TIMOTHY SEWE OGODE(CSSA0423076)

CYBER SHUJAA

WEEK 4

2. NETWORK ENUMERATION

Table of Contents

[1. INTRODUCTION 2](#_Toc137476807)

[Enumeration 2](#_Toc137476808)

[Introduction to Nmap 2](#_Toc137476809)

[2. HOST ENUMERATION 2](#_Toc137476810)

[Host Discovery 2](#_Toc137476811)

[Task 2](#_Toc137476812)

[Host and Port Scanning 2](#_Toc137476813)

[Task 3](#_Toc137476814)

[Saving the Results 3](#_Toc137476815)

[Task 4](#_Toc137476816)

[Service Enumeration 4](#_Toc137476817)

[Task 5](#_Toc137476818)

[Nmap Scripting Engine 5](#_Toc137476819)

[Task 5](#_Toc137476820)

[Performance 6](#_Toc137476821)

[3. Bypass Security Measures 6](#_Toc137476822)

[Firewall & IDPS Evasion 6](#_Toc137476823)

[Firewall & IDPS Evasion (easy lab) 6](#_Toc137476824)

[Task 6](#_Toc137476825)

[Firewall and IDS/IPS Evasion (Medium Lab) 7](#_Toc137476826)

[Task 7](#_Toc137476827)

[Firewall and IDS/IPS Evasion (Hard Lab) 7](#_Toc137476828)

[Task 7](#_Toc137476829)

[4. CONCLUSION 8](#_Toc137476830)

# INTRODUCTION

Nmap is used to identify and scan systems on the network. It is an important part of network diagnostics and evaluation of network-connected systems. In this module, we will learn the basics of this tool and how it can be used efficiently to map out the internal network by identifying live hosts and performing port scanning, service enumeration, and operating system detection.

## Enumeration

Enumeration is a critical process in cybersecurity that involves gathering detailed information about computer systems and networks. It helps security professionals understand the target environment, identify vulnerabilities, and develop effective defence strategies. By employing techniques like port scanning and service enumeration, experts can uncover crucial data such as open ports, running services, and network topology. This information allows them to prioritize efforts, patch vulnerabilities, and secure the system.

## Introduction to Nmap

Nmap, an open-source network analysis and security auditing tool, is widely used by network administrators and IT security specialists. It scans networks, identifies available hosts, and determines services, applications, and operating systems running on them. It can also assess firewall and intrusion detection system settings. With various scan techniques available, such as TCP-SYN scan, Nmap enables network mapping, port identification, vulnerability assessment, and OS detection. Its simplicity and versatility make it a valuable tool in auditing network security and conducting penetration tests.

# HOST ENUMERATION

## Host Discovery

When conducting an internal penetration test for a company's entire network, it is crucial to obtain an overview of the online systems available for testing. Nmap provides various host discovery options for actively identifying these systems on the network. One effective method is to use ICMP echo requests, which determine if a target host is alive. By scanning network ranges, IP lists, or individual IP addresses, Nmap can detect active hosts and store the results for later analysis, documentation, and reporting. This allows penetration testers to gather essential information about the network's live systems.

### Task

Based on the last result, find out which operating system it belongs to. Submit the name of the operating system as result. Windows (because of the ttl value 128 which is for windows)

