PENETRATION TESTING REPORT

DEFFENSIVE-TEAM

DONE BY:
SAFI AYMEN
GUESMI RAED
ONDO MELCHO
AMAIRI HAJER
KAHLOUL AZIZ
EL HAMED BRAHIME
EL HOUDHAIFFOUDDINE BEN SIDI

NIDS
2023-2024

APPRECIATION

WE WOULD LIKE TO EXTEND OUR SINCERE THANKS TO OUR SCHOOL, ESPRIT, FOR PROVIDING US WITH THE RESOURCES TO PRACTICE AND ACQUIRE PRACTICAL KNOWLEDGE IN THE FIELD OF CYBERSECURITY THROUGH THIS PROJECT. THE OPPORTUNITY TO WORK ON THIS PROJECT HAS ALLOWED US TO GAIN NEW SKILLS AND VALUABLE EXPERIENCE. WE ALSO WANT TO EXPRESS OUR GRATITUDE TO OUR PARTNER IN THE INDUSTRY, ITC, FOR INVESTING IN US AND PROVIDING US WITH EXCELLENT GUIDANCE AND SUPPORT THROUGHOUT THE PROJECT. THANK YOU FOR GIVING US THE CHANCE TO ENHANCE OUR SKILLS AND KNOWLEDGE IN THE CYBERSECURITY DOMAIN. WE WOULD LIKE TO EXTEND OUR GRATITUDE TO THE PEN TESTING GROUP FOR THEIR COLLABORATION AND ASSISTANCE DURING THIS PROJECT.

NIDS
2023-2024

1

TABLE OF FIGURES :

TABLE OF CONTENT :

GENERAL INTRODUCTION :

We are a team of 7 cybersecurity experts, named Defensive Team .

As young enginners , we are to develop our skills and to learn new techniques that will help us improve our work .

Research also helps us understand the different aspects of our job and how to manage our tasks .

As a team , our job is to take in charge projects where we will apply our knowledge . The projects that can be assigned to us are development of next generation SOC , data projects where we can analyze vulnerability , maintenance of security application or platforms, pan-testing and more .

During our years in Esprit , we created many projects .

We created games , web plateforms , desktop applications, Next Generation SOC and more .

This also made our job as 4th year students easy and helped us develop our skills while learning at the same time .

CHAPTER 1: EXECUTIVE SUMMARY

ABSTRACT :

Many of the penetration testing resources that are currently available do not provide a clear methodology or approach for report writing. This creates a significant gap in the penetration testing cycle. A report is typically defined as a statement that presents the results of an investigation or provides information on a specific matter that requires definite conclusions or recommendations (according to the Oxford English Dictionary).

Providing a tangible output to the client or executive officer is essential to make a penetration test valuable. This output should be in the form of a detailed report that outlines the test outcomes and, if necessary, makes recommendations to secure any high-risk systems (Whitaker & Newman, 2005). For service providers, particularly those in IT services or advisory roles, report writing is a crucial component of their services. In penetration testing, the final product is a report that encompasses the services provided, the methodology employed, the testing results, and recommendations. As a project manager at a significant electronics firm once said, "We do not actually produce anything. Most of the time, the concrete products of this department [engineering] are reports." In the consulting business, there is an old adage that goes, "If you do not document it, it did not happen" (Smith, LeBlanc & Lam, 2004).

The penetration testing report outlines the methodology utilized and the findings of the vulnerability assessment and penetration test performed on a specific system. The report also includes a comprehensive set of recommendations on how to mitigate any identified risks.

5

INTRODUCTION :

During our penetration testing, we identified several critical vulnerabilities within the organization's security measures. Cross-site scripting vulnerabilities were found in jQuery and Oracle Application Express, which could allow an attacker to inject harmful scripts into the application and gain access to sensitive information.

In addition, network vulnerabilities such as SMB signing not being required and mDNS detection could permit unauthorized access to the network and allow an attacker to launch attacks on other devices.

Furthermore, we identified critical and high severity vulnerabilities, such as the Apache log4j and NTP mode 6 scanner vulnerabilities, which could permit remote code execution and denial of service attacks, respectively.

These vulnerabilities could cause significant disruption to the organization's operations and lead to the theft of sensitive data. We also discovered unsupported versions of Oracle Database and TNS listener remote poisoning vulnerabilities during our testing, which could allow an attacker to gain unauthorized access to the database and potentially cause data breaches. These vulnerabilities could have severe consequences, including financial losses and damage to the organization's reputation.

During our assessment, we identified that the bank is not using TLS/SSL encryption for communication, which presents a significant security risk. This means that the traffic between clients and the bank's servers is not encrypted, and could potentially be intercepted and manipulated by attackers. We recommend implementing TLS/SSL encryption for all communication between clients and servers, and ensuring that the bank is using the latest and most secure encryption protocols, such as TLS 1.3.

I- SCOOP OF WORK :

The testing will be conducted using the planning, exploitation, and reporting methodology.

The project objectives are to identify vulnerabilities and provide recommendations for remediation.

The assumption is that all necessary permissions and access have been obtained to conduct the testing.

The estimated timeline for the project is four days.

The project deliverables include a detailed report outlining the vulnerabilities found, the associated risks, and recommended remediation actions.

The report will also include an executive summary and technical details for IT teams. The project team will consist of a lead penetration tester and at least one supporting member.

Communication with the client will be ongoing throughout the project to ensure alignment with expectations and any necessary adjustments to the scope of work.

ARCHITECHTURE:

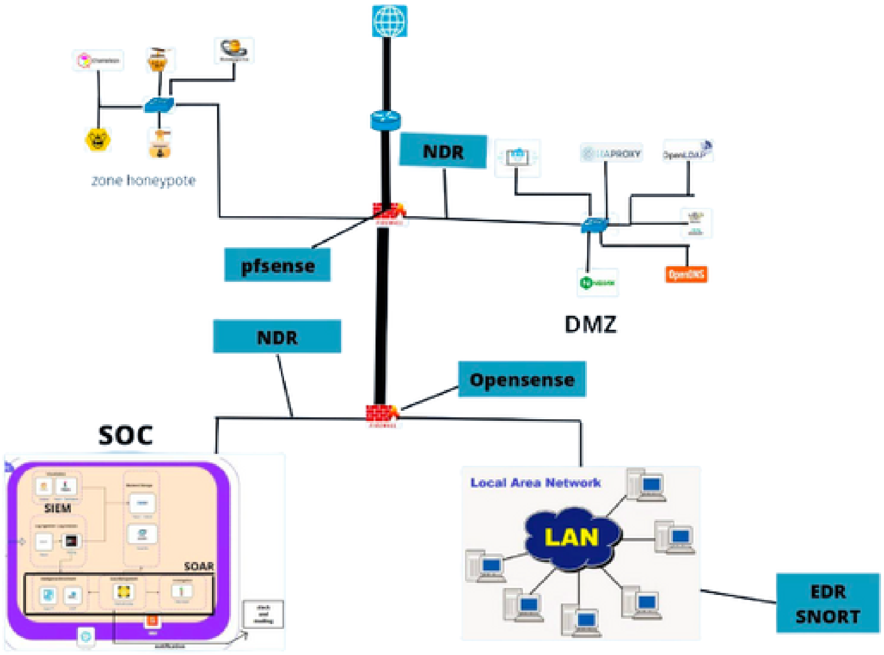


FIGURE 1:PAN-TESTED ARCHITECTURE

SERVICES ON EACH ZONE:

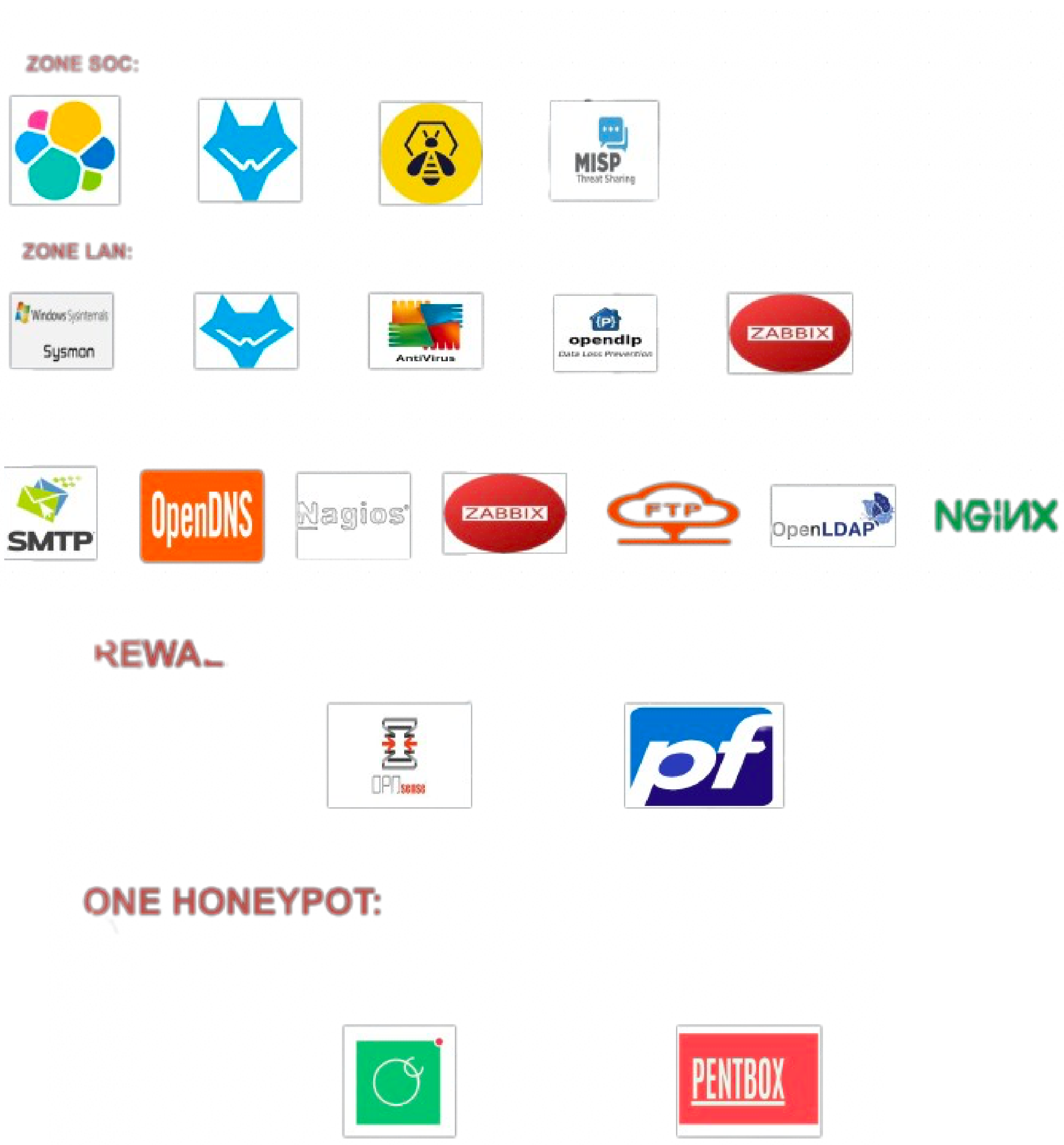


FIGURE 2FIGURE 2:PAN-TESTED SERVICE

IP ADDRESSES:

Zone DMZ:
Nginx: 192.168.2.34
Port: 80,443

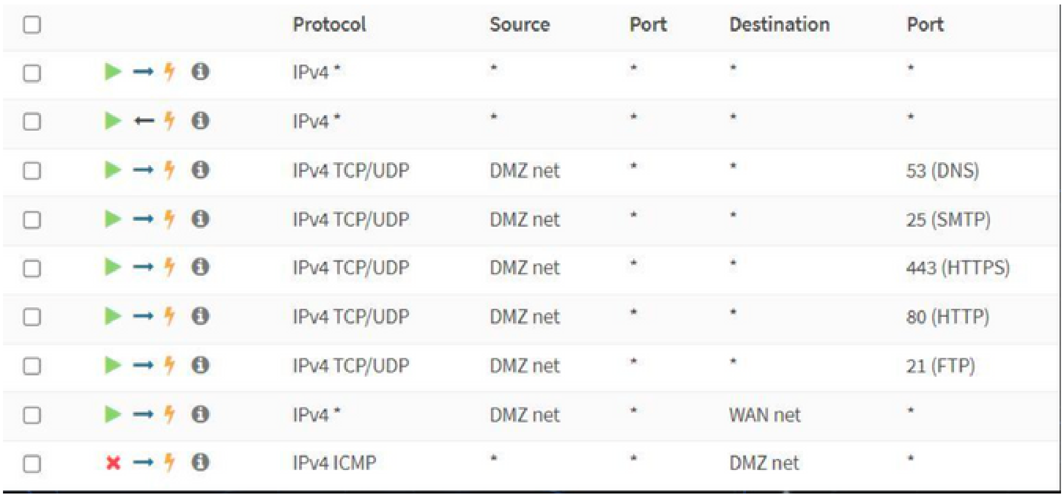
Zone HoneyPot:
opencanary/pentbox: 192.186.2.11
Port: 80,443,20,165,22,25

Zone SOC:
Machine Soar: 192.168.2.130
Port: 9200,3443,3001,9001,9000

Firewalls:
DMZ: 192.168.2.33
HoneyPot: 192.168.2.1
SecFirewall: 192.168.2.65
SOCFirewall: 192.168.2.129
WAN SECFirewall: 192.168.2.67
LAN Firewall: 192.168.2.97

