- Nmap-based Vulnerability Scanning Tool with CVE Matching (VulnScan Pro)
- Automating Network Scans and Vulnerability Reporting

- **Group:** Bootcon9
- Prepared by S. Asghar
- **Date:** January 16, 2025

Proposal Approved

Automating Nmap Scans with Python for Vulnerability Assessment on Ubuntu Systems, however, Upcoming Pics from the Report File do Detect Another Win10 Machine on The Network And Associated Ports and CVEs.

End Goal or Vulnerability Being Exploited:

The goal of this project is to automate the process of running an Nmap scan to assess and identify security vulnerabilities in a network environment. Specifically, the script will aim to identify open ports, services, and potential weaknesses in target devices that could be exploited by attackers. The focus will be on performing reconnaissance to identify common vulnerabilities in an Ubuntu environment, including misconfigured ports, outdated services, or unauthorized open access points.

Devices and/or Technologies to be Used:

1. **Ubuntu Machine** (Target System): The machine running Ubuntu will be the focus of the Nmap scan, which can be either the host itself or a set of devices on a local network.
2. **Nmap** (Network Mapper): Nmap will be the primary tool for scanning networks and identifying open ports, services, and vulnerabilities.
3. **Python**: The Python script will serve as the automation layer for running Nmap commands, parsing results, and generating reports. Libraries such as subprocess and python-nmap will be used for executing Nmap commands from within the script.
4. **Network Devices**: This may include routers, firewalls, servers, workstations, or IoT devices that are part of the network being tested.

Summary of How Devices and Technologies May Be Used:

1. **Python Script**: The Python script will be developed to automate the Nmap scanning process. It will allow the user to specify the target IP range or individual IP addresses to scan. The script will interface with Nmap using either command-line execution (subprocess) or the python-nmap library, which provides a more Pythonic interface to Nmap.
2. **Nmap Scans**: Nmap will be used to scan the target systems for open ports, services running on those ports, and other metadata related to the system (e.g., operating system detection). Different scan types can be utilized, such as TCP connect scans or stealth SYN scans, depending on the goal of the assessment.
3. **Automation and Reporting**: The Python script will automate the execution of Nmap scans on a scheduled or ad-hoc basis. The script will then parse the scan results and provide a summary of discovered vulnerabilities, such as open ports or outdated services. The results can be saved in a CSV or text format for further analysis or reporting.
4. **Vulnerability Identification**: Based on the open ports and services discovered by Nmap, the script will look for known vulnerabilities. It can be further extended to include integration with vulnerability databases (e.g., CVE, NVD) or external tools to perform deeper scans for specific exploits.

Overview of the Presentation

- **Introduction to Nmap and CVEs**
  - Learn how Nmap scans help identify open ports and services.
  - Understand CVEs and their role in identifying vulnerabilities.
- **Understanding the Code Structure**
  - Review how the script automates network scanning and CVE matching.
- **Key Features of the Application**
  - Running different Nmap scans (simple, enhanced, aggressive).
  - Automatic CVE matching based on detected services.
  - Report generation with Nmap results and CVEs.
- **Use Cases**
  - Practical scenarios like internal vulnerability scanning and targeted service vulnerability checks.
- **Practical Demonstration**
  - A hands-on walkthrough of the tool’s execution.

Introduction to Network Security

•**Network security** aims to protect a computer network from unauthorized access, data breaches, and cyber-attacks.

•**Vulnerability scanning** is an essential part of identifying weaknesses within a network.

•**CVEs (Common Vulnerabilities and Exposures)** are publicly disclosed cybersecurity vulnerabilities that help in tracking and addressing risks in software or hardware.

What is Nmap?

•**Nmap (Network Mapper)** is an open-source tool for network discovery and security auditing.

•It is used to:

- Discover hosts and services on a computer network.
- Identify open ports, service versions, and operating systems.

•**Key Nmap Features:**

- Port scanning, service version detection, OS detection, and script scanning.

What are CVEs?

•**CVE (Common Vulnerabilities and Exposures)** is a standardized identifier for publicly known cybersecurity vulnerabilities.

•**CVE's Role:**

  - Provides a way for organizations to track known vulnerabilities.
  - Assists in mitigating risks by addressing security issues based on published CVEs.

Problem Statement

•**Manual vulnerability scanning** can be time-consuming and error-prone.

•**Challenge:** Identifying vulnerabilities in a network requires a systematic approach with up-to-date CVE data.

•**Goal:** Automate the process of scanning for open services with Nmap and match detected services to known CVEs for better security management.

Solution Overview

- **Automate Nmap Scanning**:
  - The script runs Nmap to detect open services and versions.
- **Match CVEs to Detected Services**:
  - After Nmap identifies services, the script matches them to known vulnerabilities from a local CVE database.
- **Generate Detailed Reports**:
  - A report is created that includes Nmap scan results and CVE vulnerabilities associated with those services.

Key Features of the Application

- **Three Nmap Scan Types**:
  - **Simple Scan:** Basic scan to detect open ports.
  - **Enhanced Scan:** Includes version and OS detection.
  - **Aggressive Scan:** Comprehensive scan that includes script scanning and traceroute.

