INNO BLITZ HACKATHON 1.0

Vulnerability Scanner with Exploit Check

- Problem Statement Title - Student Innovation
- Theme- Blockchain & Cybersecurity
- PS Category- Software
- Team Name - DEDSEC
- Members : J. Jejo (Cyber Security)
  V. Priyadharshan (Cyber Security)
  P.S. Padmesh (Cyber Security)

Web-Prowler

Student Innovation

Purpose: A robust tool for **web security assessment.**

Key Features:

❖ Analyzes **open ports**, services, and **vulnerabilities** using Nmap and Tor.
❖ Accepts server IPs to scan websites for vulnerabilities.
❖ Cross-references data with **Exploit Database** for accurate reports.
❖ **Stealth Scan:** Uses Tor to reduce detection.
❖ **Customizable Scans:** Interactive menu for tailored assessments.

Use Cases:

Ideal for **business security checks** and **cybersecurity** professionals.

TECHNICAL APPROACH

Working:

- The script uses NMAP to **scan the open ports** in a target …
- Gains the **version and service info** that is used on that particular open port.
- Compares the version number with **exploit database**
- **List out the vulnerabilities** to gain access over the server .

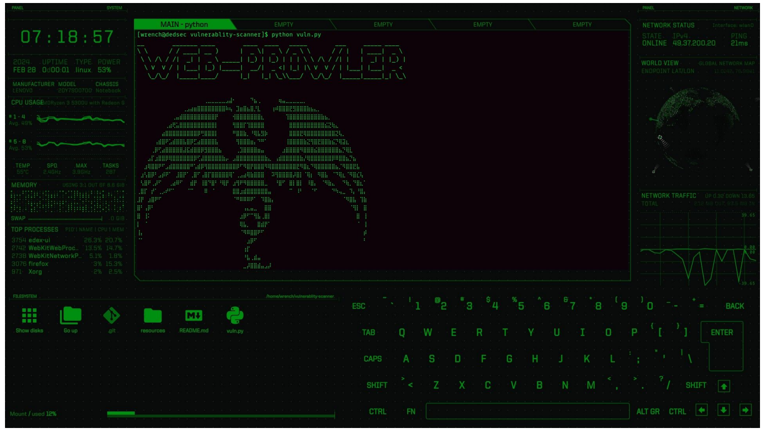
Tools Used :

