Oeson learning

SCANNING:

WIRESHARK & NMAP

PRESENTED BY YASH PATEL

www.linkedin.com/in/yash-c-patel

Oeson
learning

Warning!

The content provided hereafter is intended solely for educational purposes.

Oeson
learning

Agenda

1. Introduction
2. N & NSE
3. Wireshark
4. Project requirement & Brief
5. Wireshark IDS/Firewall evade techniques
6. NSE scanning
7. Conclusion
8. Reference

Oeson learning

Introduction

- This project is focused on mastering the techniques of scanning networks and websites through various tools and methods.

- It involves conducting network scans with Wireshark and Nmap, analyzing the outcomes, and pinpointing potential vulnerabilities or problems.

Oeson
learning

Nmap & NSE

- Nmap (Network Mapper) is an open-source network discovery and security auditing tool. Its main features include: Scan ports, identify services, and detect operating systems.

- NSE (Nmap Scripting Engine): Nmap ' s built-in scripting engine that enables users to create and share advanced scanning programs

Oeson learning

Wireshark

- Wireshark is a network protocol analyser that collects Monitor live traffic, diagnose network faults, and identify security flaws.

- Wireshark can record packets in real time, revealing precise information about their contents and allowing analysts to identify potential issues like as intrusions, strange traffic, or incorrectly configured networks.

Project requirement & Brief

- **Targets /Tools Used**

- Tools: Kali Linux, Nmap, Wireshark
- Testing Websites: www.tryhackme.org

- **Testing Scope**

- Project Outcome: Wireshark techniques for firewall/IDS evasion.
- Nmap NSE scripts for vulnerability scanning.

Task 1: Firewall/ IDS Evasion

- IDS evasion refers to bypassing Intrusion Detection Systems (IDS) to avoid detection during network scanning or penetration testing.

- In this task, I will perform three key evasion techniques using Wireshark to analyze the network traffic:

- 1. Packet Fragmentation
- 2. Source Port Manipulation
- 3. IP Address Decoy

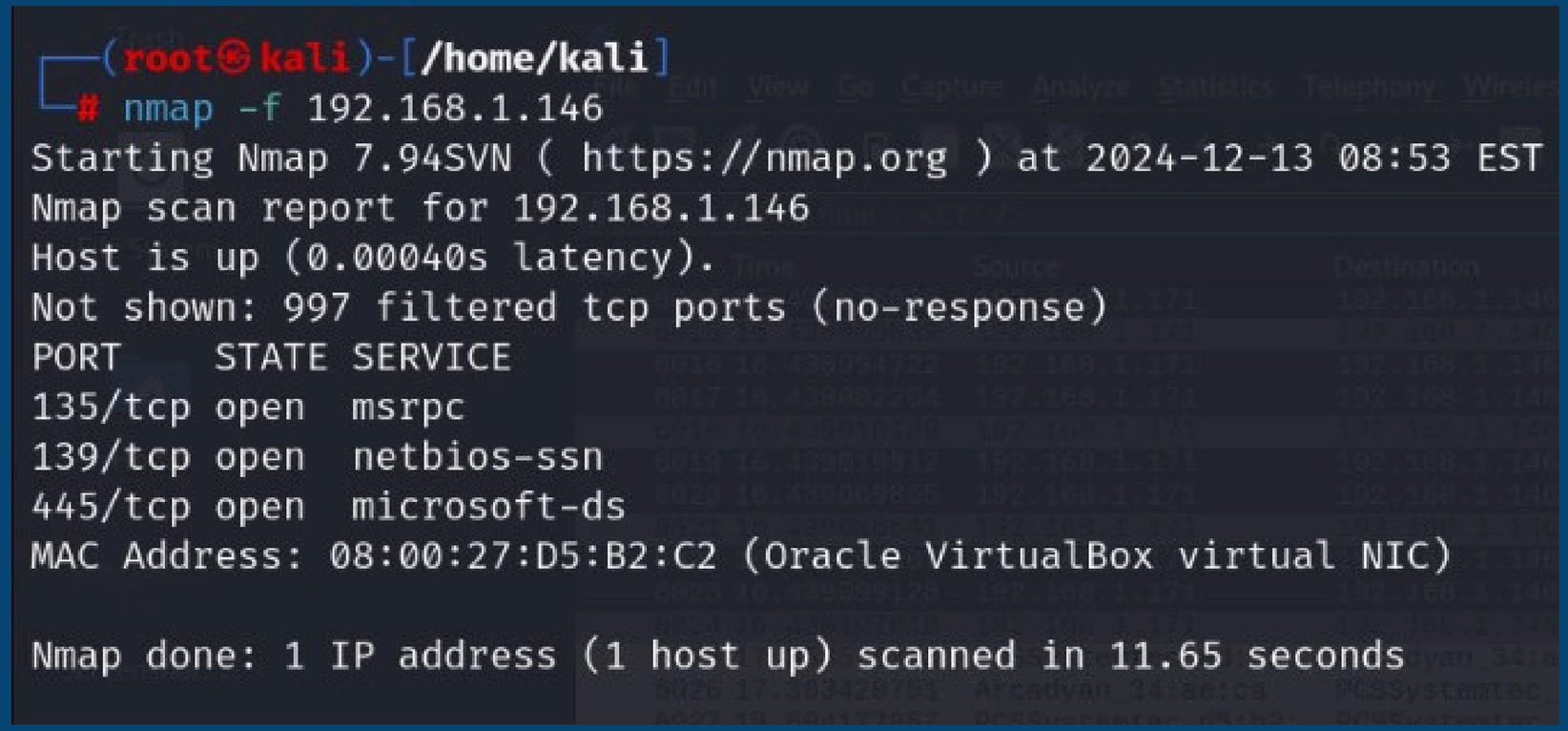
- Wireshark will be used to capture and inspect traffic during these techniques, ensuring effectiveness in evading detection.

