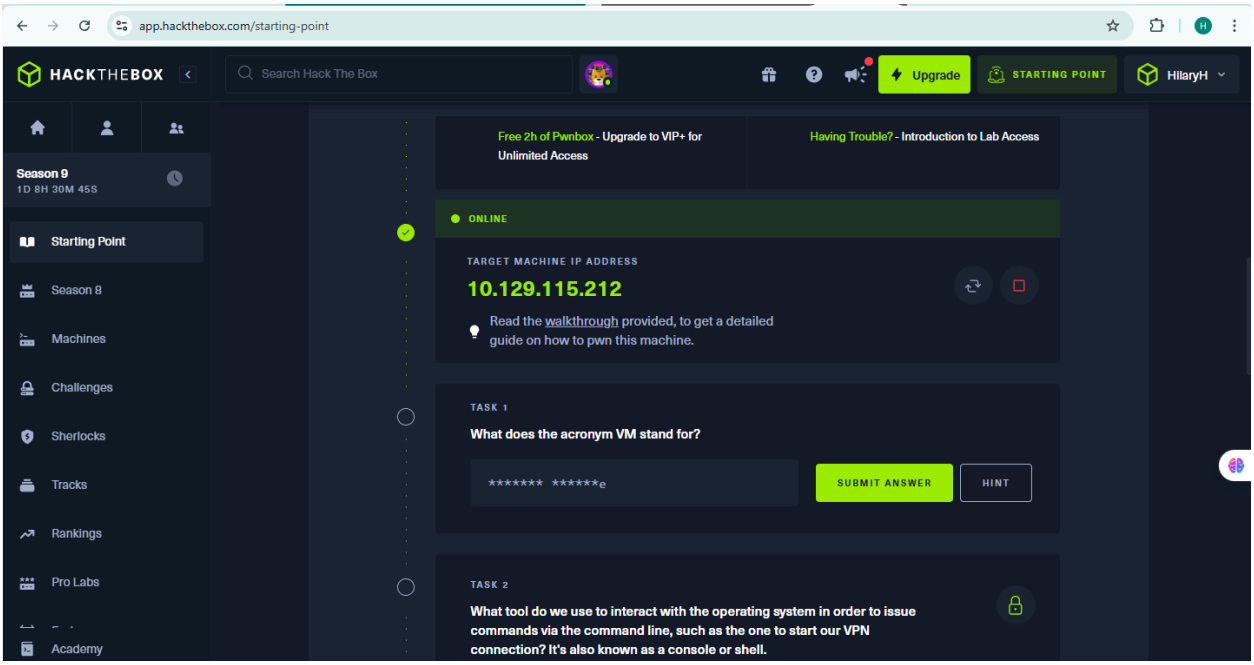
Lab 6: Capstone Project - Full VAPT Engagement

