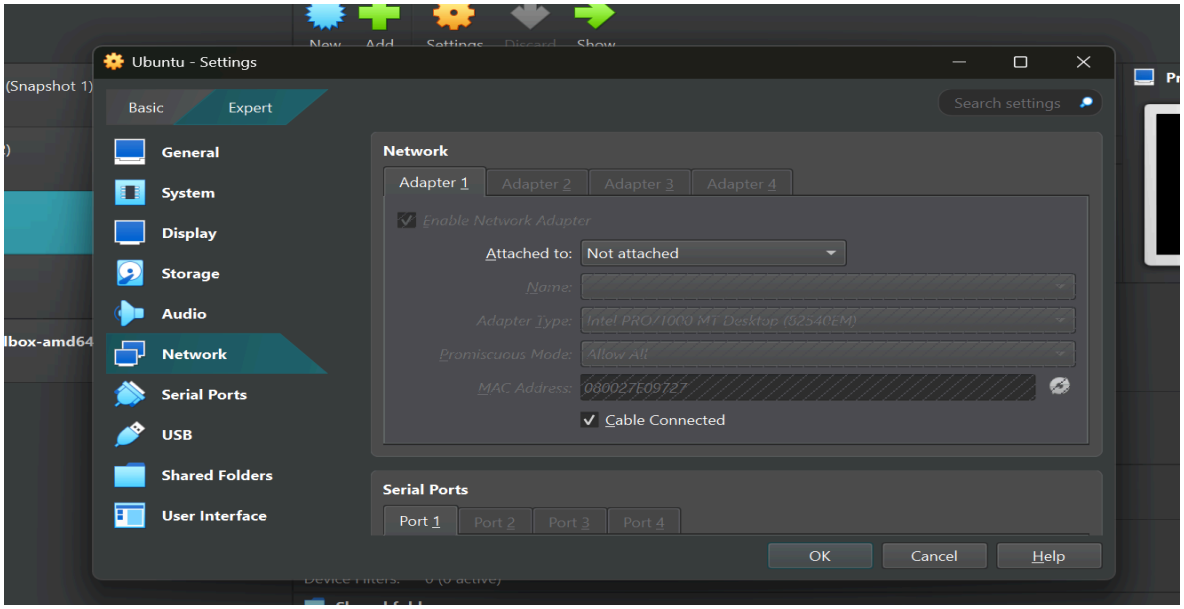
- The Ubuntu VM was isolated from the internal lab network by disconnecting it completely. This was done by selecting the "**Not Attached**" option in VirtualBox. This meant no network connectivity, no communication with the host device and complete isolation ensuring the client could no longer communicate with the Iodine server via port 53 or any other system.

- The iodine client was completely uninstalled to eliminate the DNS Tunneling attack.

BASH
sudo apt remove iodine sudo apt purge iodine sudo apt autoremove



Uninstalling Iodine

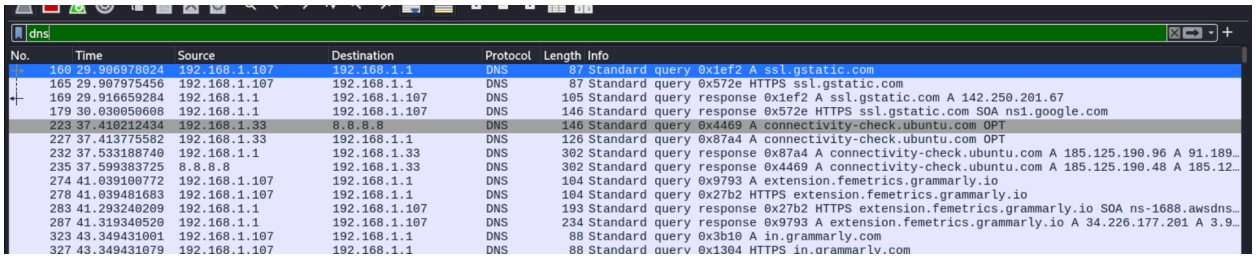


“Not Attached” in VirtualBox

- Once iodine was uninstalled, system integrity was checked to ensure no malicious configuration associated with iodine was present.

- The firewall rule was removed, and Wireshark verified that normal traffic resumed without DNS tunneling being detected.

- After confirming no further DNS tunnels were present, the system was restored to normal operations and monitored.



6.3 Communication:

- Incident reported to the SOC team lead (simulated).

6.4 Root Cause Analysis:

- The incident originated from a simulated attack using Iodine, which produces malformed DNS packets. The root cause was the installation of an Iodine client on the Ubuntu VM, which connected to the Iodine server running on Kali VM, generating NULL records and long DNS queries to evade detection.

7. Lessons Learned

- Using Suricata for detection, Wireshark for packet analysis, and Splunk for real-time monitoring was effective in tracking the network threat and gaining insights into both the malicious DNS traffic and system behavior across the environment.

8. Recommendations

- Conduct employee training on what DNS Tunneling attack is and how to detect it.
- Deploy a firewall (pfSense) for DNS filtering.

9. Conclusion

In this project, I was able to simulate a DNS Tunneling attack using Iodine, detected the malformed DNS traffic using Suricata, an IDS, carried out packet analysis using wireshark, visualized and managed Logs using Splunk.

While no real data was compromised, this project highlights how attackers can abuse DNS for command-and-control or data exfiltration, and why organizations must implement layered defenses. Going forward, DNS filtering and team training will be essential to effectively counter DNS-based threats in production environments.