Oeson learning

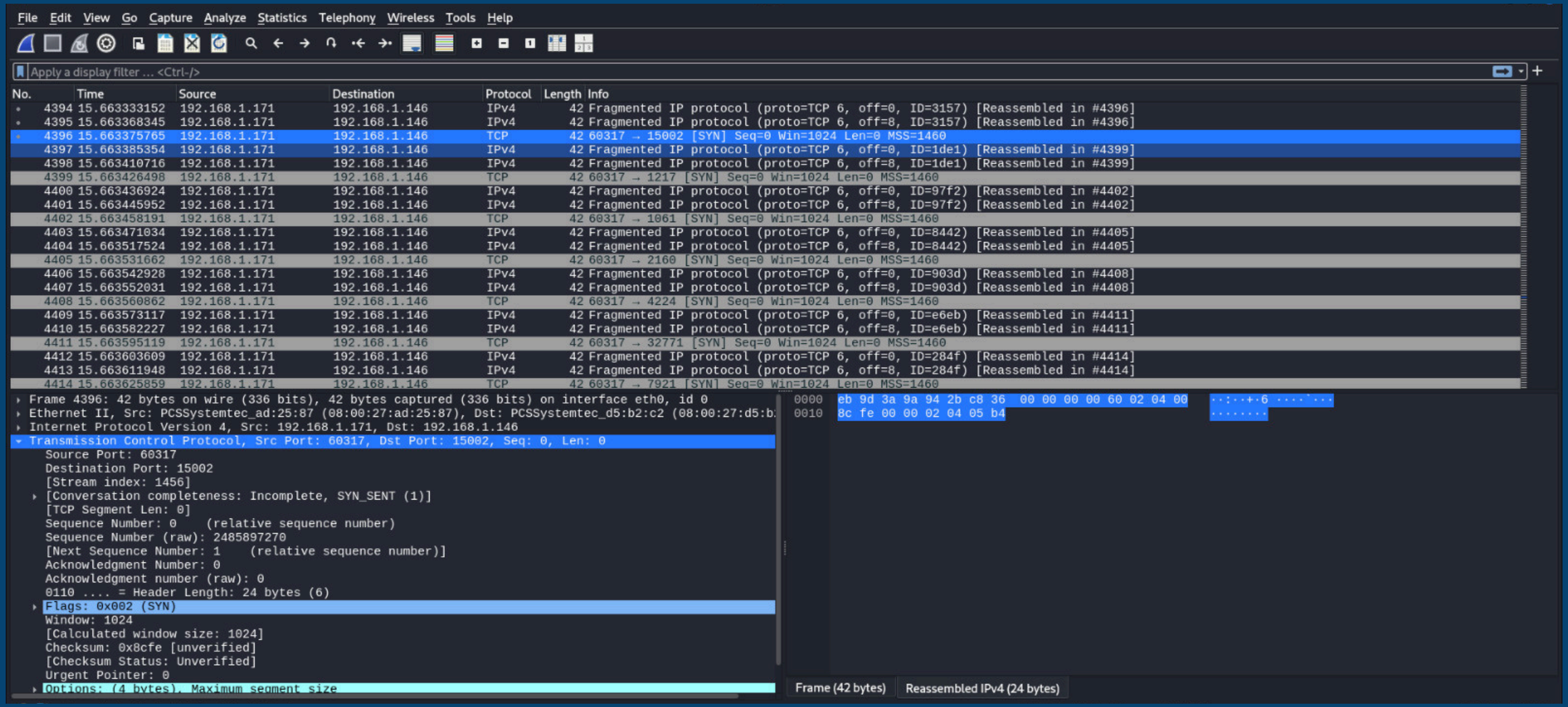
1. PACKET FRAGMENTATION

- Fragmentation is a necessary function of the TCP/IP suite, as different routers on the Internet (or internally) have different sized network links. Fragmentation dissects the packets into smaller pieces so that they can fit the smaller links as they travel the network.

