SecuScan Project Report

Exploring Nmap and Shodan.io

Group Name: SecuScan

Course: INFO 2411 (S11)

Members

*Name: Dilraj Kaur (100447804) and Sukhdeep Singh(*100447918)

Submitted to: Prof. Benjamin Kwan

Date of Submission: 26 November 2024

1. Introduction

In today's digital age, protecting networks and devices is more important than ever. Two powerful tools, **Nmap** and **Shodan**, help security professionals keep systems safe. **Nmap** is used to scan networks and find open doors (ports) that could be exploited, while **Shodan** is like a search engine for finding devices connected to the internet. Both tools are widely used in cybersecurity education and the industry for identifying vulnerabilities and improving security. The goal is to provide a clear understanding of how to use them effectively, while also discussing their ethical considerations.

---

2. Overview of Nmap

Nmap, short for **Network Mapper**, is a powerful, open-source network scanning tool for network exploration and security auditing. It is largely designed to rapidly scan large networks, although it works fine against single host. It is primarily used to discover hosts and services on a computer network. It achieves this by sending specially crafted packets to targets and analyzing their responses.

2.1 Features of Nmap

- Host Discovery: Identifies active devices on a network.
- Port Scanning: Discovers open ports and associated services.
- OS Detection: Determines the operating system of a target machine.
- Vulnerability Scanning: Highlights known weaknesses in services or systems.

2.2 Importance of Nmap

Nmap is critical for:

- Network inventory management.
- Identifying security vulnerabilities before attackers exploit them.
- Mapping network layouts for troubleshooting.

---

3. Types of Nmap Scans

Nmap offers several scan types to suit various needs. Here are the key ones:

3.1 TCP Connect Scan (-sT)

- This is the simplest type of scan.
- It connects fully to a device to see if a port is open.

- It is reliable but slower and easier to detect.

3.2 SYN Scan (-sS)

- Known as a "stealth scan," it does not fully connect to a device, making it quicker and harder to detect.
- It is great for speed and efficiency

3.3 UDP Scan (-sU)

- Checks for open UDP ports.
- Slower and less reliable due to UDP's connectionless nature.

3.4 Version Detection (-sV)

- Identifies the versions of services running on open ports.

3.5 OS Detection (-O)

- Detects the operating system based on response signatures.

3.6 Aggressive Scan (-A)

- Combines version detection, OS detection, script scanning, and traceroute.
- It is thorough but slower.

---

4. Nmap Timing Templates

Timing templates allow users to balance speed and stealth in scans. They range from **T0 (Paranoid)**

- **T0 (Paranoid)**: Extremely slow and avoids detection by IDS, suitable for highly stealthy scans.
- **T1 (Sneaky)**: Slow and stealthy, ideal for networks where avoiding detection is crucial.
- **T2 (Polite)**: Slower than normal but less likely to overwhelm the target network.
- **T3 (Normal)**: The default option, balancing speed and stealth effectively.
- **T4 (Aggressive)**: Faster and ideal for scanning local networks (LANs).
- **T5 (Insane)**: Extremely fast but risks overloading the network and being detected.

Practical Use

Compare scan times:

nmap -A -T5 target_ip

nmap -A -T3 target_ip

This command runs an aggressive, comprehensive scan on the target.

Analyzing time differences highlights how timing affects performance.

---

5. Masking Sources of Scans

Masking the source of a scan is critical for hiding the scanner's identity. Nmap offers techniques like decoys (-D).

5.1 Decoy Scanning (-D)

Sends fake IP addresses along with your real IP to confuse the target.

Command:

```
nmap -D RND:10 target_ip
```

By using tools like **Wireshark**, we can confirm that the decoys are working by watching the network traffic.

5.2 Ethical Considerations

- Always have permission before masking scans.
- Unauthorized use can lead to legal consequences.

---

6. Automating Nmap with Python

Automation enhances the efficiency of repetitive scanning tasks. Instead of typing the same Nmap commands over and over, you can use Python scripts to automate the process. Python is easy to learn and works well with Nmap.

6.1 Sample Python Script

This script runs an Nmap command and saves the output:

```
import os

# Run Nmap scan

os.system("nmap -A -T3 target_ip > scan_results.txt")
```

6.2 Practical Automation Use Cases

- Automate scans on multiple IPs.
- Schedule regular network audits.

7. Python3 in Network Security

Python3 is a programming language that makes it easy to create scripts for automating tasks. In cybersecurity, Python3 is super useful because it helps automate things like scanning networks, analyzing data, and finding vulnerabilities.

7.1 Why Use Python3?

- **Saves Time**: Instead of typing commands repeatedly, Python3 can run them automatically.
- **Works Well with Tools**: Python3 can connect to tools like Nmap and Shodan, making them even more powerful.
- **Customizable**: You can create your own scripts to suit your specific needs.

---

8. Overview of Shodan.io

Shodan is a search engine that looks for devices connected to the internet, like webcams, routers, and smart gadgets. While Google focuses on websites, Shodan focuses on devices. It's widely used in cybersecurity to find devices that may be vulnerable.

8.1 Features of Shodan

- **Device Search**: Shodan shows devices like cameras, printers, and industrial control systems connected to the internet.
- **Open Ports**: It lists the ports these devices have open and what services are running.
- **Vulnerabilities**: Shodan highlights devices with known security flaws.
- **Trends**: Researchers can use Shodan to study global trends in device usage

8.2 Benefits of Shodan

- Enables vulnerability assessment without direct scanning.
- Provides insights into global device exposure.

---

9. Using Shodan for Vulnerability Analysis

9.1 Searching for Exposed Devices

Shodan has its own search syntax, which makes it powerful but a bit technical.

- Search for webcams:

  shodan search "webcam"

- Identify devices with default passwords:

  shodan search "default password"

---

10. Relevance to the Course

- **Hands-On Learning:** Tools like Nmap are used in labs to teach students how to scan and secure networks.
- **Real-World Scenarios:** Shodan demonstrates the risks of poorly configured devices in the real world.
- **Ethical Hacking:** These tools are fundamental for penetration testing and vulnerability assessments.

---

11. Current Use in the Industry

11.1 Nmap in the Industry

- **Network Audits**: Companies use Nmap to regularly check their systems for security holes.
- **Penetration Testing**: Ethical hackers rely on Nmap to simulate attacks and find weaknesses before real hackers do.
- **Compliance**: Many security standards require vulnerability assessments, and Nmap is often the tool of choice.

11.2 Shodan in the Industry

- **oT Security**: Shodan helps identify insecure IoT devices that could be exploited.
- **Incident Response**: During cyberattacks, Shodan is used to quickly locate vulnerable systems.
- **Research**: Shodan is widely used by researchers to study global trends in internet-connected device

---

12. Ethical Use of Nmap and Shodan

While these tools are powerful, ethical guidelines must be followed:

- Always obtain permission before scanning.
- Use findings to improve security, not exploit vulnerabilities.
- Document actions transparently in professional environments.

13. Conclusion

Nmap and Shodan are essential tools for understanding and securing networks. Nmap helps scan and find vulnerabilities on local networks, while Shodan gives a global view of internet-connected devices. They are widely used in cybersecurity courses and the industry to teach practical skills and protect systems from attacks.

By learning to use these tools ethically and effectively, cybersecurity professionals can make the digital world safer for everyone.

References

Shodan Help Center. Shodan Help Center

Nmap: The Network Mapper - Free Security Scanner. Nmap: the Network Mapper - Free Security Scanner