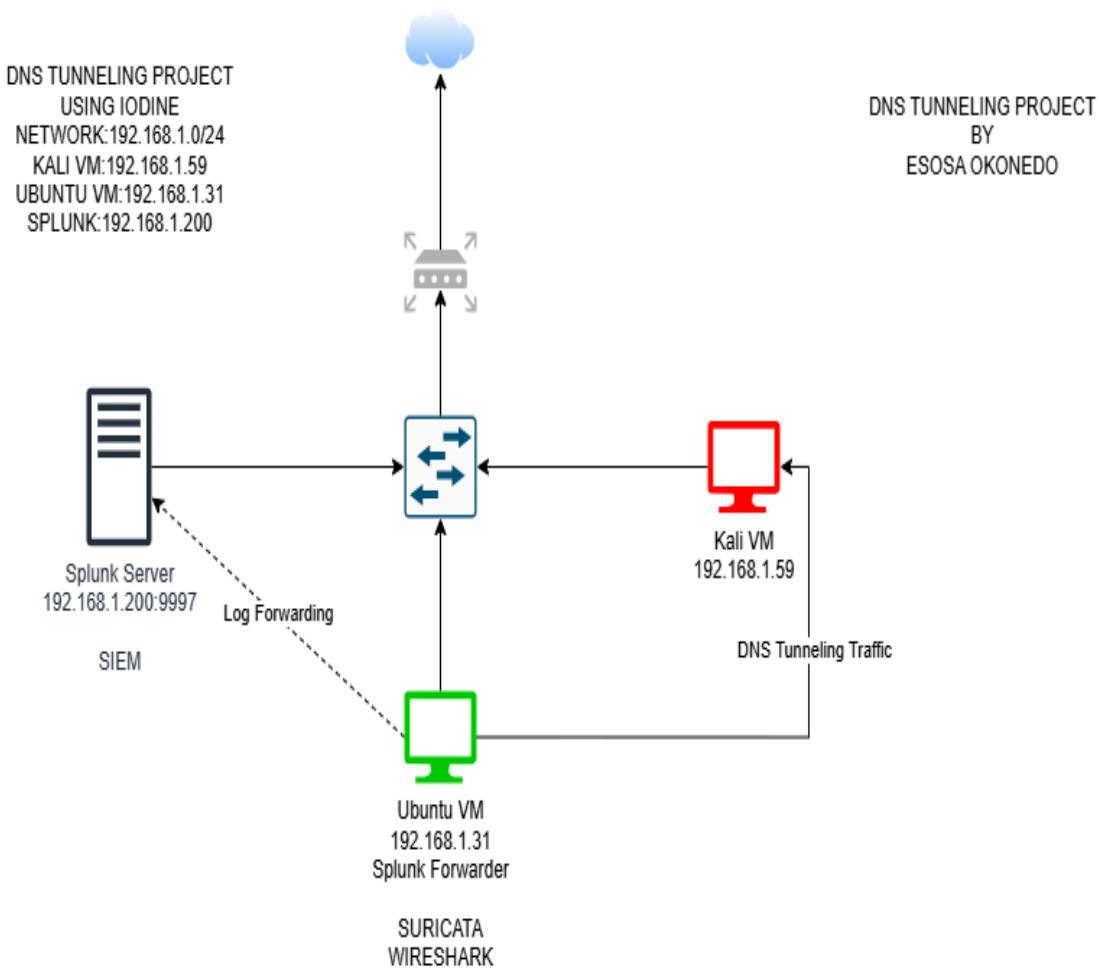


Incident Report: Detection of DNS Tunneling Attack

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.

```
(kali㉿kali)-[~]
$ sudo iodined -f -c -P secret123 10.0.0.1 tunnel.local
Opened dns0
Setting IP of dns0 to 10.0.0.1
Setting MTU of dns0 to 1130
Opened IPv4 UDP socket
Listening to dns for domain tunnel.local
```

Running iodine

Client setup in Ubuntu VM(192.168.1.31)

- Installed Iodine:

BASH

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

```
[sudo] password for Esosa:
Esosa@Ubuntu:~$ sudo apt install iodine
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  fping | oping ipcalc network-manager-iodine network-manager-iodine-gnome
The following NEW packages will be installed:
  iodine
0 upgraded, 1 newly installed, 0 to remove and 322 not upgraded.
Need to get 82.5 kB of additional disk space.
After this operation, 255 kB of additional disk space will be used.
Get:1 http://ng.archive.ubuntu.com/ubuntu noble/universe amd64 iodine amd64 0.7.0-10 [82.5 kB]
Fetched 82.5 kB in 1s (63.7 kB/s)
Preconfiguring packages ...
Selecting previously unselected package iodine.
(Reading database ... 179726 files and directories currently installed.)
Preparing to unpack .../iodine_0.7.0-10_amd64.deb ...
Unpacking iodine (0.7.0-10) ...
Setting up iodine (0.7.0-10) ...
Created symlink /etc/systemd/system/multi-user.target.wants/iodined.service → /usr/lib/systemd/system/iodined.service.
Processing triggers for man-db (2.12.0-4build2) ...
Esosa@Ubuntu:~$
```

Iodine Installation

- Connected the Iodine client to the server:

BASH

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

```
iodine: No downstream data received in 60 seconds, shutting down.  
Esosa@Ubuntu:~$ sudo iodine -f -P secret123 192.168.1.59 tunnel.local  
[sudo] password for Esosa:  
Opened dns0  
Opened IPv4 UDP socket  
Sending DNS queries for tunnel.local to 192.168.1.59  
Autodetecting DNS query type (use -T to override).  
Using DNS type NULL queries  
Version ok, both using protocol v 0x00000502. You are user #0  
Setting IP of dns0 to 10.0.0.2  
Setting MTU of dns0 to 1130  
Server tunnel IP is 10.0.0.1  
Testing raw UDP data to the server (skip with -r)  
Server is at 192.168.1.59, trying raw login: OK  
Sending raw traffic directly to 192.168.1.59  
Connection setup complete, transmitting data.
```

