PRESENTATION OF DATA EXHALATION USING DATA CENTRE TOOL

A REPORT

Submitted by
D Abhishek Reddy [RA2111030010164]

Under the Guidance of
Dr. D. Deepika
Assistant Professor, Department of Networking and Communications

In partial satisfaction of the requirements for the degree of
BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING with specialization in CYBER SECURITY

SCHOOL OF COMPUTING
COLLEGE OF ENGINEERING AND TECHNOLOGY SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR - 603203
MAY 2024

COLLEGE OF ENGINEERING & TECHNOLOGY
SRM INSTITUTE OF SCIENCE & TECHNOLOGY
S.R.M NAGAR, KATTANKULATHUR-603203

BONAFIDE CERTIFICATE

Certified that this project report "PENTESTING ON DATA CENTER is the bonafide work of “D ABHISHEK REDDY"0f III Year/Vl Sem B. Tech (CSE) who carried out the mini project work under my supervision for the course 18CSE386T PENETRATION TESTING AND VULNERABILITY ASSESSMENT in SRM Institute of Science and Technology during the academic year 2023-2024(Even sem).

SIGNATURE

Dr. D. Deepika
Assistant Professor
Networking and Communications

SIGNATURE

Dr. Annapurani Panaiyappan K
Professor and Head
Networking and Communications

CASE STUDY ON "PENTESTING ON DATA CENTRE"

EVEN Semester (2023-2024)

Course Code & Course Name: 18CSE386T — Penetration Testing and Vulnerability Assessment

Year & Semester : Ill/VI

Report Title : The Pentesting on Data Centre tool

Course Faculty : Dr. D. Deepika

Student Name : D Abhishek Reddy [RA2111030010164]

Evaluation:

S. No	Parameter	Marks
1	Problem Investigation & Methodology Used	
2	Tool used for investigation	
3	Demo of investigation	
4	Uploaded in GitHub	
5	Viva	
6	Report	
	Total	

Date:

Staff Name:

Signature:

TABLE OF CONTENTS

INTRODUCTION

Cybersecurity is a critical aspect of data center operations, as data centers handle sensitive information and mission-critical applications. A comprehensive introduction to data center cybersecurity should cover the following key areas:

Threat Landscape

- Common cyber threats targeting data centers, such as DDoS attacks, malware, insider threats, and advanced persistent threats (APTs)

- Emerging trends in data center cybersecurity, including the rise of ransomware and the increasing sophistication of attackers Security Frameworks and Standards

- Widely adopted security frameworks like NIST CSF, ISO 27001, and PCI DSS, and their relevance to data center security

- Compliance requirements specific to the industry or region where the data center operates

Physical Security

- Perimeter security measures, such as fencing, gates, and surveillance cameras

- Access control systems, including biometrics and two-factor authentication

- Secure zones and cages within the data center to segregate critical systems Network Security

- Firewalls, intrusion detection and prevention systems

(IDS/IPS), and web application firewalls (WAFs)

- Encryption of data at rest and in transit, using technologies like SSL/TLS and disk encryption

- Backup and disaster recovery strategies to ensure data availability and integrity

- Data retention policies and secure data disposal methods

Regular vulnerability assessments and penetration testing to identify and mitigate security weaknesses

- Patch management processes to keep systems up-to-date with the latest security patches and updates

Incident response plans and procedures to detect, contain, and recover from security incidents

- Disaster recovery plans to ensure business continuity in the event of a major incident or disaster

By addressing these key areas, data center operators can enhance their cybersecurity posture and protect their critical infrastructure and data assets from various threats.

SCOPE

The security assessment will encompass a holistic evaluation of XYZ Corporation's cybersecurity landscape, covering the following key areas:

1.Network Security: Review the design and implementation of network security controls, including firewalls, intrusion detection/prevention systems (IDS/IPS), VPNs, and network segmentation, to identify potential entry points for unauthorized access and data breaches.

