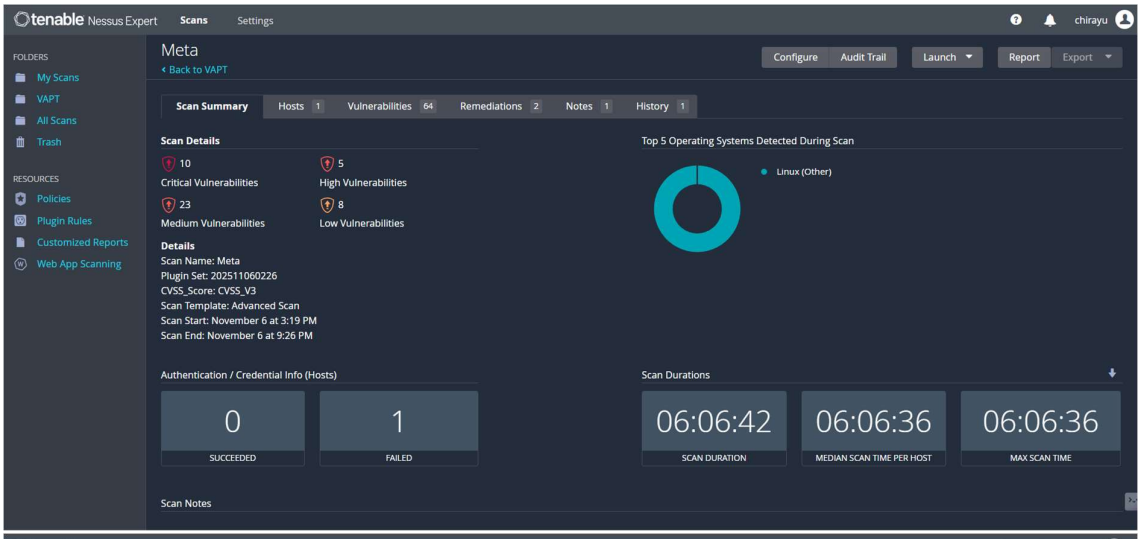
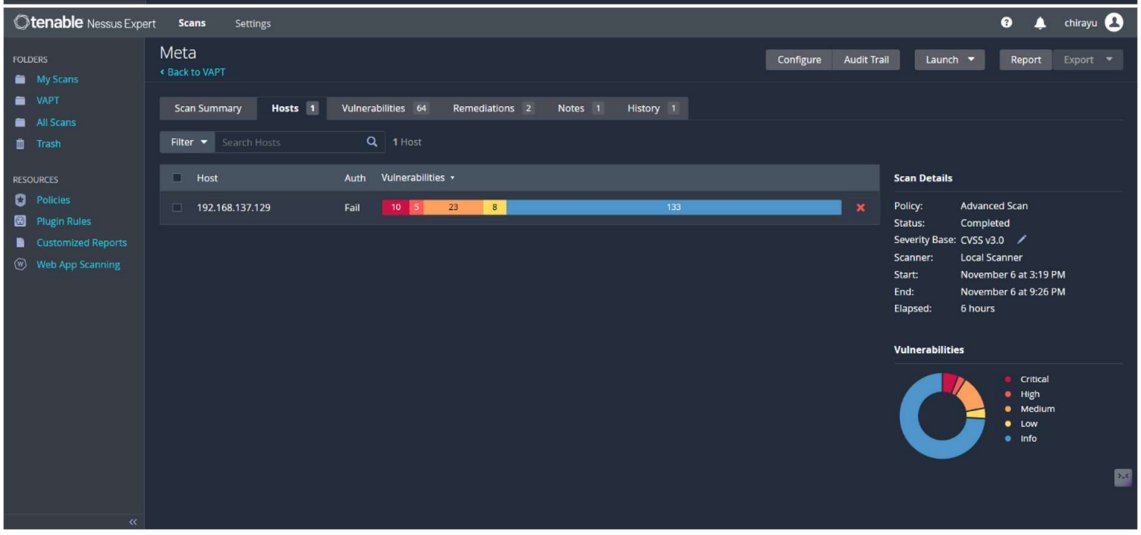
# VAPT T2 Report