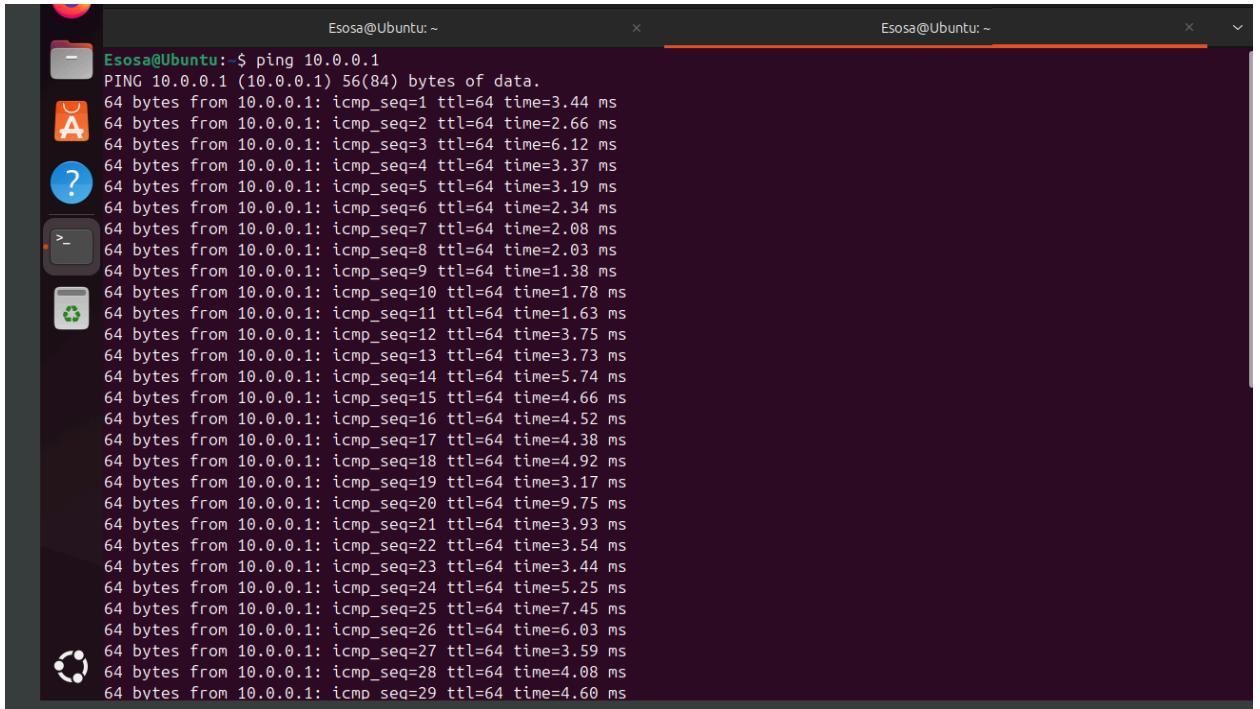
Running Iodine Client

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
```



Esosa@Ubuntu:~\$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=3.44 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=2.66 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=6.12 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=3.37 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=64 time=3.19 ms
64 bytes from 10.0.0.1: icmp_seq=6 ttl=64 time=2.34 ms
64 bytes from 10.0.0.1: icmp_seq=7 ttl=64 time=2.08 ms
64 bytes from 10.0.0.1: icmp_seq=8 ttl=64 time=2.03 ms
64 bytes from 10.0.0.1: icmp_seq=9 ttl=64 time=1.38 ms
64 bytes from 10.0.0.1: icmp_seq=10 ttl=64 time=1.78 ms
64 bytes from 10.0.0.1: icmp_seq=11 ttl=64 time=1.63 ms
64 bytes from 10.0.0.1: icmp_seq=12 ttl=64 time=3.75 ms
64 bytes from 10.0.0.1: icmp_seq=13 ttl=64 time=3.73 ms
64 bytes from 10.0.0.1: icmp_seq=14 ttl=64 time=5.74 ms
64 bytes from 10.0.0.1: icmp_seq=15 ttl=64 time=4.66 ms
64 bytes from 10.0.0.1: icmp_seq=16 ttl=64 time=4.52 ms
64 bytes from 10.0.0.1: icmp_seq=17 ttl=64 time=4.38 ms
64 bytes from 10.0.0.1: icmp_seq=18 ttl=64 time=4.92 ms
64 bytes from 10.0.0.1: icmp_seq=19 ttl=64 time=3.17 ms
64 bytes from 10.0.0.1: icmp_seq=20 ttl=64 time=9.75 ms
64 bytes from 10.0.0.1: icmp_seq=21 ttl=64 time=3.93 ms
64 bytes from 10.0.0.1: icmp_seq=22 ttl=64 time=3.54 ms
64 bytes from 10.0.0.1: icmp_seq=23 ttl=64 time=3.44 ms
64 bytes from 10.0.0.1: icmp_seq=24 ttl=64 time=5.25 ms
64 bytes from 10.0.0.1: icmp_seq=25 ttl=64 time=7.45 ms
64 bytes from 10.0.0.1: icmp_seq=26 ttl=64 time=6.03 ms
64 bytes from 10.0.0.1: icmp_seq=27 ttl=64 time=3.59 ms
64 bytes from 10.0.0.1: icmp_seq=28 ttl=64 time=4.08 ms
64 bytes from 10.0.0.1: icmp_seq=29 ttl=64 time=4.60 ms

Generating ICMP traffic

BASH
sudo ssh kali@10.0.0.1

The screenshot shows a terminal window with two tabs. The left tab, titled 'Esosa@Ubuntu:~', displays the command 'sudo ssh kali@10.0.0.1' followed by the password prompt 'kali@10.0.0.1's password: and the system information 'Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64'. The right tab, titled 'kali@kali:~', shows the message 'The programs included with the Kali GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.' Below this, it states 'Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.' and 'Last login: Wed May 21 05:34:33 2025 from 10.0.0.2'. The terminal window has a dark background with light-colored text and icons for file, terminal, and help.