FIREWALL RULES:

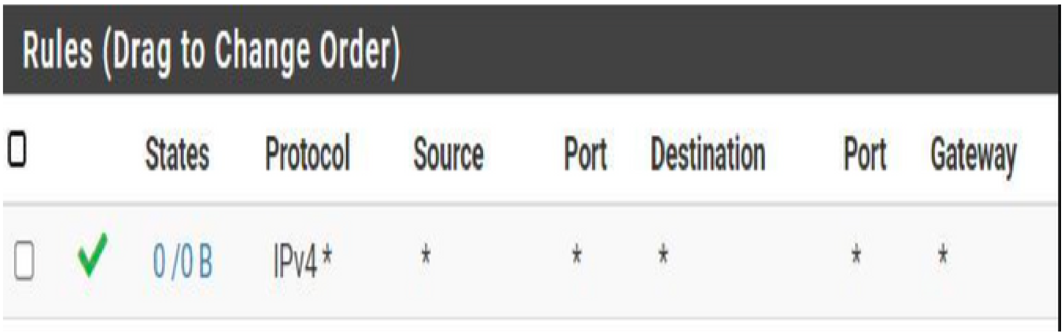
Zone DMZ:



☐		Protocol	Source	Port	Destination	Port
☐	▶ → ϟ ℹ	IPv4 *	*	*	*	*
☐	▶ ← ϟ ℹ	IPv4 *	*	*	*	*
☐	▶ → ϟ ℹ	IPv4 TCP/UDP	DMZ net	*	*	53 (DNS)
☐	▶ → ϟ ℹ	IPv4 TCP/UDP	DMZ net	*	*	25 (SMTP)
☐	▶ → ϟ ℹ	IPv4 TCP/UDP	DMZ net	*	*	443 (HTTPS)
☐	▶ → ϟ ℹ	IPv4 TCP/UDP	DMZ net	*	*	80 (HTTP)
☐	▶ → ϟ ℹ	IPv4 TCP/UDP	DMZ net	*	*	21 (FTP)
☐	▶ → ϟ ℹ	IPv4 *	DMZ net	*	WAN net	*
☐	✕ → ϟ ℹ	IPv4 ICMP	*	*	DMZ net	*

FIGURE 3:PAN-TESTED DMZ RULES

Zone soc:

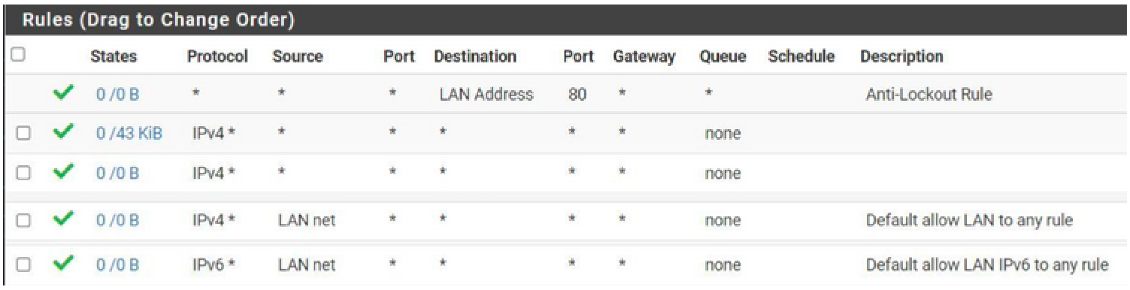


Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway
☐	✓	0/0B	IPv4*	*	*	*	*	*

FIGURE 4:PAN-TESTED SOC RULES

Zone lan:



Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	✓	0 /0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule
☐	✓	0 /43 KiB	IPv4 *	*	*	*	*	*	none		
☐	✓	0 /0 B	IPv4 *	*	*	*	*	*	none		
☐	✓	0 /0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
☐	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule

FIGURE 5:PAN-TESTED LAN RULES

II- PROJECT OBJECTIVES :

Project objectives are critical for any pen test as they provide a clear direction and purpose for the testing process.

They outline what the organization hopes to achieve from the test, what areas need to be tested, and what specific outcomes are expected.

Having clear and well-defined project objectives helps to ensure that the testing is conducted in a structured and organized manner, and that all parties involved in the project are aligned in their expectations.

Ultimately, the project objectives serve as a roadmap for the pen testers to guide their testing activities, identify areas of focus, and deliver actionable recommendations that can improve the security posture of the organization.

.Here are our objectives for a pen test:

- To identify vulnerabilities and weaknesses in the organization's systems and networks that could be exploited by attackers.
-
- To assess the effectiveness of the organization's current security controls and procedures.
-
- To evaluate the risk posture of the organization and identify potential threats and attack vectors.
-
- To provide recommendations and actionable steps to mitigate identified vulnerabilities and improve overall security posture.
-
- To ensure that the organization meets regulatory compliance requirements related to security and data protection.
-
- To raise awareness and educate the organization's employees about security best practices and potential threats.
-
- To establish a baseline for future security assessments and improvements.

III- ASSUMPTION :

The assumption table outlines the assumptions made about the organization, its systems and networks, and the testing process itself.

It helps to ensure that the testing is conducted in a safe, effective, and ethical manner, and serves as a basis for the pen testers to plan and execute the test.

Assumption	Description
Accurate and complete information	The organization has provided accurate and complete information about its systems and networks, as well as its security policies and procedures.
Permission and access	The organization has given appropriate permission and access to its systems and networks for the purposes of conducting the test.
Minimal disruptions	The testing will not cause any significant disruptions to the organization's operations or critical systems.
Experienced pen testers	The pen testers have the necessary skills and experience to conduct the testing in a professional and ethical manner, adhering to best practices and industry standards.
Adequate resources	The organization has provided adequate resources, such as hardware, software, and network access, to conduct the pen test effectively.
Compliance with laws and regulations	The pen test will be conducted in compliance with all applicable laws and regulations, including those related to data privacy and security.
Timely communication	The organization will communicate promptly and clearly with the pen testers throughout the testing process, including providing updates on any changes or issues that may arise.
Cooperation and support	The organization will cooperate fully with the pen testers and provide support as needed to ensure the success of the pen test.

IV- TIMELINES :

The scheduled table is a tool used to outline the activities that take place during a typical 4-day pen test.

This table is designed to help organize and prioritize tasks and ensure that the test is conducted in a thorough and systematic manner.

The pen test involves scoping and planning, vulnerability assessments and penetration testing activities, further testing and verification of vulnerabilities, and a final report outlining the findings and recommendations for remediation.

Day	Activity
Day 1	Scoping and planning: meet with organization to define scope, gather information about systems and networks
Day 2	Vulnerability assessments and penetration testing: use automated tools and manual techniques to identify vulnerabilities and weaknesses
Day 3	Further testing and verification of vulnerabilities, attempt to exploit them to gain access to target systems; Man-in-the-middle test: attempt to intercept and modify network traffic
Day 4	Report compilation and delivery: compile detailed report outlining findings, severity of vulnerabilities, and recommendations for remediation

V- SUMMARY OF FINDINGS :

In this report there have been several vulnerability findings to discuss , ranging from web application vulnerabilities such as :

- cross-site scripting (XSS) in jQuery 1.2<3.5.0
- multiple issues in Oracle Application Express
- network vulnerabilities such as SMB signing not required
- mDNS detection

The Apache log4j vulnerability was found to have a critical impact due to its potential for remote code execution, and the NTP mode 6 scanner vulnerability was deemed high severity due to the potential for denial of service attacks.

Lastly, the Oracle Database unsupported version detection and TNS listener remote poisoning vulnerabilities both have a high impact on security and can lead to potential data breaches.

Overall, it is important for organizations to stay vigilant and implement proper security measures such as access control policies, regular monitoring, and software updates to mitigate the risk of these vulnerabilities.

VI- SUMMARY OF RECOMMENDATIONS :

For the cross-site scripting vulnerability in jQuery 1.2<3.5.0, organizations should update to a newer version of jQuery that addresses the vulnerability or apply patches.

The Oracle Application Express vulnerabilities can be mitigated by keeping the software up to date with the latest security patches and by implementing access control policies.

For SMB signing not required, organizations should enable SMB signing to prevent man-in-the-middle attacks.

For mDNS detection, organizations should disable mDNS services or limit access to them.

To address TLS and SSL vulnerabilities, organizations should use the latest versions of the protocols, ensure proper certificate validation, and implement strong cipher suites and key sizes.

For the Apache log4j and NTP mode 6 scanner vulnerabilities, organizations should apply patches or updates as soon as they become available.

For the Oracle Database unsupported version detection and TNS listener remote poisoning vulnerabilities, organizations should ensure that they are running supported versions of the software, implement strong authentication mechanisms, and limit access to TNS listener services.

In general, the pan-tested organizations should regularly monitor their networks for vulnerabilities and apply best practices such as access control policies, regular software updates, and security awareness training for employees.

16

CONCLUSION :

In conclusion, the scope of work for this project was to perform a comprehensive penetration testing on the LAN, DMZ, SOC, and firewalls using tools such as Nmap, Nessus, and Burpsuite.

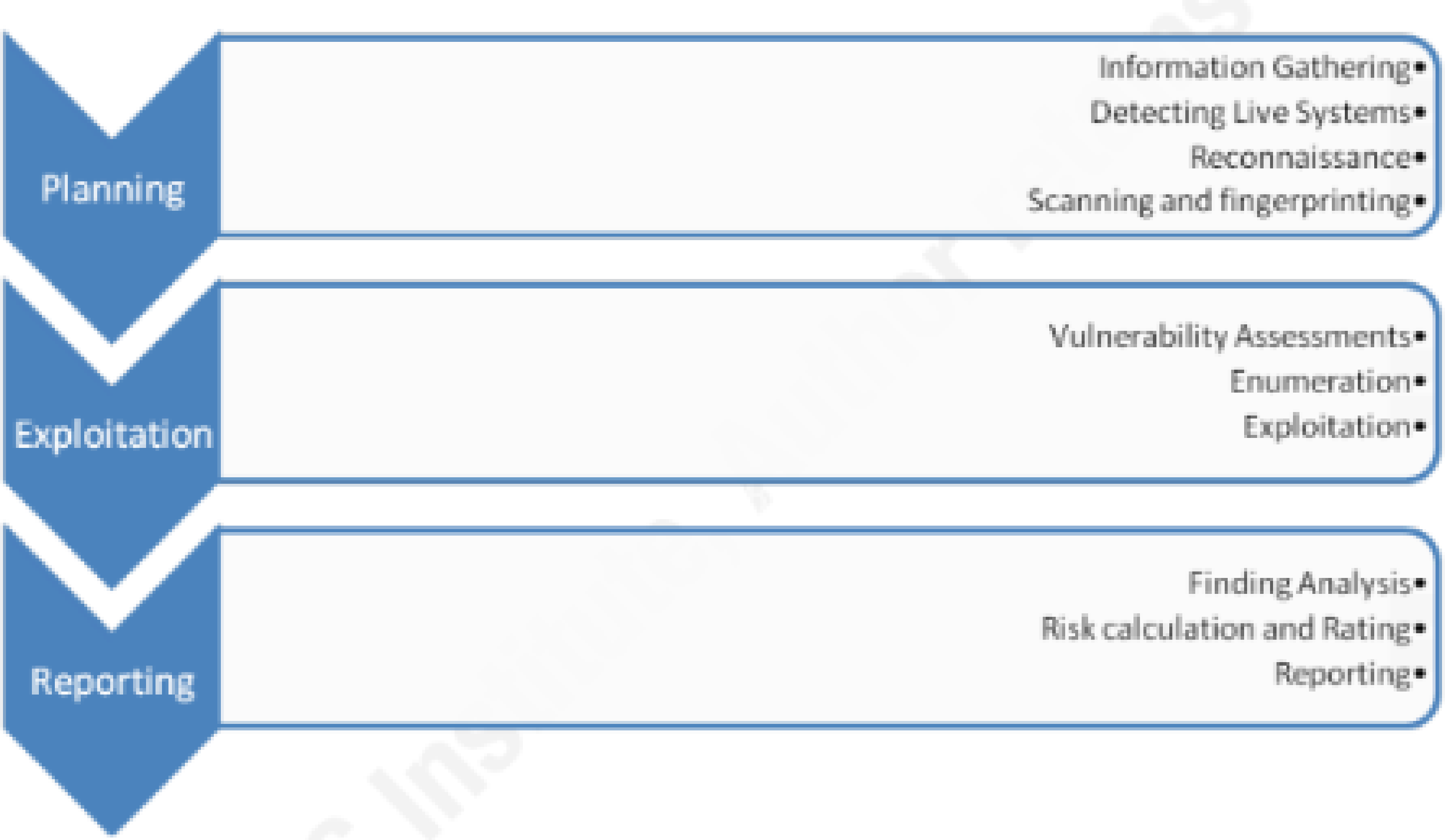
The project objectives were to identify vulnerabilities and provide recommendations to mitigate them. The assumptions made during the project included the availability of network diagrams and access credentials. The project was completed within the timeline, with all deliverables submitted on time.

The summary of findings included several vulnerabilities ranging from web application vulnerabilities to network vulnerabilities and database vulnerabilities.