Nmap

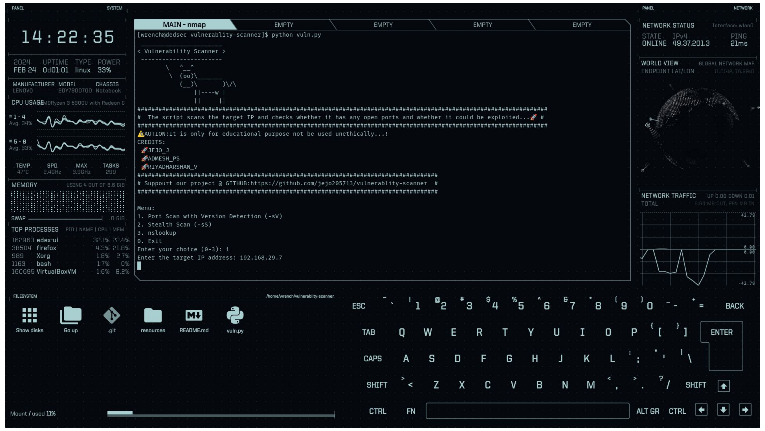
Nslookup

Exploit DB

Tor

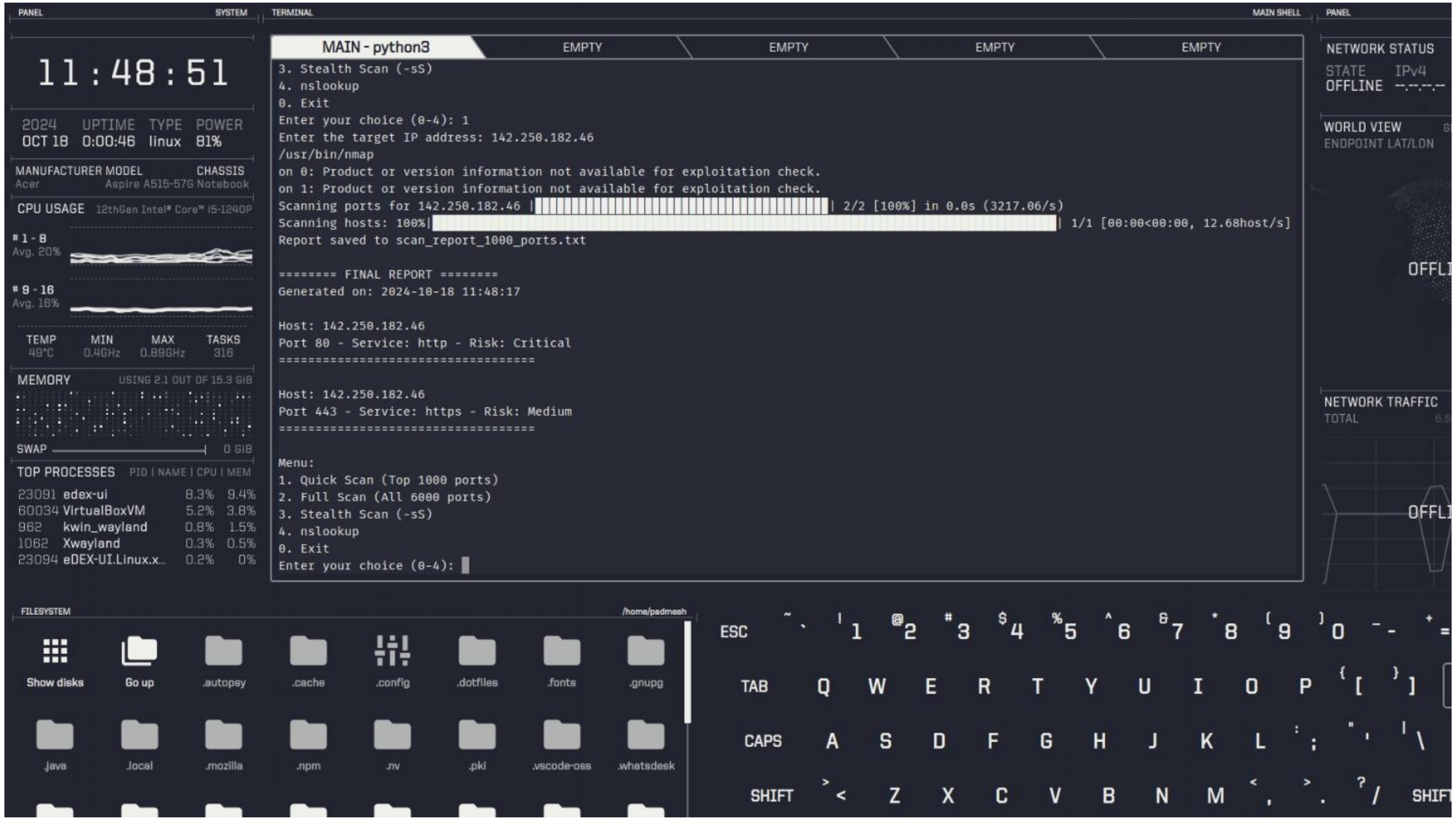


```
[wrench@dedsec vulnerablity-scanner]$ python vuln.py
```



```
[wrench@dedsec vulnerablity-scanner]$ python vuln.py
 ______________________
< Vulnerability Scanner >
 ----------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
##########################################################################################
#  The script scans the target IP and checks whether it has any open ports and whether it could be exploited...🚀 #
##########################################################################################
⚠CAUTION:It is only for educational purpose not be used unethically...!
CREDITS:
 🚀JEJO_J
 🚀ADMESH_PS
 🚀PRIYADHARSHAN_V
##################################################################
# Suppourt our project @ GITHUB:https://github.com/jejo205713/vulnerablity-scanner  #
##################################################################

Menu:
1. Port Scan with Version Detection (-sV)
2. Stealth Scan (-sS)
3. nslookup
0. Exit
Enter your choice (0-3): 1
Enter the target IP address: 192.168.29.7
```