```
May 21 09:37
kali@kali:~ Q E
kali@kali:~ x
Esosa@Ubuntu:~ sudo ssh kali@10.0.0.1
kali@10.0.0.1's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May 21 05:34:33 2025 from 10.0.0.2
(kali㉿kali)-[~]
```

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.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns && p.addr == 192.168.1.59

No.	Time	Source	Destination	Protocol	Length	Info
4241	550.879707505	192.168.1.59	192.168.1.31	DNS	136	Unknown operation (3) response 0x10d1[Malformed Packet]
4246	551.879242097	192.168.1.31	192.168.1.59	DNS	136	Unknown operation (3) response 0x10d1[Malformed Packet]
4247	551.879769523	192.168.1.59	192.168.1.31	DNS	136	Unknown operation (3) response 0x10d1[Malformed Packet]
4252	552.885485122	192.168.1.31	192.168.1.59	DNS	136	Unknown operation (3) response 0x10d1[Malformed Packet]
4253	552.885724159	192.168.1.59	192.168.1.31	DNS	136	Unknown operation (3) response 0x10d1[Malformed Packet]
4254	553.886281699	192.168.1.31	192.168.1.59	DNS	136	Unknown operation (3) response 0x10d1[Malformed Packet]
4255	553.886552384	192.168.1.59	192.168.1.31	DNS	136	Unknown operation (3) response 0x10d1[Malformed Packet]
4258	554.886705639	192.168.1.31	192.168.1.59	DNS	136	Unknown operation (3) response 0x10d1[Malformed Packet]
4259	554.887150796	192.168.1.59	192.168.1.31	DNS	136	Unknown operation (3) response 0x10d1[Malformed Packet]
4264	555.888999679	192.168.1.31	192.168.1.59	DNS	136	Unknown operation (3) response 0x10d1[Malformed Packet]
4265	555.889388842	192.168.1.59	192.168.1.31	DNS	136	Unknown operation (3) response 0x10d1[Malformed Packet]
4268	557.002084802	192.168.1.31	192.168.1.59	DNS	137	Unknown operation (3) response 0x10d1[Malformed Packet]
4269	557.003004145	192.168.1.59	192.168.1.31	DNS	137	Unknown operation (3) response 0x10d1[Malformed Packet]

```

> Frame 4155: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits) on interface
> Ethernet II, Src: PCSSystemtec_e0:97:27 (08:00:27:e0:97:27), Dst: PCSSystemtec_6e (00:0c:29:6e:00:00)
> Internet Protocol Version 4, Src: 192.168.1.31, Dst: 192.168.1.59
> User Datagram Protocol, Src Port: 60917, Dst Port: 53
> [Malformed Packet: DNS]

```

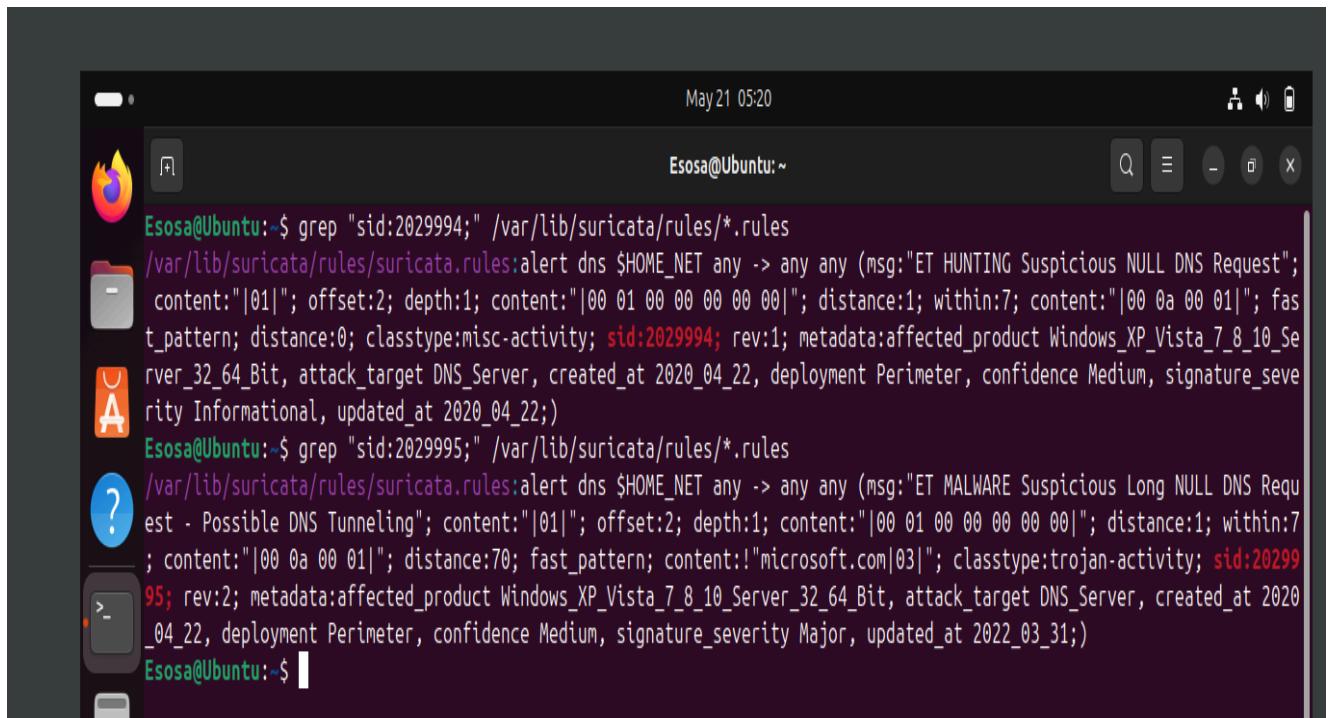
Malformed Packets in Wireshark

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 (dnsqry.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.

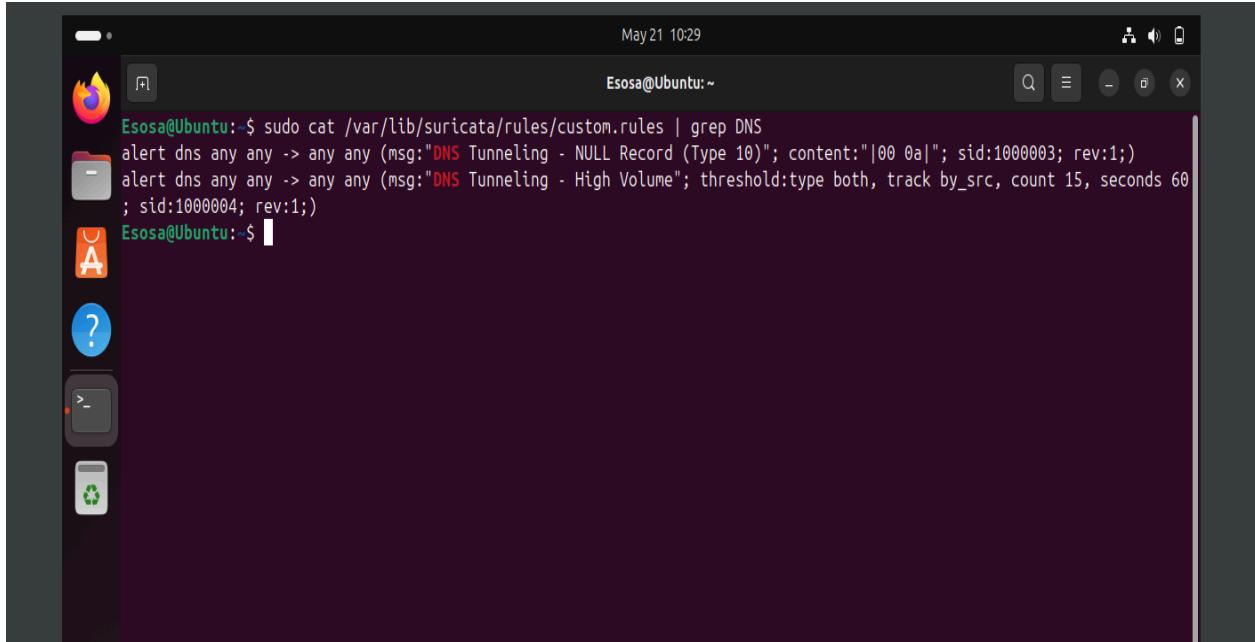


The screenshot shows a terminal window on an Ubuntu desktop environment. The terminal title is "Esosa@Ubuntu:~". The window contains two command outputs:

```
Esosa@Ubuntu: $ grep "sid:2029994;" /var/lib/suricata/rules/*.rules
/var/lib/suricata/rules/suricata.rules:alert dns $HOME_NET any -> any any (msg:"ET HUNTING Suspicious NULL DNS Request";
content:"|01|"; offset:2; depth:1; content:"|00 01 00 00 00 00 00|"; distance:1; within:7; content:"|00 0a 00 01|"; fast_pattern;
distance:0; classtype:misc-activity; sid:2029994; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target DNS_Server, created_at 2020_04_22, deployment_Perimeter, confidence Medium, signature_severity Informational,
updated_at 2020_04_22;)

Esosa@Ubuntu: $ grep "sid:2029995;" /var/lib/suricata/rules/*.rules
/var/lib/suricata/rules/suricata.rules:alert dns $HOME_NET any -> any any (msg:"ET MALWARE Suspicious Long NULL DNS Request - Possible DNS Tunneling";
content:"|01|"; offset:2; depth:1; content:"|00 01 00 00 00 00 00|"; distance:1; within:7; content:"|00 0a 00 01|"; distance:70; fast_pattern;
content:!\"microsoft.com|03|"; classtype:trojan-activity; sid:2029995; rev:2; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit,
attack_target DNS_Server, created_at 2020_04_22, deployment_Perimeter, confidence Medium, signature_severity Major,
updated_at 2022_03_31;)
```

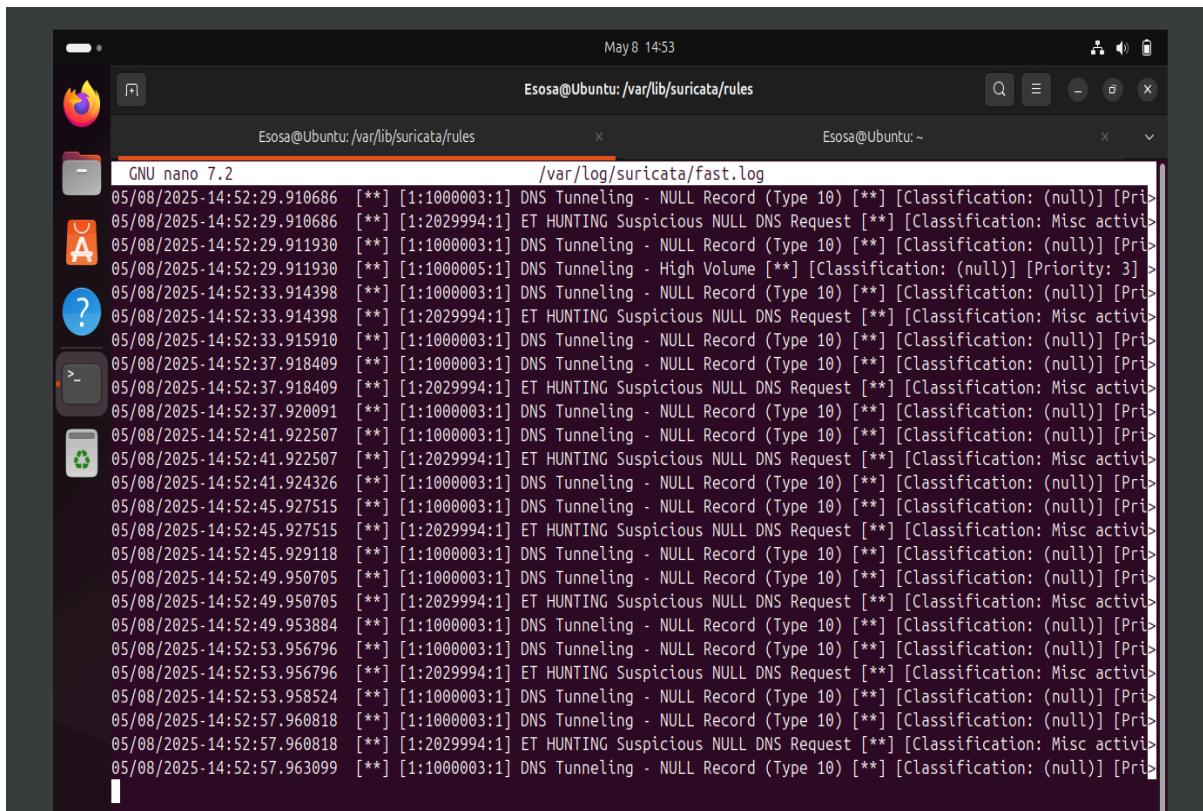
Default DNS SURICATA Rules.



May 21 10:29
Esosa@Ubuntu:~\$ sudo cat /var/lib/suricata/rules/custom.rules | grep DNS
alert dns any any -> any any (msg:"DNS Tunneling - NULL Record (Type 10)"; content:"|00 0a|"; sid:1000003; rev:1;)
alert dns any any -> any any (msg:"DNS Tunneling - High Volume"; threshold:type both, track_by_src, count 15, seconds 60
; sid:1000004; rev:1;)
Esosa@Ubuntu:~\$

Custom SURICATA Rules.

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



May 8 14:53
Esosa@Ubuntu: /var/lib/suricata/rules
Esosa@Ubuntu: ~
GNU nano 7.2
/var/log/suricata/fast.log
05/08/2025-14:52:29.910686 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:29.910686 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activity]
05/08/2025-14:52:29.911930 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:29.911930 [**] [1:1000005:1] DNS Tunneling - High Volume [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:33.914398 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:33.914398 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activity]
05/08/2025-14:52:33.915910 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:37.918409 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:37.918409 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activity]
05/08/2025-14:52:37.920091 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:41.922507 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:41.922507 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activity]
05/08/2025-14:52:41.924326 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:45.927515 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:45.927515 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activity]
05/08/2025-14:52:45.929118 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:49.950705 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:49.950705 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activity]
05/08/2025-14:52:49.953884 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:53.956796 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:53.956796 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activity]
05/08/2025-14:52:53.958524 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:57.960818 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]
05/08/2025-14:52:57.960818 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activity]
05/08/2025-14:52:57.963099 [**] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [**] [Classification: (null)] [Priority: 3]

May 8 14:55