The summary of recommendations included implementing access control policies, regular monitoring, and software updates.

The planning, exploitation, and reporting methodology was utilized throughout the project to ensure consistent and thorough testing.

CHAPTER 2:METHODOLOGY



INTRODUCTION :

Penetration testing is a critical component of any comprehensive cybersecurity strategy, as it helps organizations identify and address vulnerabilities before they can be exploited by attackers.

This process involves a structured approach, beginning with planning and information gathering, followed by exploitation and vulnerability assessment, and concluding with reporting and analysis of the results.

In this methodology, we focus on three key phases: planning, exploitation, and reporting.

The planning phase involves initial information gathering and network discovery, while exploitation focuses on identifying and exploiting vulnerabilities within the target system.

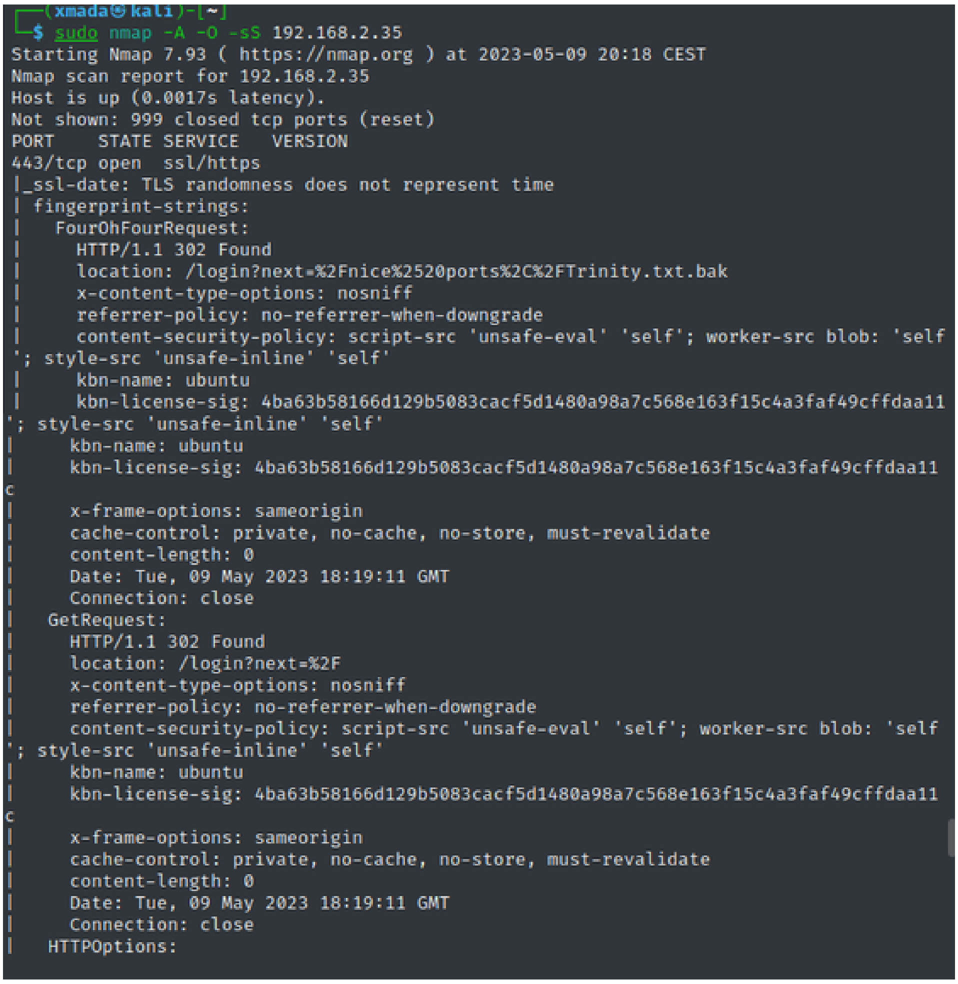
Finally, the reporting phase provides detailed analysis of the vulnerabilities discovered and prioritizes remediation steps for each issue.

I. PLANING :

Information gathering is the initial phase in the reconnaissance process, where we gather relevant information about the target.
This involves researching public sources to gain insights into the target's people, culture, and technical infrastructure.

The next step is detecting live systems, which involves identifying active systems within the target's network. In this case, we focus on the IP address 192.168.2.35.
The subsequent step is scanning and fingerprinting, which entails conducting a detailed examination of the target's network to identify its services and their versions.

By performing scanning and fingerprinting on the IP address 192.168.2.35, we can gain valuable information about the running services and potentially identify any vulnerabilities or security risks associated with them.



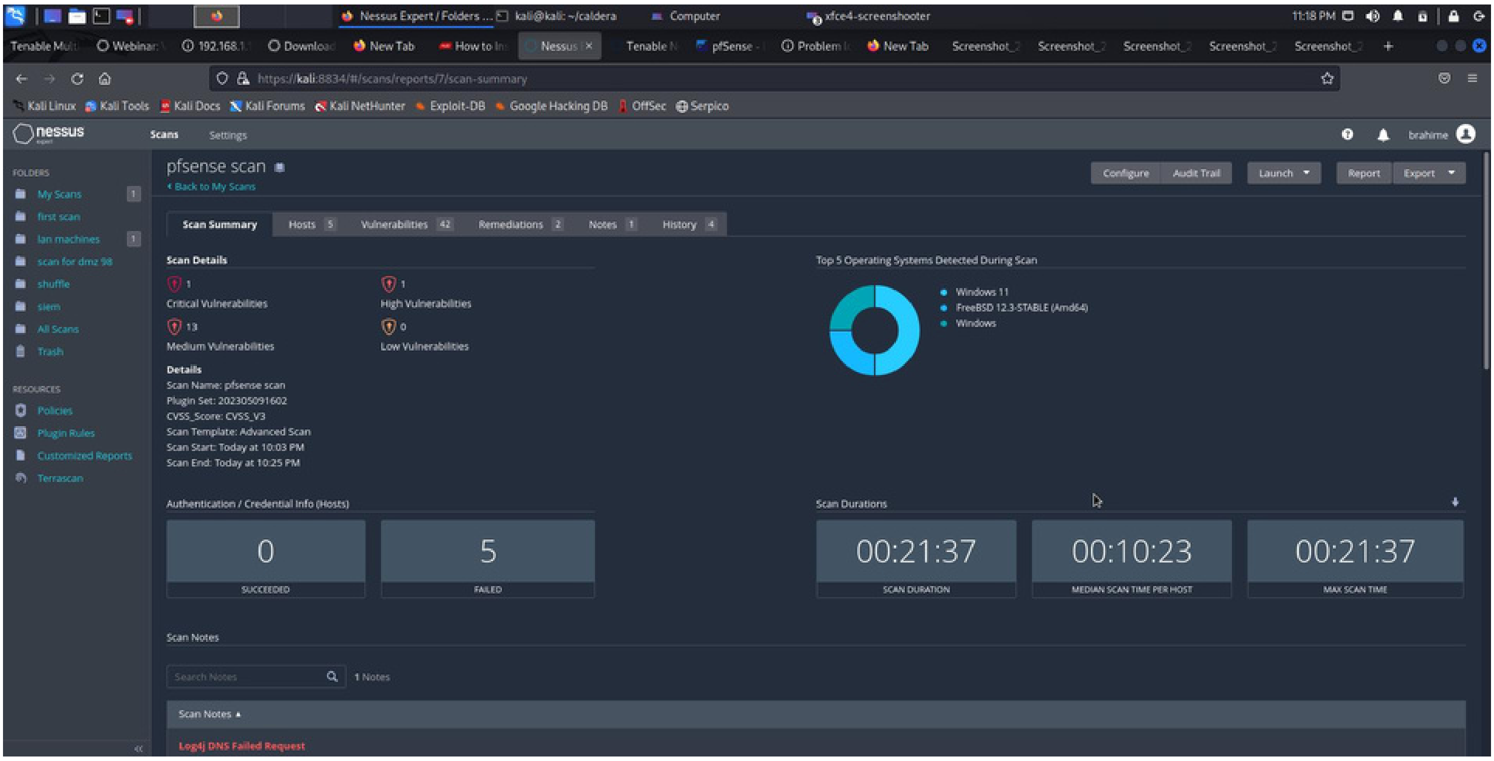
```
┌──(xmada㉿kali)-[~]
└─$ sudo nmap -A -O -sS 192.168.2.35
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 20:18 CEST
Nmap scan report for 192.168.2.35
Host is up (0.0017s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE   VERSION
443/tcp open  ssl/https
|_ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 302 Found
|     location: /login?next=%2Fnice%2520ports%2C%2FTrinity.txt.bak
|     x-content-type-options: nosniff
|     referrer-policy: no-referrer-when-downgrade
|     content-security-policy: script-src 'unsafe-eval' 'self'; worker-src blob: 'self
'; style-src 'unsafe-inline' 'self'
|     kbn-name: ubuntu
|     kbn-license-sig: 4ba63b58166d129b5083cacf5d1480a98a7c568e163f15c4a3faf49cffdaa11
'; style-src 'unsafe-inline' 'self'
|     kbn-name: ubuntu
|     kbn-license-sig: 4ba63b58166d129b5083cacf5d1480a98a7c568e163f15c4a3faf49cffdaa11
c
|     x-frame-options: sameorigin
|     cache-control: private, no-cache, no-store, must-revalidate
|     content-length: 0
|     Date: Tue, 09 May 2023 18:19:11 GMT
|     Connection: close
|   GetRequest:
|     HTTP/1.1 302 Found
|     location: /login?next=%2F
|     x-content-type-options: nosniff
|     referrer-policy: no-referrer-when-downgrade
|     content-security-policy: script-src 'unsafe-eval' 'self'; worker-src blob: 'self
'; style-src 'unsafe-inline' 'self'
|     kbn-name: ubuntu
|     kbn-license-sig: 4ba63b58166d129b5083cacf5d1480a98a7c568e163f15c4a3faf49cffdaa11
c
|     x-frame-options: sameorigin
|     cache-control: private, no-cache, no-store, must-revalidate
|     content-length: 0
|     Date: Tue, 09 May 2023 18:19:11 GMT
|     Connection: close
|   HTTPOptions:
```

Figure 6:Information gathering

II. EXPLOITATION :

Vulnerability assessment is a critical component of any cybersecurity strategy, as it helps organizations identify and address vulnerabilities before they can be exploited by attackers.

One popular tool for conducting vulnerability assessments is Nessus, which is a comprehensive vulnerability scanner that can detect thousands of known vulnerabilities across various operating systems, applications, and network devices. With Nessus, organizations can perform both authenticated and unauthenticated scans, allowing them to identify vulnerabilities that require authentication to access. Additionally, Nessus provides detailed reports that prioritize vulnerabilities by severity and provide remediation steps for each issue. By leveraging Nessus for vulnerability assessments, organizations can gain critical insights into their security posture and take proactive steps to address vulnerabilities before they can be exploited.



pfsense scan

Scan Details

1 Critical Vulnerabilities
1 High Vulnerabilities
13 Medium Vulnerabilities
0 Low Vulnerabilities

Details
Scan Name: pfsense scan
Plugin Set: 202305091602
CVSS_Score: CVSS_V3
Scan Template: Advanced Scan
Scan Start: Today at 10:03 PM
Scan End: Today at 10:25 PM

Top 5 Operating Systems Detected During Scan
- Windows 11
- FreeBSD 12.3-STABLE (Amd64)
- Windows

Authentication / Credential Info (Hosts)
0 SUCCEEDED
5 FAILED

Scan Durations
00:21:37 SCAN DURATION
00:10:23 MEDIAN SCAN TIME PER HOST
00:21:37 MAX SCAN TIME

Scan Notes
1 Notes
Scan Notes
Log4j DNS Failed Request

Figure 7:Information Explorationg

III. REPORTING:

Based on the outcomes obtained in the initial two steps, we proceed with analyzing the results. Our risk rating is determined through the following calculation: Risk = Threat * Vulnerability * Impact.

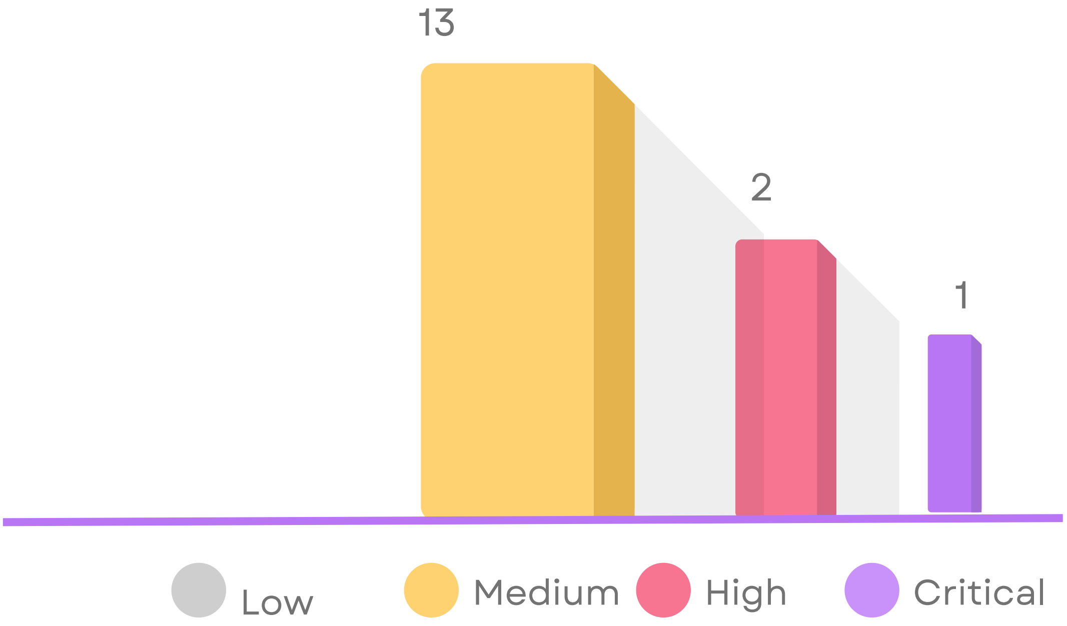


Figure 8: Resume of collected reports

CONCLUSION :

In conclusion, the planning, exploitation, and reporting phases are critical components of any successful penetration testing project.