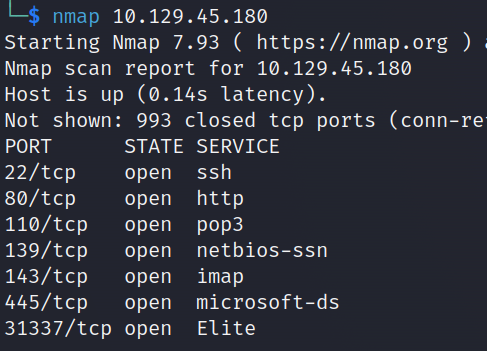


## Host and Port Scanning

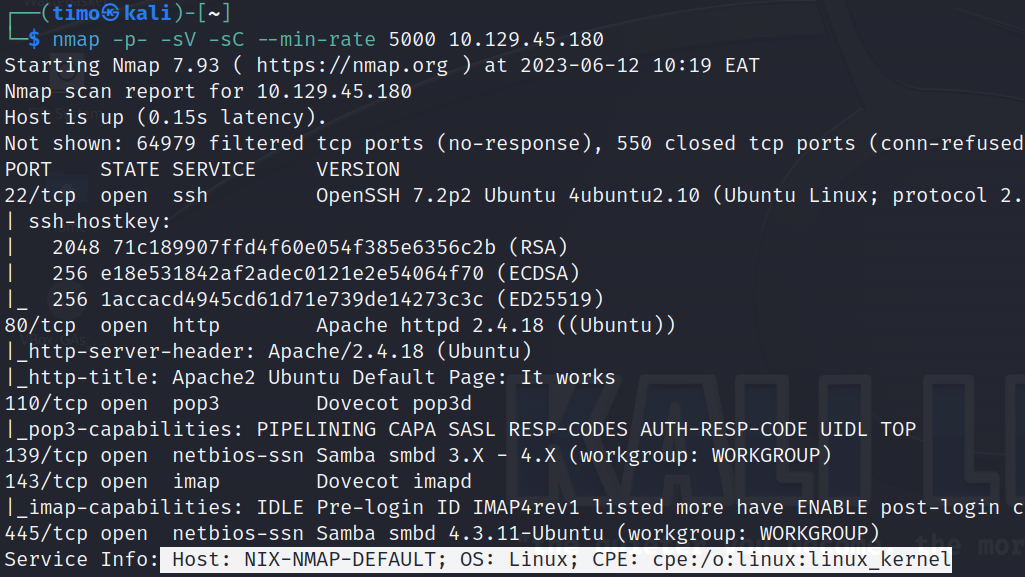
In order to understand the scanning methods and obtain more accurate information about a system, we analyse various aspects. These include identifying open ports and their associated services, service versions, information provided by the services, and the operating system. Nmap offers different states for scanned ports, such as open, closed, filtered, unfiltered, open|filtered, and closed|filtered. The tool allows scanning specific ports, top ports, or all ports, depending on the requirements. The Connect scan (TCP) is commonly used for accurate port detection while minimizing detection. Additionally, filtered ports may indicate the presence of firewalls with specific rules. UDP scans provide insights into open UDP ports, although they are slower due to the stateless nature of UDP.

### Task

Find all TCP ports on your target. Submit the total number of found TCP ports as the answer. 7



Enumerate the hostname of your target and submit it as the answer. nix-nmap-default