- **Automatic CVE Matching**:
  - Based on detected services, the script checks for vulnerabilities using the CVE data.

- **Report Generation**:
  - Detailed reports that include Nmap results and CVEs in a structured format.

Code Overview

•The code is structured into **several key functions**:

- **run_simple_nmap_scan()** – Runs a basic Nmap scan.
- **run_enhanced_nmap_scan()** – Runs an enhanced Nmap scan.
- **run_aggressive_nmap_scan()** – Runs an aggressive Nmap scan.
- **parse_nmap_for_services()** – Extracts open ports and services from Nmap output.
- **load_cve_data()** – Loads CVE data from a JSON file.
- **display_cve_data_for_service()** – Displays CVEs based on the matched services.

Nmap Scanning Types

- **Simple Scan**:
  - Basic Nmap scan with fewer details.
  - Command: nmap -T4 <target>

- **Enhanced Scan**:
  - Includes version and OS detection.
  - Command: nmap -p- -sV -O <target>

- **Aggressive Scan**:
  - Comprehensive scan with additional features like script scanning and traceroute.
  - Command: nmap -A <target>

Code Breakdown: Nmap Scanning

- **Simple Scan**:
  - Uses the -T4 option to speed up the scan.
  - Focuses on scanning the most common ports.

- **Enhanced Scan**:
  - Uses -p- for all ports, -sV for version detection, and -O for OS detection.

- **Aggressive Scan**:
  - Uses -A for full OS and version detection, script scanning, and traceroute.

Code Breakdown: CVE Matching

•The Nmap scan results are parsed to detect **services**.

•Each service (e.g., SSH, SMTP) is checked against **CVE data**.

•If a service matches a CVE entry, the relevant CVE details are displayed.

Function: run_simple_nmap_scan()

•**Purpose**: Runs a basic Nmap scan to detect open ports.

•**Example**:

```
nmap -T4 192.1.1.1
```

•**Returns**: Scan results in text format.

Function: run_enhanced_nmap_scan()

- **Purpose**: Runs an enhanced Nmap scan with detailed version and OS detection.
- **Example**:

```
nmap -p- -sV -O 192.1.1.1
```

- **Returns**: Detailed scan results.

Function: run_aggressive_nmap_scan()

- **Purpose**: Runs an aggressive scan with script scanning and traceroute.
- **Example**:

```
nmap -A 192.1.1.1
```

- **Returns**: Comprehensive results with extra information.

Function: parse_nmap_for_services()

- **Purpose**: Extracts open ports, services, and versions from the Nmap output.

- **Example**: Extracts data like:
    - **Port 22/tcp**: OpenSSH 8.9p1 Ubuntu

Function: load_cve_data()

- **Purpose**: Loads CVE data from a local JSON file (cve_vuln_data.json).

- **Example CVE Data**:
  - **CVE ID**: CVE-2021-41617
  - **Description**: OpenSSH 8.7 and 8.8 privilege escalation.

Function: display_cve_data_for_service()

•**Purpose**: Displays CVE information for services found in Nmap output.

•**Example**:

- **Service**: SSH
- **CVE**: CVE-2021-41617 (Privilege escalation)

User Interaction Flow

•**Step 1**: User decides whether to scan an entire network or specific IP.

•**Step 2**: User selects the type of Nmap scan.

•**Step 3**: The script runs the selected scan and parses results.

•**Step 4**: CVEs are matched with the detected services, and results are displayed.

Network Detection

- The script uses ip a to detect the local network.
- Users can choose to scan an entire network or input a specific IP to target.

Example of Simple Nmap Scan

- **Command**: nmap -T4 192.1.1.1
- **Output**:

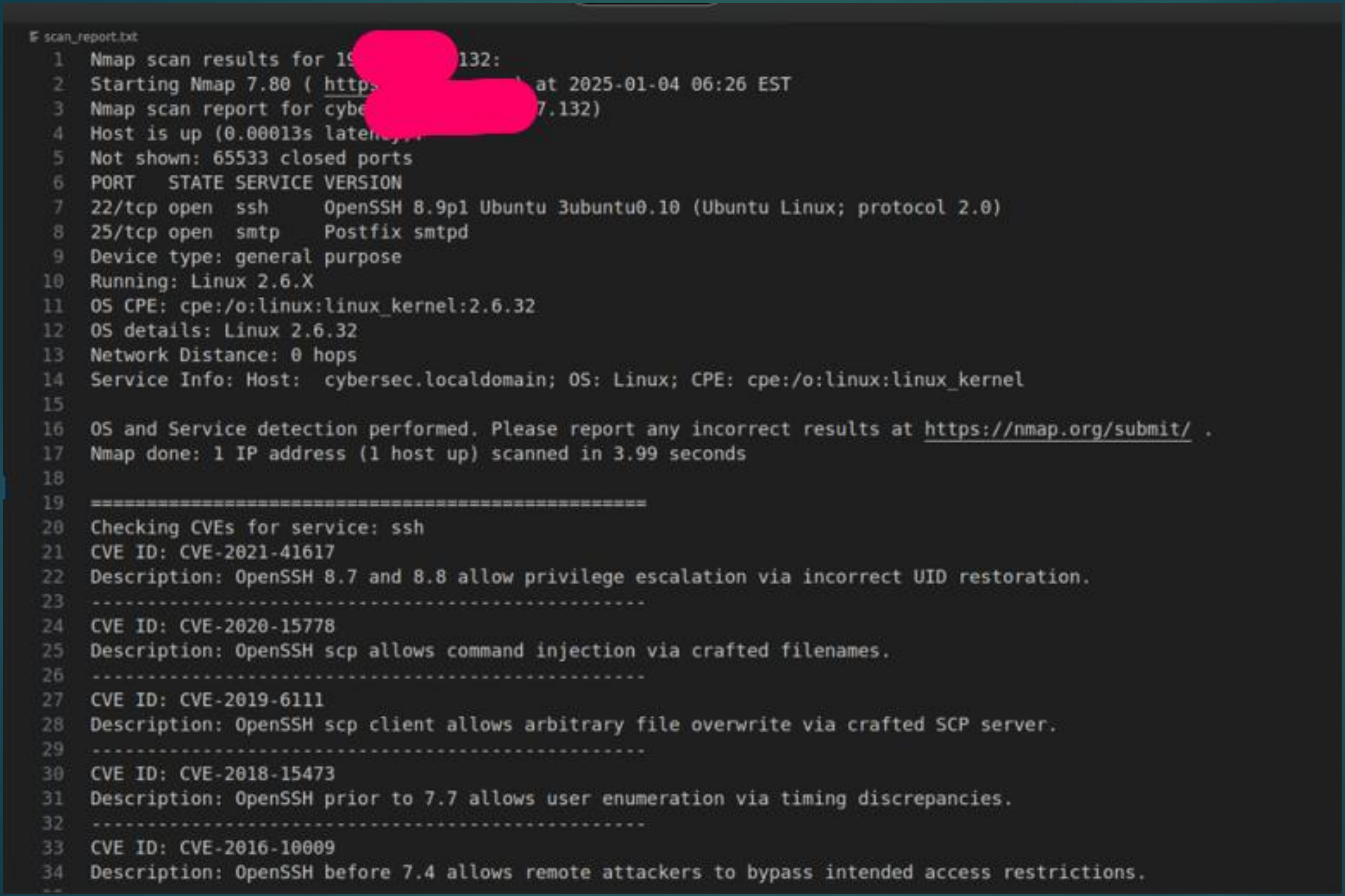
```
PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.9p1 25/tcp open smtp Postfix smtpd
```

Example of Enhanced Nmap Scan

•**Command**: nmap -p- -sV -O 192.18……..

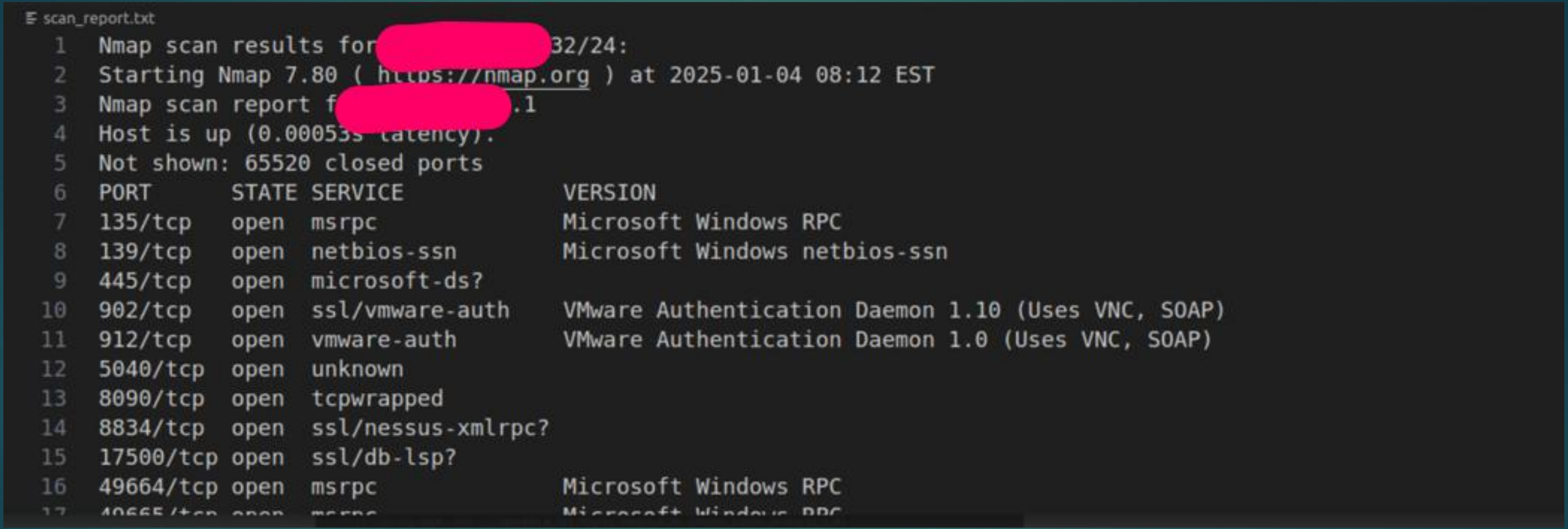
•**Output**:

```
PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.9p1 Ubuntu 25/tcp open smtp Postfix
smtpd OS: Linux 2.6.32
```