2.Application Security: Assess the security posture of internally developed and third-party applications utilized by XYZ Corporation, focusing on vulnerabilities such as SQL injection, cross-site scripting (XSS), authentication flaws, and inadequate input validation.

3.Data Security: Evaluate the measures in place to safeguard sensitive data, including encryption mechanisms, access controls, data classification, data loss prevention (DLP) strategies, and compliance with data protection regulations (e.g., GDPR, CCPA).

4.Endpoint Security: Analyze the security controls deployed on employee devices (e.g., laptops, desktops, mobile devices), including antivirus software, endpoint detection and response (EDR) solutions, patch management processes, and device encryption, to mitigate the risk of malware infections and unauthorized access.

5.Security Policies and Procedures: Review the organization's security policies, procedures, and incident response plans to assess their effectiveness, clarity, and enforcement mechanisms, ensuring alignment with industry best practices and regulatory requirements.

Objective:

The primary objective of the security assessment is to comprehensively evaluate the state of cybersecurity within XYZ Corporation, identifying potential vulnerabilities and weaknesses across its IT infrastructure, policies, and procedures. This assessment aims to provide actionable insights and recommendations to enhance the overall security posture of the organization, thereby reducing the likelihood and impact of cyber threats. The specific goals include:

1. **Identification of Vulnerabilities:** Through thorough analysis and testing, identify weaknesses, misconfigurations, and vulnerabilities present in the network, applications, data handling processes, endpoint devices, and security policies.
2. **Risk Mitigation:** Assess the level of risk associated with discovered vulnerabilities and weaknesses, prioritizing them based on severity and potential impact on the organization's operations, assets, and data.
3. **Recommendations for Improvement:** Provide detailed recommendations and best practices for remediation actions to address identified vulnerabilities and weaknesses, aiming to bolster the organization's resilience against cyber threats.
4. **Enhancing Security Awareness:** Evaluate the effectiveness of existing security policies, procedures, and employee awareness training programs to ensure that personnel are adequately informed and equipped to mitigate security risks.
5. **Compliance and Regulatory Alignment:** Ensure that XYZ Corporation's security practices align with relevant industry standards, regulations, and compliance requirements, safeguarding the organization against legal and regulato

TOOL DESCRIPTION

Tool: Data center

Penetration testing tools play a critical role in assessing data center security. These tools, like Kali Linux, Metasploit, and SQLMap, are used to identify vulnerabilities and weaknesses in network security

Feature's Of Data center:

1. *Visualize Scan Results*: Tools like Pentest-Tools.com provide a dashboard to visualize scan activity and vulnerabilities found

2. *Detailed Reports*: These tools focus on creating human-readable reports with visual summaries, findings, and recommendations for fixing vulnerabilities

3. *Automated Testing*: Utilize Pentest Robots to automate manual tasks, allowing focus on quality results and complex issues at scale

4. *Attack Surface Mapping*: Automatically detect open ports, services, and software, providing a centralized view of scan results[1].

5. *Scheduled Scans*: Schedule periodic scans to monitor system security continuously, receiving reports via email for timely insights

The main source of information:

The main source of information for data center penetration testing includes a variety of tools and techniques. These tools, whether licensed or open-source like Kali Linux, Metasploit, and SQLMap, are crucial for identifying vulnerabilities in data center security.

They encompass methods such as automated scanning, vulnerability scanning, and network sniffing to evaluate security measures and detect weaknesses.

Additionally, physical security considerations, like tailgating and human factors, are highlighted as key aspects to address in data center security assessments

TOOL INSTALLATION PROCEDURE

The installation procedure for penetration testing tools in a data center typically involves the following steps:

1. **Identify the appropriate tools** based on the specific requirements and scope of the penetration test, such as Kali Linux, Metasploit, or SQLMap.

2. **Ensure that the necessary hardware and software dependencies** are met for the selected tools to function properly in the data center environment.

3. **Obtain the necessary licenses or permissions** to use the tools, especially if they are commercial or require specific authorization.