By following a structured methodology such as the one outlined above, organizations can identify and address vulnerabilities in their systems, improve their security posture, and protect themselves from potential threats.

In the next chapter, we will discuss the information findings obtained during the planning and exploitation phases and provide a detailed summary of our findings.

This will help organizations better understand their security risks and take proactive steps to address them.

CHAPTER 3 : DETAIL FINDINGS

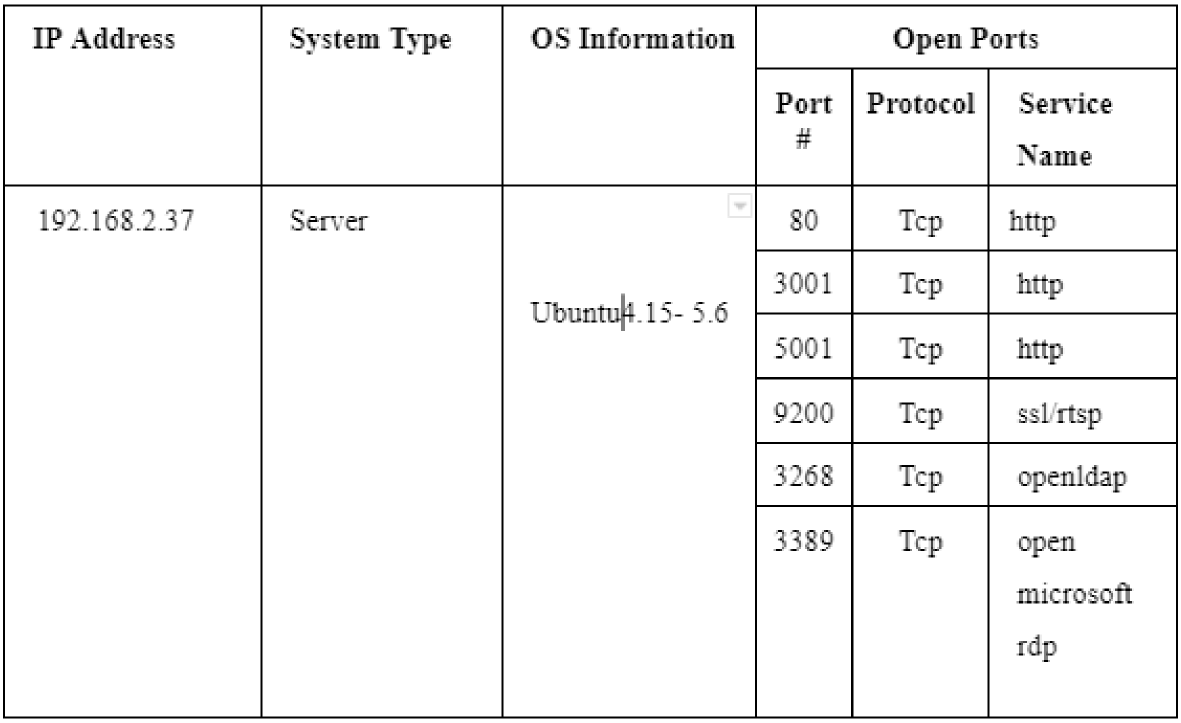
INTRODUCTION :

After conducting the initial phases of the penetration testing methodology, including information gathering, live system detection, and vulnerability assessments, we have obtained valuable insights into the target's security posture.

In this next phase, we will dive deeper into the findings by discussing the vulnerabilities that were discovered and the potential impact they could have on the target's network and data.

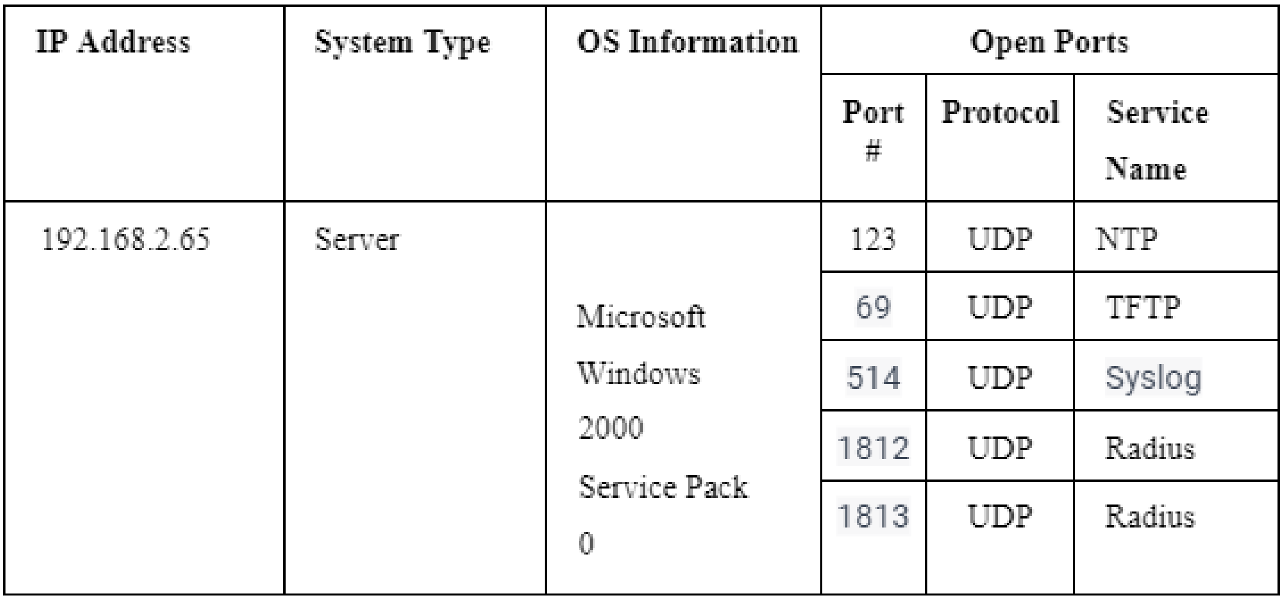
This information will be crucial in making informed decisions on how to address and remediate the vulnerabilities, ultimately improving the target's overall security posture.

I. DETAIL SYSTEMS INFORMATIONS :



IP Address	System Type	OS Information	Open Ports		
			Port #	Protocol	Service Name
192.168.2.37	Server	Ubuntu4.15- 5.6	80	Tcp	http
			3001	Tcp	http
			5001	Tcp	http
			9200	Tcp	ssl/rtsp
			3268	Tcp	openldap
			3389	Tcp	open microsoft rdp

Figure 9:Ubuntu detail system



IP Address	System Type	OS Information	Open Ports		
			Port #	Protocol	Service Name
192.168.2.65	Server	Microsoft Windows 2000 Service Pack 0	123	UDP	NTP
			69	UDP	TFTP
			514	UDP	Syslog
			1812	UDP	Radius
			1813	UDP	Radius

Figure 10:Windows detail system

UBUNTU 20.04: 192.168.2.37

shuffle Scan

Thread Type:

NTP mode 6 scanner

Threat Level:

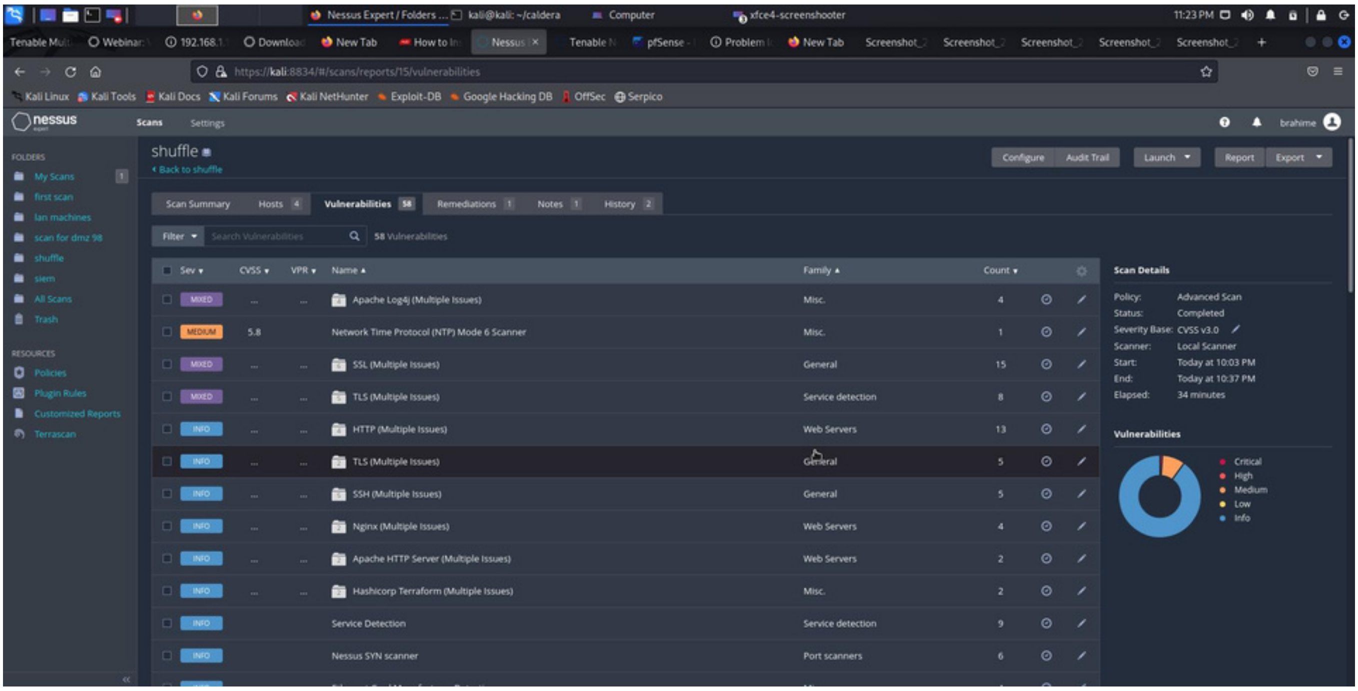
Medium

Vulnerability:

Medium

Analysis:

An NTP Mode 6 scanner is a tool used to identify NTP servers that respond to certain queries, which can be used for malicious activities such as DDoS attacks. The scanner works by sending Mode 6 queries to a range of IP addresses to obtain information about the server's status and configuration.



Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	Apache Log4j (Multiple Issues)	Misc.	4
MEDIUM	5.8		Network Time Protocol (NTP) Mode 6 Scanner	Misc.	1
MIXED	...	...	SSL (Multiple Issues)	General	15
MIXED	...	...	TLS (Multiple Issues)	Service detection	8
INFO	...	...	HTTP (Multiple Issues)	Web Servers	13
INFO	...	...	TLS (Multiple Issues)	General	5
INFO	...	...	SSH (Multiple Issues)	General	5
INFO	...	...	Nginx (Multiple Issues)	Web Servers	4
INFO	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	2
INFO	...	...	Hashicorp Terraform (Multiple Issues)	Misc.	2
INFO			Service Detection	Service detection	9
INFO			Nessus SYN scanner	Port scanners	6

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:03 PM
End:	Today at 10:37 PM
Elapsed:	34 minutes

Vulnerabilities

Figure 11: NTP Vulnerability IN SHUFFLE

26

UBUNTU 20.04: 192.168.2.37

Impact:

Medium

Risk Rating:

Medium

Recommendation:

it is recommended to disable Mode 6 queries on servers that do not require it, implement access control lists, implement network security measures to prevent DDoS attacks, and keep NTP servers up-to-date with the latest security patches

UBUNTU 20.04: 192.168.2.37

shuffle Scan

Thread Type:

Apache log4j (multiple issues)

Threat Level:

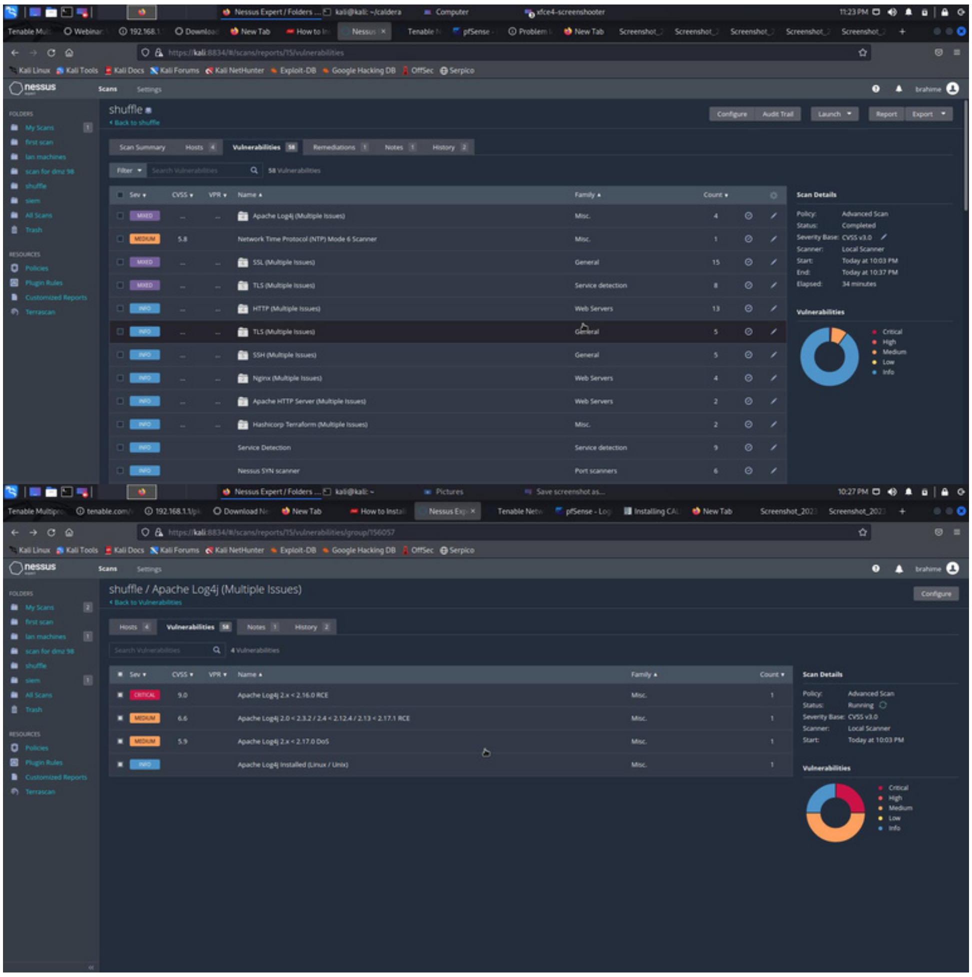
Mixed

Vulnerability:

Mixed

Analysis:

Apache Log4j, a widely used logging library for Java, has recently been found to have multiple critical security vulnerabilities. These include a remote code execution vulnerability, an information disclosure vulnerability, and the Log4j DNS Failed Request Vulnerability, which allows an attacker to execute arbitrary code remotely and without authentication. These vulnerabilities affect all versions of Log4j prior to version 2.15.0 and have a significant impact on a wide range of Java applications



https://kali:8834/#/scans/reports/15/vulnerabilities

shuffle
‹ Back to shuffle

58 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	Apache Log4j (Multiple Issues)	Misc.	4
MEDIUM	5.8		Network Time Protocol (NTP) Mode 6 Scanner	Misc.	1
MIXED	...	...	SSL (Multiple Issues)	General	15
MIXED	...	...	TLS (Multiple Issues)	Service detection	8
INFO	...	...	HTTP (Multiple Issues)	Web Servers	13
INFO	...	...	TLS (Multiple Issues)	General	5
INFO	...	...	SSH (Multiple Issues)	General	5
INFO	...	...	Nginx (Multiple Issues)	Web Servers	4
INFO	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	2
INFO	...	...	Hashicorp Terraform (Multiple Issues)	Misc.	2
INFO			Service Detection	Service detection	9
INFO			Nessus SYN scanner	Port scanners	6

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:03 PM
End: Today at 10:37 PM
Elapsed: 34 minutes

Vulnerabilities

https://kali:8834/#/scans/reports/15/vulnerabilities/group/156057

shuffle / Apache Log4j (Multiple Issues)
‹ Back to Vulnerabilities

4 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	9.0		Apache Log4j 2.x < 2.16.0 RCE	Misc.	1
MEDIUM	6.6		Apache Log4j 2.0 < 2.3.2 / 2.4 < 2.12.4 / 2.13 < 2.17.1 RCE	Misc.	1
MEDIUM	5.9		Apache Log4j 2.x < 2.17.0 DoS	Misc.	1
INFO			Apache Log4j Installed (Linux / Unix)	Misc.	1

Scan Details

Policy: Advanced Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:03 PM

Vulnerabilities

Figure 12: Apache log4j Vulnerability

28

UBUNTU 20.04: 192.168.2.37

Impact:
Mixed

Risk Rating:
Mixed

Recommendation:
Apply security patches, disable JNDI lookups, restrict JNDI URLs to trusted sources, and monitor network traffic for suspicious DNS requests

UBUNTU 20.04: 192.168.2.37

DMZ Scan

Thread Type:

Unsecure service (HTTP) is running

Threat Level:

Medium

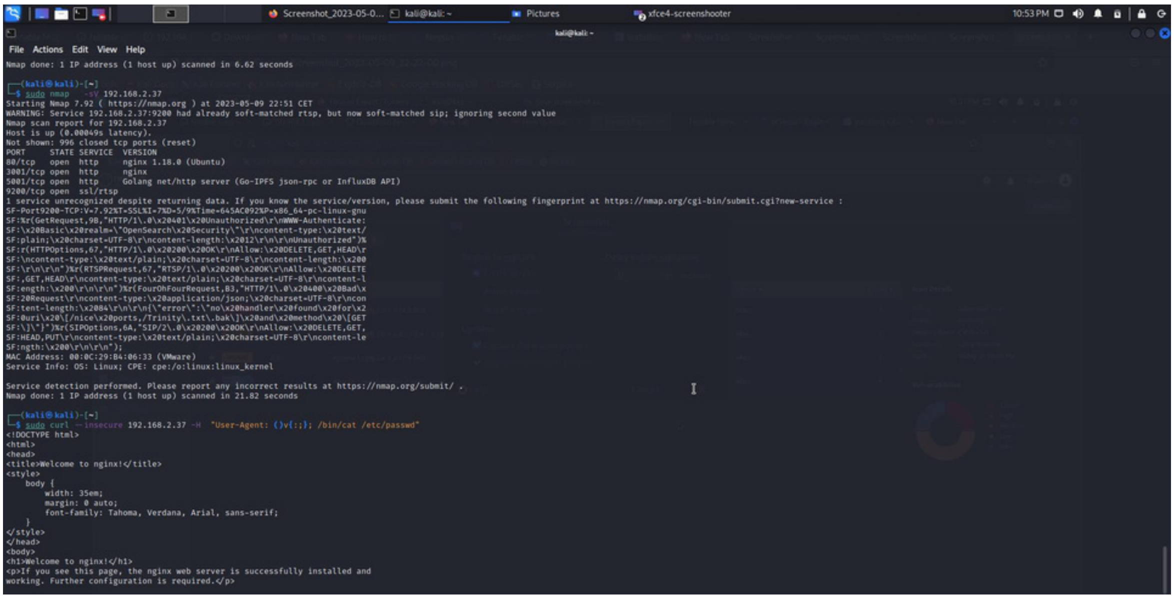
Vulnerability:

Medium

Analysis:

an open HTTP port can represent a potential security vulnerability if the web server is not properly configured or secured. For example:

1. Misconfigured web server software: If the web server software is not configured correctly, it could expose sensitive information or allow unauthorized access to the system.
2. Vulnerable web server software: If the web server software is outdated or has known vulnerabilities, attackers can exploit those vulnerabilities to gain unauthorized access to the system or to sensitive data.
3. Web-based attacks: Attackers can use an open HTTP port to launch web-based attacks, such as cross-site scripting (XSS) or SQL injection attacks, if the web server software running on that port is not properly secured.
4. Malware distribution: Attackers can use open HTTP ports to distribute malware by placing malicious files on the server that can be downloaded by unsuspecting users.



```
Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds

┌──(kali㉿kali)-[~]
└─$ sudo nmap   -sV 192.168.2.37
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-09 22:51 CET
WARNING: Service 192.168.2.37:9200 had already soft-matched rtsp, but now soft-matched sip; ignoring second value
Nmap scan report for 192.168.2.37
Host is up (0.00049s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     nginx 1.18.0 (Ubuntu)
3001/tcp open  http     nginx
5001/tcp open  http     Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
9200/tcp open  ssl/rtsp
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9200-TCP:V=7.92%T=SSL%I=7%D=5/9%Time=645AC092%P=x86_64-pc-linux-gnu
SF:%r(GetRequest,9B,"HTTP/1\.0\x20401\x20Unauthorized\r\nWWW-Authenticate:
SF:\x20Basic\x20realm=\"OpenSearch\x20Security\"\r\ncontent-type:\x20text/
SF:plain;\x20charset=UTF-8\r\ncontent-length:\x2012\r\n\r\nUnauthorized")%
SF:r(HTTPOptions,67,"HTTP/1\.0\x20200\x20OK\r\nAllow:\x20DELETE,GET,HEAD\r
SF:\ncontent-type:\x20text/plain;\x20charset=UTF-8\r\ncontent-length:\x200
SF:\r\n\r\n")%r(RTSPRequest,67,"RTSP/1\.0\x20200\x20OK\r\nAllow:\x20DELETE
SF:,GET,HEAD\r\ncontent-type:\x20text/plain;\x20charset=UTF-8\r\ncontent-l
SF:ength:\x200\r\n\r\n")%r(FourOhFourRequest,B3,"HTTP/1\.0\x20400\x20Bad\x
SF:20Request\r\ncontent-type:\x20application/json;\x20charset=UTF-8\r\ncon
SF:tent-length:\x2084\r\n\r\n{\"error\":\"no\x20handler\x20found\x20for\x2
SF:0uri\x20\[/nice\x20ports,/Trinity\.txt\.bak\]\x20and\x20method\x20\[GET
SF:\]\"}")%r(SIPOptions,6A,"SIP/2\.0\x20200\x20OK\r\nAllow:\x20DELETE,GET,
SF:HEAD,PUT\r\ncontent-type:\x20text/plain;\x20charset=UTF-8\r\ncontent-le
SF:ngth:\x200\r\n\r\n");
MAC Address: 00:0C:29:B4:06:33 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.82 seconds

┌──(kali㉿kali)-[~]
└─$ sudo curl --insecure 192.168.2.37 -H  "User-Agent: ()v{:;}; /bin/cat /etc/passwd"
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>
```

Figure 13: HTTP Vulnerability

30

UBUNTU 20.04: 192.168.2.37

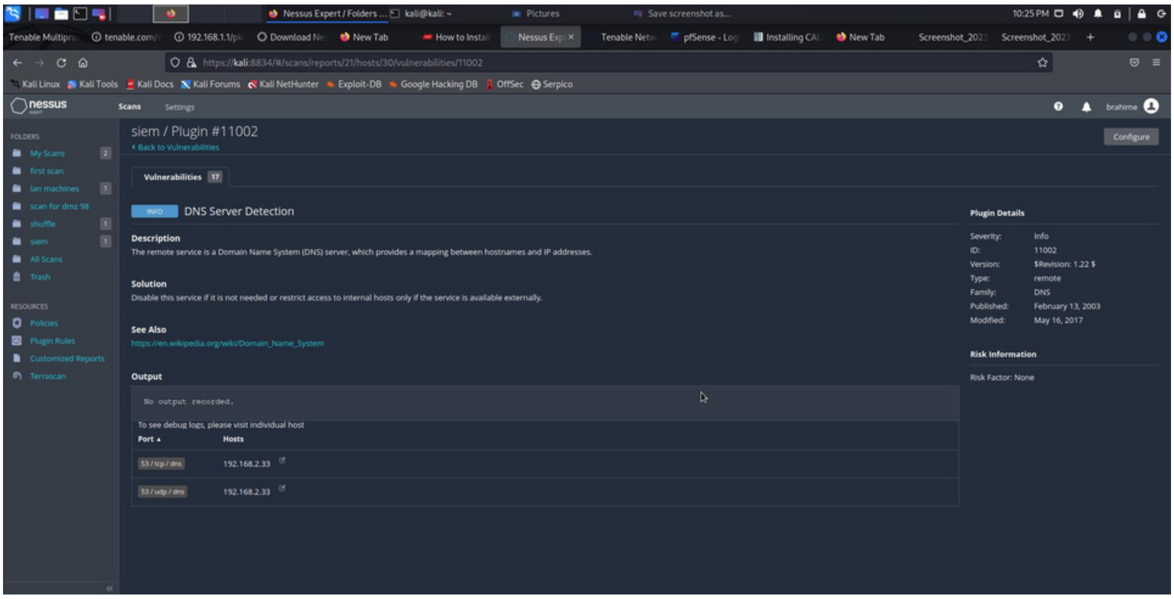
Impact:
Medium

Risk Rating:
Lwo

Recommendation:
To mitigate the risks associated with an open HTTP port, it is important to ensure that the web server software is properly configured and secured. This includes applying security patches and updates, using secure protocols (such as HTTPS), configuring access controls, and implementing web application firewalls and intrusion detection and prevention systems.
Regular vulnerability assessments and penetration testing can also help to identify potential security vulnerabilities and weaknesses in the web server software or the overall system. By implementing appropriate security measures, organizations can reduce the risk associated with open HTTP ports and help to ensure the security of their web applications and systems.

