NETWORK VULNERABLITY ASSESEMENT

Project-1

Gudipati Rohith Kumar Reddy

Table of Contents

Project Overview:

The project aims to conduct a comprehensive assessment of the network infrastructure of [Spoorthi college] to identify and mitigate potential vulnerabilities. The assessment will encompass both internal and external network components to ensure a thorough evaluation.

Project Objectives:

1. Identify Vulnerabilities: Conduct a thorough scan and analysis of the network to identify potential vulnerabilities.

2. Assess Risk Levels: Evaluate the severity and potential impact of identified vulnerabilities on the network.

3. Recommend Mitigation Strategies: Propose effective strategies and countermeasures to mitigate identified vulnerabilities.

4. Enhance Security Posture: Improve overall network security by implementing recommended changes and best practices.

Project Scope:

1. Network Components: Assess all critical network components including routers, switches, firewalls, servers, and endpoints.

2. Network Protocols: Evaluate vulnerabilities related to TCP/IP protocols, DNS, DHCP, etc.
3. External Assessment: Perform external scans to identify vulnerabilities accessible from outside the organization's network.

4. Internal Assessment: Conduct internal scans to identify vulnerabilities within the organization's internal network.

5. Wireless Network: Assess vulnerabilities related to Wi-Fi networks and access points.

6. Web Applications: Scan web applications hosted on the network for security vulnerabilities.

Project Methodology:

1. Preparation: o Define scope and objectives. o Obtain necessary permissions and approvals. o Set up scanning tools and resources.

2. Vulnerability Scanning:

o Conduct external and internal network scans using appropriate vulnerability scanning tools (e.g., Nessus, OpenVAS, and Nmap).

o Analyse scan results to identify vulnerabilities.

3. Risk Assessment:

o Prioritize identified vulnerabilities based on severity (e.g., CVSS scores).

o Assess potential impact on network security and operations.

4. Mitigation Strategy:

o Develop a plan to address identified vulnerabilities.

o Prioritize mitigation efforts based on risk assessment.

5. Implementation:

o Implement recommended changes and security patches.

o Verify effectiveness of mitigation measures.

6. Documentation and Reporting:

o Compile assessment findings into a comprehensive report.

o Create an executive summary and presentation for stakeholders.

Resources Required:

- Vulnerability Scanning Tools: Nessus, OpenVAS, Nmap, Wapplazyer.
- Documentation Tools: Microsoft Office Suite, reporting templates.
- Communication Tools: Email, Mobiles, WhatsApp.

Tools used in project:

- Nessus: A comprehensive vulnerability scanning tool that can identify a wide range of vulnerabilities across the network infrastructure.
- Nexpose Community: An open-source vulnerability-scanning tool developed by Rapid7 that can automatically detect new devices and evaluate vulnerabilities.
- Nikto: An open-source web server scanner that can check for outdated server versions and scan for potentially dangerous files and programs.
- Wireshark: A powerful network protocol analyzer that can capture and analyze network traffic to identify security issues.
- Aircrack: A tool focused on Wi-Fi security that can be used for network auditing and retrieving lost encryption keys.
- Nmap: A network reconnaissance tool that can be used to identify active hosts, open ports, and running services on the target network.
- Maltego: A vulnerability assessment tool that can prioritize scanning, detect vulnerabilities, and generate comprehensive reports.

Purpose of the Network Vulnerability Assessment:

The main Aim of Network Vulnerability test has to identify the vulnerabilities in network and Websites Using the Above tools.

