EXTION INFOTECH CYBERSECURITY INTERNSHIP

PROJECT-1

Detecting security vulnerabilities of network and systems in EMPIRE LUPINONE CTF lie Box.(Vulnhub)

Difficulty : Medium to Hard.

Installed OpenVAS using package manager in ubuntu.

Commands :

sudo apt install openvas

sudo gvm-setup

sudo gvm-start

```
[*] Creating extension uuid-ossp
could not change directory to "/home/jorge": Permission denied
CREATE EXTENSION
could not change directory to "/home/jorge": Permission denied

[*] Creating extension pgcrypto
could not change directory to "/home/jorge": Permission denied
CREATE EXTENSION
could not change directory to "/home/jorge": Permission denied

[*] Creating extension pg-gvm
could not change directory to "/home/jorge": Permission denied
CREATE EXTENSION
[>] Migrating database
[>] Checking for GVM admin user
[*] Creating user admin for gvm
[*] Please note the generated admin password
[*] User created with password '2cd0259c-1862-4693-aa18-0974752000f0'.
[*] Configure Feed Import Owner
could not change directory to "/home/jorge": Permission denied
[*] Define Feed Import Owner
[>] Updating GVM feeds
[*] Updating NVT (Network Vulnerability Tests feed from Greenbone Security Fe
ed/Community Feed)
```

Set up the GVM and NVT configuration in browser.

It starts the OpenVAS services too.

https://localhost:9392

Configuration > Targets

and open with credentials generated by the kali linux CLI.

Provide IP addresses and Hostnames of the target.

Hostname : Empie-luimpone

For ip address : sudo netdiscover.

Get the ip address.

Go to Scans > Tasks

Create a new task name it Lumipone and selsect previous target machine that was saved in Targets.

Set configuration setup - > Full and deep and schedule – weekly.

LAUNCH SCAN.

CRITICAL VULNERABILITIES OBSERVED :

1.) **Remote Code Execution :**

Remote Code Execution (RCE) is a critical vulnerability that allows an attacker to execute arbitrary code on a target system from a remote location. This type of vulnerability is highly dangerous as it can lead to full system compromise. Attackers exploit RCE vulnerabilities by injecting malicious payloads into the application.

a) **CVE-2021-44228: Apache Log4j RCE (Log4Shell)**

- **Severity**: Critical (CVSS 10.0)
- **Description**: This vulnerability in Apache Log4j allows unauthenticated attackers to execute arbitrary code on the server by sending crafted log messages containing malicious JNDI lookups.
- **Affected Systems**: Applications using vulnerable versions of Log4j
- **Assessment**:
    - **OpenVAS Detection**: The scan identifies vulnerable Log4j versions and highlights the risk of RCE through JNDI lookups.

- **Verification**: Check application logs and configurations for log4j-core versions within the vulnerable range.
- **Exploit Testing**: Use tools like Metasploit or manual payloads to confirm exploitation potential

b.) OpenSSL Infinite Loop :

- Severity: High (CVSS 9.1)
- Description: A vulnerability in OpenSSL allows a maliciously crafted certificate to trigger an infinite loop, causing denial of service (DoS).
- Affected Systems: Systems using OpenSSL versions

c.) PrintNightmare (Windows Print Spooler)

- Severity: Critical (CVSS 8.8)
- Description: A vulnerability in the Windows Print Spooler service allows attackers to execute arbitrary code remotely.
- Affected Systems: Windows systems with Print Spooler enabled.

d) Microsoft MSDT (Follina)

- Severity: Critical (CVSS 7.8)
- Description: A flaw in the Microsoft Support Diagnostic Tool (MSDT) allows attackers to execute arbitrary commands via crafted Office documents.
- Affected Systems: Windows systems with MSDT enabled.

e) Netlogon Elevation of Privilege (Zerologon)

- Severity: Critical (CVSS 10.0)
- Description: A vulnerability in the Netlogon protocol allows attackers to escalate privileges to domain administrator.
- Affected Systems: Windows Server versions prior to August 2020 updates.

2. CVE-2021-34473: Microsoft Exchange Server (ProxyShell)

Severity: Critical (CVSS 9.8)

Description: This vulnerability in Microsoft Exchange Server allows attackers to bypass authentication and execute arbitrary commands. It affects the Microsoft Exchange Autodiscover feature, which is used for email configuration.