```
GNU nano 7.2                               /var/log/suricata/fast.log
Esosa@Ubuntu:/var/lib/suricata/rules          Esosa@Ubuntu:~
```

```
05/08/2025-14:50:10.293856 [**] [1:1000001:1] ICMP PACKET DETECTED [**] [Classification: (null)] [Priority: 3] [IPv6-I>
05/08/2025-14:50:12.247885 [**] [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>
05/08/2025-14:50:13.725499 [**] [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>
05/08/2025-14:50:21.304963 [**] [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>
```

GNU nano 7.2

Help Write Out Where Is Cut Execute Location Undo Set Mark

Exit Read File Replace Paste Justify Go To Line Redo Copy

May 10 18:09

```
GNU nano 7.2                               /var/log/suricata/fast.log
Esosa@Ubuntu:~          Esosa@Ubuntu:~
```

```
05/10/2025-18:04:05.091469 [**] [1:2029995:2] ET MALWARE Suspicious Long 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>
05/10/2025-18:04:05.111149 [**] [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 [**] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [**] [Classification: Misc activi>
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
```

GNU nano 7.2

Help Write Out Where Is Cut Execute Location Undo Set Mark

Exit Read File Replace Paste Justify Go To Line Redo 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

No.	Time	Source	Destination	Protocol	Length	Info
123	27.143263648	192.168.1.31	192.168.1.59	DNS	79	Standard query 0xaeec1 NULL yrmbmx.tunnel.local
124	27.143743614	192.168.1.59	192.168.1.31	DNS	139	Standard query response 0xaeec1 NULL yrmbmx.tunnel.local NULL yrmbmx.tunnel.local
125	27.144821176	192.168.1.31	192.168.1.59	DNS	84	Standard query 0xcd10 NULL vaaaakavqha.tunnel.local
126	27.144973827	192.168.1.59	192.168.1.31	DNS	105	Standard query response 0xcd10 NULL vaaaakavqha.tunnel.local NULL vaaaakavqha.tunnel.local
127	27.146262579	192.168.1.31	192.168.1.59	DNS	105	Standard query 0xeb3f NULL lacwolppzijpbboxkcwr1e5an0s31ao1.tunnel.local
128	27.146372522	192.168.1.59	192.168.1.31	DNS	142	Standard query response 0xeb3f NULL lacwolppzijpbboxkcwr1e5an0s31ao1.tunnel.local NULL lacwolppzijpbboxkcwr1e5an0s31ao1.tunnel.local
129	27.190549784	192.168.1.31	192.168.1.59	DNS	78	Standard query 0x096e NULL iambo.tunnel.local
130	27.190740097	192.168.1.59	192.168.1.31	DNS	95	Standard query response 0x096e NULL iambo.tunnel.local NULL iambo.tunnel.local
131	27.198200155	192.168.1.31	192.168.1.59	DNS	62	Unknown operation (3) response 0x10d1[Malformed Packet]
132	27.198367752	192.168.1.59	192.168.1.31	DNS	62	Unknown operation (3) response 0x10d1[Malformed Packet]
133	27.199176939	192.168.1.31	192.168.1.59	DNS	89	Unknown operation (3) response 0x10d1 Unknown (1052) <Root>[Malformed Packet]
134	27.200772932	192.168.1.31	192.168.1.59	DNS	60	Unknown operation (3) response 0x10d1[Malformed Packet]
135	27.200885422	192.168.1.59	192.168.1.31	DNS	46	Unknown operation (3) response 0x10d1[Malformed Packet]
251	47.213094920	192.168.1.31	192.168.1.59	DNS	60	Unknown operation (3) response 0x10d1[Malformed Packet]

Malformed DNS traffic

Malformed DNS Traffic

Name: tambo.com.net.local
[Name Length: 18]
[Label Count: 3]
Type: NULL (10) (RR)
Class: IN (0x0001)
[Response Ttl: 120]

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.

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec		
Format Show 20 Per Page View List		
Hide Fields	>All Fields	
	i Time Event	
	6:22:24 529 PM 8.1.31.52738 -> 192.168.1.31:59:53 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
>	5/0/25 05/10/2025-18:22:24.529428 [*] [1:1000003:1] DNS Tunneling - High Volume [*] [Classification: (null)] [Priority: 3] (UDP) 192.168.1.31:52738 -> 192.168.1.31:59:53 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
>	5/0/25 05/10/2025-18:22:24.529428 [*] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [*] [Classification: (null)] [Priority: 3] (UDP) 192.168.1.31:52738 -> 192.168.1.31:59:53 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
>	5/0/25 05/10/2025-18:22:28.534347 [*] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [*] [Classification: (null)] [Priority: 1] (UDP) 192.168.1.31:59:53 -> 192.20:524 PM 8.1.31.52738 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
>	5/0/25 05/10/2025-18:22:28.534347 [*] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [*] [Classification: Misc activity] [Priority: 3] (UDP) 192.168.1.31:52738 -> 192.168.1.31:59:53 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