- we see packets sent from a device with the MAC address SagemcomBroa_53:4e. These are ARP (Address Resolution Protocol) packets that respond to queries for an IP address. Packet fragmentation is used to split packets into smaller parts, which can help evade detection by intrusion detection systems (IDS). In this case, the packets are 60 bytes in size, indicating they are relatively small, which could be the result of fragmentation.



here I entered Nmap cmmand ‘nmap -f’ and target IP.



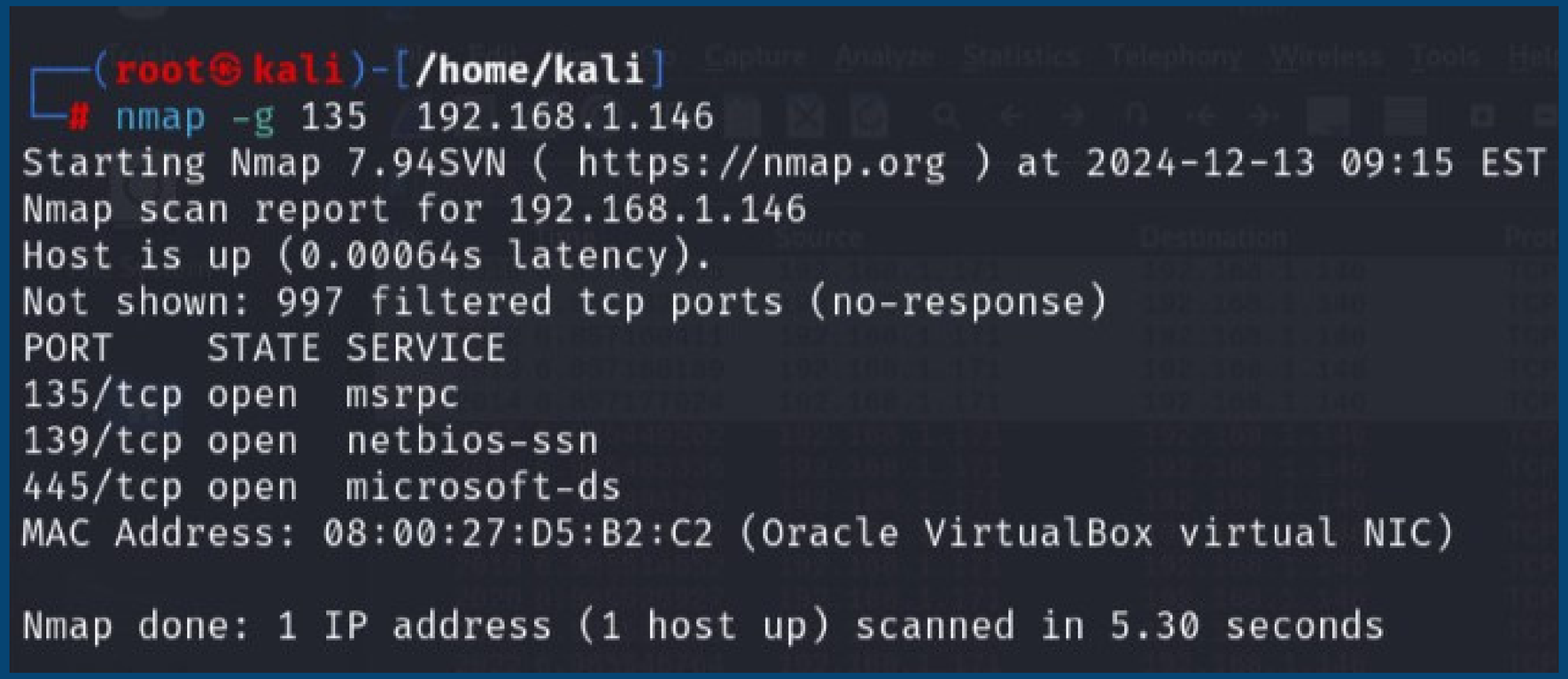
The figure shows frame 4396 sent to 192.168.1.146. The highlighted part shows that this frame was reassembled in IP frame 4396. and fragmentation was done successfully

