Personal Portfolio

Puri Jagannadh

Aspiring Cyber Security Analyst

Who I Am:

I am an aspiring cybersecurity Trainee with foundational training in Networking and Operating Systems, Network and Packet Analysis, Vulnerability Management, Basics of Python, Exploitation, Basics of Penetration Testing and SIEM Tools. Passionate about learning and building practical skills to protect digital systems from emerging threats.

Career Objective:

My career objective is to build a progressive career as a SOC Analyst, specializing in threat detection, incident response, and continuous security monitoring. I am committed to mastering advanced SIEM tools and cybersecurity frameworks to strengthen organizational defense mechanisms. With a strong focus on proactive threat mitigation and analytical precision, I aim to evolve into an expert-level SOC professional who ensures robust and resilient security operations.

Experience & Education:

- Digit Defense Company - Cyber Security Analyst Intern
  Madhapur, Hyderabad, Telangana
  Oct 2025 - Present

- Skillogic - Cyber Security Trainee
  Madhapur, Hyderabad, Telangana
  Aug 2025 - Sep 2025

- Godavari Institute of Engineering & Technology
  B.Tech | Electronics and Communication Engineering
  Rajahmundry, Konaseema Dist, AP
  Sep 2021 - May 2025

Skills:

- Networking & Operating Systems
- Vulnerability Scanning & Assessment
- Network Discovery
- Basics of Python
- Endpoint Detection and response tools
- Network Analysis & Traffic Monitoring
- SIEM Tools

Tools Learned:

- OpenVAS (GreenBone)
- Tenable Nessus
- Acunetix 11
- Wireshark
- Nmap
- Angry IP Scanner
- Splunk
- Wazuh
- Kali Linux
- John The Ripper
- Owasp ZAP
- Cryptography - Encryption/Decryption
- IBM Q Radar
- MetaDefender EDR
- WAFw00f
- Phish Tool
- MXtoolbox
- VirusTotal
- urlscan.io
- URL extractor
- Who is

Projects:

Vulnerability Assessment on Kali Linux Using OpenVAS

- Conducted a comprehensive vulnerability scan on Kali Linux using OpenVAS to detect system weaknesses and misconfigurations.
- Analyzed scan results to identify critical, high, and medium-risk vulnerabilities and potential exploitation paths.
- Prepared a detailed report with actionable recommendations to strengthen system security and mitigate risks.

Projects:

Network Traffic Monitoring and Threat Analysis Project

- Captured and analyzed network packets using Wireshark to detect anomalies and suspicious traffic.
- Identified common protocols (TCP, UDP, ICMP) and inspected headers for potential DoS or SYN flood patterns.
- Created a report summarizing traffic behavior, threats, and mitigation insights.

Mini-Projects:

- Scan Your Local Network for Open Ports using Nmap.
- Analyze a Phishing Email Sample.
- Perform a Basic Vulnerability Scan on Your PC.
- Setup and Use a Firewall on Windows/Linux.
- Capture and Analyze Network Traffic Using Wireshark.
- Create a Strong Password and Evaluate Its Strength.
- Identify and Remove Suspicious Browser Extensions.
- Working with VPNs.