>	5/0/25 05/10/2025-18:22:28.534347 [*] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [*] [Classification: (null)] [Priority: 3] (UDP) 192.168.1.31:52738 -> 192.20:508 PM 8.1.31.52738 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
>	5/0/25 05/10/2025-18:22:28.534347 [*] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [*] [Classification: (null)] [Priority: 3] (UDP) 192.168.1.31:52738 -> 192.168.1.31:59:53 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
>	5/0/25 05/10/2025-18:22:16.511684 [*] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [*] [Classification: (null)] [Priority: 3] (UDP) 192.168.1.31:59:53 -> 192.16:51 PM 8.1.31.52738 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	

Splunk

Events (1,348) Patterns Statistics Visualization		
Timeline format ~ Zoom Out + Zoom to Selection X Deleted 1 day per column		
Format Show 20 Per Page View List		
Hide Fields	All Fields	
	i Time Event	
SELECTED FIELDS	a.host_1 a.source_1 a.sourcetype_1	
INTERESTING FIELDS	#date_hour #date_mday_3 #date_minute_56 #date_month_1 #date_second_60 #date_wday_3 #date_year_1 #date_zone_1 #index_1 #linecount_2 #punct_4	
	> 5/0/25 05/10/2025-18:22:48.584347 [*] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [*] [Classification: (null)] [Priority: 1] (UDP) 192.168.1.31:59:53 -> 6:22:40:584 PM 8.1.31.52738 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
	> 5/0/25 05/10/2025-18:22:48.579438 [*] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [*] [Classification: Misc activity] [Priority: 3] (UDP) 192.168.1.31:59:53 -> 6:22:40:579 PM 8.1.31.52738 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
	> 5/0/25 05/10/2025-18:22:48.579438 [*] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [*] [Classification: (null)] [Priority: 3] (UDP) 192.168.1.31:52738 -> 6:22:40:579 PM 8.1.31.52738 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
	> 5/0/25 05/10/2025-18:22:36.573219 [*] [1:1000003:1] DNS Tunneling - NULL Record (Type 10) [*] [Classification: (null)] [Priority: 3] (UDP) 192.168.1.31:59:53 -> 6:22:36:573 PM 8.1.31.52738 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
	> 5/0/25 05/10/2025-18:22:36.572018 [*] [1:2029994:1] ET HUNTING Suspicious NULL DNS Request [*] [Classification: Misc activity] [Priority: 3] (UDP) 192.168.1.31:59:53 -> 6:22:36:570 PM 8.1.31.52738 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	

Splunk

Events (1,348) Patterns Statistics Visualization		
Timeline format ~ Zoom Out + Zoom to Selection X Deleted 1 day per column		
Format Show 20 Per Page View List		
Hide Fields	All Fields	
	i Time Event	
SELECTED FIELDS	a.host_1 a.source_1 a.sourcetype_1	
INTERESTING FIELDS	#date_hour #date_mday_3 #date_minute_56 #date_month_1 #date_second_60 #date_wday_3 #date_year_1 #date_zone_1 #index_1 #linecount_2 #punct_1 #splunk_server_1 #timewindow_1 #timestamp_1	
	> 5/0/25 05/10/2025-18:04:14.142683 [*] [1:2029995:2] ET MWARE Suspicious Long NULL DNS Request - Possible DNS Tunneling [*] [Classification: A Network Troj an was detected] [Priority: 1] (UDP) 192.168.1.31:52738 -> 192.168.1.31:59:53 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
	> 5/0/25 05/10/2025-18:04:14.138846 [*] [1:2029995:2] ET MWARE Suspicious Long NULL DNS Request - Possible DNS Tunneling [*] [Classification: A Network Troj an was detected] [Priority: 1] (UDP) 192.168.1.31:52738 -> 192.168.1.31:59:53 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
	> 5/0/25 05/10/2025-18:04:13.134137 [*] [1:2029995:2] ET MWARE Suspicious Long NULL DNS Request - Possible DNS Tunneling [*] [Classification: A Network Troj an was detected] [Priority: 1] (UDP) 192.168.1.31:52738 -> 192.168.1.31:59:53 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
	> 5/0/25 05/10/2025-18:04:12.124243 [*] [1:2029995:2] ET MWARE Suspicious Long NULL DNS Request - Possible DNS Tunneling [*] [Classification: A Network Troj an was detected] [Priority: 1] (UDP) 192.168.1.31:52738 -> 192.168.1.31:59:53 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	
	> 5/0/25 05/10/2025-18:04:11.130846 [*] [1:2029995:2] ET MWARE Suspicious Long NULL DNS Request - Possible DNS Tunneling [*] [Classification: A Network Troj an was detected] [Priority: 1] (UDP) 192.168.1.31:52738 -> 192.168.1.31:59:53 host = Ubuntu source = /var/log/sircata/test.log sourcetype = sircata:fast	

Splunk

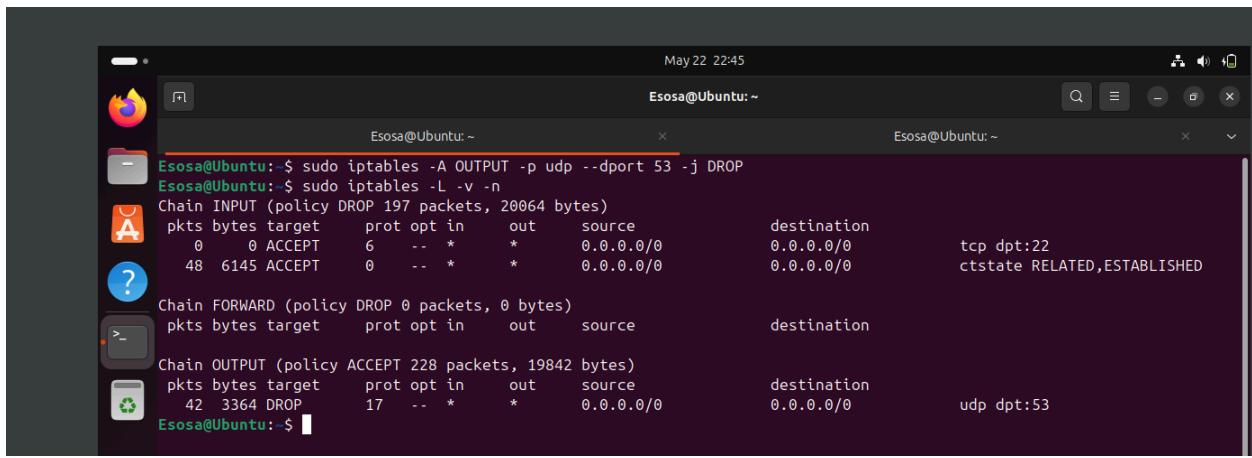
6. Response Actions

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
```