4. **Install the tools on a secure and isolated system** within the data center, ensuring that they do not interfere with or compromise the production environment.

5. **Configure the tools** according to the manufacturer's instructions and the specific requirements of the penetration test.

6. **Test the tools** to ensure that they are functioning correctly and can effectively simulate attacks and identify vulnerabilities.

7. **Regularly update the tools** to ensure that they are equipped with the latest security patches and can detect and exploit newly discovered vulnerabilities.

TOOL IMPLEMENTATION PROCEDURE

1. Download DATA CENTRE:

   wget <download url>

2. Make Installer Executable:

   chmod a+x <installer flle>

3. Run the Installer:

   sudo ./<installer file>

4. Follow Installation Wizard:

   sudo <datacentre installation directory>/bin/start-datacentre.sh

5. Access DATA CENTRE:

   http://localhost:8080 or http://<server_ip>:8080

Steps of Ethical Hacking that you have done on your applications using DATA CENTRE tool

The tool installation procedure for penetrating testing a data center typically involves the following steps:

1. **Understand the policies of the cloud provider** and which services can be tested.

2. **Create a penetration testing plan** by communicating with the customer to determine the test scope, gather information about the cloud architecture and potential access points.

3. **Select appropriate penetration testing tools** that can effectively simulate actual attack scenarios and find vulnerabilities. Common tools include port scanners, vulnerability scanners, network sniffers, web proxies, and password crackers.

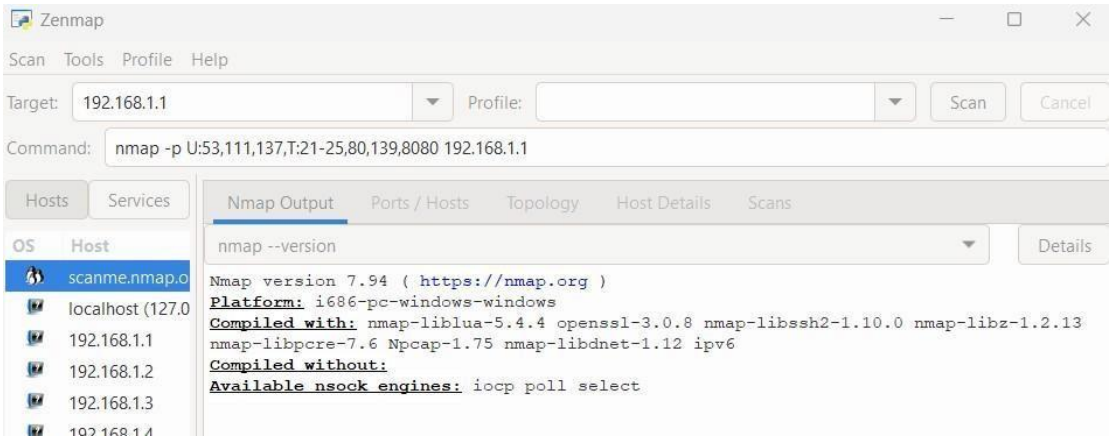
4. **Analyze the responses from the automated tools and manual tests**, document the findings, and decide if they are false positives or need to be reported as vulnerabilities.

5. **Find and eliminate the identified vulnerabilities** by discussing their severity and impact with the penetration testing team. Prepare a final vulnerability report with recommendations for remediation.