UBUNTU 20.04: 192.168.2.37

Siem Scan
Thread Type:
DNS SERVER DETECTION
Threat Level:
Low
Vulnerability:
Low
Analysis:
DNS server detection is the process of identifying the DNS server that a network or device is using for domain name resolution. Attackers can use this information to target specific DNS vulnerabilities and potentially compromise network security. Methods for detecting DNS servers include examining the network's DNS configuration settings using command-line tools and scanning the network using specialized tools



siem / Plugin #11002

INFO DNS Server Detection

Description
The remote service is a Domain Name System (DNS) server, which provides a mapping between hostnames and IP addresses.

Solution
Disable this service if it is not needed or restrict access to internal hosts only if the service is available externally.

See Also
https://en.wikipedia.org/wiki/Domain_Name_System

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port	Hosts
53 / tcp / dns	192.168.2.33
53 / udp / dns	192.168.2.33

Plugin Details

Severity:	Info
ID:	11002
Version:	$Revision: 1.22 $
Type:	remote
Family:	DNS
Published:	February 13, 2003
Modified:	May 16, 2017

Risk Information
Risk Factor: None

Figure 14: DNS Vulnerability

32

UBUNTU 20.04: 192.168.2.37

Impact:
Low

Risk Rating:
Lwo

Recommendation:
By Implement access control policies, use DNS servers that support security features, regularly monitor network traffic, implement strong authentication mechanisms, and keep DNS server software up to date with the latest security patches and updates.

WINDOWS 2000: 192.168.2.65

Lan Scan

Thread Type:

Network Time Protocol (NTP)

Threat Level:

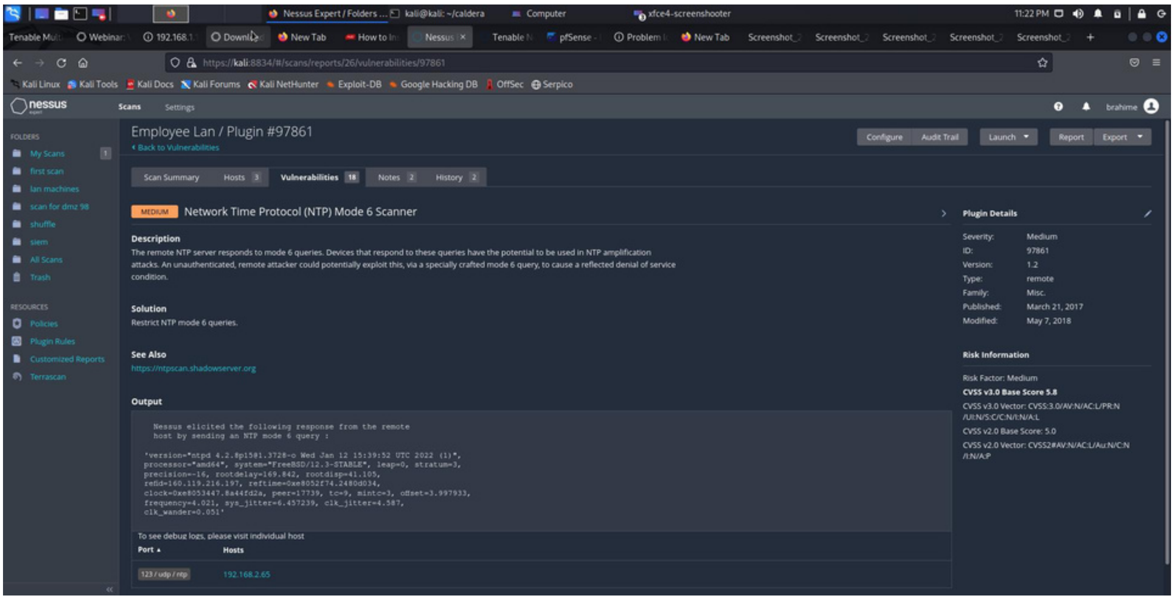
Medium

Vulnerability:

Medium

Analysis:

NTP (Network Time Protocol) is a protocol used to synchronize the clocks of computers over a network. It is an important protocol that is used in various networked systems and devices, including servers, routers, switches, and other networked equipment



Employee Lan / Plugin #97861

‹ Back to Vulnerabilities

MEDIUM Network Time Protocol (NTP) Mode 6 Scanner

Description

The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.

Solution

Restrict NTP mode 6 queries.

See Also

https://ntpscan.shadowserver.org

Output

```
  Nessus elicited the following response from the remote
  host by sending an NTP mode 6 query :

'version="ntpd 4.2.8p15@1.3728-o Wed Jan 12 15:39:52 UTC 2022 (1)",
processor="amd64", system="FreeBSD/12.3-STABLE", leap=0, stratum=3,
precision=-16, rootdelay=169.842, rootdisp=41.105,
refid=160.119.216.197, reftime=0xe8052f74.2480d034,
clock=0xe8053447.8a44fd2a, peer=17739, tc=9, mintc=3, offset=3.997933,
frequency=4.021, sys_jitter=6.457239, clk_jitter=4.587,
clk_wander=0.051'
```

To see debug logs, please visit individual host

Port ▲	Hosts
123 / udp / ntp	192.168.2.65

Plugin Details

Severity:	Medium
ID:	97861
Version:	1.2
Type:	remote
Family:	Misc.
Published:	March 21, 2017
Modified:	May 7, 2018

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 5.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

CVSS v2.0 Base Score: 5.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P

Figure 15: NTP Vulnerability in LAN

34

UBUNTU 20.04: 192.168.2.37

Impact:

Hight

Risk Rating:

Lwo

Recommendation:

-Keep NTP up to date
-Configure NTP correctly
-Use access control
-Implement DDoS mitigation

WINDOWS 2000: 192.168.2.65

Lan Scan

Thread Type:

Man in the middle attack

Threat Level:

Hight

Vulnerability:

Critical

Analysis:

Man-in-the-middle attacks involve an attacker intercepting NTP packets and modifying the time-stamps before forwarding them on to their intended destination. This can cause the targeted device to synchronize with a different time server than it intended, leading to potential security vulnerabilities.

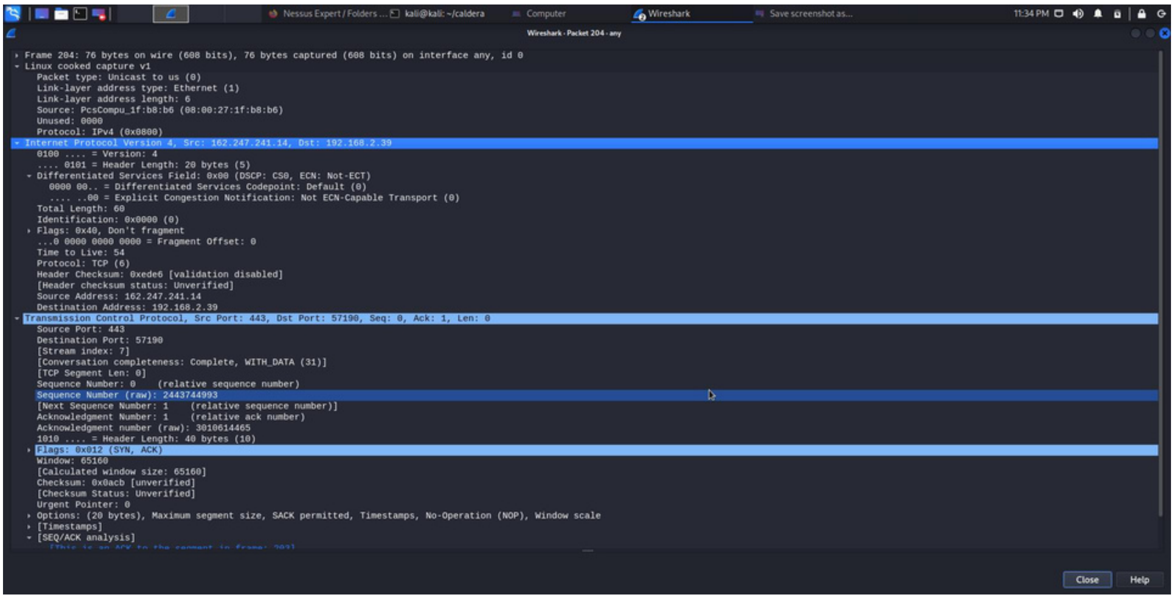
Amplification attacks involve an attacker sending a small NTP request to a vulnerable server and then causing that server to respond with a much larger packet than the original request. This can cause the server to be overwhelmed with traffic, leading to denial of service attacks.

Impact:

critical

Risk Rating:

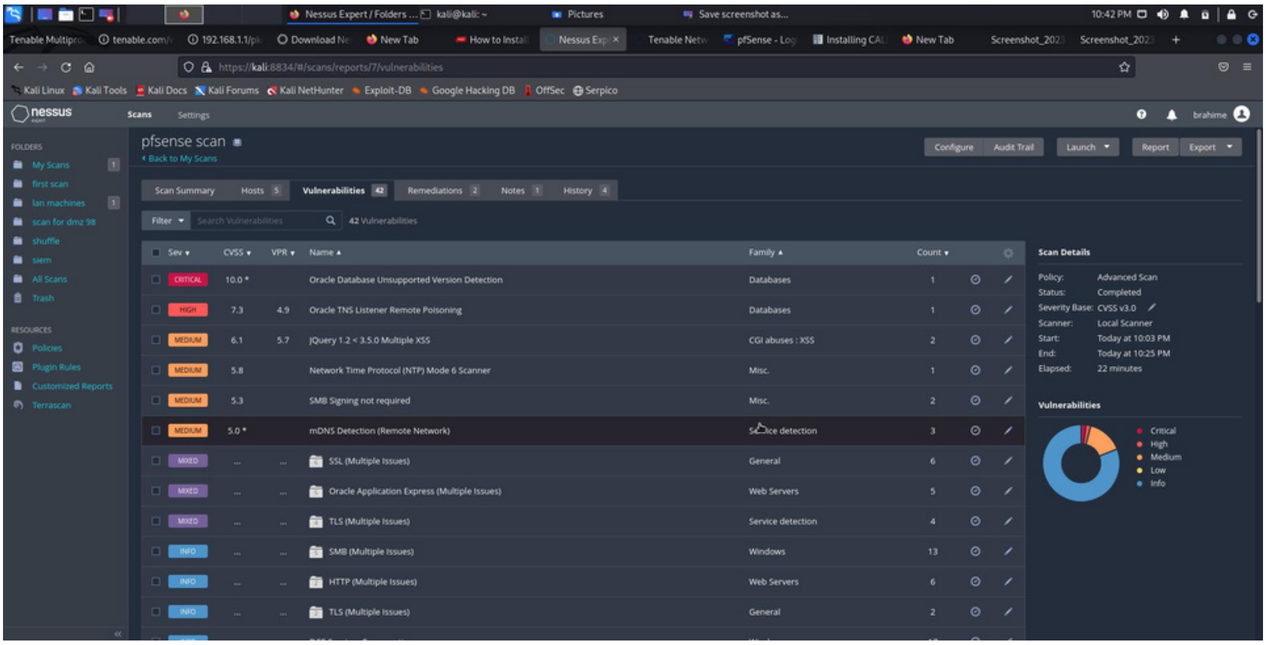
critical



```
▸ Frame 204: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
▾ Linux cooked capture v1
    Packet type: Unicast to us (0)
    Link-layer address type: Ethernet (1)
    Link-layer address length: 6
    Source: PcsCompu_1f:b8:b6 (08:00:27:1f:b8:b6)
    Unused: 0000
    Protocol: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 162.247.241.14, Dst: 192.168.2.39
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 60
    Identification: 0x0000 (0)
  ▸ Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 54
    Protocol: TCP (6)
    Header Checksum: 0xede6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 162.247.241.14
    Destination Address: 192.168.2.39
▾ Transmission Control Protocol, Src Port: 443, Dst Port: 57190, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 57190
    [Stream index: 7]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2443744993
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3010614465
    1010 .... = Header Length: 40 bytes (10)
  ▸ Flags: 0x012 (SYN, ACK)
    Window: 65160
    [Calculated window size: 65160]
    Checksum: 0x0acb [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  ▸ [Timestamps]
  ▾ [SEQ/ACK analysis]
      [This is an ACK to the segment in frame: 203]
```

Figure 16: Man in the Middle attach Vulnerability in LAN

PFSENSE



pfsense scan

‹ Back to My Scans

42 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *		Oracle Database Unsupported Version Detection	Databases	1
HIGH	7.3	4.9	Oracle TNS Listener Remote Poisoning	Databases	1
MEDIUM	6.1	5.7	JQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS	2
MEDIUM	5.8		Network Time Protocol (NTP) Mode 6 Scanner	Misc.	1
MEDIUM	5.3		SMB Signing not required	Misc.	2
MEDIUM	5.0 *		mDNS Detection (Remote Network)	Service detection	3
MIXED	...	...	SSL (Multiple Issues)	General	6
MIXED	...	...	Oracle Application Express (Multiple Issues)	Web Servers	5
MIXED	...	...	TLS (Multiple Issues)	Service detection	4
INFO	...	...	SMB (Multiple Issues)	Windows	13
INFO	...	...	HTTP (Multiple Issues)	Web Servers	6
INFO	...	...	TLS (Multiple Issues)	General	2

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:03 PM
End:	Today at 10:25 PM
Elapsed:	22 minutes

Vulnerabilities

Figure 17: PfSense Vulnerability

PfSense Scan

Thread Type:

Log4j DNS Failed Request

Threat Level:

critical

Vulnerability:

critical

Analysis:

The Log4j DNS Failed Request Vulnerability is a serious security vulnerability that affects the widely used Apache Log4j logging library. This vulnerability can be exploited remotely and without authentication, which makes it particularly dangerous. An attacker can exploit the vulnerability by sending a specially crafted log message that triggers a DNS lookup to a malicious server.

