

MIT WORLD PEACE UNIVERSITY

Vulnerability Identification and Penetration Testing
Third Year B. Tech, Semester 6

CREATING PROTOCOL-SPECIFIC TARGET LISTS
FOR VULNERABILITY DISCOVERY

ASSIGNMENT 5

Prepared By

Krishnaraj Thadesar
Cyber Security and Forensics
Batch A1, PA 10

April 21, 2024

Contents

1	Aim	1
2	Objectives	1
3	Theory	1
3.1	grep	1
3.2	Uses	1
3.3	Advantages	1
3.4	Disadvantages	1
4	Implementation	1
4.1	Greppable Scan for Port 22 on Target IP Address	1
5	Platform	2
6	FAQs	2
7	Conclusion	3

1 Aim

To create protocol-specific target lists for vulnerability discovery.

2 Objectives

1. To understand the concept of protocol-specific target lists.
2. To create a target list for a specific protocol.
3. To use Grep to search for vulnerabilities in the target list.

3 Theory

3.1 grep

3.2 Uses

- Searching for patterns or text within files.
- Filtering command output based on specific criteria.
- Extracting relevant information from large datasets.
- Automating tasks through scripting and regular expressions.

3.3 Advantages

- Fast and efficient searching capability.
- Support for regular expressions, enabling complex pattern matching.
- Versatility in handling various file formats and input sources.
- Integration with other command-line tools and scripting languages.

3.4 Disadvantages

- Limited graphical user interface (GUI), requiring familiarity with command-line usage.
- Learning curve for mastering regular expressions and advanced search techniques.
- May produce overwhelming output in certain scenarios, requiring careful filtering.
- Reliance on textual data, making it less suitable for analyzing binary or structured data.

4 Implementation

4.1 Greppable Scan for Port 22 on Target IP Address

Syntax

```
$ nmap -p <port> -oG <target>
```

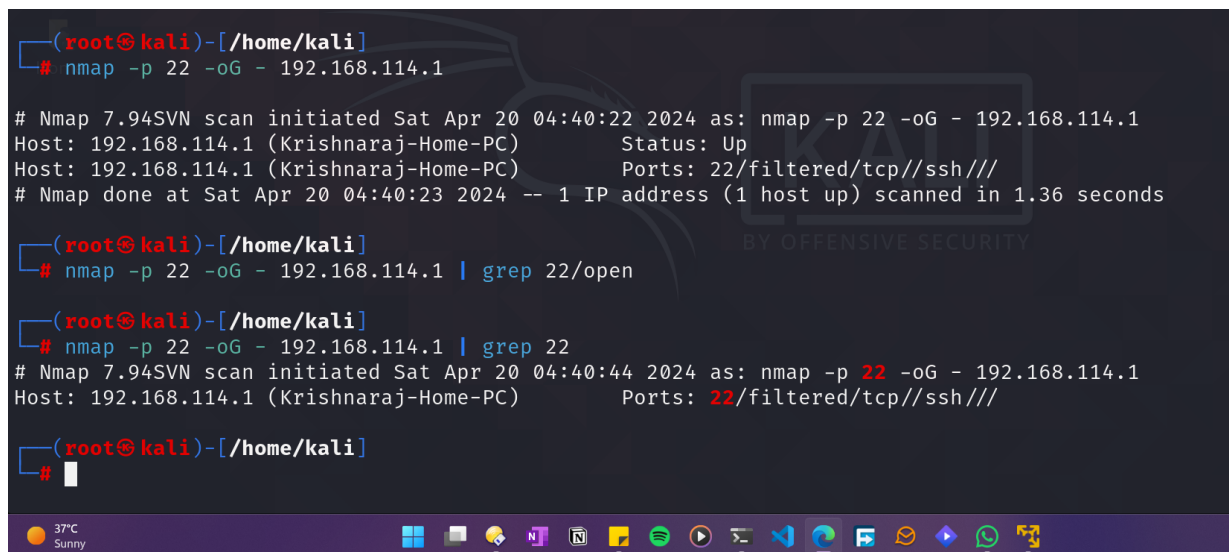
Command

```
$ nmap -p 22 -oG 192.168.114.1
```

Purpose

This command performs a grepable scan specifically for port 22 on the target IP address

Output



```
(root@kali)-[/home/kali]
# nmap -p 22 -oG - 192.168.114.1

# Nmap 7.94SVN scan initiated Sat Apr 20 04:40:22 2024 as: nmap -p 22 -oG - 192.168.114.1
Host: 192.168.114.1 (Krishnaraj-Home-PC) Status: Up
Host: 192.168.114.1 (Krishnaraj-Home-PC) Ports: 22/filtered/tcp//ssh//
# Nmap done at Sat Apr 20 04:40:23 2024 -- 1 IP address (1 host up) scanned in 1.36 seconds

(root@kali)-[/home/kali]
# nmap -p 22 -oG - 192.168.114.1 | grep 22/open

(root@kali)-[/home/kali]
# nmap -p 22 -oG - 192.168.114.1 | grep 22
# Nmap 7.94SVN scan initiated Sat Apr 20 04:40:44 2024 as: nmap -p 22 -oG - 192.168.114.1
Host: 192.168.114.1 (Krishnaraj-Home-PC) Ports: 22/filtered/tcp//ssh//

(root@kali)-[/home/kali]
#
```

Figure 1: Output of the command

5 Platform

Operating System: Arch Linux X8664

IDEs or Text Editors Used: Visual Studio Code

6 FAQs

1. What the different scanning flags are there in nmap? Explain them.

- **-sS (TCP SYN scan):** Stealthy scan technique that sends SYN packets to target ports to determine their state.
- **-sT (TCP connect scan):** Establishes full TCP connections to target ports, suitable for systems where SYN packets are blocked.
- **-sU (UDP scan):** Scans for open UDP ports by sending UDP packets to target ports and analyzing responses.
- **-sF (TCP FIN scan):** Sends TCP FIN packets to target ports to determine their state, useful for evading detection by firewalls.

- **-sX (Xmas scan)**: Sends TCP packets with FIN, PSH, and URG flags set to target ports, used for detecting firewall filtering rules.
2. **What is a grepable format?**
 - Grepable format: A machine-readable format produced by Nmap that allows for easy parsing and filtering of scan results using command-line tools like grep.
 - Each line in the output corresponds to a single host or port, with fields separated by tabs for easy processing.
 3. **Write a command to perform a grepable scan for port number 80 to check status as closed.**
 - `nmap -p80 -open -oG scanresults.txt <target>` (Replace <target> with the target IP address or hostname)
 - This command performs a grepable scan specifically for port 80 to check if it is closed, saving the results to a file named "scanresults.txt".

7 Conclusion

In this assignment, we learned about creating protocol-specific target lists for vulnerability discovery. We explored the concept of grepable formats and how they can be used to search for vulnerabilities in target lists. By creating custom target lists and using grep to filter the results, we can identify potential security issues and take appropriate actions to mitigate them.