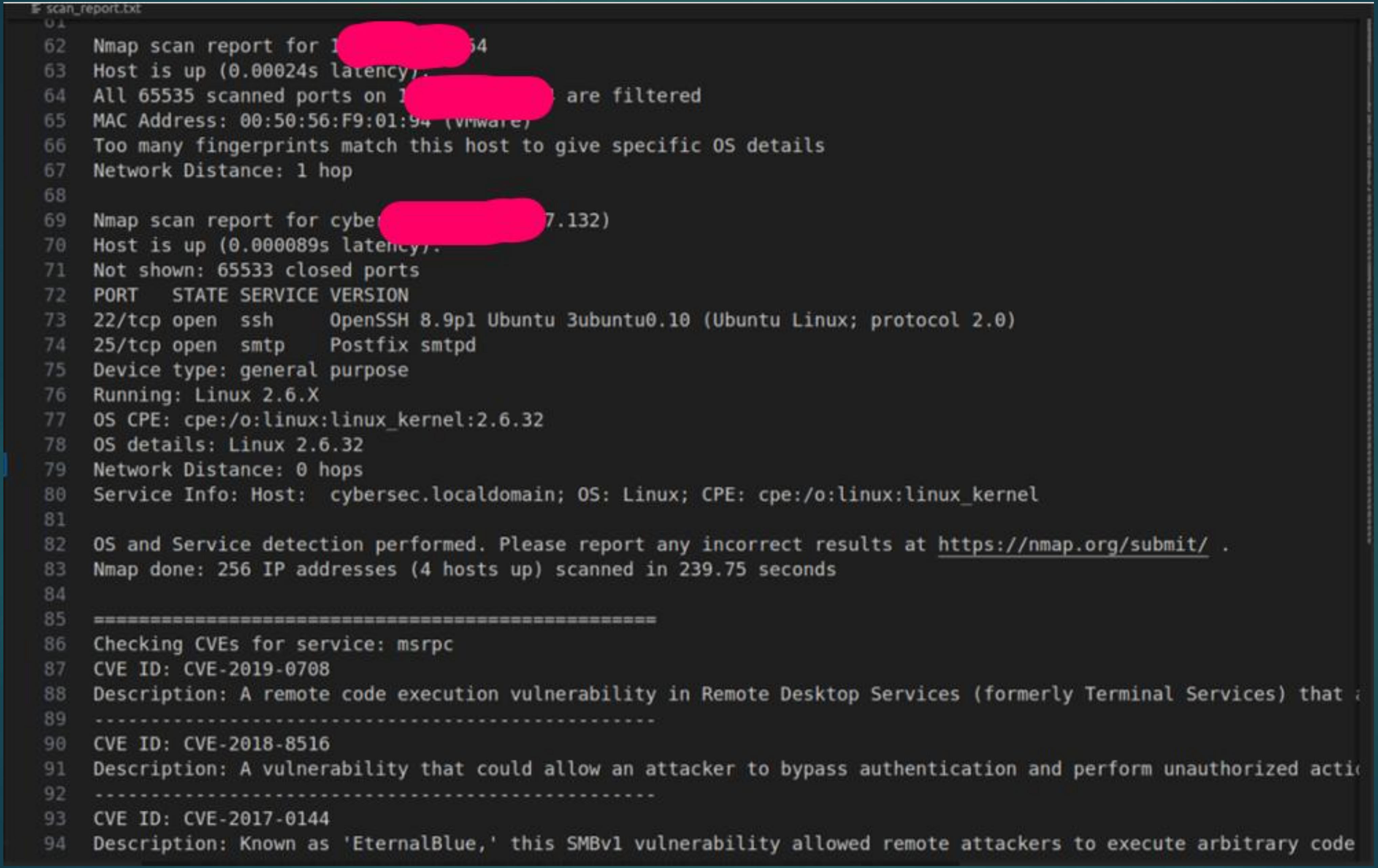
scan_report.txt

```
Nmap scan results for 19[redacted]132:
Starting Nmap 7.80 ( https[redacted] at 2025-01-04 06:26 EST
Nmap scan report for cybe[redacted]7.132)
Host is up (0.00013s laten[redacted]
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
25/tcp open  smtp    Postfix smtpd
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: Host:  cybersec.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.99 seconds

==================================================
Checking CVEs for service: ssh
CVE ID: CVE-2021-41617
Description: OpenSSH 8.7 and 8.8 allow privilege escalation via incorrect UID restoration.
--------------------------------------------------
CVE ID: CVE-2020-15778
Description: OpenSSH scp allows command injection via crafted filenames.
--------------------------------------------------
CVE ID: CVE-2019-6111
Description: OpenSSH scp client allows arbitrary file overwrite via crafted SCP server.
--------------------------------------------------
CVE ID: CVE-2018-15473
Description: OpenSSH prior to 7.7 allows user enumeration via timing discrepancies.
--------------------------------------------------
CVE ID: CVE-2016-10009
Description: OpenSSH before 7.4 allows remote attackers to bypass intended access restrictions.
```