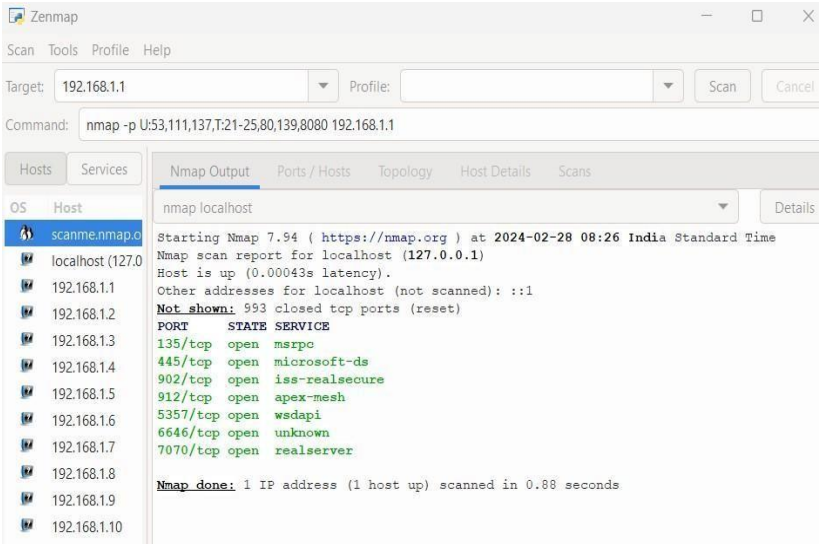
The key is to have a well-defined scope, use the right tools to simulate real-world attacks, analyze the results thoroughly, and provide actionable remediation guidance to improve the data center's security posture.

Screenshots:

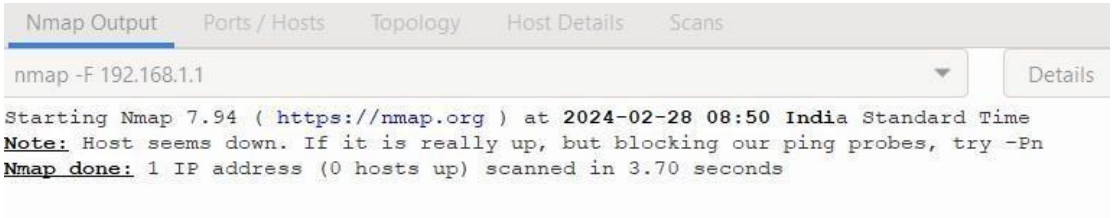
Installation 0f nmap



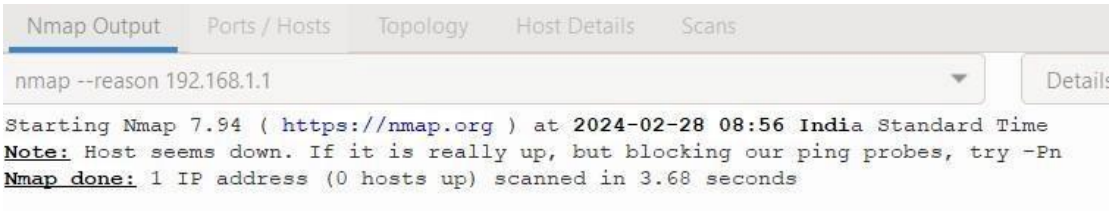
Scanning Local Host



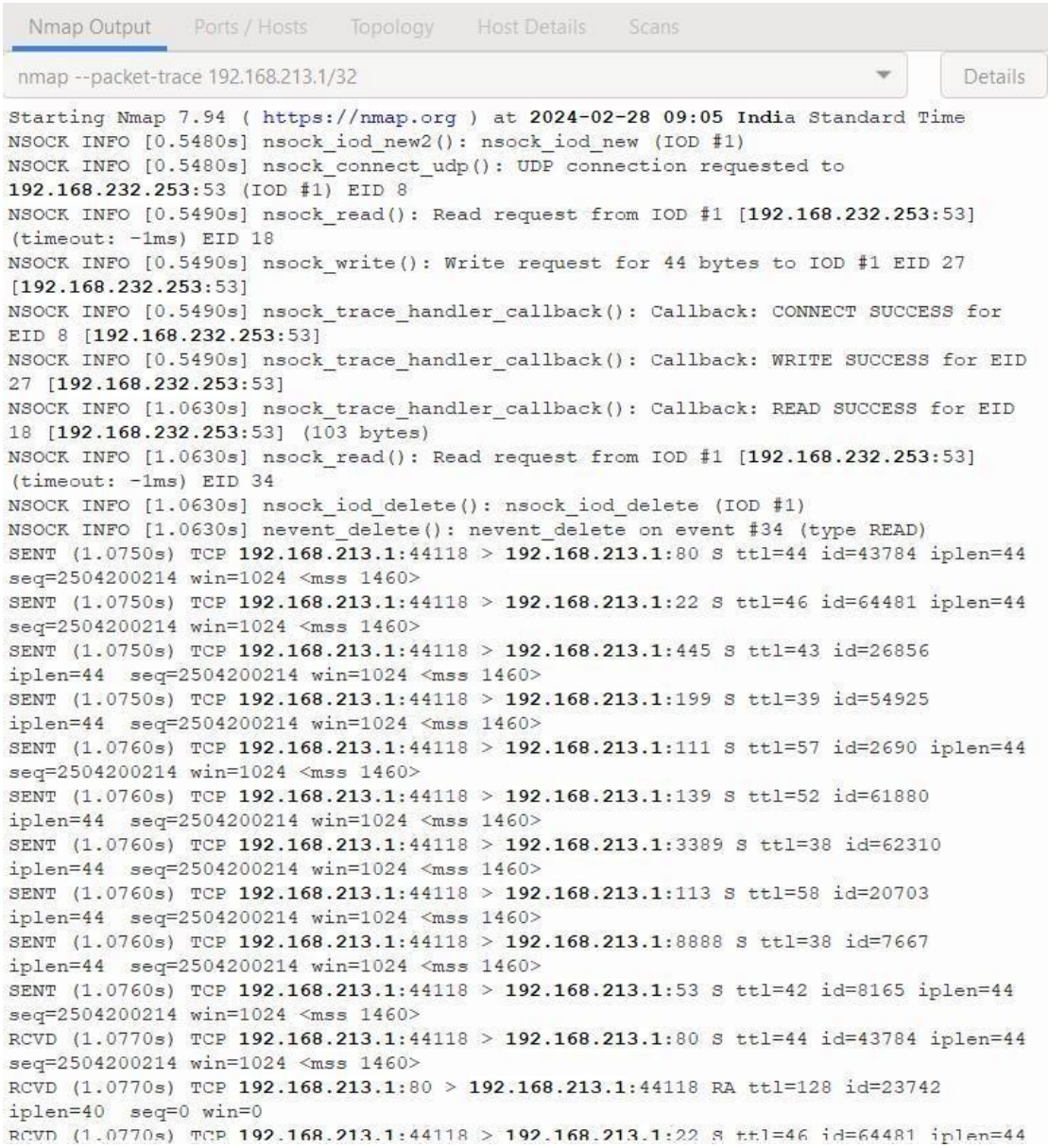
to perform fast scann which will only scan important ports nmap -F 192.168.1.1



The option --reason will make Nmap include the packet type that determined the port and host state nmap --reason 192.168.1.1



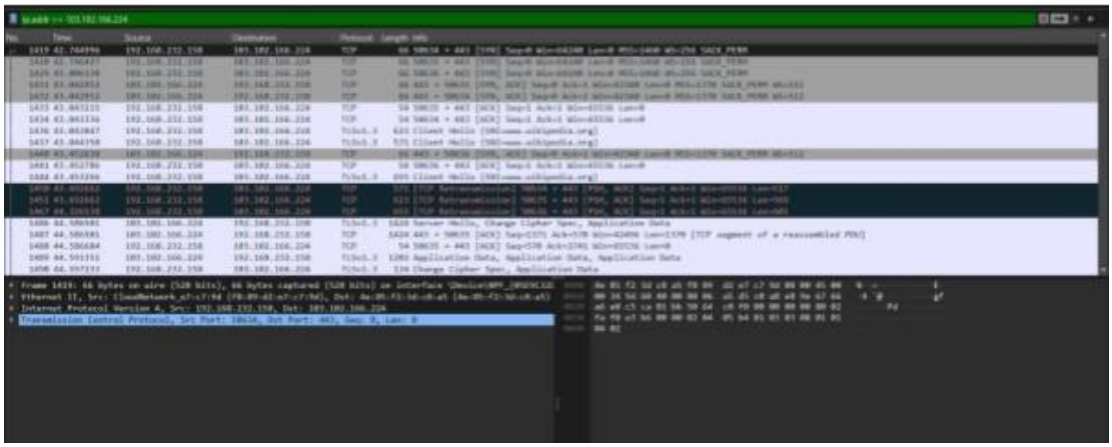
To only show open ports nmap --packet-trace 192.168.1.1