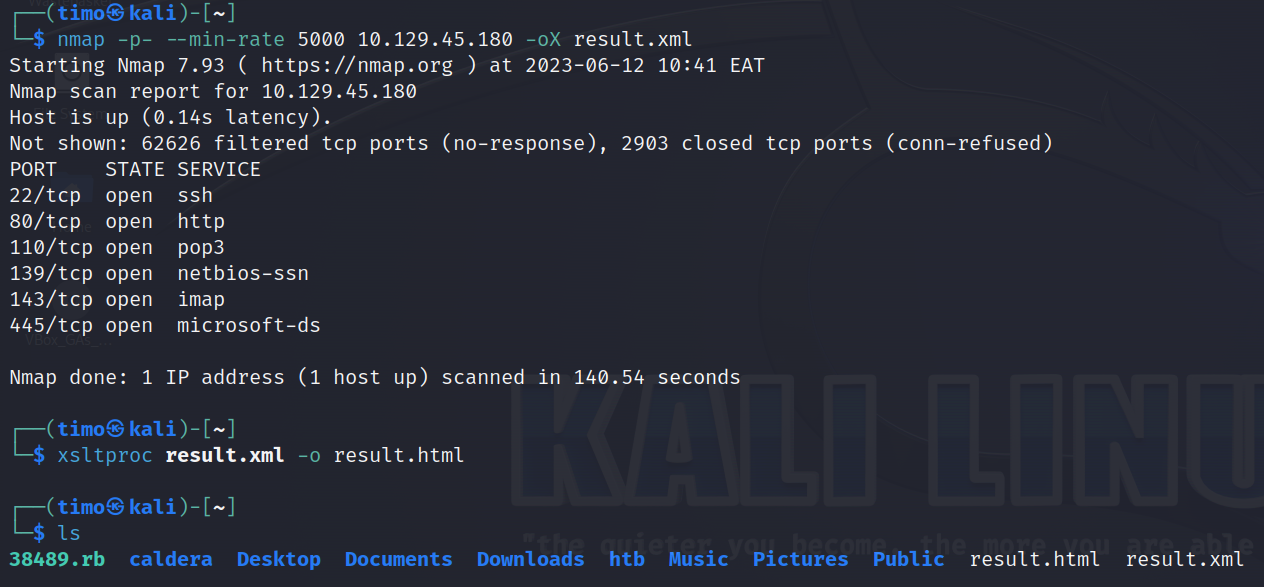


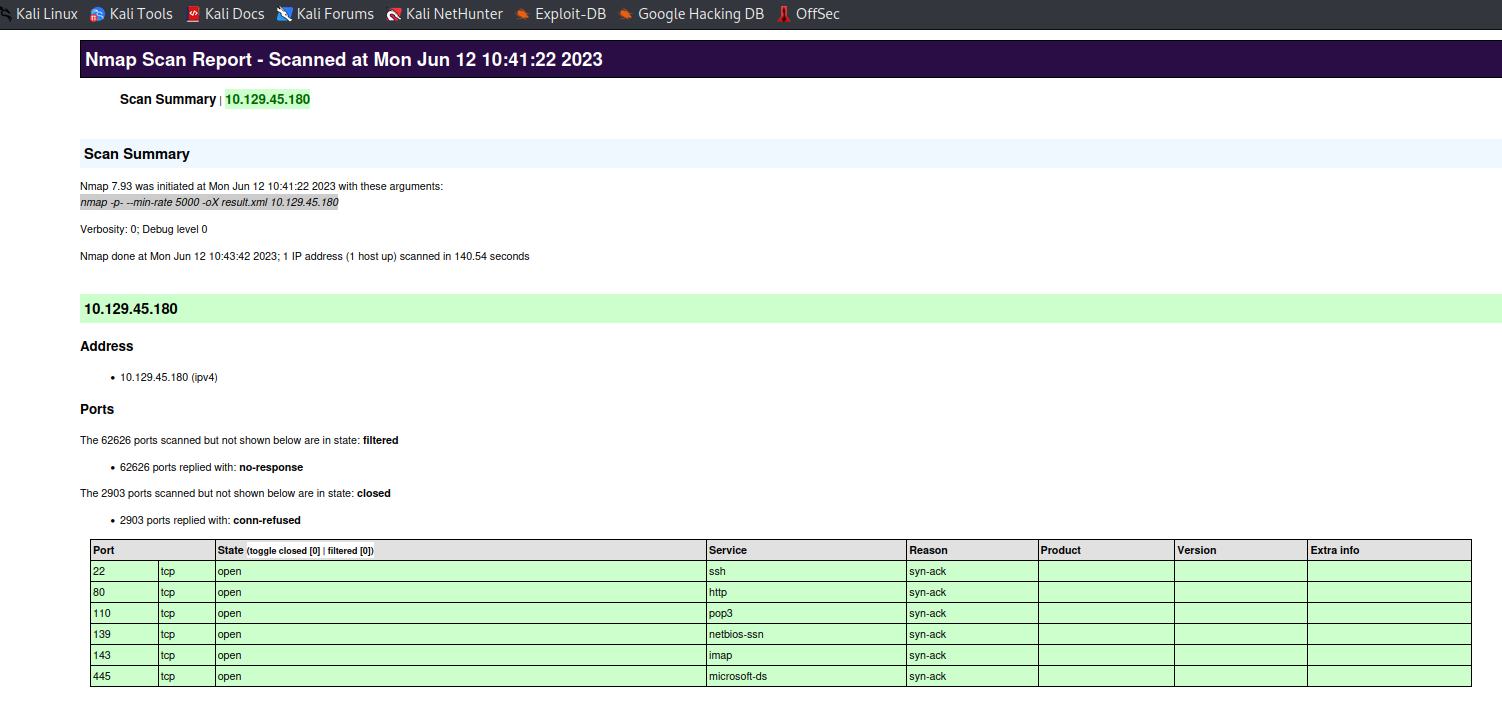
## Saving the Results

When running different scans, it is important to save the results for later analysis. Nmap provides three formats for saving the results: normal output (-oN) with the .nmap file extension, grepable output (-oG) with the .gnmap file extension, and XML output (-oX) with the .xml file extension. Alternatively, the option (-oA) can be used to save the results in all formats. By executing the command, Nmap will generate files named according to the specified target. These files can be found in the current directory. The normal output contains a concise summary of the scan, the grepable output provides machine-parseable information, and the XML output allows for easy conversion to HTML reports.