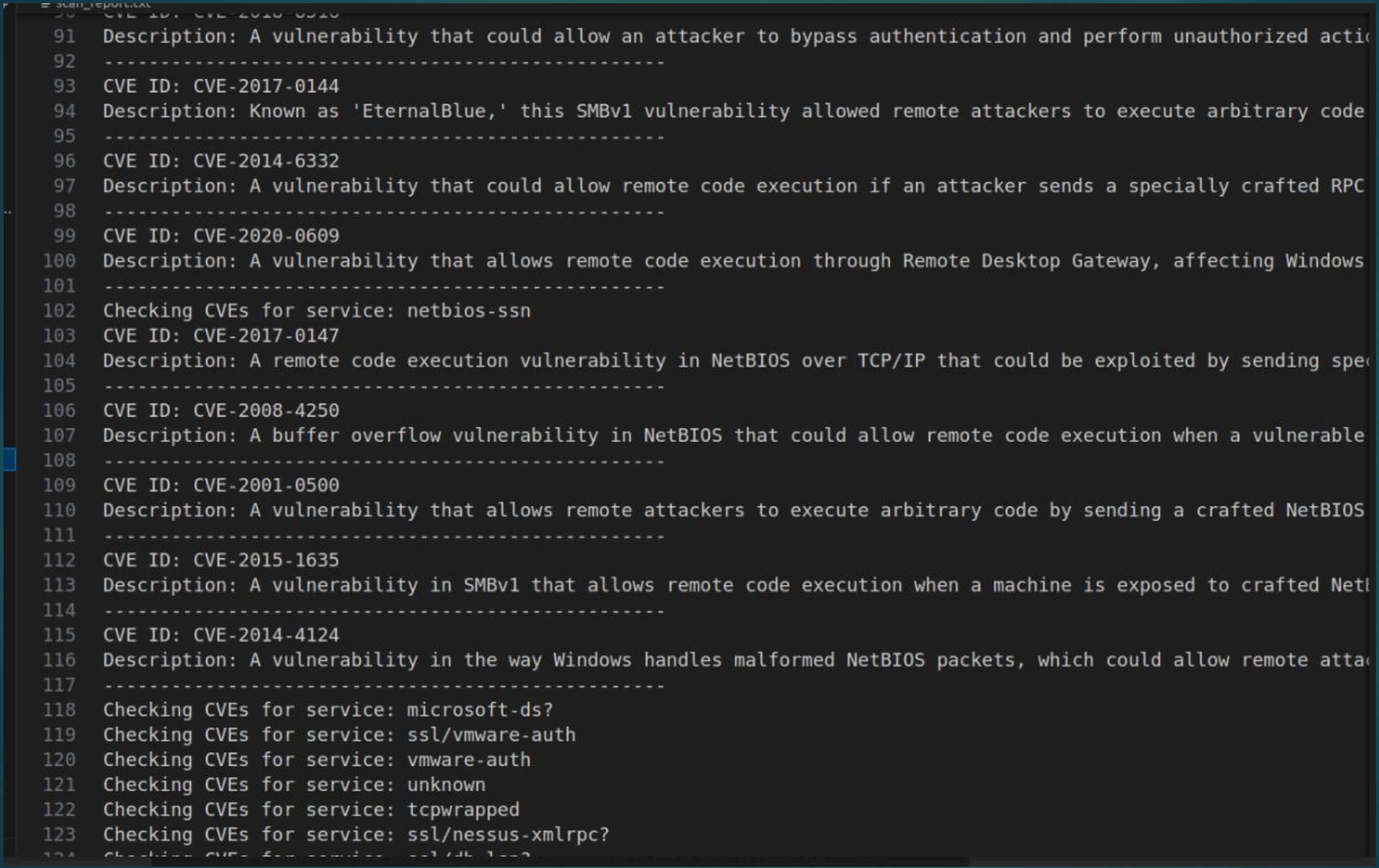
scan_report.txt

```
Nmap scan results for [redacted]32/24:
Starting Nmap 7.80 ( https://nmap.org ) at 2025-01-04 08:12 EST
Nmap scan report f[redacted].1
Host is up (0.00053s latency).
Not shown: 65520 closed ports
PORT      STATE SERVICE           VERSION
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
902/tcp   open  ssl/vmware-auth   VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth       VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5040/tcp  open  unknown
8090/tcp  open  tcpwrapped
8834/tcp  open  ssl/nessus-xmlrpc?
17500/tcp open  ssl/db-lsp?
49664/tcp open  msrpc             Microsoft Windows RPC
49665/tcp open  msrpc             Microsoft Windows RPC
```