Oeson learning

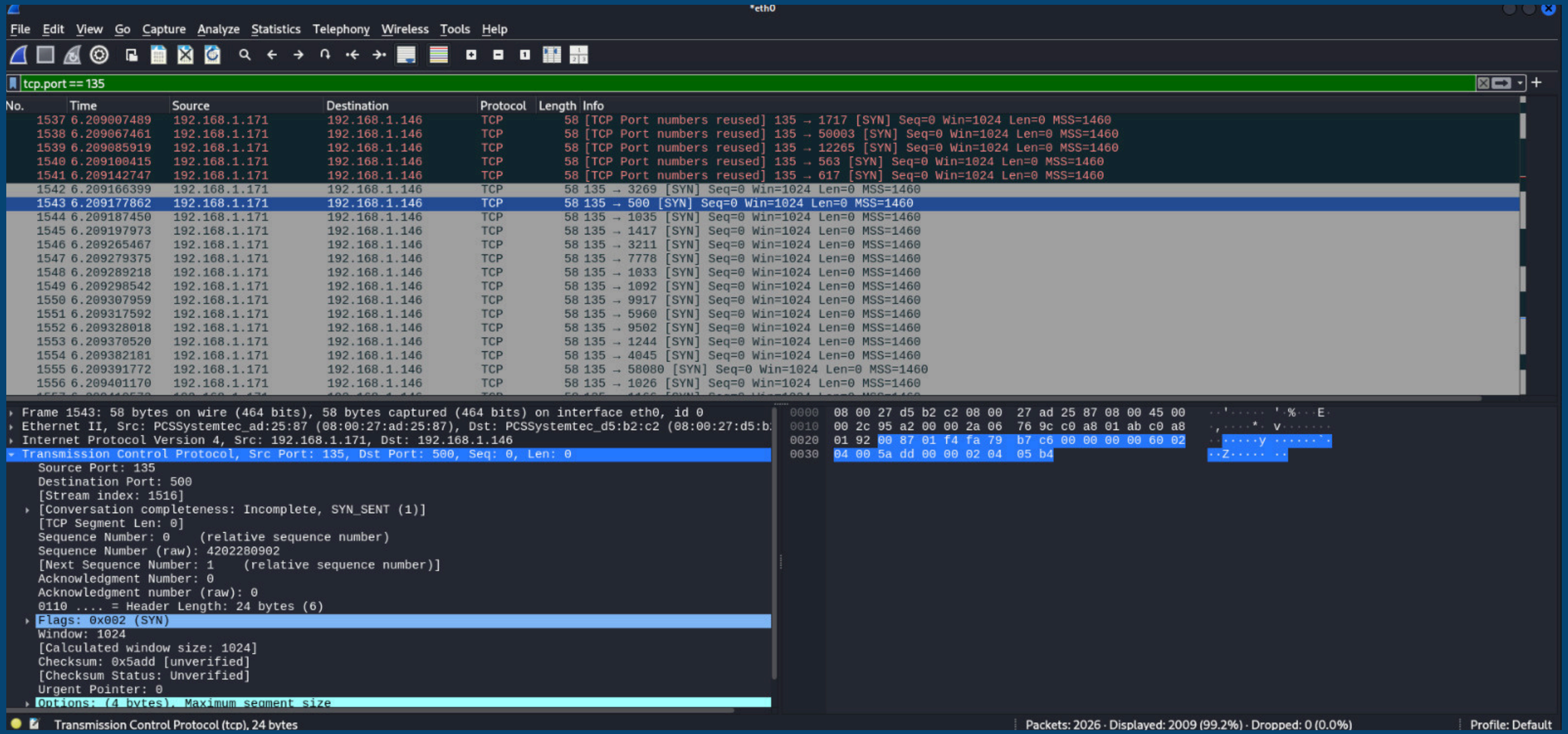
2. Source Port Manipulation

- A method used to evade detection and enhance security by altering the default port settings of services or applications.

- By changing the listening ports, attackers or defenders can obscure the presence of services, making it more difficult for unauthorized users to identify and exploit them. This technique is often employed to bypass firewalls and intrusion detection systems.



here I entered Nmap cmmand ‘nmap -g 135’ and target IP.