### Task

Perform a full TCP port scan on your target and create an HTML report. Submit the number of the highest port as the answer. 31337



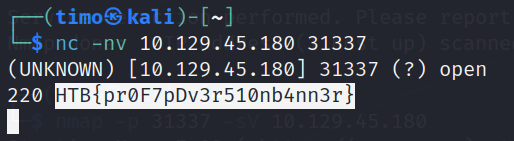


## Service Enumeration

Performing a comprehensive scan of a target system involves determining the application and its version accurately. This information enables scanning for known vulnerabilities and analysing the source code. Quick port scans provide an overview of available ports while minimizing traffic to avoid detection. The version scan helps identify specific ports and their corresponding services. Increasing verbosity levels provides more detailed information about open ports. After the scan, Nmap displays the port status, service name, and hostname. Sometimes, the target server provides additional information through banners or intercepted network traffic, which may not be shown by Nmap. Intercepting network traffic using tools like tcpdump or manually connecting to the service with nc can reveal hidden information.

### Task

Enumerate all ports and their services. One of the services contains the flag you have to submit as the answer. HTB{pr0F7pDv3r510nb4nn3r}



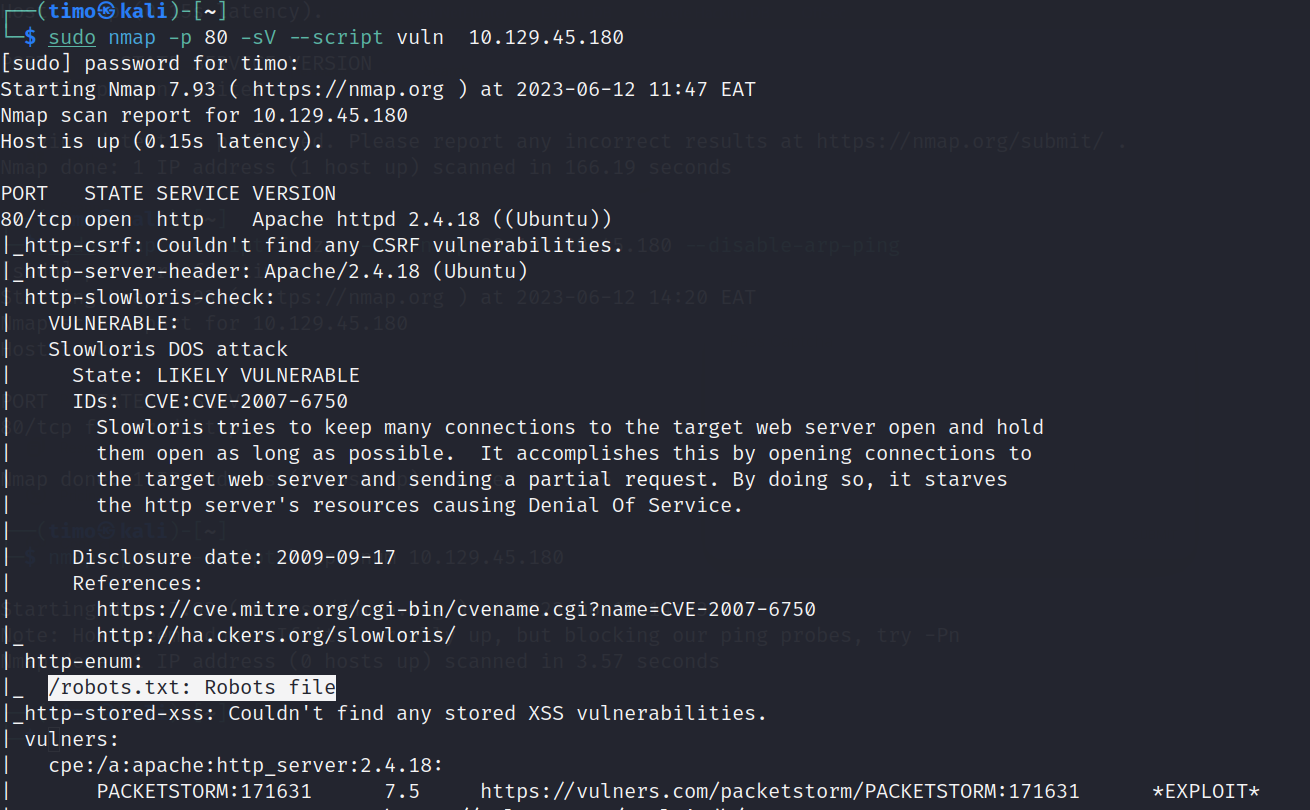
## Nmap Scripting Engine

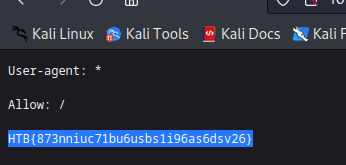
The Nmap Scripting Engine (NSE) is a useful feature that allows the creation of Lua scripts for interacting with specific services. There are 14 categories of scripts, including authentication, broadcast, brute force, default, discovery, DoS, exploit, external, fuzzer, intrusive, malware, safe, version, and vuln. NSE scripts can be specified in three ways: using default scripts with the -sC option, using specific scripts with the --script <category> option, or defining individual scripts with the --script <script-name>,<script-name>,... option. Examples of script usage include identifying the Ubuntu distribution of Linux and available commands on an SMTP server. Nmap also offers an aggressive scan option (-A) that combines multiple scan types. By using the vuln category, vulnerabilities in web applications can be assessed.