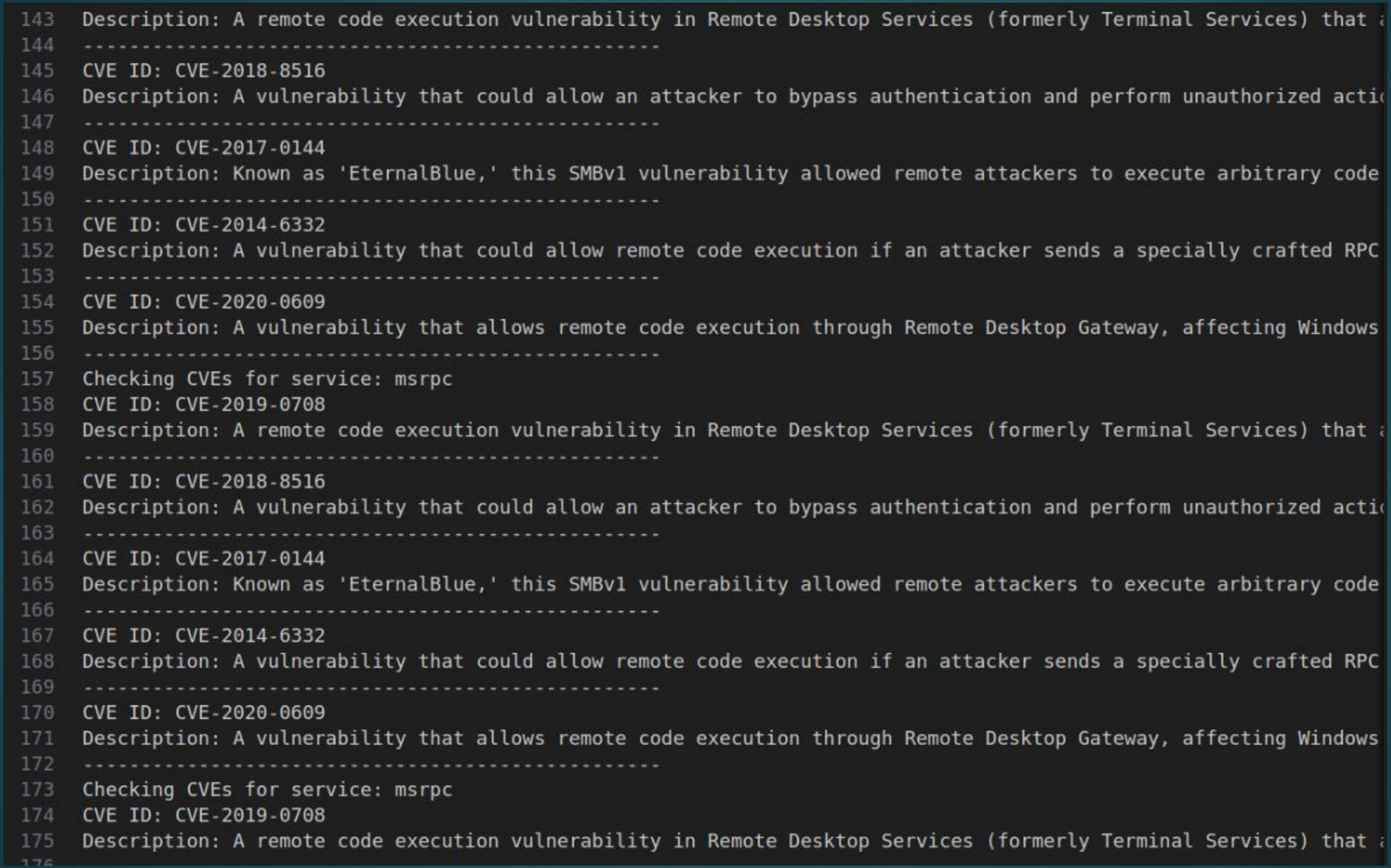


scan_report.txt

```
Nmap scan report for 1[redacted]4
Host is up (0.00024s latency).
All 65535 scanned ports on 1[redacted] are filtered
MAC Address: 00:50:56:F9:01:94 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for cybe[redacted]7.132)
Host is up (0.000089s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
25/tcp open  smtp    Postfix smtpd
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: Host:  cybersec.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 239.75 seconds

==================================================
Checking CVEs for service: msrpc
CVE ID: CVE-2019-0708
Description: A remote code execution vulnerability in Remote Desktop Services (formerly Terminal Services) that
--------------------------------------------------
CVE ID: CVE-2018-8516
Description: A vulnerability that could allow an attacker to bypass authentication and perform unauthorized acti
--------------------------------------------------
CVE ID: CVE-2017-0144
Description: Known as 'EternalBlue,' this SMBv1 vulnerability allowed remote attackers to execute arbitrary code
```



```
Description: A vulnerability that could allow an attacker to bypass authentication and perform unauthorized acti
--------------------------------------------------
CVE ID: CVE-2017-0144
Description: Known as 'EternalBlue,' this SMBv1 vulnerability allowed remote attackers to execute arbitrary code
--------------------------------------------------
CVE ID: CVE-2014-6332
Description: A vulnerability that could allow remote code execution if an attacker sends a specially crafted RPC
--------------------------------------------------
CVE ID: CVE-2020-0609
Description: A vulnerability that allows remote code execution through Remote Desktop Gateway, affecting Windows
--------------------------------------------------
Checking CVEs for service: netbios-ssn
CVE ID: CVE-2017-0147
Description: A remote code execution vulnerability in NetBIOS over TCP/IP that could be exploited by sending spe
--------------------------------------------------
CVE ID: CVE-2008-4250
Description: A buffer overflow vulnerability in NetBIOS that could allow remote code execution when a vulnerable
--------------------------------------------------
CVE ID: CVE-2001-0500
Description: A vulnerability that allows remote attackers to execute arbitrary code by sending a crafted NetBIOS
--------------------------------------------------
CVE ID: CVE-2015-1635
Description: A vulnerability in SMBv1 that allows remote code execution when a machine is exposed to crafted Net