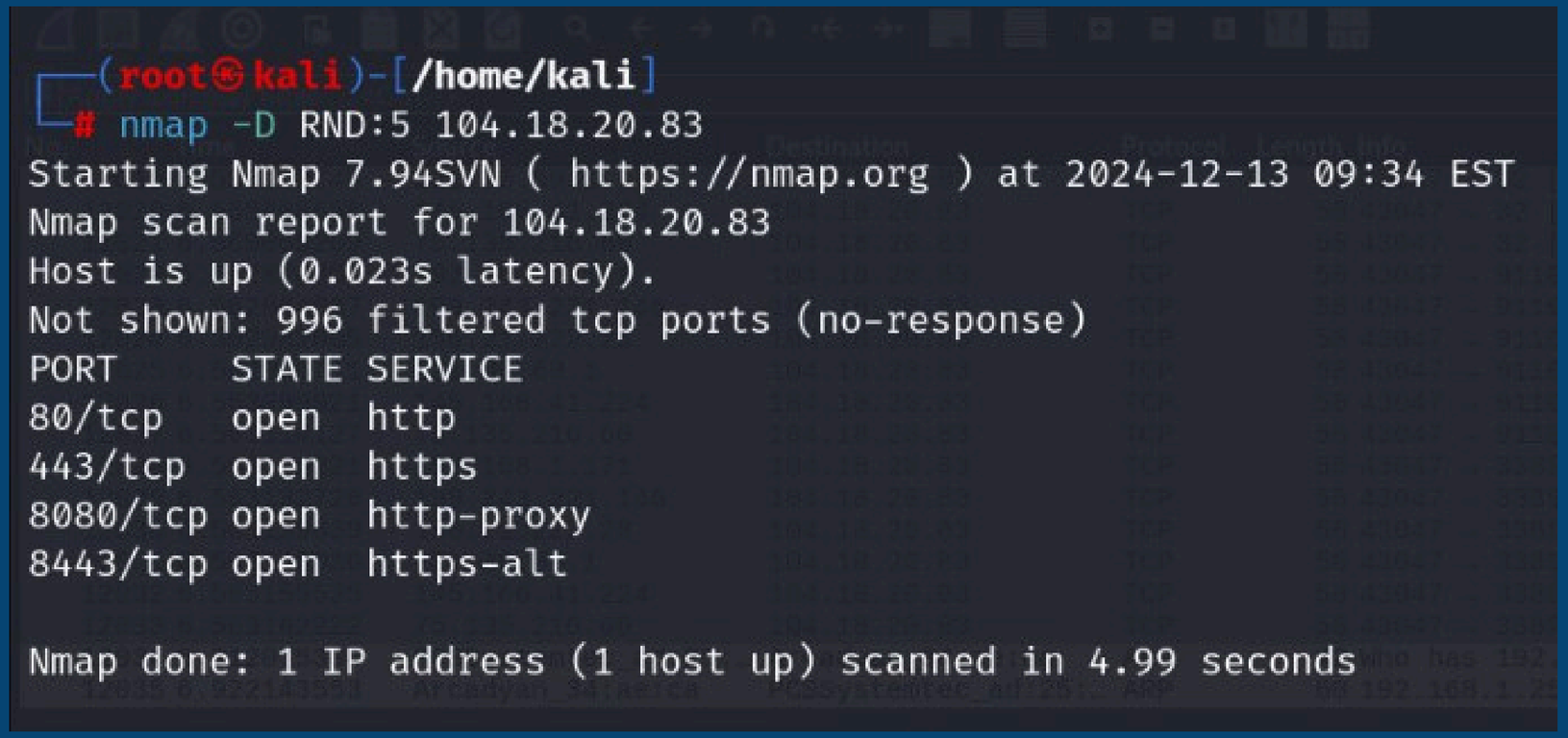


The source port of packets can be specified using the - source-port or -g flag. The packets transmitted as a result of running the aforementioned command are seen in the image. It is evident that all SYN packets have port 500 as their source.