### Task

Use NSE and its scripts to find the flag that one of the services contain and submit it as the answer.

Ans HTB{873nniuc71bu6usbs1i96as6dsv26} type in browser <ip>/robots.txt





## Performance

Scanning performance in Nmap can be optimized through various options. These include adjusting the scan speed (-T <1-5>), frequency (--min-parallelism <number>), timeouts (--max-rtt-timeout <time>), packet concurrency (--min-rate <number>), and port retry count (--max-retries <number>). Fine-tuning these settings enhances scan efficiency, but caution is needed to avoid overlooking hosts or triggering security systems. By leveraging timeout, retry, and rate adjustments, Nmap enables faster scans while maintaining accuracy. Additionally, Nmap provides timing templates (-T <0-5>) that offer preconfigured options for different network environments. Balancing speed and thoroughness allows effective scanning in diverse scenarios.

# Bypass Security Measures

## Firewall & IDPS Evasion

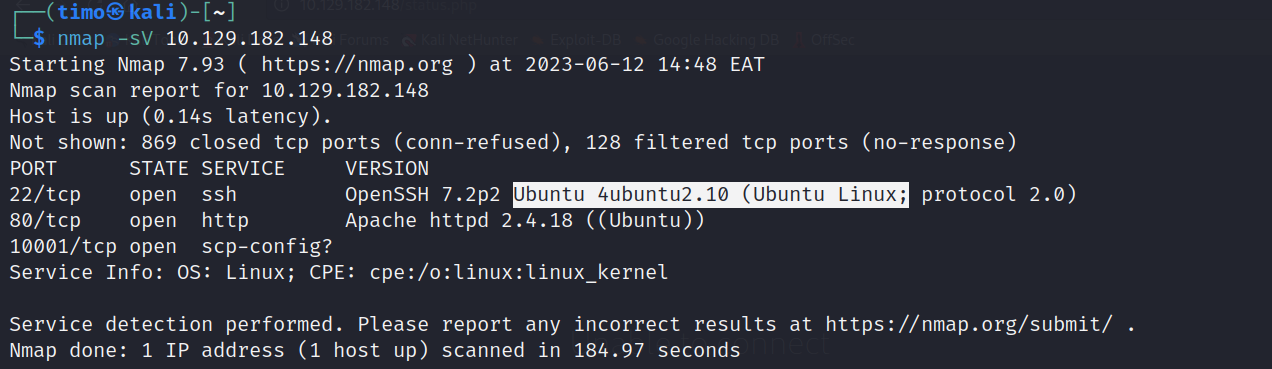
Nmap provides various methods to bypass firewall rules and IDS/IPS, such as packet fragmentation and decoy usage. Firewalls are software components that monitor and control network traffic based on predefined rules to prevent unauthorized connections. IDS and IPS are also software components that detect and respond to potential attacks. Determining firewall rules involves analysing filtered and rejected packets. Nmap's TCP ACK scan method is harder to filter compared to SYN or Connect scans. IDS/IPS detection is more challenging as these systems passively monitor network traffic. Decoys can be used to disguise the origin of packets. Testing firewall rules and identifying IPS systems require specific scanning techniques.