--------------------------------------------------
CVE ID: CVE-2014-4124
Description: A vulnerability in the way Windows handles malformed NetBIOS packets, which could allow remote atta
--------------------------------------------------
Checking CVEs for service: microsoft-ds?
Checking CVEs for service: ssl/vmware-auth
Checking CVEs for service: vmware-auth
Checking CVEs for service: unknown
Checking CVEs for service: tcpwrapped
Checking CVEs for service: ssl/nessus-xmlrpc?
```



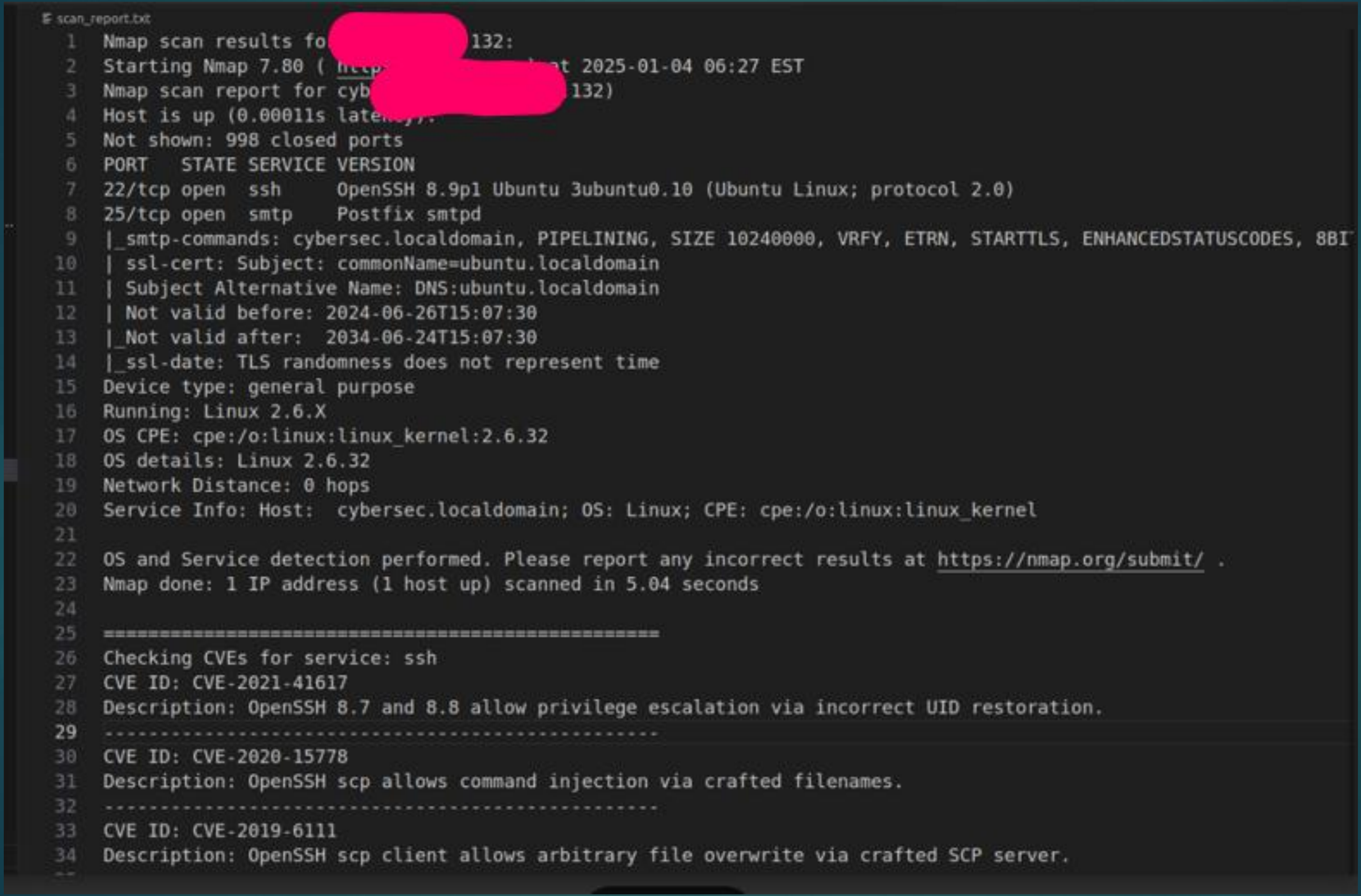
```
Description: A remote code execution vulnerability in Remote Desktop Services (formerly Terminal Services) that
--------------------------------------------------
CVE ID: CVE-2018-8516
Description: A vulnerability that could allow an attacker to bypass authentication and perform unauthorized acti
--------------------------------------------------
CVE ID: CVE-2017-0144
Description: Known as 'EternalBlue,' this SMBv1 vulnerability allowed remote attackers to execute arbitrary code
--------------------------------------------------
CVE ID: CVE-2014-6332
Description: A vulnerability that could allow remote code execution if an attacker sends a specially crafted RPC
--------------------------------------------------
CVE ID: CVE-2020-0609
Description: A vulnerability that allows remote code execution through Remote Desktop Gateway, affecting Windows
--------------------------------------------------
Checking CVEs for service: msrpc
CVE ID: CVE-2019-0708
Description: A remote code execution vulnerability in Remote Desktop Services (formerly Terminal Services) that
--------------------------------------------------
CVE ID: CVE-2018-8516
Description: A vulnerability that could allow an attacker to bypass authentication and perform unauthorized acti
--------------------------------------------------
CVE ID: CVE-2017-0144
Description: Known as 'EternalBlue,' this SMBv1 vulnerability allowed remote attackers to execute arbitrary code
--------------------------------------------------
CVE ID: CVE-2014-6332
Description: A vulnerability that could allow remote code execution if an attacker sends a specially crafted RPC
--------------------------------------------------
CVE ID: CVE-2020-0609
Description: A vulnerability that allows remote code execution through Remote Desktop Gateway, affecting Windows
--------------------------------------------------
Checking CVEs for service: msrpc
CVE ID: CVE-2019-0708
Description: A remote code execution vulnerability in Remote Desktop Services (formerly Terminal Services) that
```