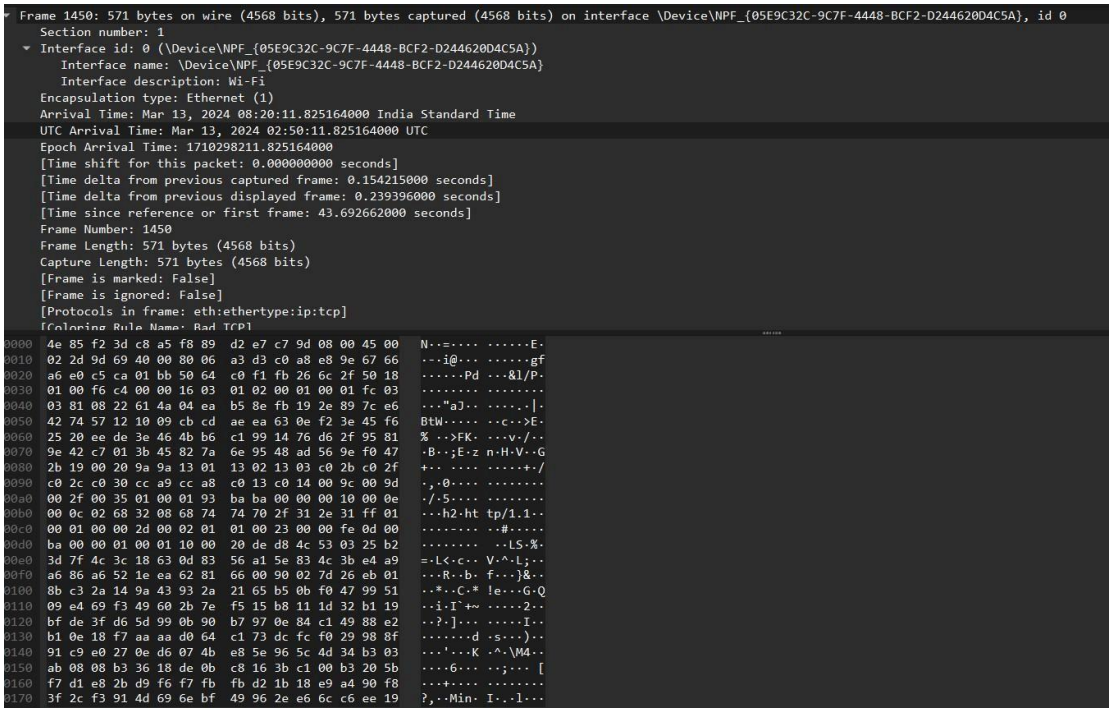
Wireshark and Nessus

Capturing packets in wire sark

```
Microsoft Windows [Version 10.0.22631.3155]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Pavana Narasimha>ping www.wikipedia.org

Pinging dyna.wikimedia.org [103.102.166.224] with 32 bytes of data:
Reply from 103.102.166.224: bytes=32 time=148ms TTL=51
Reply from 103.102.166.224: bytes=32 time=99ms TTL=51
Request timed out.
Reply from 103.102.166.224: bytes=32 time=106ms TTL=51

Ping statistics for 103.102.166.224:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 99ms, Maximum = 148ms, Average = 117ms

C:\Users\Pavana Narasimha>
```