## Firewall & IDPS Evasion (easy lab)

A company hired us to test their IT security defences, including their IDS and IPS systems. Our client wants to increase their IT security and will, therefore, make specific improvements to their IDS/IPS systems after each successful test. We do not know, however, according to which guidelines these changes will be made. Our goal is to find out specific information from the given situations. We are only ever provided with a machine protected by IDS/IPS systems and can be tested.

### Task

Our client wants to know if we can identify which operating system their provided machine is running on. Submit the OS name as the answer. Ubuntu(did a simple service scan without being banned)



## Firewall and IDS/IPS Evasion (Medium Lab)

After we conducted the first test and submitted our results to our client, the administrators made some changes and improvements to the IDS/IPS and firewall. We could hear that the administrators were not satisfied with their previous configurations during the meeting, and they could see that the network traffic could be filtered more strictly.

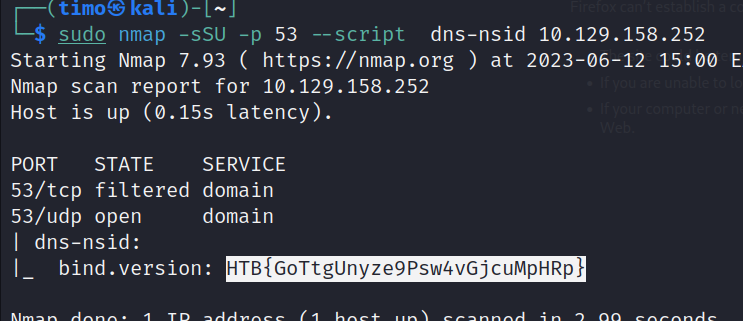
### Task

After the configurations are transferred to the system, our client wants to know if it is possible to find out our target's DNS server version. Submit the DNS server version of the target as the answer.

Ans= HTB{GoTtgUnyze9Psw4vGjcuMpHRp}

Previously we were given link to lists of scripts that can be used and I found a dns id script which I will use in this case. >Sudo nmap -sSU -p 53 --script dns-nsid 10.129.158.252

"-sSU" specifies the scan type. "sS" performs a TCP SYN scan, "sU" performs a UDP scan, and "SU" combines both TCP and UDP scans. "-p 53" specifies the port number to scan, in this case, port 53 which is commonly used for DNS (Domain Name System) services. "--script dns-nsid" indicates that the Nmap script "dns-nsid" should be executed during the scan.



## Firewall and IDS/IPS Evasion (Hard Lab)

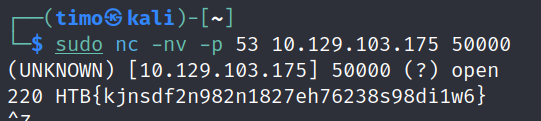
client was able to gain new insights and sent one of its administrators to a training course for IDS/IPS systems. As our client told us, the training would last one week. Now the administrator has taken all the necessary precautions and wants us to test this again because specific services must be changed, and the communication for the provided software had to be modified.

### Task

Now our client wants to know if it is possible to find out the version of the running services. Identify the version of service our client was talking about and submit the flag as the answer.

Ans= HTB{kjnsdf2n982n1827eh76238s98di1w6} Sudo nc -nv -p 53 10.129.103.175 50000

Used netcat listener here



# CONCLUSION

In conclusion, the enumeration process using Nmap proved to be an effective method for gathering essential information about the target system. By scanning open ports, identifying services running on those ports, and using NSE scripts to detect vulnerabilities, we were able to gain insights into the system's configuration and potential security risks. This information can serve as a foundation for further analysis and security measures to mitigate any identified vulnerabilities and enhance the overall security posture of the system.

Though I believe it's part of the work, this module needed a significant amount of outside research. The key to this game is not having a perfect memory, but rather understanding where to seek for the right tool for the job at hand. [**LINK**](https://academy.hackthebox.com/achievement/643478/19)