Target Network: Spoorthi.in

Website URL: https://spurthy.in/

Registration on: 2022-05-12

Expires on: 2025-05-12

Server Names

ns1.dns-parking.com 162.159.24.201

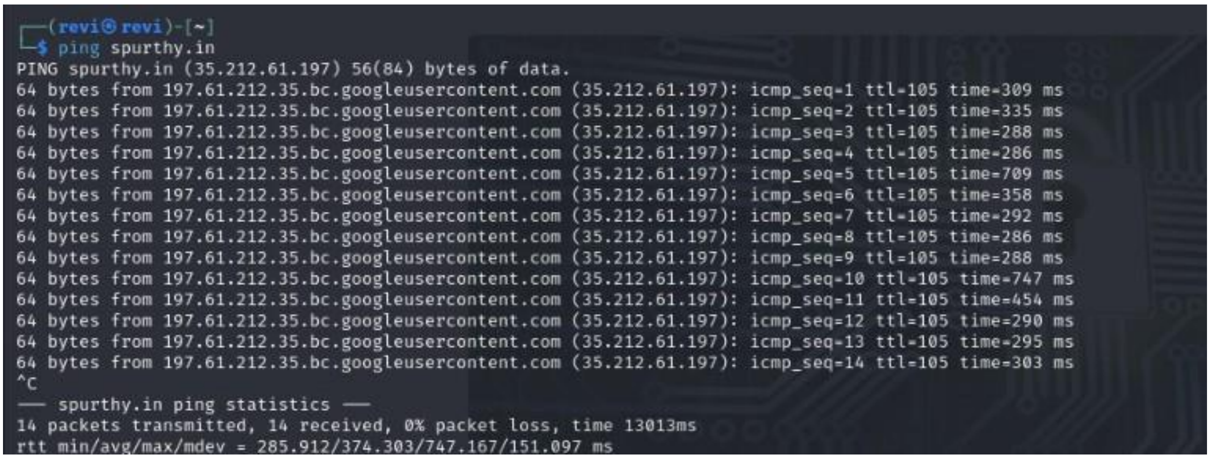
ns2.dns-parking.com 162.159.25.42

IPV4: 35.212.61.197

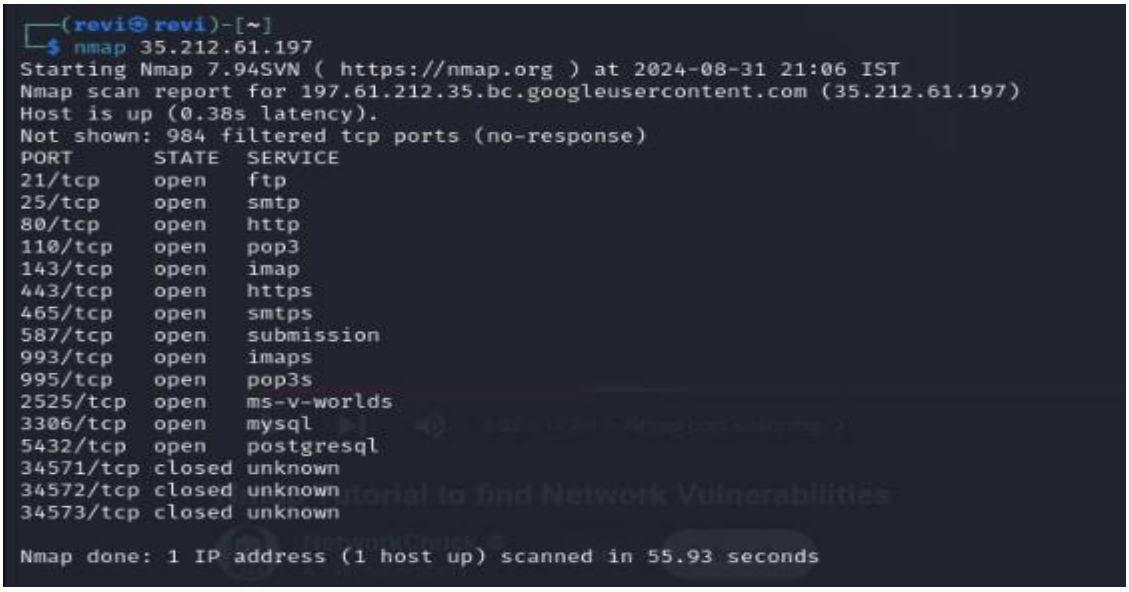
Usage of the tools in this project

NMAP (Port Scanner) - I performed Nmap for port scanning on this website, there some open ports