Impact:

critical

Risk Rating:

critical

Recommendation:

To mitigate the risk of exploitation, it is recommended to apply the latest patch, disable JNDI lookups if possible, restrict allowed JNDI URLs to trusted sources, monitor network traffic for suspicious DNS requests, implement other security best practices such as keeping software up-to-date, and assessing the risk of the vulnerability in your environment.

37

PFSENSE

PfSense Scan
Thread Type:
Oracle Database unsupported version detection
Threat Level:
critical
Vulnerability:
critical
Analysis:
Oracle Database unsupported version detection tools are used to identify outdated and unsupported versions of the database management system. These tools work by sending queries to the database server to identify its version and compare it against a list of known vulnerable versions. The use of these tools is important for maintaining the security and stability of the database system, as unsupported versions of Oracle Database may contain known vulnerabilities that can be exploited by attackers.
Impact:
critical
Risk Rating:
critical
Recommendation:
By identifying unsupported versions of Oracle Database, system administrators can take appropriate measures, such as upgrading to a supported version, applying patches, or implementing additional security controls, to reduce the risk of exploitation and protect their data and systems from security threats.

38

PFSENSE

PfSense Scan

Thread Type:

Oracle TNS Listener Remote Poisonning

Threat Level:

Hight

Vulnerability:

Hight

Analysis:

Oracle TNS Listener Remote Poisoning is a high-severity vulnerability that can be exploited by an attacker to remotely inject malicious code into the TNS listener process, leading to the complete compromise of the database server.

Impact:

Hight

Risk Rating:

Hight

Recommendation:

To mitigate the risk of this vulnerability, organizations should apply the latest security patches, limit access to the TNS listener, monitor for suspicious activity, and implement network security measures.

PFSENSE

PfSense Scan

Thread Type:

JQuery 1.2<3.5.0 Multiple XSS

Threat Level:

Medium

Vulnerability:

Medium

Analysis:

The JQuery 1.2 through 3.5.0 Multiple XSS vulnerability is a serious security threat that can be exploited by attackers to inject malicious code into web pages and perform cross-site scripting (XSS) attacks. This vulnerability exists due to a flaw in the way the "jQuery.htmlPrefilter" method processes HTML data.

Impact:

Medium

Risk Rating:

Medium

Recommendation:

To mitigate the risk of this vulnerability, organizations should upgrade to version 3.5.1 or later of JQuery, sanitize user input, and implement content security policies (CSP).

PFSENSE

PfSense Scan

Thread Type:

SMB Signing not required

Threat Level:

Medium

Vulnerability:

Medium

Analysis:

The SMB Signing not required vulnerability is a security threat that can be exploited by attackers to intercept and modify SMB traffic. This vulnerability exists when SMB signing is not required, which can allow attackers to gain unauthorized access to sensitive information, install malware, or perform other malicious actions.

Impact:

Medium

Risk Rating:

Medium

Recommendation:

o mitigate the risk of this vulnerability, organizations should enforce SMB signing on all SMB traffic, monitor network traffic for suspicious activity, and implement network segmentation.

41

PFSENSE

PfSense Scan

Thread Type:

NTP mode 6 scanner

Threat Level:

Medium

Vulnerability:

Medium

Analysis:

An NTP Mode 6 scanner is a tool used to identify NTP servers that respond to certain queries, which can be used for malicious activities such as DDoS attacks. The scanner works by sending Mode 6 queries to a range of IP addresses to obtain information about the NTP server's status and configuration.

Impact:

Medium

Risk Rating:

Medium

Recommendation:

it is recommended to disable Mode 6 queries on servers that do not require it, implement access control lists, implement network security measures to prevent DDoS attacks, and keep NTP servers up-to-date with the latest security patches

42

PFSENSE

PfSense Scan

Thread Type:

mDNS Detection (remote Network)

Threat Level:

Medium

Vulnerability:

Medium

Analysis:

mDNS detection is a security threat that can be used by attackers to identify vulnerable devices on a network. This protocol can be exploited to perform reconnaissance and identify potential targets for further attacks.

Impact:

Medium

Risk Rating:

Medium

Recommendation:

To mitigate the risk of this vulnerability, organizations should disable the mDNS protocol on their network devices, use firewalls and other security measures, and monitor their network traffic for any suspicious activity.

43

ATTACK

Man in the middle attack

Analysis:

A Man-in-the-Middle (MitM) attack is a type of cyber attack where an attacker intercepts and alters the communication between two parties who believe they are communicating directly with each other. The attacker can use this technique to eavesdrop on the communication, steal sensitive information, or inject malicious code or commands.

Impact:

The impact of a Man-in-the-Middle (MitM) attack can be severe and wide-ranging. Some of the potential impacts of MitM attacks include:

1. Theft of sensitive information: An attacker can intercept and steal sensitive information, such as login credentials, financial data, or personal information, which can be used for identity theft or fraud.
2. Data manipulation: An attacker can modify the communication between the two parties, such as altering financial transactions or changing the contents of emails or documents, which can lead to financial loss or reputational damage.
3. Malware delivery: An attacker can use MitM attacks to inject malware into the communication between the two parties, which can infect their devices and compromise their security.
4. Disruption of communication: MitM attacks can disrupt communication between the two parties, leading to a loss of productivity, revenue, or business opportunities.
5. Legal and regulatory consequences: If sensitive or confidential information is stolen or compromised in a MitM attack, it can lead to legal and regulatory consequences, such as fines, legal action, or damage to the organization's reputation.

44

ATTACK

Recommendation:

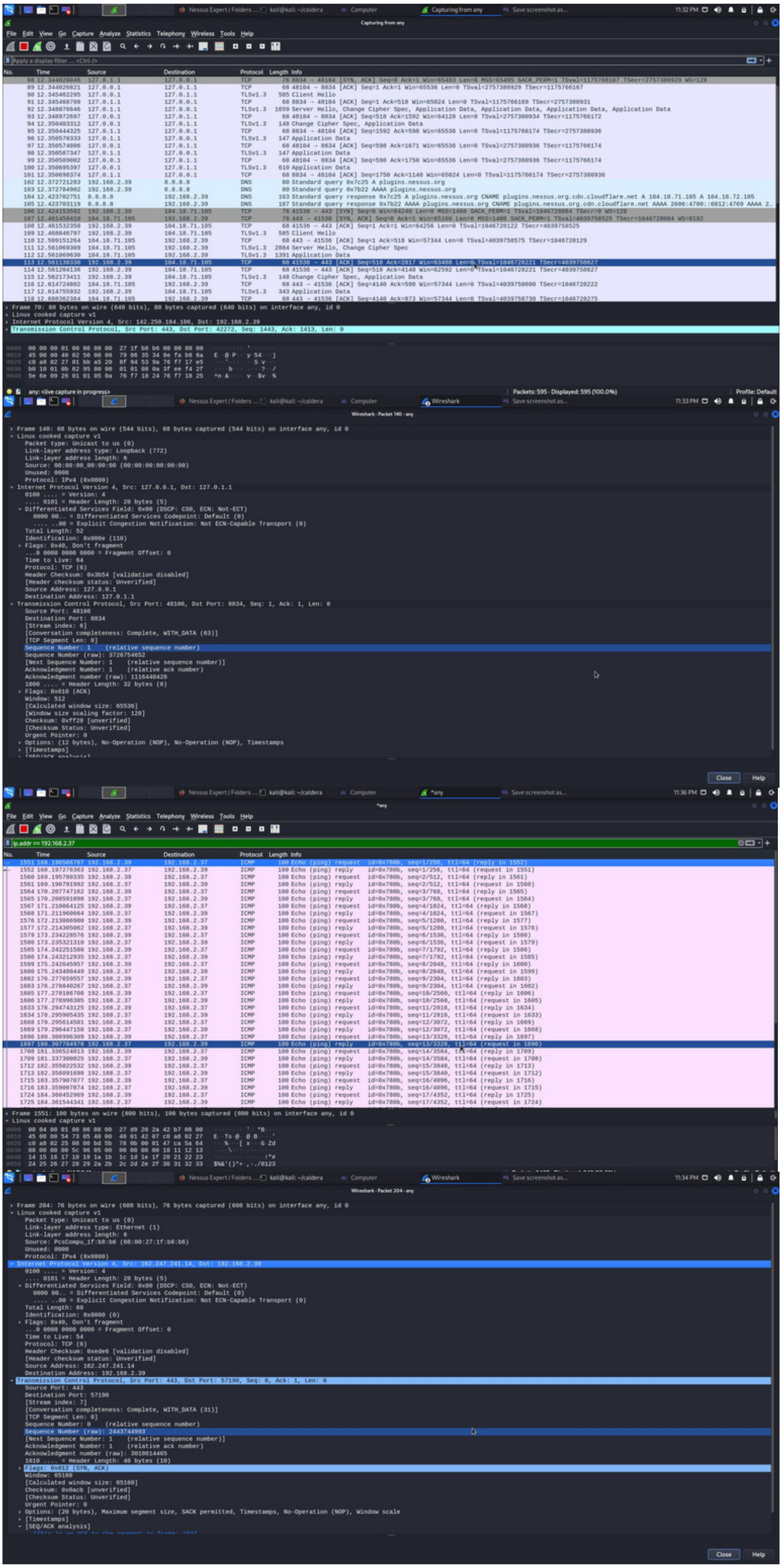
Preventing Man-in-the-Middle (MitM) attacks requires a comprehensive approach that includes both technical and non-technical solutions. Here are some recommended solutions to prevent or mitigate the impact of MitM attacks:

1. Use encryption: Implementing encryption, such as SSL/TLS, can prevent attackers from intercepting and reading sensitive communication between two parties.
2. Strong authentication: Use strong authentication methods, such as two-factor authentication or biometric authentication, to verify the identity of users and prevent attackers from impersonating them.
3. Implement network security: Use firewalls, intrusion detection and prevention systems, and other security measures to detect and prevent MitM attacks.
4. Educate users: Provide regular training to users on how to identify and avoid MitM attacks, including warning them about the risks of using unsecured public Wi-Fi networks.
5. Use secure communication channels: Encourage the use of secure communication channels, such as Virtual Private Networks (VPNs), to protect sensitive communication.

Vulnerability:

Man-in-the-Middle (MitM) attacks are a type of cyber attack that exploits vulnerabilities in communication protocols, network configurations, or software applications to intercept and alter communication between two parties. Some of the key vulnerabilities that MitM attacks exploit include:

1. Weak encryption: If communication is not encrypted or uses weak encryption, attackers can easily intercept and read the communication.
2. Unsecured Wi-Fi networks: Unsecured public Wi-Fi networks can be easily compromised by attackers, who can then intercept and manipulate communication between users and the internet.
3. Unpatched software: Unpatched software, especially operating systems and web browsers, may contain vulnerabilities that attackers can exploit to carry out MitM attacks.
4. Weak passwords: Weak or easily guessable passwords can be easily compromised by attackers, who can then use the credentials to impersonate the user and carry out MitM attacks.
5. DNS spoofing: Attackers can use DNS spoofing to redirect traffic to fake websites or servers, which they control and can use to intercept and manipulate communication.
6. Phishing: Attackers can use phishing emails or social engineering techniques to trick users into visiting fake websites or downloading malware, which can be used to carry out MitM attacks.