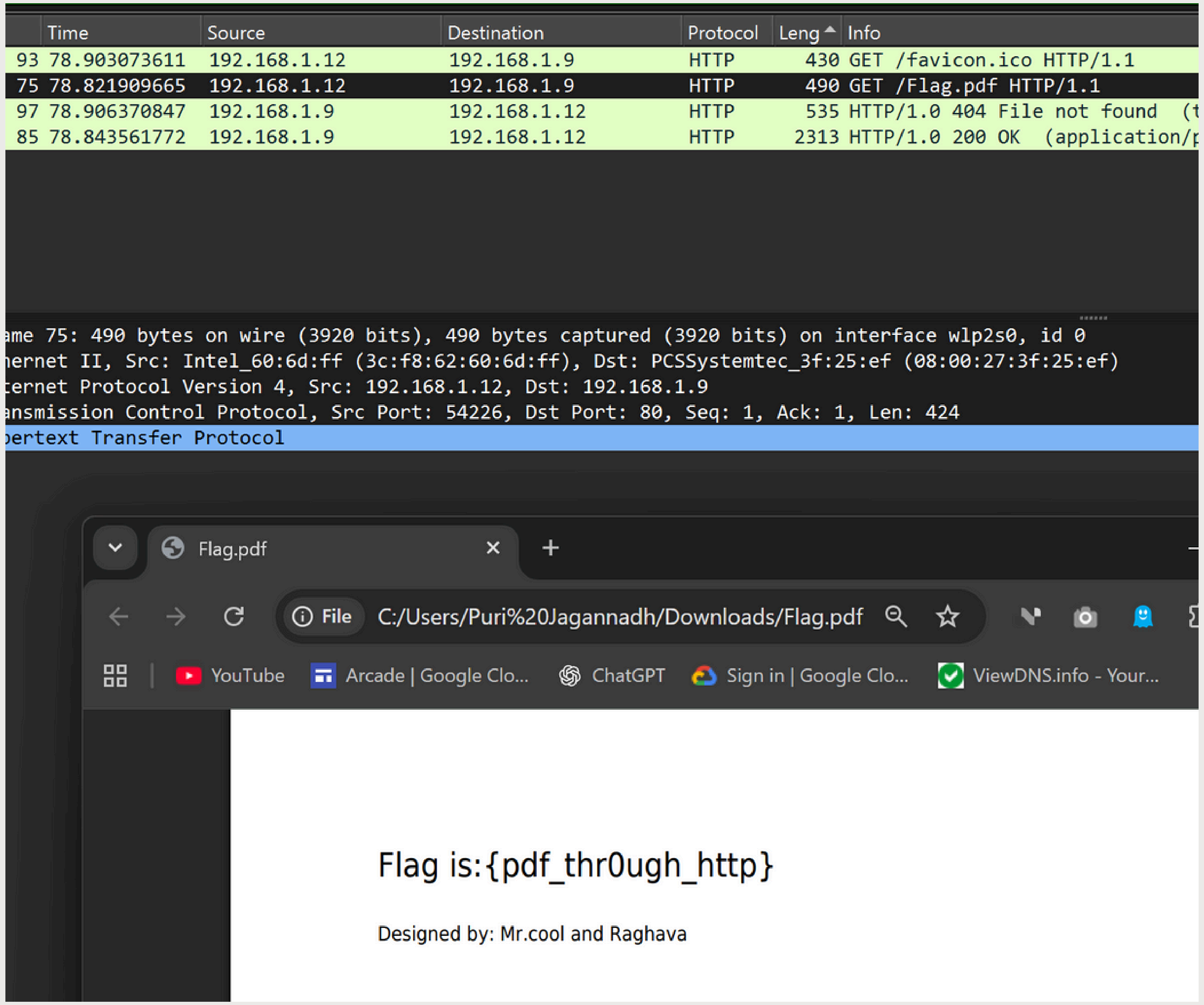
Lab Work:

Capture The Flag (CTF)

- Completed a Capture the Flag (CTF) lab activity to test cybersecurity concepts.

- Solved multiple security challenges to capture flags in simulated environments.

- Gained hands-on experience in identifying and resolving basic security tasks.



```
   Time           Source         Destination    Protocol Leng Info
93 78.903073611   192.168.1.12   192.168.1.9    HTTP      430 GET /favicon.ico HTTP/1.1
75 78.821909665   192.168.1.12   192.168.1.9    HTTP      490 GET /Flag.pdf HTTP/1.1
97 78.906370847   192.168.1.9    192.168.1.12   HTTP      535 HTTP/1.0 404 File not found  (t
85 78.843561772   192.168.1.9    192.168.1.12   HTTP     2313 HTTP/1.0 200 OK  (application/p
```

```
ame 75: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits) on interface wlp2s0, id 0
nernet II, Src: Intel_60:6d:ff (3c:f8:62:60:6d:ff), Dst: PCSSystemtec_3f:25:ef (08:00:27:3f:25:ef)
ternet Protocol Version 4, Src: 192.168.1.12, Dst: 192.168.1.9
ansmission Control Protocol, Src Port: 54226, Dst Port: 80, Seq: 1, Ack: 1, Len: 424
pertext Transfer Protocol
```