Example of Aggressive Nmap Scan

•**Command**: nmap -A 192.168.47.132

•**Output**:

```
PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 8.9p1 25/tcp open smtp Postfix smtpd
```



scan_report.txt

```
Nmap scan results fo[redacted]132:
Starting Nmap 7.80 ( http[redacted]t 2025-01-04 06:27 EST
Nmap scan report for cyb[redacted]132)
Host is up (0.00011s late[redacted].
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
25/tcp open  smtp    Postfix smtpd
|_smtp-commands: cybersec.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BI
| ssl-cert: Subject: commonName=ubuntu.localdomain
| Subject Alternative Name: DNS:ubuntu.localdomain
| Not valid before: 2024-06-26T15:07:30
|_Not valid after:  2034-06-24T15:07:30
|_ssl-date: TLS randomness does not represent time
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: Host:  cybersec.localdomain; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds

==================================================
Checking CVEs for service: ssh
CVE ID: CVE-2021-41617
Description: OpenSSH 8.7 and 8.8 allow privilege escalation via incorrect UID restoration.
--------------------------------------------------
CVE ID: CVE-2020-15778
Description: OpenSSH scp allows command injection via crafted filenames.
--------------------------------------------------
CVE ID: CVE-2019-6111
Description: OpenSSH scp client allows arbitrary file overwrite via crafted SCP server.
```

Matching CVEs with Nmap Output

•**SSH**: OpenSSH 8.9p1 matched with CVE-2021-41617 (Privilege escalation) besides others.

•**SMTP**: Postfix matched with CVE-2023-42116 (Remote code execution) besides others.

Generating Vulnerability Report

•The tool generates a report that includes:

- Nmap scan results.
- CVE IDs and descriptions for vulnerable services.

- **All Pictures in This Presentation Are From The Report File**

Report Generation

•The report is saved to a file, e.g., scan_report.txt.

•Contains Nmap output and matched CVEs.

Report Example: Nmap Scan + CVE Matching

•**Scan Results**:

- **Port 22/tcp**: OpenSSH 8.9p1
- **Port 25/tcp**: Postfix SMTP

•**CVE Matches**:

- **OpenSSH**: CVE-2021-41617 (Privilege escalation)
- **Postfix**: CVE-2023-42116 (Remote code execution)

•Practical Demonstration

- A hands-on walkthrough of the tool’s execution.

single ip scan link

Entire network scan link

Future Enhancements

•Add functionality to handle more service types and CVEs.

•Include a web-based interface for easier interaction.

•Integrate with automated patching tools to address vulnerabilities.

Conclusion

•This tool automates the process of detecting vulnerabilities in a network.

•By combining Nmap scans with CVE data, organizations can identify and prioritize security risks.

•Regular vulnerability scanning helps maintain a secure network environment.

Q&A

•the floor is Open for any questions.