- 21/tcp ftp
- 143/tcp imap
- 443/tcp https
- 993/tcp imaps
- 995/tcp pop3s
- 2525/tcp ms-v-worlds
- 3306/tcp mysql
- 5432/tcp postgresql

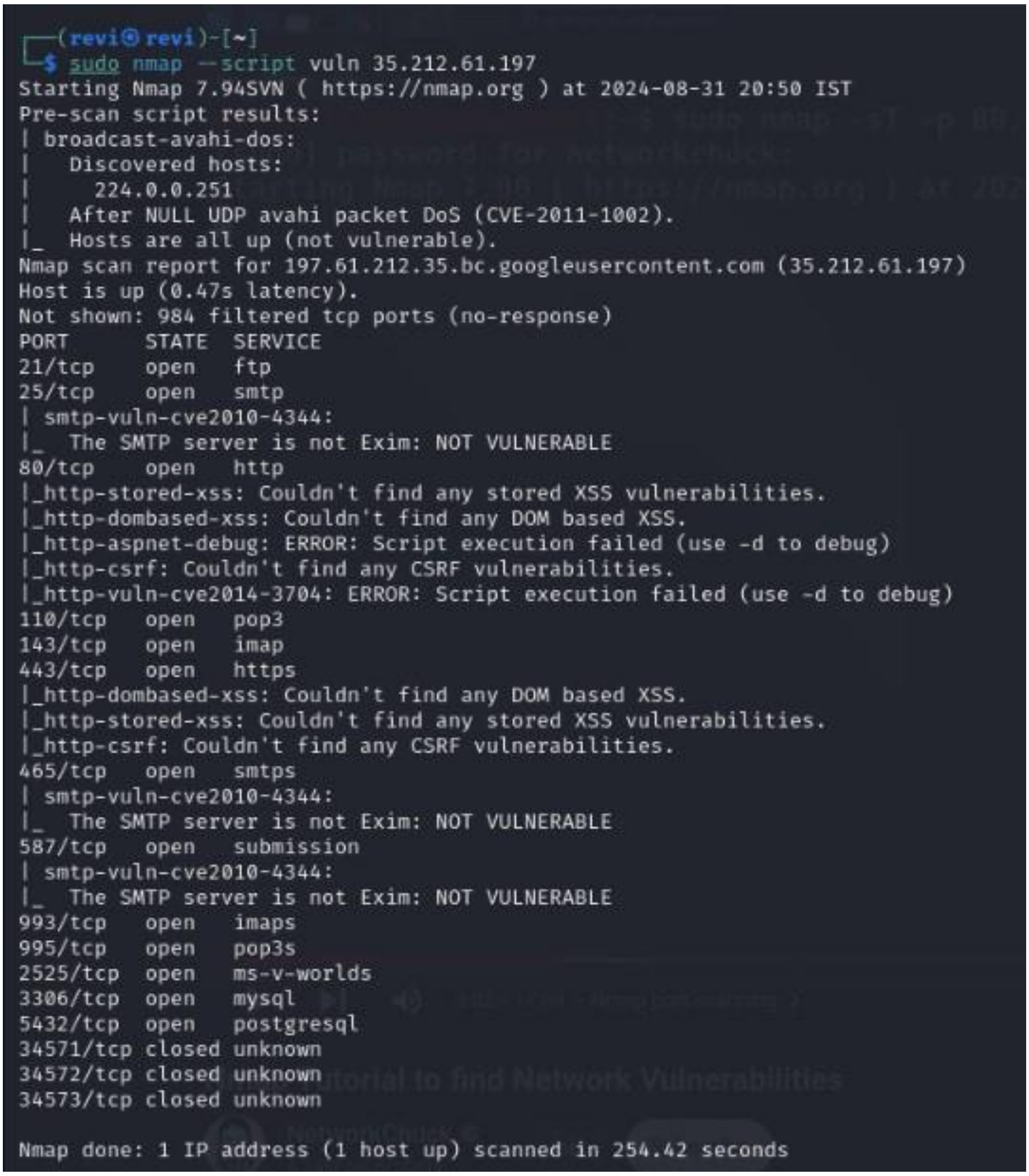


```
┌──(revi㉿revi)-[~]
└─$ ping spurthy.in
PING spurthy.in (35.212.61.197) 56(84) bytes of data.
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=1 ttl=105 time=309 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=2 ttl=105 time=335 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=3 ttl=105 time=288 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=4 ttl=105 time=286 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=5 ttl=105 time=709 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=6 ttl=105 time=358 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=7 ttl=105 time=292 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=8 ttl=105 time=286 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=9 ttl=105 time=288 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=10 ttl=105 time=747 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=11 ttl=105 time=454 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=12 ttl=105 time=290 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=13 ttl=105 time=295 ms
64 bytes from 197.61.212.35.bc.googleusercontent.com (35.212.61.197): icmp_seq=14 ttl=105 time=303 ms
^C
── spurthy.in ping statistics ──
14 packets transmitted, 14 received, 0% packet loss, time 13013ms
rtt min/avg/max/mdev = 285.912/374.303/747.167/151.097 ms
```



```
┌──(revi㉿revi)-[~]
└─$ nmap 35.212.61.197
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 21:06 IST
Nmap scan report for 197.61.212.35.bc.googleusercontent.com (35.212.61.197)
Host is up (0.38s latency).
Not shown: 984 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
25/tcp    open   smtp
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
465/tcp   open   smtps
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
2525/tcp  open   ms-v-worlds
3306/tcp  open   mysql
5432/tcp  open   postgresql
34571/tcp closed unknown
34572/tcp closed unknown
34573/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 55.93 seconds
```



```
┌──(revi㉿revi)-[~]
└─$ sudo nmap --script vuln 35.212.61.197
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-31 20:50 IST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 197.61.212.35.bc.googleusercontent.com (35.212.61.197)
Host is up (0.47s latency).
Not shown: 984 filtered tcp ports (no-response)
PORT      STATE  SERVICE
21/tcp    open   ftp
25/tcp    open   smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
80/tcp    open   http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
465/tcp   open   smtps
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
587/tcp   open   submission
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
993/tcp   open   imaps
995/tcp   open   pop3s
2525/tcp  open   ms-v-worlds
3306/tcp  open   mysql
5432/tcp  open   postgresql
34571/tcp closed unknown
34572/tcp closed unknown
34573/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 254.42 seconds
```