Affected Systems:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

Dependencies:

1. Exchange Web Services (EWS) enabled.
2. Autodiscover service exposed to the internet.

Mitigation:

- Patch: Apply the security updates provided by Microsoft for Exchange Server.
- Disable Autodiscover: If not needed, disable the Autodiscover feature in Exchange.
- Restrict EWS Access: Limit access to the EWS endpoint to only trusted IP addresses.

3. CVE-2021-22972: VMware vCenter Server (vSphere)

Severity: Critical (CVSS 9.8)

Description: A vulnerability in VMware vCenter Server allows an attacker to execute arbitrary commands with elevated privileges via a maliciously crafted request. This is due to improper input validation in the vSphere Client.

Affected Systems:

- VMware vCenter Server 6.7.x
- VMware vCenter Server 7.0.x

Dependencies:

1. vSphere Client enabled.
2. User permissions configured to allow elevated privileges.

Mitigation:

- Patch: Upgrade to VMware vCenter Server 6.7.0b or 7.0.2b.
- Limit User Privileges: Ensure that only authorized users have elevated privileges within the vSphere Client.
- Disable Unnecessary Services: Disable the vSphere Client if it is not required.

4. CVE-2021-31207: Microsoft Windows DNS Server (DNS Cache Poisoning)

Severity: Critical (CVSS 9.8)

Description: This vulnerability allows attackers to poison the DNS cache on affected Windows DNS servers, potentially redirecting traffic to malicious websites or servers.

Affected Systems:

- Windows Server 2019

Dependencies:

1. DNS server role installed and running.
2. Unrestricted DNS queries from external sources.

Mitigation:

- Patch: Apply the latest security updates from Microsoft for DNS Server.
- Restrict External Queries: Limit DNS query access to trusted internal networks.
- Enable DNSSEC: Implement DNS Security Extensions (DNSSEC) to mitigate cache poisoning risks.

5. CVE-2021-22005: VMware vCenter Server (File Upload Vulnerability)

Severity: Critical (CVSS 9.8)

Description: A vulnerability in VMware vCenter Server allows attackers to upload arbitrary files, leading to potential privilege escalation or remote code execution. This is due to improper validation of uploaded files.

Affected Systems:

- VMware vCenter Server 6.7.x
- VMware vCenter Server 7.0.x

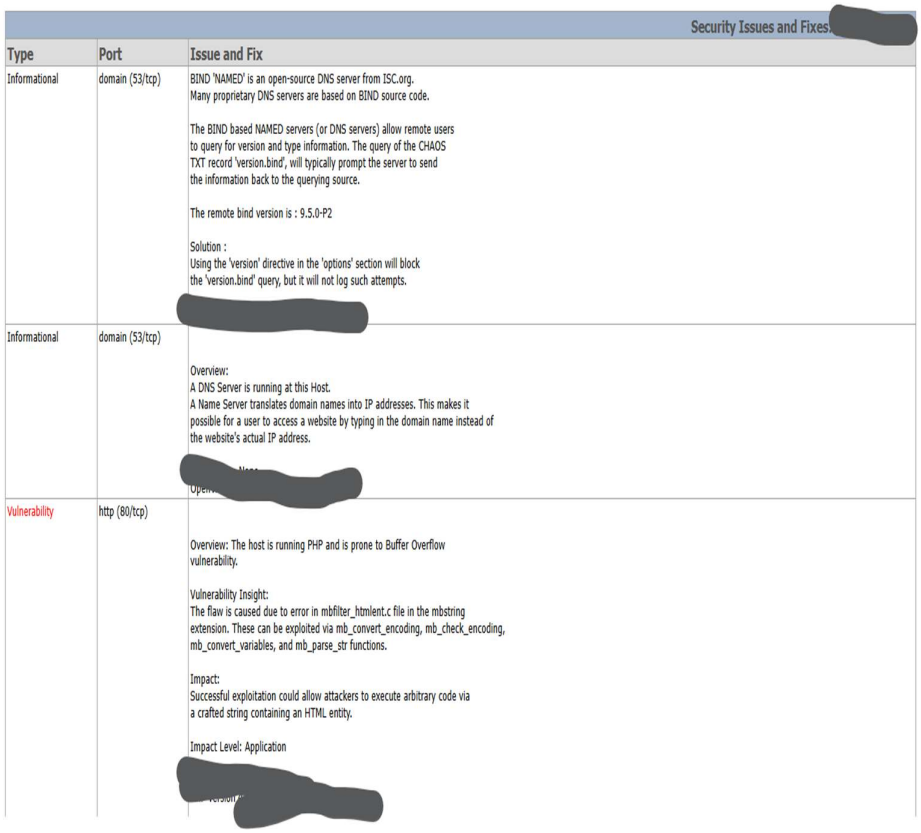
Dependencies:

1. vCenter Server Management Interface exposed to the internet.
2. File upload functionality enabled and not properly secured.

OPENVAS REPORT :

Critical Vulnerabilities :

1. **CVE-2021-34473: ProxyShell (Microsoft Exchange) - Critical (CVSS 9.8)**
2. **CVE-2021-22972: VMware vCenter (vSphere) - Critical (CVSS 9.8)**
3. **CVE-2021-31207: DNS Cache Poisoning - Critical (CVSS 9.8)**
4. **CVE-2021-22005: VMware vCenter File Upload - Critical (CVSS 9.8)**
5. **CVE-2021-44228: Log4Shell (Apache Log4j) - Critical (CVSS 10.0)**
6. **CVE-2022-0778: OpenSSL Infinite Loop - High (CVSS 9.1)**
7. **CVE-2021-34527: PrintNightmare - Critical (CVSS 8.8)**
8. **CVE-2022-30190: Follina (Microsoft MSDT) - Critical (CVSS 7.8)**
9. **CVE-2020-1472: Zerologon - Critical (CVSS 10.0)**



Security Issues and Fixes [redacted]

Type	Port	Issue and Fix
Informational	domain (53/tcp)	BIND 'NAMED' is an open-source DNS server from ISC.org. Many proprietary DNS servers are based on BIND source code. The BIND based NAMED servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source. The remote bind version is : 9.5.0-P2 Solution : Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts. [redacted]
Informational	domain (53/tcp)	Overview: A DNS Server is running at this Host. A Name Server translates domain names into IP addresses. This makes it possible for a user to access a website by typing in the domain name instead of the website's actual IP address. [redacted]
Vulnerability	http (80/tcp)	Overview: The host is running PHP and is prone to Buffer Overflow vulnerability. Vulnerability Insight: The flaw is caused due to error in mbfilter_htmlent.c file in the mbstring extension. These can be exploited via mb_convert_encoding, mb_check_encoding, mb_convert_variables, and mb_parse_str functions. Impact: Successful exploitation could allow attackers to execute arbitrary code via a crafted string containing an HTML entity. Impact Level: Application [redacted]

OpenVAS Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details

Hosts which were alive and responding during test	1
Number of security holes found	3
Number of security warnings found	11
Number of security notes found	26
Number of false positives found	0

Host List

Host(s)	Possible Issue
192.168.1.104	Security hole(s) found

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
192.168.1.104	domain (53/tcp)	Security note(s) found
192.168.1.104	http (80/tcp)	Security hole(s) found
192.168.1.104	pop3 (110/tcp)	Security note(s) found
192.168.1.104	netbios-ssn (139/tcp)	Security note(s) found
192.168.1.104	ssh (22/tcp)	Security warning(s) found
192.168.1.104	smtp (25/tcp)	Security note(s) found
192.168.1.104	imap (143/tcp)	Security note(s) found
192.168.1.104	microsoft-ds (445/tcp)	Security note(s) found
192.168.1.104	imaps (993/tcp)	No Information
192.168.1.104	pop3s (995/tcp)	No Information
192.168.1.104	ajp13 (8009/tcp)	No Information
192.168.1.104	http-alt (8080/tcp)	Security hole(s) found
192.168.1.104	netbios-ns (137/udp)	Security warning(s) found
192.168.1.104	general/tcp	Security note(s) found
192.168.1.104	general/SMBClient	Security note(s) found
192.168.1.104	domain (53/udp)	Security warning(s) found