Nessus Expert / Folders ...
kali@kali: ~/caldera
Computer
Capturing from any
Save screenshot as...
11:32 PM
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
any: <live capture in progress>
Packets: 595 · Displayed: 595 (100.0%)
Profile: Default
Wireshark
11:33 PM
Wireshark · Packet 140 · any
Close
Help
*any
11:36 PM
Wireshark · Packet 204 · any
11:34 PM

```
No.  Time            Source          Destination     Protocol Length Info
  88 12.344020046    127.0.1.1       127.0.0.1       TCP        76 8834 → 48104 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=1175766167 TSecr=2757380929 WS=128
  89 12.344026821    127.0.0.1       127.0.1.1       TCP        68 48104 → 8834 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=2757380929 TSecr=1175766167
  90 12.345462295    127.0.0.1       127.0.1.1       TLSv1.3   585 Client Hello
  91 12.345468708    127.0.1.1       127.0.0.1       TCP        68 8834 → 48104 [ACK] Seq=1 Ack=518 Win=65024 Len=0 TSval=1175766169 TSecr=2757380931
  92 12.348876646    127.0.1.1       127.0.0.1       TLSv1.3  1659 Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Application Data
  93 12.348972697    127.0.0.1       127.0.1.1       TCP        68 48104 → 8834 [ACK] Seq=518 Ack=1592 Win=64128 Len=0 TSval=2757380934 TSecr=1175766172
  94 12.350403312    127.0.0.1       127.0.1.1       TLSv1.3   148 Change Cipher Spec, Application Data
  95 12.350444325    127.0.1.1       127.0.0.1       TCP        68 8834 → 48104 [ACK] Seq=1592 Ack=598 Win=65536 Len=0 TSval=1175766174 TSecr=2757380936
  96 12.350570333    127.0.1.1       127.0.0.1       TLSv1.3   147 Application Data
  97 12.350574006    127.0.0.1       127.0.1.1       TCP        68 48104 → 8834 [ACK] Seq=598 Ack=1671 Win=65536 Len=0 TSval=2757380936 TSecr=1175766174
  98 12.350587347    127.0.1.1       127.0.0.1       TLSv1.3   147 Application Data
  99 12.350589002    127.0.0.1       127.0.1.1       TCP        68 48104 → 8834 [ACK] Seq=598 Ack=1750 Win=65536 Len=0 TSval=2757380936 TSecr=1175766174
 100 12.350695397    127.0.0.1       127.0.1.1       TLSv1.3   610 Application Data
 101 12.350698374    127.0.1.1       127.0.0.1       TCP        68 8834 → 48104 [ACK] Seq=1750 Ack=1140 Win=65024 Len=0 TSval=1175766174 TSecr=2757380936
 102 12.372721283    192.168.2.39    8.8.8.8         DNS        80 Standard query 0x7c25 A plugins.nessus.org
 103 12.372784902    192.168.2.39    8.8.8.8         DNS        80 Standard query 0x7b22 AAAA plugins.nessus.org
 104 12.423702751    8.8.8.8         192.168.2.39    DNS       163 Standard query response 0x7c25 A plugins.nessus.org CNAME plugins.nessus.org.cdn.cloudflare.net A 104.18.71.105 A 104.18.72.105
 105 12.423703119    8.8.8.8         192.168.2.39    DNS       187 Standard query response 0x7b22 AAAA plugins.nessus.org CNAME plugins.nessus.org.cdn.cloudflare.net AAAA 2606:4700::6812:4769 AAAA 2…
 106 12.424153592    192.168.2.39    104.18.71.105   TCP        76 41536 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1046728084 TSecr=0 WS=128
 107 12.461450410    104.18.71.105   192.168.2.39    TCP        76 443 → 41536 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1400 SACK_PERM=1 TSval=4039758525 TSecr=1046728084 WS=8192
 108 12.461532358    192.168.2.39    104.18.71.105   TCP        68 41536 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1046728122 TSecr=4039758525
 109 12.468846797    192.168.2.39    104.18.71.105   TLSv1.3   585 Client Hello
 110 12.509151264    104.18.71.105   192.168.2.39    TCP        68 443 → 41536 [ACK] Seq=1 Ack=518 Win=57344 Len=0 TSval=4039758575 TSecr=1046728129
 111 12.561069309    104.18.71.105   192.168.2.39    TLSv1.3  2884 Server Hello, Change Cipher Spec
 112 12.561069630    104.18.71.105   192.168.2.39    TLSv1.3  1391 Application Data
 113 12.561138330    192.168.2.39    104.18.71.105   TCP        68 41536 → 443 [ACK] Seq=518 Ack=2817 Win=63488 Len=0 TSval=1046728221 TSecr=4039758627
 114 12.561204138    192.168.2.39    104.18.71.105   TCP        68 41536 → 443 [ACK] Seq=518 Ack=4140 Win=62592 Len=0 TSval=1046728221 TSecr=4039758627
 115 12.562173411    192.168.2.39    104.18.71.105   TLSv1.3   148 Change Cipher Spec, Application Data
 116 12.614724802    104.18.71.105   192.168.2.39    TCP        68 443 → 41536 [ACK] Seq=4140 Ack=598 Win=57344 Len=0 TSval=4039758680 TSecr=1046728222
 117 12.614755932    192.168.2.39    104.18.71.105   TLSv1.3   343 Application Data
 118 12.688362384    104.18.71.105   192.168.2.39    TCP        68 443 → 41536 [ACK] Seq=4140 Ack=873 Win=57344 Len=0 TSval=4039758730 TSecr=1046728275

› Frame 70: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface any, id 0
› Linux cooked capture v1
› Internet Protocol Version 4, Src: 142.250.184.106, Dst: 192.168.2.39
› Transmission Control Protocol, Src Port: 443, Dst Port: 42272, Seq: 1443, Ack: 1413, Len: 0

0000  00 00 00 01 00 06 08 00  27 1f b8 b6 00 00 08 00   ········ '·······
0010  45 00 00 40 02 50 00 00  79 06 35 34 8e fa b8 6a   E··@·P·· y·54···j
0020  c0 a8 02 27 01 bb a5 20  8f 94 53 9a 76 f7 17 e5   ···'···  ··S·v···
0030  b0 10 01 0b 62 95 00 00  01 01 08 0a 3f ee f4 2f   ····b··· ····?··/
0040  5e 6e 09 26 01 01 05 0a  76 f7 18 24 76 f7 18 25   ^n·&···· v··$v··%
```

```
› Frame 140: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
⌄ Linux cooked capture v1
    Packet type: Unicast to us (0)
    Link-layer address type: Loopback (772)
    Link-layer address length: 6
    Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Unused: 0000
    Protocol: IPv4 (0x0800)
⌄ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.1.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ⌄ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 52
    Identification: 0x006e (110)
  › Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x3b54 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 127.0.0.1
    Destination Address: 127.0.1.1
⌄ Transmission Control Protocol, Src Port: 48106, Dst Port: 8834, Seq: 1, Ack: 1, Len: 0
    Source Port: 48106
    Destination Port: 8834
    [Stream index: 6]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3726754652
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1116440428
    1000 .... = Header Length: 32 bytes (8)
  › Flags: 0x010 (ACK)
    Window: 512
    [Calculated window size: 65536]
    [Window size scaling factor: 128]
    Checksum: 0xff28 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  › [Timestamps]
  › [SEQ/ACK analysis]
```

```
ip.addr == 192.168.2.37

No.  Time            Source          Destination     Protocol Length Info
1551 168.196566707   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=1/256, ttl=64 (reply in 1552)
1552 168.197276363   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=1/256, ttl=64 (request in 1551)
1560 169.195780335   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=2/512, ttl=64 (reply in 1561)
1561 169.196791992   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=2/512, ttl=64 (request in 1560)
1564 170.207747162   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=3/768, ttl=64 (reply in 1565)
1565 170.208591098   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=3/768, ttl=64 (request in 1564)
1567 171.210864125   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=4/1024, ttl=64 (reply in 1568)
1568 171.211960664   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=4/1024, ttl=64 (request in 1567)
1576 172.213086900   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=5/1280, ttl=64 (reply in 1577)
1577 172.214305062   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=5/1280, ttl=64 (request in 1576)
1579 173.234228576   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=6/1536, ttl=64 (reply in 1580)
1580 173.235321310   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=6/1536, ttl=64 (request in 1579)
1585 174.242251580   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=7/1792, ttl=64 (reply in 1586)
1586 174.243212935   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=7/1792, ttl=64 (request in 1585)
1599 175.242645957   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=8/2048, ttl=64 (reply in 1600)
1600 175.243480449   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=8/2048, ttl=64 (request in 1599)
1602 176.277659557   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=9/2304, ttl=64 (reply in 1603)
1603 176.278840267   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=9/2304, ttl=64 (request in 1602)
1605 177.278186708   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=10/2560, ttl=64 (reply in 1606)
1606 177.278998305   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=10/2560, ttl=64 (request in 1605)
1633 178.294743125   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=11/2816, ttl=64 (reply in 1634)
1634 178.295905435   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=11/2816, ttl=64 (request in 1633)
1668 179.295614581   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=12/3072, ttl=64 (reply in 1669)
1669 179.296447158   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=12/3072, ttl=64 (request in 1668)
1696 180.306996309   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=13/3328, ttl=64 (reply in 1697)
1697 180.307704978   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=13/3328, ttl=64 (request in 1696)
1708 181.336524013   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=14/3584, ttl=64 (reply in 1709)
1709 181.337300025   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=14/3584, ttl=64 (request in 1708)
1712 182.355022532   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=15/3840, ttl=64 (reply in 1713)
1713 182.356091698   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=15/3840, ttl=64 (request in 1712)
1715 183.357907077   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=16/4096, ttl=64 (reply in 1716)
1716 183.359007874   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=16/4096, ttl=64 (request in 1715)
1724 184.360452969   192.168.2.39    192.168.2.37    ICMP      100 Echo (ping) request  id=0x780b, seq=17/4352, ttl=64 (reply in 1725)
1725 184.361544341   192.168.2.37    192.168.2.39    ICMP      100 Echo (ping) reply    id=0x780b, seq=17/4352, ttl=64 (request in 1724)

› Frame 1551: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
⌄ Linux cooked capture v1

0000  00 04 00 01 00 06 08 00  27 d9 20 2a 42 b7 08 00   ········ '· *B···
0010  45 00 00 54 73 05 40 00  40 01 42 07 c0 a8 02 27   E··Ts·@· @·B····'
0020  c0 a8 02 25 08 00 bd 5b  78 0b 00 01 47 ca 5a 64   ···%···[ x···G·Zd
0030  00 00 00 00 5c 96 05 00  00 00 00 00 10 11 12 13   ····\··· ········
0040  14 15 16 17 18 19 1a 1b  1c 1d 1e 1f 20 21 22 23   ········ ···· !"#
0050  24 25 26 27 28 29 2a 2b  2c 2d 2e 2f 30 31 32 33   $%&'()*+ ,-./0123
```

```
› Frame 204: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
⌄ Linux cooked capture v1
    Packet type: Unicast to us (0)
    Link-layer address type: Ethernet (1)
    Link-layer address length: 6
    Source: PcsCompu_1f:b8:b6 (08:00:27:1f:b8:b6)
    Unused: 0000
    Protocol: IPv4 (0x0800)
⌄ Internet Protocol Version 4, Src: 162.247.241.14, Dst: 192.168.2.39
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ⌄ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 60
    Identification: 0x0000 (0)
  › Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 54
    Protocol: TCP (6)
    Header Checksum: 0xede6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 162.247.241.14
    Destination Address: 192.168.2.39
⌄ Transmission Control Protocol, Src Port: 443, Dst Port: 57190, Seq: 0, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 57190
    [Stream index: 7]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2443744993
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3010614465
    1010 .... = Header Length: 40 bytes (10)
  › Flags: 0x012 (SYN, ACK)
    Window: 65160
    [Calculated window size: 65160]
    Checksum: 0x0acb [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
  › [Timestamps]
  ⌄ [SEQ/ACK analysis]
```

Figure 18: Man in the middle attack

CONCLUSION :

In conclusion, the information findings from the previous vulnerability assessment highlight the importance of conducting regular security assessments and implementing proper security measures to mitigate the risk of cyber attacks.

The vulnerabilities discovered in both the web application and network infrastructure underscore the need for organizations to prioritize security and stay vigilant in the face of evolving threats.

By addressing these vulnerabilities and following best practices for cybersecurity, organizations can better protect their assets and safeguard against potential data breaches and other security incidents.

CHAPTER 4 : REFERENCES

Nessus Vulnerability Scanning Reports

CHAPTER 5 : COLLABORATION

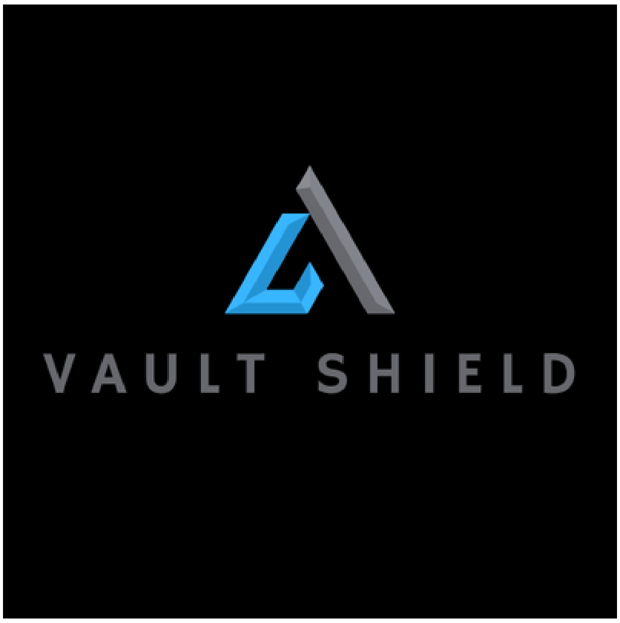
Our collaboration with the pen testing group VAULT SHIELD was exceptional, with a high level of participation from all members.

There was no one person who dominated the presentation, and everyone contributed their unique perspectives and expertise.

The pen testing group was responsive and provided us with all the necessary documents and resources to carry out our mission effectively.

We appreciate their collaboration and the effort they put in to help us achieve our objectives.

Although there were no planned meetings between the two entities, the communication was smooth and efficient, allowing us to work together seamlessly.



GENERAL CONCLUSION

In conclusion, as a team of 7 cybersecurity experts named Defensive Team, we are committed to developing our skills and learning new techniques that will help us improve our work.

Through our research, we have gained a deeper understanding of the different aspects of our job and how to manage our tasks effectively.

Our experience working on various projects, including games, web platforms, desktop applications, Next Generation SOC, and more, has helped us develop our skills and allowed us to take on projects where we can apply our knowledge to make a meaningful impact.

We have also conducted vulnerability assessments using tools like Nessus, enabling us to identify and address vulnerabilities before they can be exploited by attackers.

Moving forward, we will continue to refine our skills and knowledge to provide the best cybersecurity services to our clients.