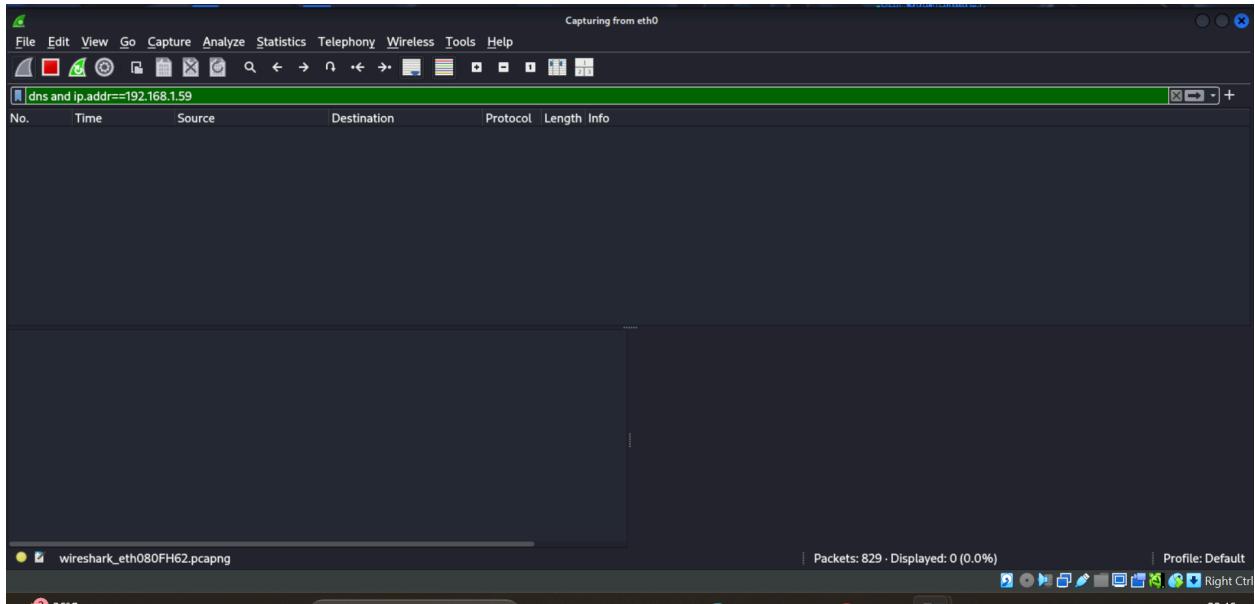
The screenshot shows a terminal window with a dark theme. The title bar says "May 22 22:45" and "Esosa@Ubuntu: ~". The terminal content is as follows:

```
Esosa@Ubuntu:~$ sudo iptables -A OUTPUT -p udp --dport 53 -j DROP
Esosa@Ubuntu:~$ sudo iptables -L -v -n
Chain INPUT (policy DROP 197 packets, 20064 bytes)
pkts bytes target  prot opt in     out      source         destination
    0     0 ACCEPT   6  --  *      *      0.0.0.0/0          0.0.0.0/0          tcp  dpt:22
    48   6145 ACCEPT   0  --  *      *      0.0.0.0/0          0.0.0.0/0          ctstate RELATED,ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target  prot opt in     out      source         destination

Chain OUTPUT (policy ACCEPT 228 packets, 19842 bytes)
pkts bytes target  prot opt in     out      source         destination
    42   3364 DROP    17  --  *      *      0.0.0.0/0          0.0.0.0/0          udp  dpt:53
Esosa@Ubuntu:~$
```