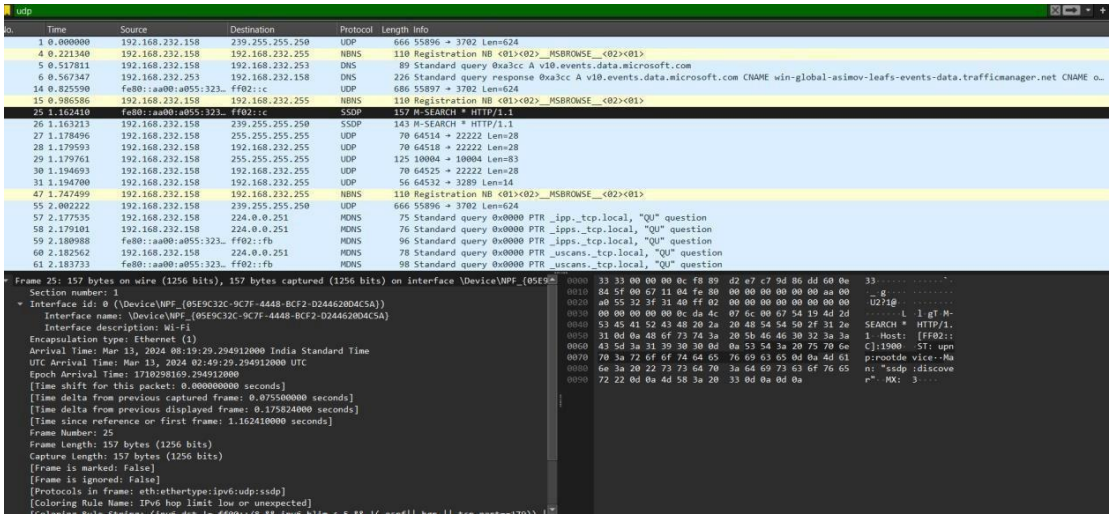
File capturing



Explore the coloring rules of wireshark

Color in Wireshark	Packet Type
Light purple	TCP
Light blue	UDP
Black	Packets with errors
Light green	HTTP traffic
Light yellow	Windows-specific traffic, including Server Message Blocks (SMB) and NetBIOS
Dark yellow	Routing
Dark gray	TCP SYN, FIN and ACK traffic