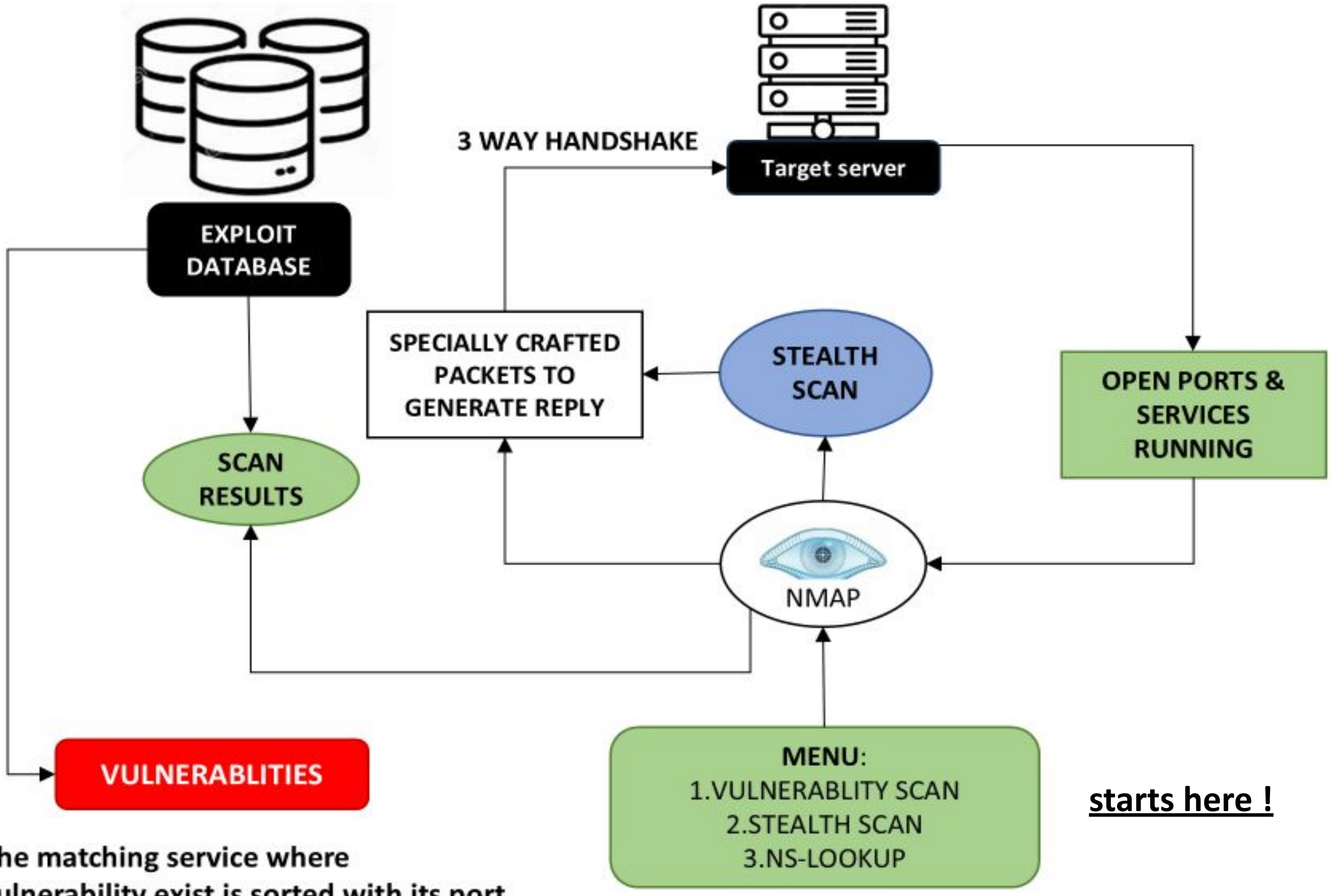
SIMULATING ATTACK ON A SECURE SERVER(google.com)



```
3. Stealth Scan (-sS)
4. nslookup
0. Exit
Enter your choice (0-4): 1
Enter the target IP address: 142.250.182.46
/usr/bin/nmap
on 0: Product or version information not available for exploitation check.
on 1: Product or version information not available for exploitation check.
Scanning ports for 142.250.182.46 |████████████████████████████████████████| 2/2 [100%] in 0.0s (3217.06/s)
Scanning hosts: 100%|████████████████████████████████████████████████████████████████████| 1/1 [00:00<00:00, 12.68host/s]
Report saved to scan_report_1000_ports.txt

======== FINAL REPORT ========
Generated on: 2024-10-18 11:48:17

Host: 142.250.182.46
Port 80 - Service: http - Risk: Critical
===================================

Host: 142.250.182.46
Port 443 - Service: https - Risk: Medium
===================================

Menu:
1. Quick Scan (Top 1000 ports)
2. Full Scan (All 6000 ports)
3. Stealth Scan (-sS)
4. nslookup
0. Exit
Enter your choice (0-4):
```