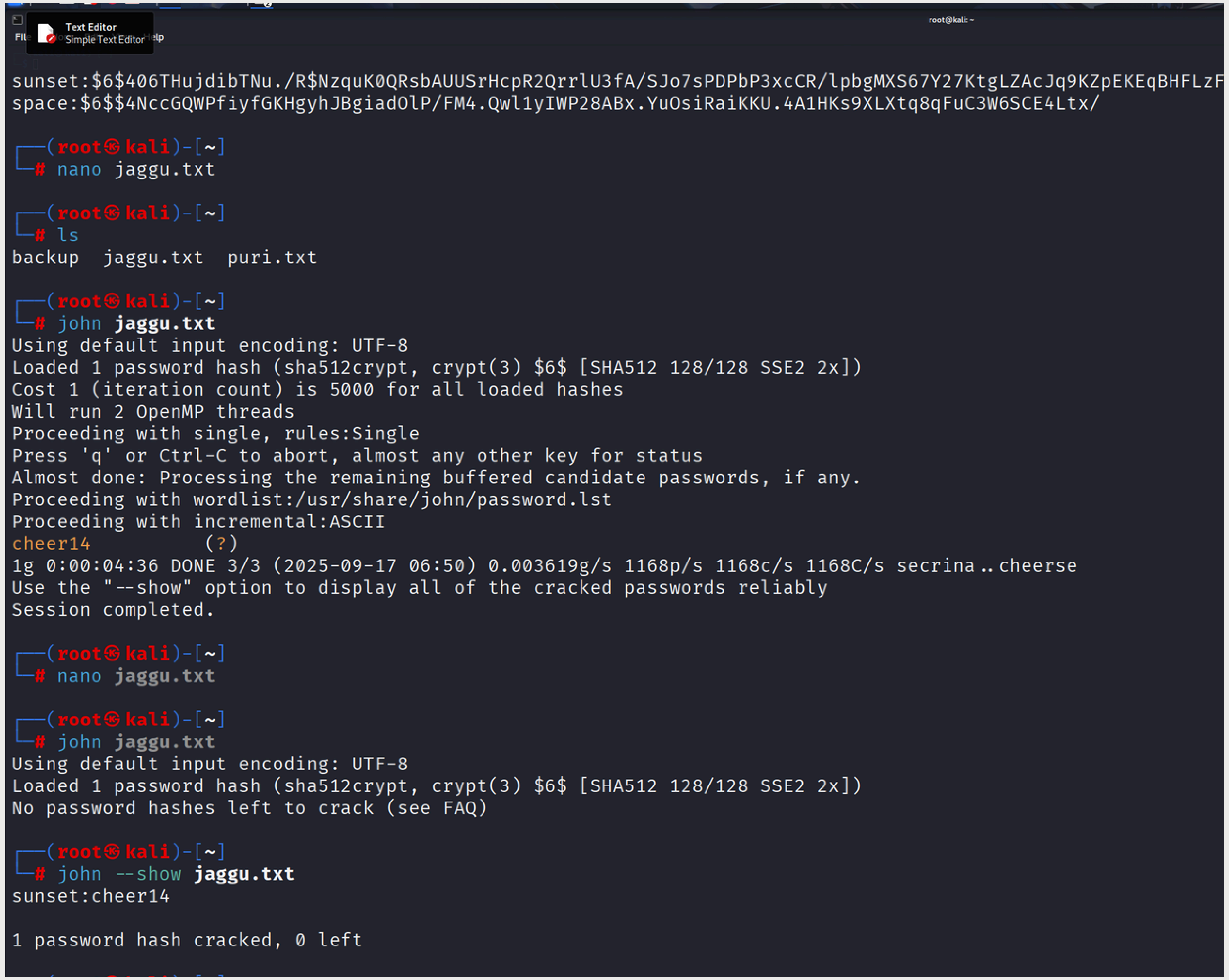
Flag is:{pdf_thr0ugh_http}

Designed by: Mr.cool and Raghava

Lab Work:

Sunset Server Hacking

- Completed a controlled Sunset Server compromise and documented each step.
- Created a clear, reproducible report with screenshots and remediation steps.
- Performed an authorized server hack to retrieve passwords and validated recovered credentials.



```
sunset:$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpR2QrrlU3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9KZpEKEqBHFLzF
space:$6$$4NccGQWPfiyfGKHgyhJBgiadOlP/FM4.Qwl1yIWP28ABx.YuOsiRaiKKU.4A1HKs9XLXtq8qFuC3W6SCE4Ltx/

┌──(root㉿kali)-[~]
└─# nano jaggu.txt

┌──(root㉿kali)-[~]
└─# ls
backup  jaggu.txt  puri.txt

┌──(root㉿kali)-[~]
└─# john jaggu.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
cheer14          (?)
1g 0:00:04:36 DONE 3/3 (2025-09-17 06:50) 0.003619g/s 1168p/s 1168c/s 1168C/s secrina..cheerse
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[~]
└─# nano jaggu.txt

┌──(root㉿kali)-[~]
└─# john jaggu.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
No password hashes left to crack (see FAQ)

┌──(root㉿kali)-[~]
└─# john --show jaggu.txt
sunset:cheer14

1 password hash cracked, 0 left
```

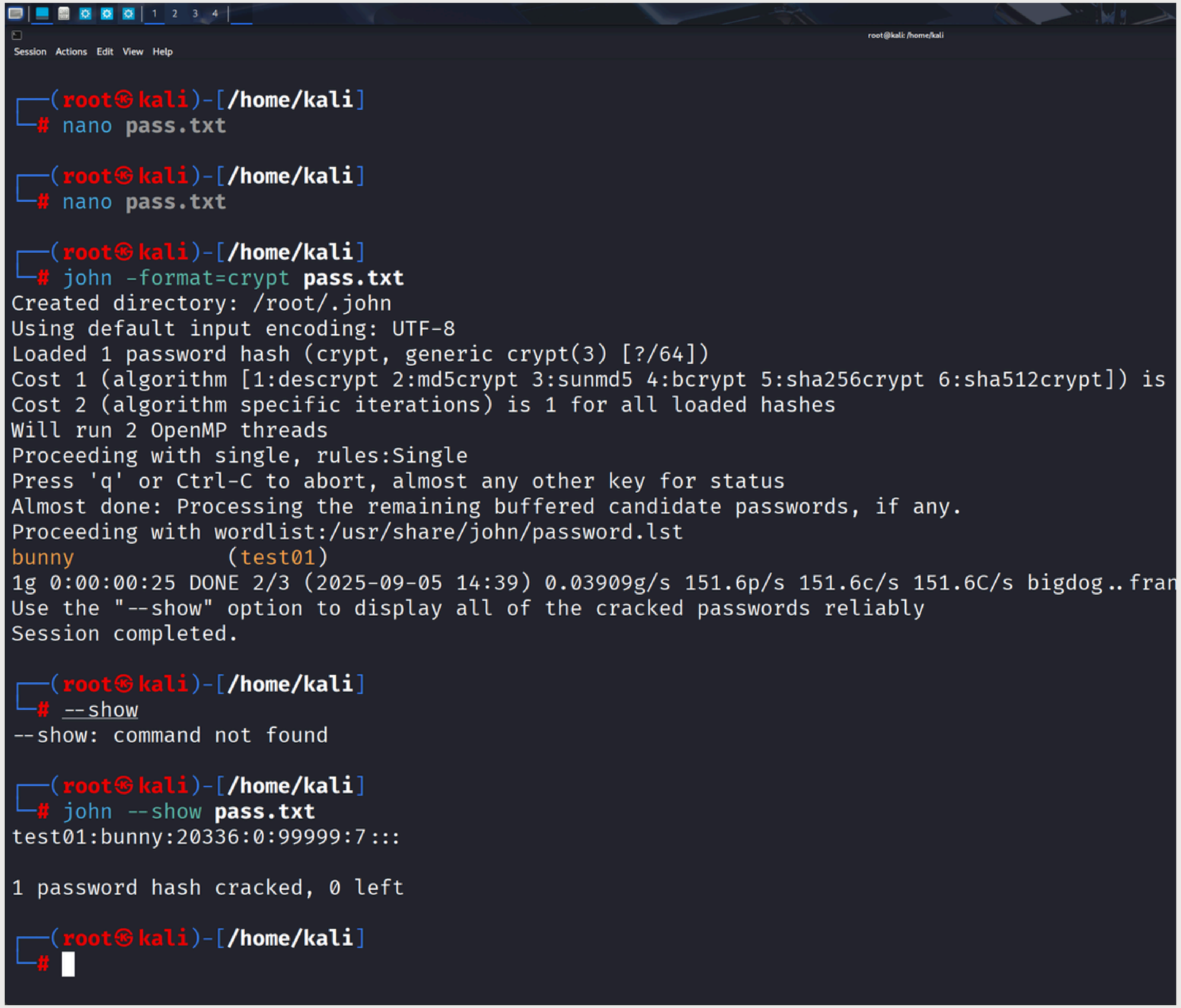
Lab Work:

Password Cracking Using John The Ripper

- Successfully cracked a user's password using John the Ripper in a controlled lab environment.

- Thoroughly documented all hash types, commands executed, and recommended remediation steps.

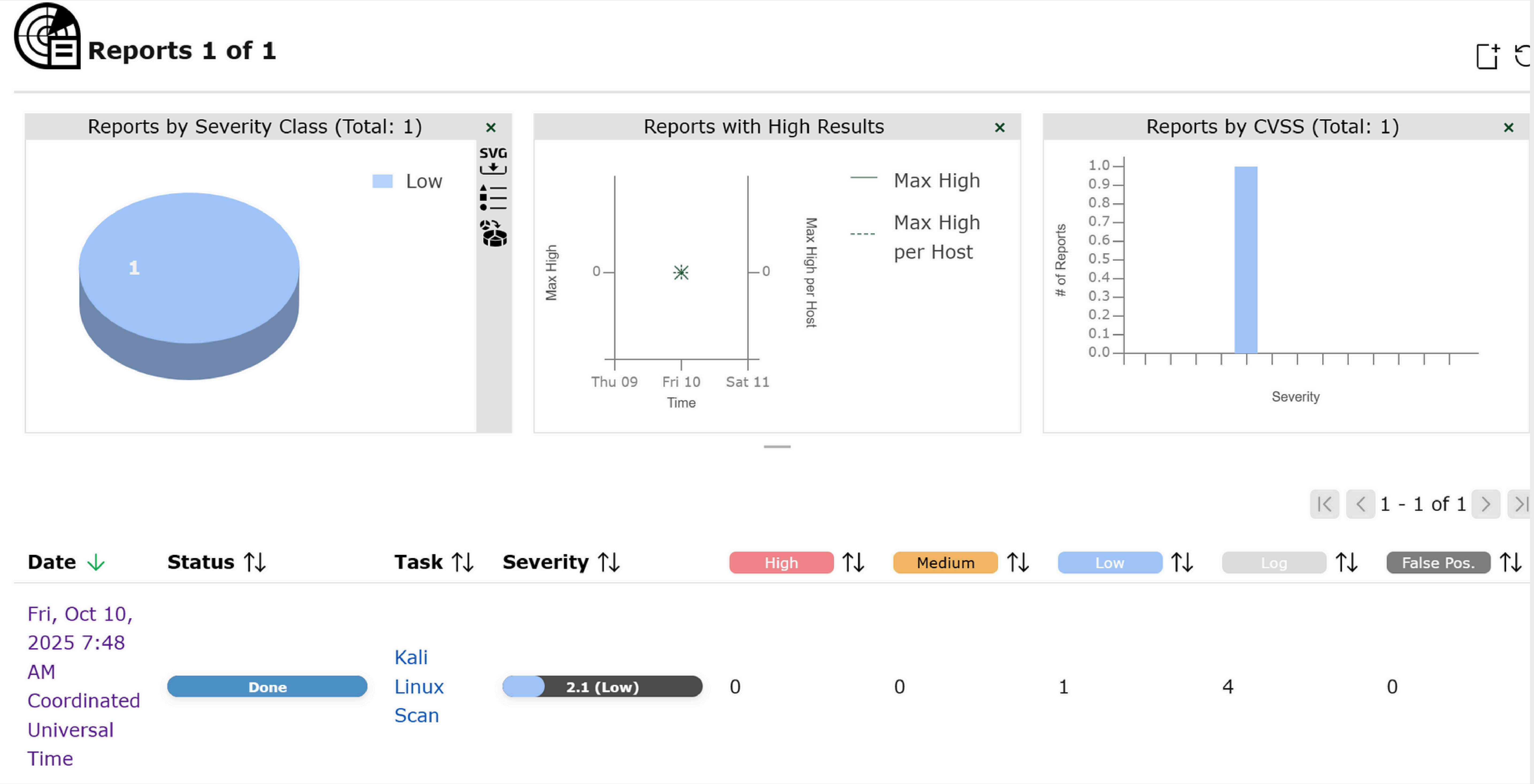
- Gained practical experience and effectively mastered John the Ripper and password-cracking techniques.



```
┌──(root㉿kali)-[/home/kali]
└─# nano pass.txt

┌──(root㉿kali)-[/home/kali]
└─# nano pass.txt

┌──(root㉿kali)-[/home/kali]
└─# john -format=crypt pass.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
bunny            (test01)
1g 0:00:00:25 DONE 2/3 (2025-09-05 14:39) 0.03909g/s 151.6p/s 151.6c/s 151.6C/s bigdog..fran
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[/home/kali]
└─# --show
--show: command not found

┌──(root㉿kali)-[/home/kali]
└─# john --show pass.txt
test01:bunny:20336:0:99999:7:::

1 password hash cracked, 0 left

┌──(root㉿kali)-[/home/kali]
└─# █
```