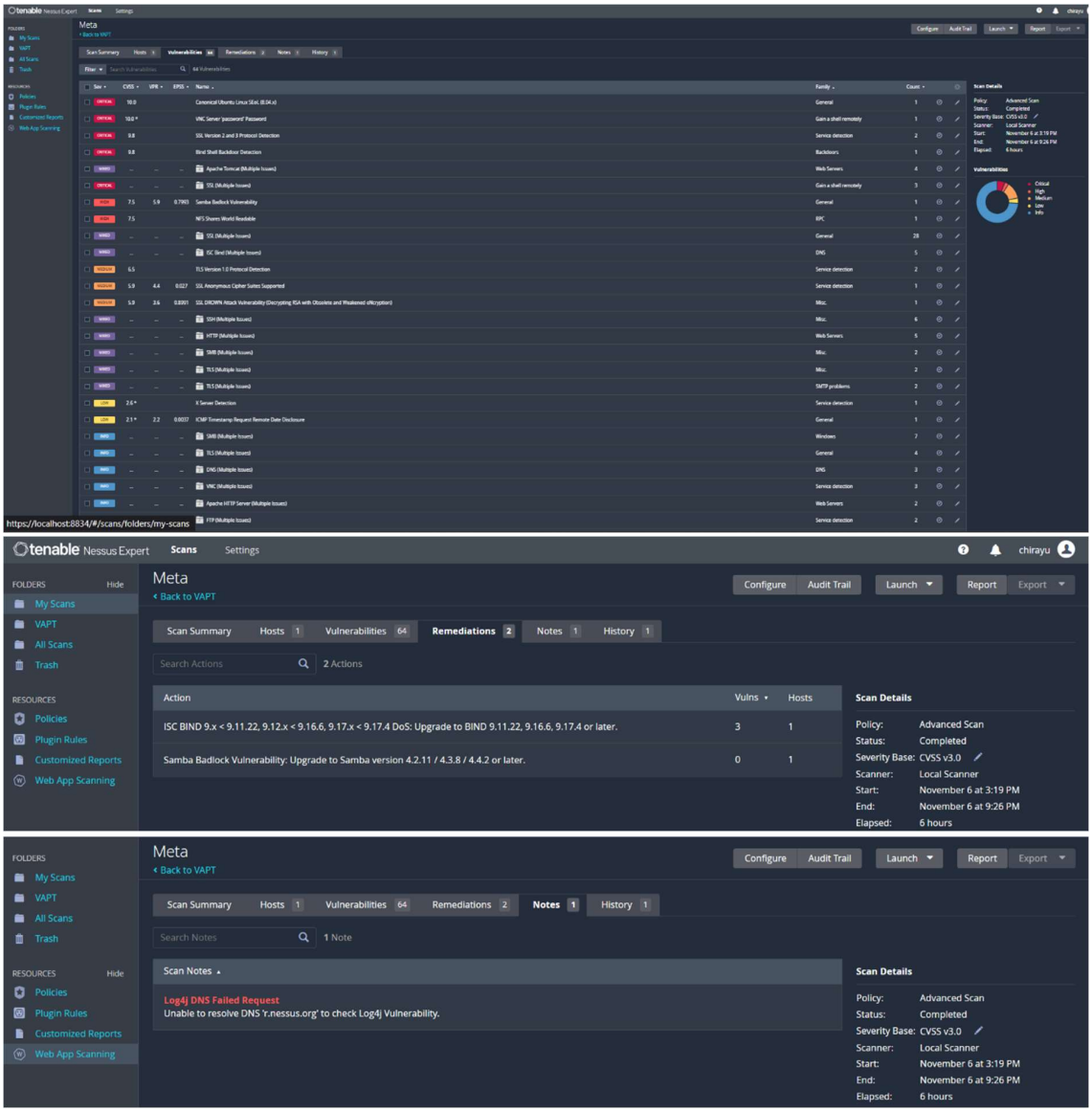
## 1 – Vulnerability scanning

Target: 192.168.137.129
Tools: Nmap, Nessus, Nikto

Evidence: Nessus Screenshots






NMAP and NIKTO findings attached in folder

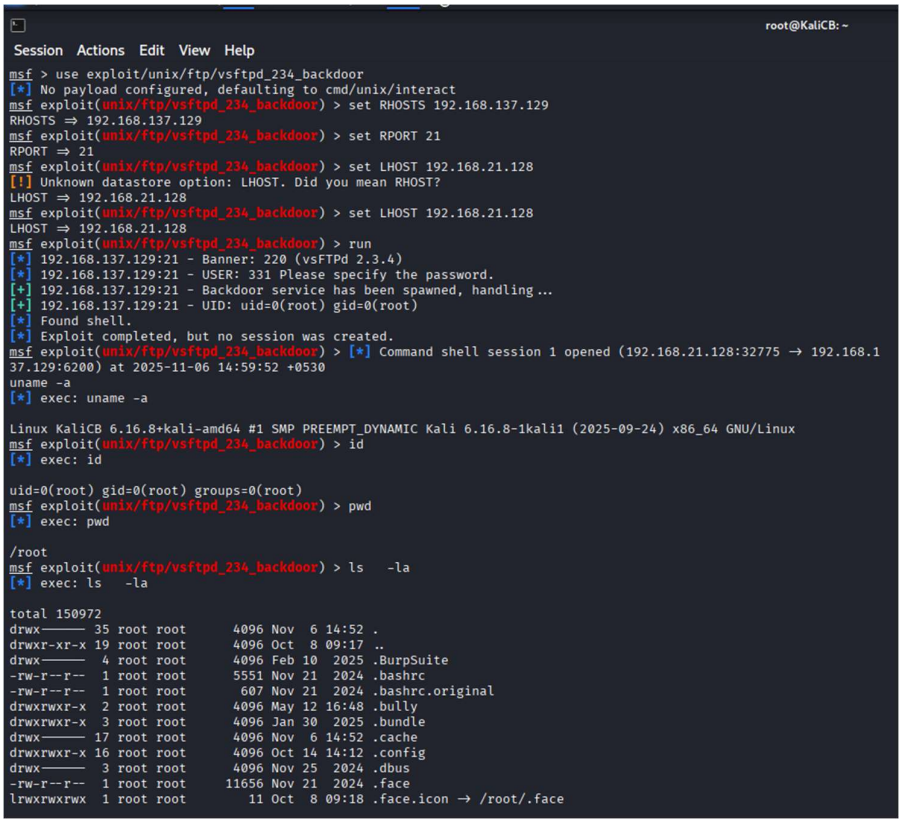
## 2 – Prioritization and CVSS

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| Outdated openSSH | 8.3 | High | 192.168.137.129 |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



## 4 – Post-Exploitation Evidence collection

Description:
Password list from target

Evidence:
.txt Included