Iptables



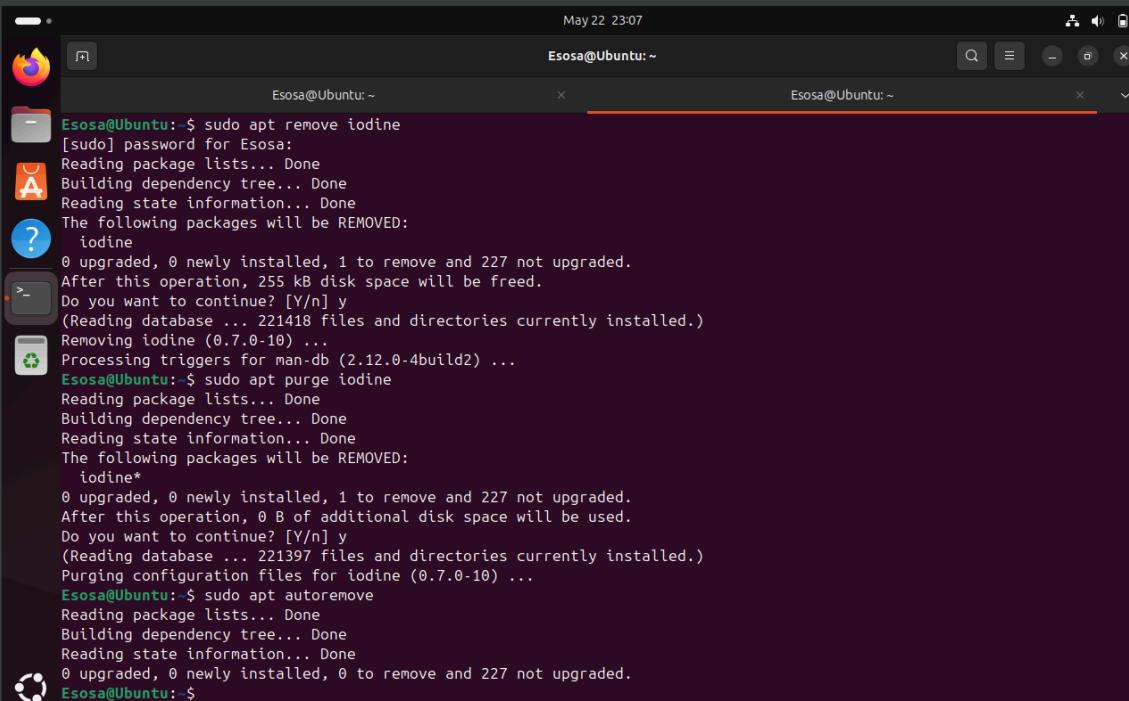
No DNS Traffic

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
```

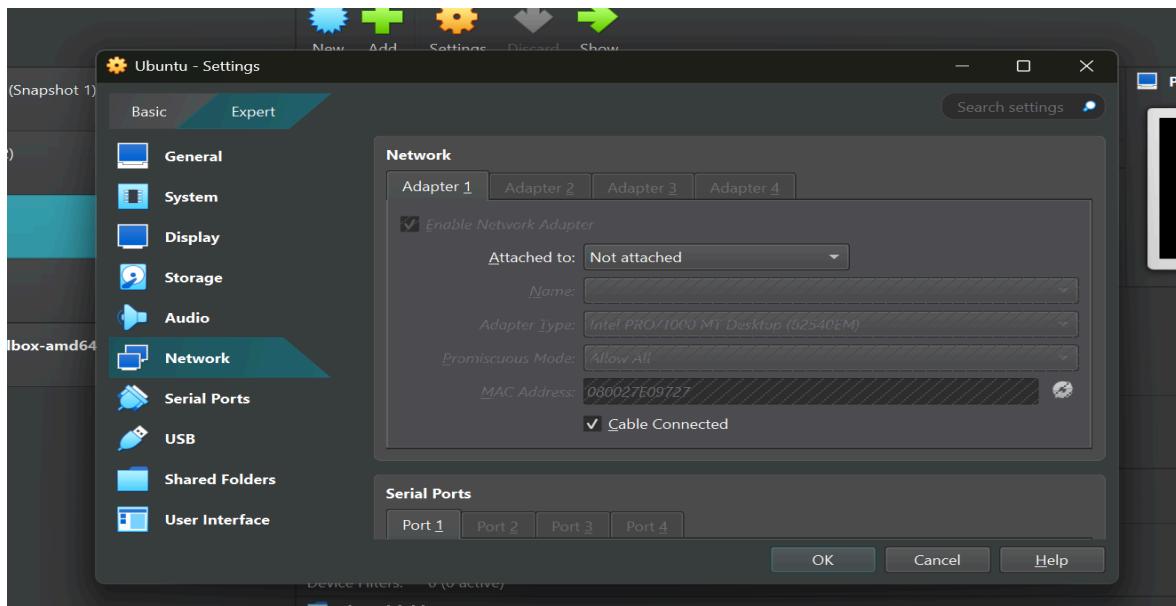


May 22 23:07

Esosa@Ubuntu:~

```
Esosa@Ubuntu:~$ sudo apt remove iodine
[sudo] password for Esosa:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  iodine
0 upgraded, 0 newly installed, 1 to remove and 227 not upgraded.
After this operation, 255 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 221418 files and directories currently installed.)
Removing iodine (0.7.0-10) ...
Processing triggers for man-db (2.12.0-4build2) ...
Esosa@Ubuntu:~$ sudo apt purge iodine
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  iodine*
0 upgraded, 0 newly installed, 1 to remove and 227 not upgraded.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n] y
(Reading database ... 221397 files and directories currently installed.)
Purging configuration files for iodine (0.7.0-10) ...
Esosa@Ubuntu:~$ sudo apt autoremove
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 227 not upgraded.
Esosa@Ubuntu:~$
```

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.

No.	Time	Source	Destination	Protocol	Length	Info
160	29.906978024	192.168.1.107	192.168.1.1	DNS	87	Standard query 0x1ef2 A ssl.gstatic.com
165	29.907975456	192.168.1.107	192.168.1.1	DNS	87	Standard query 0x572e HTTPS ssl.gstatic.com
169	29.916659284	192.168.1.1	192.168.1.107	DNS	105	Standard query response 0x1ef2 A ssl.gstatic.com A 142.250.201.67
179	30.030805968	192.168.1.1	192.168.1.107	DNS	146	Standard query response 0x572e HTTPS ssl.gstatic.com SOA ns1.google.com
223	37.410212434	192.168.1.33	8.8.8.8	DNS	146	Standard query 0x4469 A connectivity-check.ubuntu.com OPT
227	37.413775982	192.168.1.33	192.168.1.1	DNS	126	Standard query 0x87a4 A connectivity-check.ubuntu.com OPT
232	37.533188746	192.168.1.1	192.168.1.33	DNS	302	Standard query response 0x87a4 A connectivity-check.ubuntu.com A 185.125.190.96 A 91.189...
235	37.599383725	192.168.1.1	192.168.1.33	DNS	302	Standard query response 0x4469 A connectivity-check.ubuntu.com A 185.125.190.48 A 185.12...
274	41.039109772	192.168.1.107	192.168.1.1	DNS	184	Standard query 0x9793 A extension.grammarly.io
278	41.039481683	192.168.1.107	192.168.1.1	DNS	184	Standard query 0x27b2 HTTPS extension.grammarly.io
283	41.293246269	192.168.1.1	192.168.1.107	DNS	193	Standard query response 0x27b2 HTTPS extension.grammarly.io SOA ns-1688.awsdns...
287	41.319340520	192.168.1.1	192.168.1.107	DNS	234	Standard query response 0x9793 A extension.grammarly.io A 34.226.177.201 A 3.9...
323	43.348431061	192.168.1.107	192.168.1.1	DNS	88	Standard query 0x3b10 A in.grammarly.com
327	43.349431079	192.168.1.107	192.168.1.1	DNS	88	Standard query duerv 0x1304 HTTPS in.grammarly.com

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.