Lab Work:

Vulnerability Scanning using OpenVAS

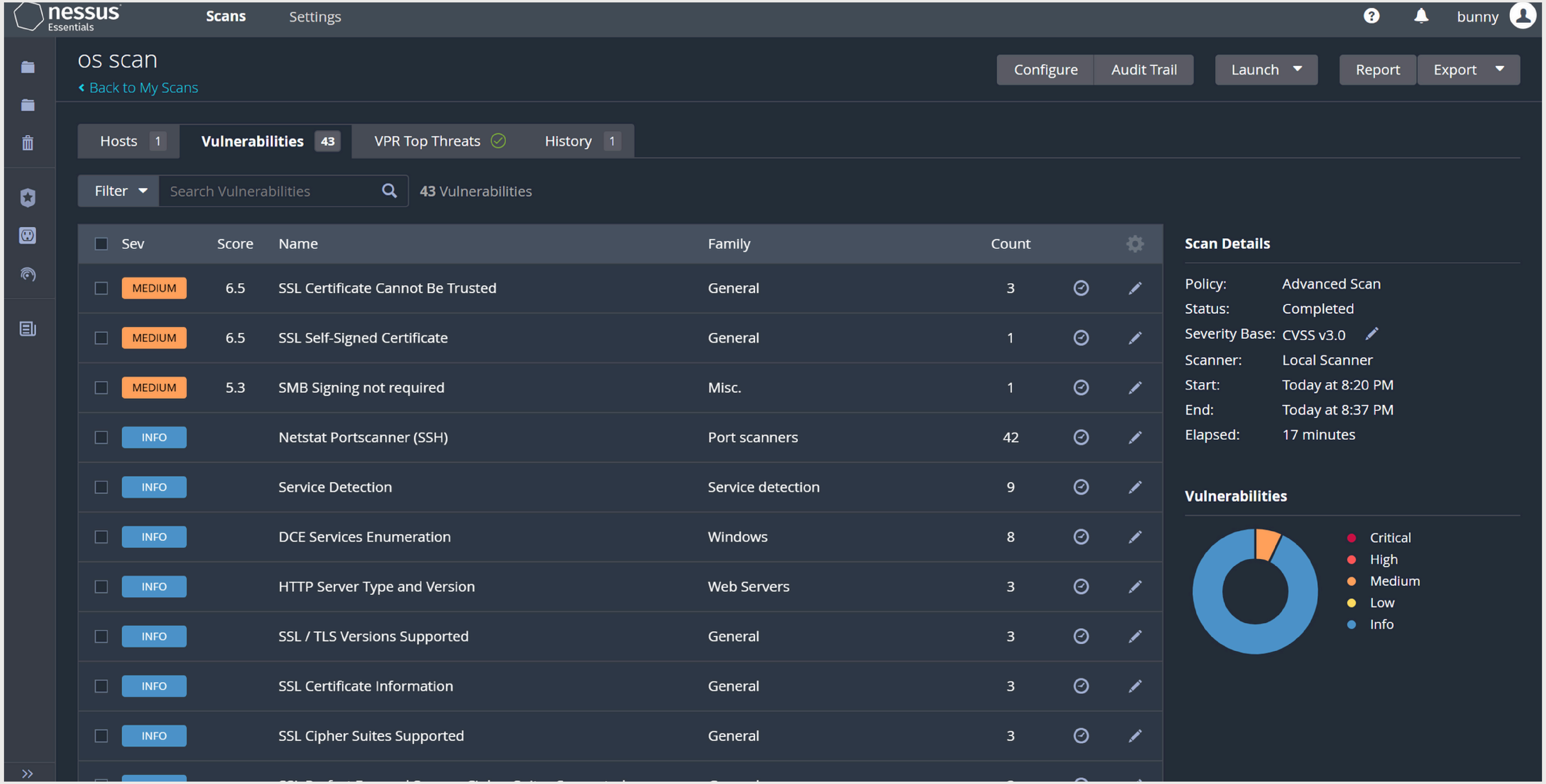


Reports 1 of 1

Date ↓	Status ⇅	Task ⇅	Severity ⇅	High ⇅	Medium ⇅	Low ⇅	Log ⇅	False Pos. ⇅
Fri, Oct 10, 2025 7:48 AM Coordinated Universal Time	Done	Kali Linux Scan	2.1 (Low)	0	0	1	4	0

Lab Work:

Vulnerability Scanning Using Nessus:



os scan

‹ Back to My Scans

Hosts 1 | Vulnerabilities 43 | VPR Top Threats | History 1

43 Vulnerabilities

Sev	Score	Name	Family	Count
MEDIUM	6.5	SSL Certificate Cannot Be Trusted	General	3
MEDIUM	6.5	SSL Self-Signed Certificate	General	1
MEDIUM	5.3	SMB Signing not required	Misc.	1
INFO		Netstat Portscanner (SSH)	Port scanners	42
INFO		Service Detection	Service detection	9
INFO		DCE Services Enumeration	Windows	8
INFO		HTTP Server Type and Version	Web Servers	3
INFO		SSL / TLS Versions Supported	General	3
INFO		SSL Certificate Information	General	3
INFO		SSL Cipher Suites Supported	General	3

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:20 PM
End: Today at 8:37 PM
Elapsed: 17 minutes

Vulnerabilities

Project Links:

- **Password Cracking Using John The Ripper**
  https://github.com/JAGANNADH18/Password-Cracking-Project
- **Phishing Email Analysis**
  https://github.com/JAGANNADH18/3-Days-Phishing-Analysis-Challenge