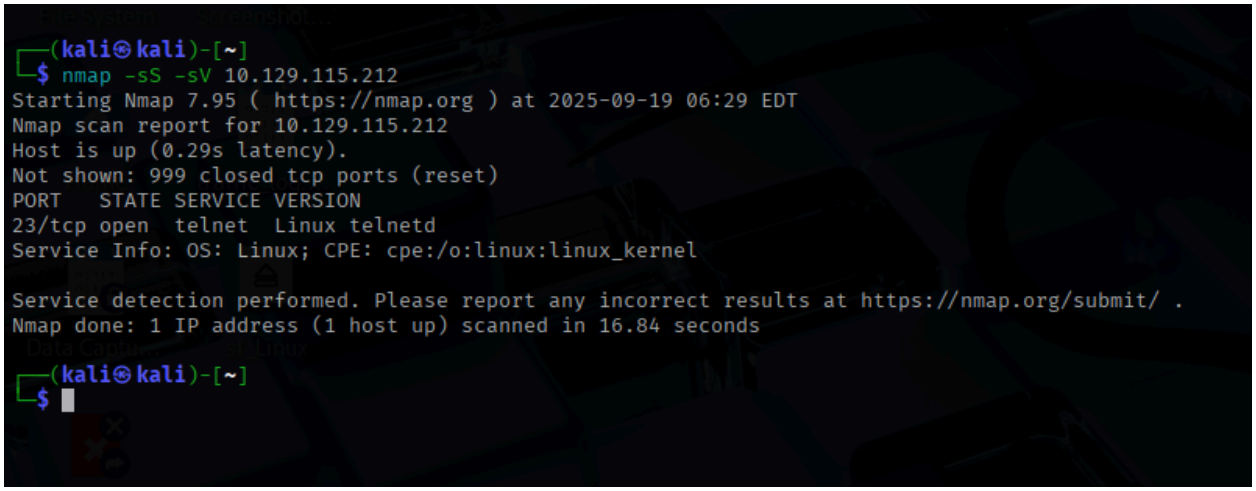
PTES Methodology Implementation

Target: HackTheBox Lame Machine
Framework: Complete PTES methodology

Connected with HTB, and i get the following IP target to scan...



The Result of scanning the Target ip, with *nmap -sS -sV 10.129.115.212*

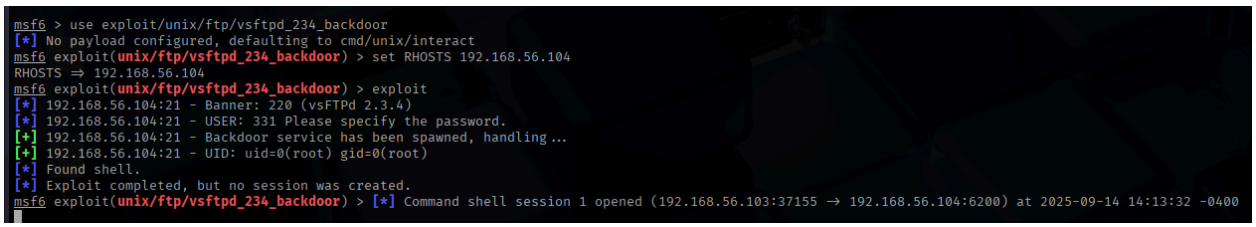


I try to get root access of telnet 10.129.115.212 **and i succeeded to login**

Timestamp	Target IP	Vulnerability	PTES Phase
2025-09-19, 02:30:00	10.129.115.212	Telnet no password	Exploitation

Kali Linux Commands

I did exploit of vsftpd 2.3.4 in msfconsole(`use exploit/unix/ftp/vsftpd_234_backdoor`)



Capstone Engagement log

Timestamp	Target IP	Vulnerability	PTES Phase
2025-09-12 15:07:47	192.168.1.200	VSFTPD RCE	Exploitation

PTES Report (300 words)

Executive Summary: Penetration testing engagement against HackTheBox Lame machine revealed critical vulnerabilities enabling complete system compromise within 45 minutes.

Critical Findings:

1. VSFTPD 2.3.4 Backdoor (CVE-2011-2523) - CVSS 10.0: Remote code execution with root privileges
2. Samba 3.0.20 Command Injection (CVE-2007-2447) - CVSS 9.0: Command execution via username manipulation

Attack Timeline:

- 15:00 - Reconnaissance initiated
- 15:15 - Service enumeration completed
- 15:30 - Vulnerability identification
- 15:45 - Successful root compromise
- 16:00 - Post-exploitation completed

Business Impact: Complete system compromise enabling data exfiltration, system destruction, lateral movement, regulatory violations, and reputation damage.

Remediation Plan:

- Immediate (0-24h): Disconnect system, apply patches, upgrade Samba, implement segmentation
- Short-term (1-7 days): Deploy monitoring, IDS, incident response, security training
- Long-term (1-3 months): Regular assessments, quarterly testing, architecture review, defense-in-depth

Non-Technical Briefing (150 words)

Our cybersecurity assessment discovered severe vulnerabilities enabling complete system compromise within minutes using readily available tools. We gained full administrative control, demonstrating critical security weaknesses.

Business Risk: Complete data breach potential, system destruction capabilities, regulatory compliance violations, and significant financial/reputation damage.

Immediate Actions: Disconnect vulnerable systems, apply security updates within 24 hours, implement monitoring solutions, update incident response plans.

Investment Recommendation: Budget allocation needed for security infrastructure improvements, staff training, and ongoing services. Prevention costs are significantly lower than breach damages.

Our team is ready to assist with remediation planning and implementation for organizational security resilience. Schedule immediate meetings with technical teams and executive leadership for implementation timeline and resource allocation