- The ports are open
- but the server remains safe

Flowchart



starts here !

The matching service where vulnerability exist is sorted with its port number and service version...

Web-Prowler

IMPACT AND BENEFITS

Impact on the Target Audience

- **Risk Management**: Helps businesses identify vulnerabilities to secure networks.
- **Operational Impact** : Automates scanning and reporting, saving time for IT teams.
- **Simple Interface:** Easy to use, allowing anyone to perform scans regardless of their technical background.
- **Customizable and Scalable**: Can be tailored to specific business needs and integrated with other tools.

Benefits of the Solution

- **EASE OF ACCESS:** Cyber security is a basic necessity , Even a common man can asses his website's security with our script & and fix them .
- **PRICING :** Compared to the existing solution this is by far the affordable option and closes the market gap.
- **Unmatched in Market:** No existing solution matches the robustness and comprehensive features of WEB-PROWLER

BUSINESS PLAN

Current Problem:

- Scanning tools often lack detailed risk assessment and **exploit checks**.
- Reporting is frequently inadequate, creating **security gaps**.

Market Gap:

- Need for a **user-friendly tool** that combines deep scanning with real-time exploit identification.
- Existing tools fail to balance scan **speed, depth,** and **clarity of risk levels.**

Web-Prowler's Solution:

- **Scans**: Quick, Full, and Stealth modes.
- **Features**: Real-time risk and exploit analysis.
- **Reports**: Clear and accessible for fast decision-making.
- **Post-Fix**: A set of scripts that mitigates the found Vulnerabilities

Target Users:

- **Global Cybersecurity Market:** Expected to grow from **$217 billion (2021)** to **$345 billion** by **2026**.
- **SMBs as Key Market:** 43% of cyberattacks target SMBs, highlighting the need for affordable security tools like WEB-PROWLER.

RESEARCH AND REFERENCES

Target Users /customers:

- Business owners
- Security professionals
- It managers
- System administrators
- Students & Researchers

Research:

1) https://www.researchgate.net/publication/261182006_Vulnerability_Scanners-A_Proactive_Approach_To_Assess_Web_Application_Security

2) https://www.researchgate.net/publication/362137419_Vulnerability_Scanning