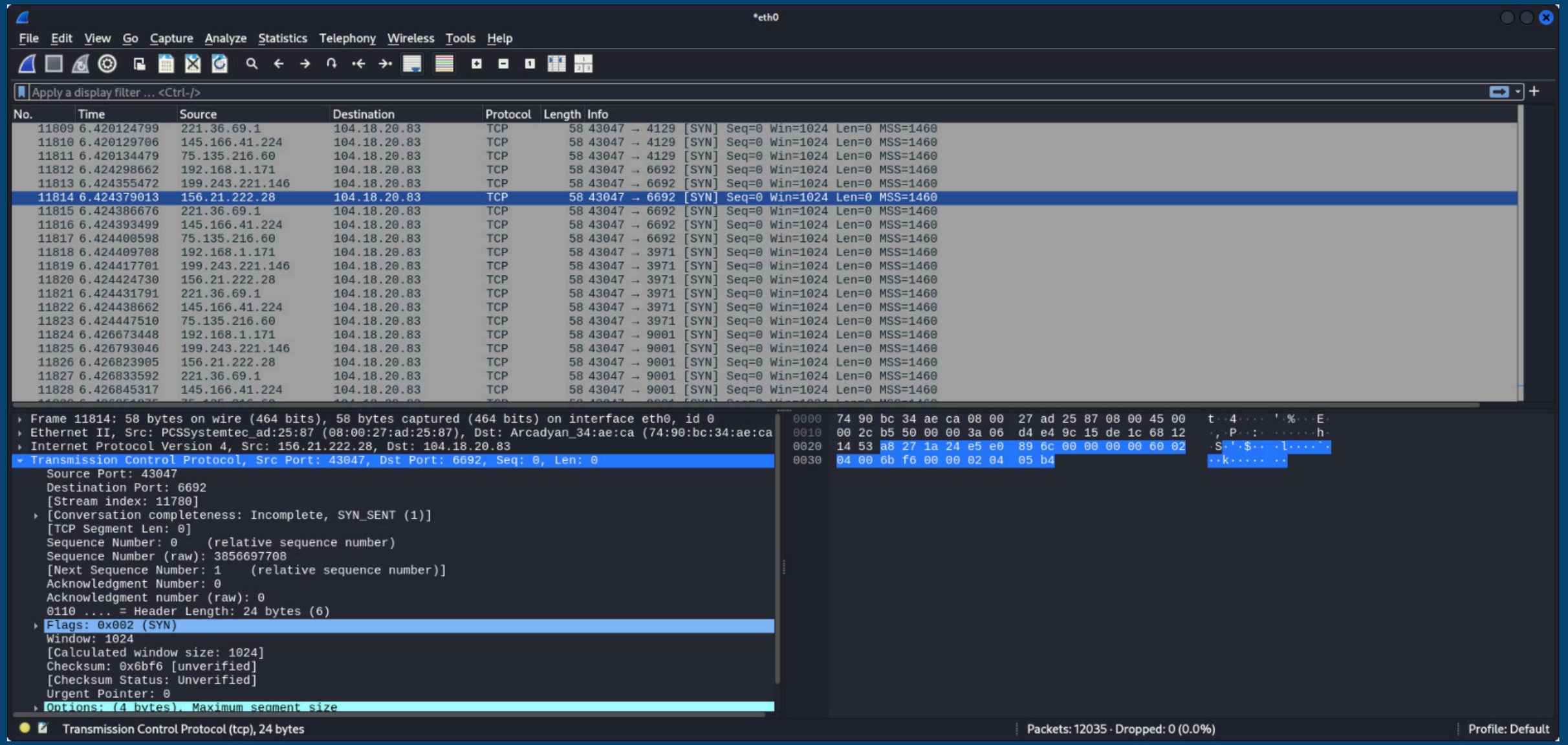
Oeson learning

3. IP Address Decoy

- A technique used to conceal the true source of network traffic by sending packets from multiple decoy IP addresses.
- This approach confuses the target about the actual origin of the attack or request, making it difficult for security systems to track and mitigate malicious activities. It is commonly used in both offensive and defensive cybersecurity strategies to enhance anonymity.



When performing this type of scan, there is two option.
nmap-D decoy1, decoy2, decoy3 etc.
This option allows you to manually specify the IP addresses of the decoys
nmap-D RND:5 [Target IP or Target website] This option generates a random number of decoys.



traffic from multiple IP addresses is displayed. The device 192.168.1.171 is sending queries to various IP addresses (e.g., 221.36.69.1). This type of traffic may result from using the -D option in Nmap, where scanning is performed using multiple IP addresses (both real and decoy), making it harder to identify the true source of the scan

Task 2: NSE Scanning

- In this task, I will perform Network Scanning using Nmap Scripting Engine (NSE). NSE allows for advanced network scanning by running scripts to automate various tasks, such as vulnerability detection, authentication bypass, and more. I will use the following 3 NSE scripts for testing:

- 1. http-headers.nse
- 2. http-auth.nse
- 3. daytime.nse

Target Websites/System:

www.tryhackme.org
192.168.1.146

- By running these scripts, I aim to gather information about the target websites, including server headers, authentication mechanisms, WAF presence, and any potential internal IP disclosure.

Oeson learning

1. http-headers.nse

Description:

This Nmap NSE script performs HTTP header analysis by sending a HEAD request to the root directory ("/") of a web server. The script retrieves important server details such as server information, content type, and connection status. If the HEAD request fails, the script switches to a GET request automatically.