- **Vulnerability Scanning using Tenable Nessus**
  https://github.com/JAGANNADH18/Project-on-Nessus
- **Nmap-Scanning-Local-Network**
  https://github.com/JAGANNADH18/Nmap-Scanning-Local-Network
- **Elevate-Labs-Projects-Tasks**
  https://github.com/JAGANNADH18/Elevate-Labs-Projects-Tasks
- **Network-Vulnerability-Scanning-Mitigation**
  https://github.com/JAGANNADH18/Network-Vulnerability-Scanning-Mitigation

Achievements:

- Successfully covered the fundamentals of Cybersecurity, Ethical Hacking, and Vulnerability Management, completing all module assessments with strong technical understanding.
- Recognized for consistent performance in lab simulations and practical exercises, demonstrating strong analytical and troubleshooting skills.
- Participated in realistic, case-based cybersecurity simulations, strengthening capabilities in incident handling, reporting, and threat response documentation.

Contact Information:

- Name: U.S.Puri Jagannadh
- Email: jagannadhulapalli@gmail.com
- Phone: +91 9133014476
- Linkedin: https://www.linkedin.com/in/puri-jagannadh-ulapalli
- Github: https://github.com/JAGANNADH18
- Portfolio: https://jagannadh18.github.io/Portfolio/
- Try Hack me: https://tryhackme.com/p/PuriJagannadh

Thank You

Crafted by
Puri Jagannadh