Air crack: - A tool focused on Wi-Fi security that can be used for network auditing and retrieving lost encryption keys. Using this tool, I will be able to find wireless connection security vulnerability that maintain username & Password is Default like Admin & admin.

- I will Update the Username and Password
- Password Encryption Become stronger
- Apply Mac Filtration
- Ip Scanning and Device Identification
- Ip Camera Device Authentication check.

Wireshark: A powerful network protocol analyser that can capture and analyse network traffic to identify security issues.

- Packet sniffing
- Packet Capturing
- Username and Password Capturing (Sniff)
- Traffic analyser

Nexpose Community: An open-source vulnerability-scanning tool developed by rapid7 that can automatically detect new devices and evaluate vulnerabilities. This tool generally checks for hardware vulnerability and operating system bugs or outdated software's, drivers about the device. I check this organization everything will be fine and not detect any hardware vulnerability and change router will be change for greater hardware support for wireless Internet.

Conclusion

In conclusion, penetration testing plays a crucial role in strengthening an organization's security posture. By simulating real-world attacks, pentesting helps identify vulnerabilities before malicious actors can exploit them, allowing for timely remediation. This proactive approach not only enhances the security of systems and data but also builds resilience against potential breaches.

Effective penetration testing involves a thorough assessment of an organization's IT infrastructure, applications, and network configurations. The insights gained from these tests provide valuable feedback for improving security policies, practices, and technologies.

Regular pentesting, combined with continuous monitoring and updates, ensures that security measures evolve alongside emerging threats.

Ultimately, the benefits of penetration testing extend beyond merely addressing weaknesses; they foster a culture of security awareness and preparedness within the organization. By prioritizing and investing in pentesting, organizations can better safeguard their assets, protect sensitive information, and maintain trust with clients and stakeholders.