- Users can customize the path (e.g., /index.php) or force a GET request through script arguments.
- It is categorized as safe for discovery tasks during network scanning.

```
local http = require "http"
local shortport = require "shortport"
local stdnse = require "stdnse"
local table = require "table"

description = [[
Performs a HEAD request for the root folder ("/") of a web server and displays the HTTP headers returned.
]]

---
-- @output
-- PORT   STATE SERVICE
-- 80/tcp open  http
-- | http-headers:
-- |   Date: Fri, 25 Jan 2013 17:39:08 GMT
-- |   Server: Apache/2.2.14 (Ubuntu)
-- |   Accept-Ranges: bytes
-- |   Vary: Accept-Encoding
-- |   Connection: close
-- |   Content-Type: text/html
-- |
-- |_  (Request type: HEAD)
--
--@args path The path to request, such as <code>/index.php</code>. Default <code>/</code>.
--@args useget Set to force GET requests instead of HEAD.
--
--@see http-security-headers.nse
```

Outputs:

- Displays the server's HTTP headers.
- Indicates whether a HEAD or GET request was used.

Oeson learning

1. http-headers.nse

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script http-headers.nse www.tryhackme.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 10:09 EST
Nmap scan report for www.tryhackme.org (70.32.1.32)
Host is up (0.093s latency).
rDNS record for 70.32.1.32: ip-70.32.1.32.hosted.by.gigenet.com
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE  SERVICE
53/tcp closed domain
80/tcp open   http
| http-headers:
|   date: Fri, 13 Dec 2024 15:09:23 GMT
|   server: Apache
|   set-cookie: __tad=1734102563.4913642; expires=Mon, 11-Dec-2034 15:09:23 GMT; Max-Age=315360000
|   vary: Accept-Encoding
|   content-length: 1049
|   content-type: text/html; charset=UTF-8
|   connection: close
|
|_  (Request type: GET)

Nmap done: 1 IP address (1 host up) scanned in 20.54 seconds
```

NSE Script executed of testing website ‘www.tryhackme.org

Oeson learning

2. http-auth.nse

Description:

This Nmap NSE script is used to retrieve authentication schemes and realms from web services requiring authentication. When a web service responds with a 401 Unauthorized status, the script analyzes the WWW-Authenticate header to extract details such as:

- Authentication methods (e.g., Basic, NTLM, Digest)
- Relevant parameters like realm, nonce, and algorithm
- Users can customize the target path (e.g., /login) using script arguments.

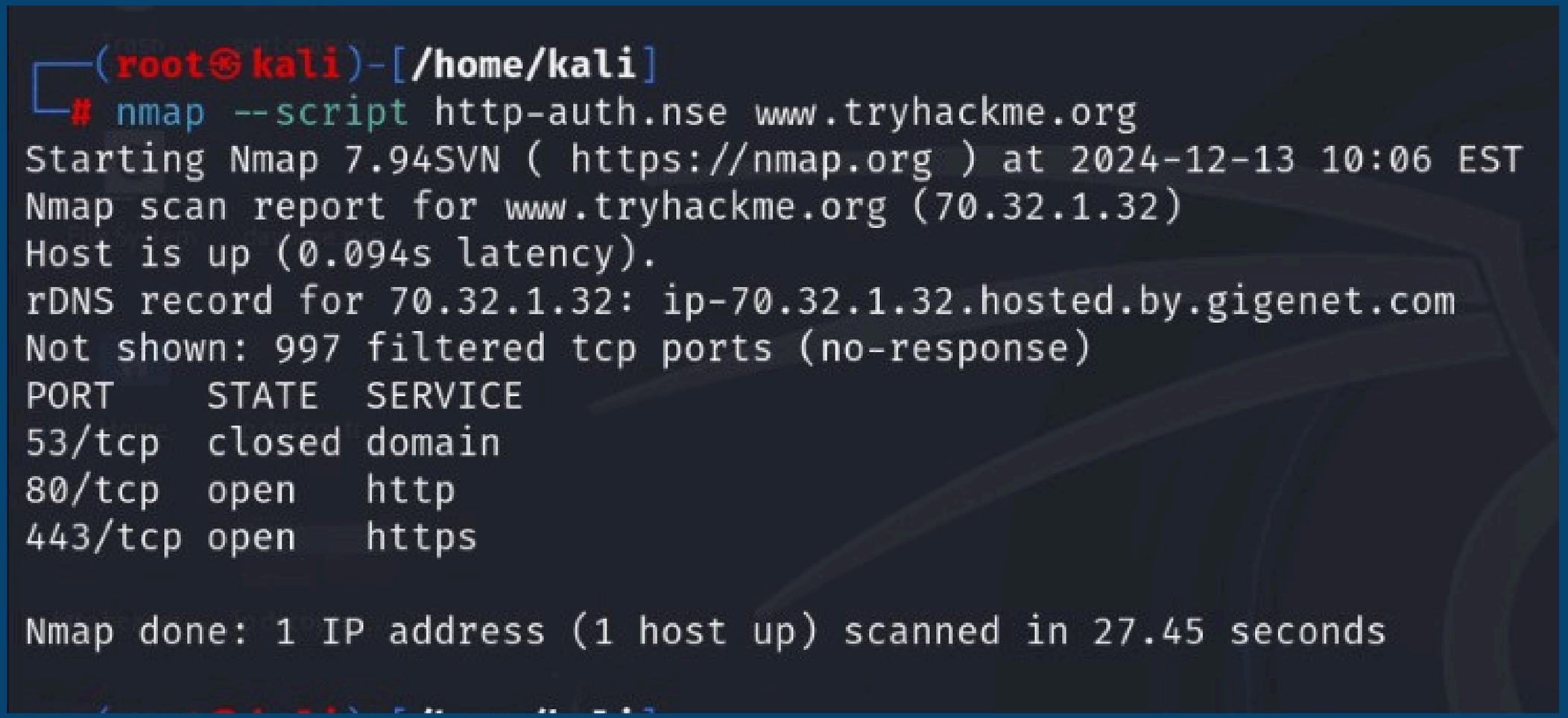
```
1 local http = require "http"
2 local shortport = require "shortport"
3 local stdnse = require "stdnse"
4 local string = require "string"
5 local table = require "table"
6
7 description = [[
8 Retrieves the authentication scheme and realm of a web service that requires
9 authentication.
10 ]]
11
12 ---
13 -- @usage
14 -- nmap --script http-auth [--script-args http-auth.path=/login] -p80 <host>
15 --
16 -- @output
17 -- PORT   STATE SERVICE REASON
18 -- 80/tcp open  http    syn-ack
19 -- | http-auth:
20 -- | HTTP/1.1 401 Unauthorized
21 -- |   Negotiate
22 -- |   NTLM
23 -- |   Digest charset=utf-8 nonce=+Upgraded+v1e4e256b4afb7f89be014e ... 968ccd60affb7c qop=auth algorithm=MD5-sess realm=example.com
24 -- |_  Basic realm=example.com
25 --
```

Outputs:

- Lists the authentication schemes used by the web service.
- Displays associated parameters, such as the realm and algorithm.

Oeson learning

2. http-auth.nse



NSE Script executed of testing website www.tryhackme.org

3. daytime.nse

Descriptions:

This Nmap NSE script use to Retrieves the day and time from the Daytime service and it is categorized in discovery and safe route.

Outputs:

- Here's a sample output from the daytime.nse script:

PORT STATE SERVICE 13/tcp open daytime |_daytime:
Wed Mar 31 14:48:58 MDT 2010