use filter packet with different protocols for the captures packets


udp
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.232.158 239.255.255.250 UDP 666 55896 → 3702 Len=624
4 0.221340 192.168.232.158 192.168.232.255 NBNS 110 Registration NB <01><02>__MSBROWSE__<02><01>
5 0.517811 192.168.232.158 192.168.232.253 DNS 89 Standard query 0xa3cc A v10.events.data.microsoft.com
6 0.567347 192.168.232.253 192.168.232.158 DNS 226 Standard query response 0xa3cc A v10.events.data.microsoft.com CNAME win-global-asimov-leafs-events-data.trafficmanager.net CNAME o…
14 0.825590 fe80::aa00:a055:323… ff02::c UDP 686 55897 → 3702 Len=624
15 0.986586 192.168.232.158 192.168.232.255 NBNS 110 Registration NB <01><02>__MSBROWSE__<02><01>
25 1.162410 fe80::aa00:a055:323… ff02::c SSDP 157 M-SEARCH * HTTP/1.1
26 1.163213 192.168.232.158 239.255.255.250 SSDP 143 M-SEARCH * HTTP/1.1
27 1.178496 192.168.232.158 255.255.255.255 UDP 70 64514 → 22222 Len=28
28 1.179593 192.168.232.158 192.168.232.255 UDP 70 64518 → 22222 Len=28
29 1.179761 192.168.232.158 255.255.255.255 UDP 125 10004 → 10004 Len=83
30 1.194693 192.168.232.158 192.168.232.255 UDP 70 64525 → 22222 Len=28
31 1.194700 192.168.232.158 192.168.232.255 UDP 56 64532 → 3289 Len=14
47 1.747499 192.168.232.158 192.168.232.255 NBNS 110 Registration NB <01><02>__MSBROWSE__<02><01>
55 2.002222 192.168.232.158 239.255.255.250 UDP 666 55896 → 3702 Len=624
57 2.177535 192.168.232.158 224.0.0.251 MDNS 75 Standard query 0x0000 PTR _ipp._tcp.local, "QU" question
58 2.179101 192.168.232.158 224.0.0.251 MDNS 76 Standard query 0x0000 PTR _ipps._tcp.local, "QU" question
59 2.180988 fe80::aa00:a055:323… ff02::fb MDNS 96 Standard query 0x0000 PTR _ipps._tcp.local, "QU" question
60 2.182562 192.168.232.158 224.0.0.251 MDNS 78 Standard query 0x0000 PTR _uscans._tcp.local, "QU" question
61 2.183733 fe80::aa00:a055:323… ff02::fb MDNS 98 Standard query 0x0000 PTR _uscans._tcp.local, "QU" question
Frame 25: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface \Device\NPF_{05E9
Section number: 1
Interface id: 0 (\Device\NPF_{05E9C32C-9C7F-4448-BCF2-D244620D4C5A})
Interface name: \Device\NPF_{05E9C32C-9C7F-4448-BCF2-D244620D4C5A}
Interface description: Wi-Fi
Encapsulation type: Ethernet (1)
Arrival Time: Mar 13, 2024 08:19:29.294912000 India Standard Time
UTC Arrival Time: Mar 13, 2024 02:49:29.294912000 UTC
Epoch Arrival Time: 1710298169.294912000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.075500000 seconds]
[Time delta from previous displayed frame: 0.175824000 seconds]
[Time since reference or first frame: 1.162410000 seconds]
Frame Number: 25
Frame Length: 157 bytes (1256 bits)
Capture Length: 157 bytes (1256 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ipv6:udp:ssdp]
[Coloring Rule Name: IPv6 hop limit low or unexpected]
0000 33 33 00 00 00 0c f8 89 d2 e7 c7 9d 86 dd 60 0e 33 ..... `.
0010 84 5f 00 67 11 04 fe 80 00 00 00 00 00 00 aa 00 ._.g ....
0020 a0 55 32 3f 31 40 ff 02 00 00 00 00 00 00 00 00 .U2?1@ ....
0030 00 00 00 00 00 0c da 4c 07 6c 00 67 54 19 4d 2d .... L .l.gT.M-
0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 5b 46 46 30 32 3a 3a 1..Host: [FF02::
0060 43 5d 3a 31 39 30 30 0d 0a 53 54 3a 20 75 70 6e C]:1900 .ST: upn
0070 70 3a 72 6f 6f 74 64 65 76 69 63 65 0d 0a 4d 61 p:rootde vice--Ma
0080 6e 3a 20 22 73 73 64 70 3a 64 69 73 63 6f 76 65 n: "ssdp :discove
0090 72 22 0d 0a 4d 58 3a 20 33 0d 0a 0d 0a r"..MX: 3....

CONCLUSION

By conducting a comprehensive security assessment, XYZ Corporation endeavors to proactively identify and address potential security gaps and vulnerabilities, fortifying its defenses against cyber threats and safeguarding its assets, data, and reputation. The insights and recommendations derived from the assessment will empower the organization to prioritize security investments, implement targeted remediation measures, and foster a culture of continuous improvement and vigilance in the face of evolving cybersecurity challenges.

References

https://www.datacenterdynamics.com/en/analysis/how-to-break-into-a-data-center-pen-testers-reveal-their-secrets/

https://plusclouds.com/blog/track-all-the-vulnerabilities-within-your-data-center-penetration-testing

https://www.prplbx.com/resources/blog/cloud-pentesting/

https://www.cloud4c.com/blogs/organizational-best-practices-penetration-testing-planning-and-documentation

https://www.hackthebox.com/blog/aws-pentesting-guide