```
local comm = require "comm"
local shortport = require "shortport"
local oops = require "oops"

description = [[
Retrieves the day and time from the Daytime service.
]]

---
-- @output
-- PORT   STATE SERVICE
-- 13/tcp open  daytime
-- |_daytime: Wed Mar 31 14:48:58 MDT 2010

author = "Diman Todorov"

license = "Same as Nmap--See https://nmap.org/book/man-legal.html"

categories = {"discovery", "safe"}


portrule = shortport.port_or_service(13, "daytime", {"tcp", "udp"})

action = function(host, port)
  return oops.output(comm.exchange(host, port, "dummy", {lines=1}))
end
```

Oeson learning

3. daytime.nse

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script daytime.nse 192.168.1.146
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 10:13 EST
Nmap scan report for 192.168.1.146
Host is up (0.0010s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:D5:B2:C2 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.07 seconds
```

NSE Script executed of testing System ip 192.168.1.146

Oeson learning

Conclusion

- Nmap and Wireshark are both essential tools for network security, each serving distinct roles. Nmap is used for network scanning, identifying active hosts, open ports, and potential vulnerabilities, offering a broad overview of the network's security.

- Wireshark excels in real-time traffic capture and analysis, providing detailed insights into data exchanges and detecting anomalies. When used together, Nmap uncovers vulnerabilities, and Wireshark helps analyze traffic to identify suspicious activities or exploits. Together, these tools offer a comprehensive approach to network reconnaissance, vulnerability scanning, and cybersecurity assessments.

Oeson learning

Reference

- Nmap Guide:
  https://nmap.org/book/man.html
- Wireshark User Guide:
  https://www.wireshark.org/docs/wsug_htm l_chunked
- https://www.infosecmatter.com/nmap-nse-library
- Testing Website:
  http://www.tryhackme.org

THANK YOU

By Yash Patel