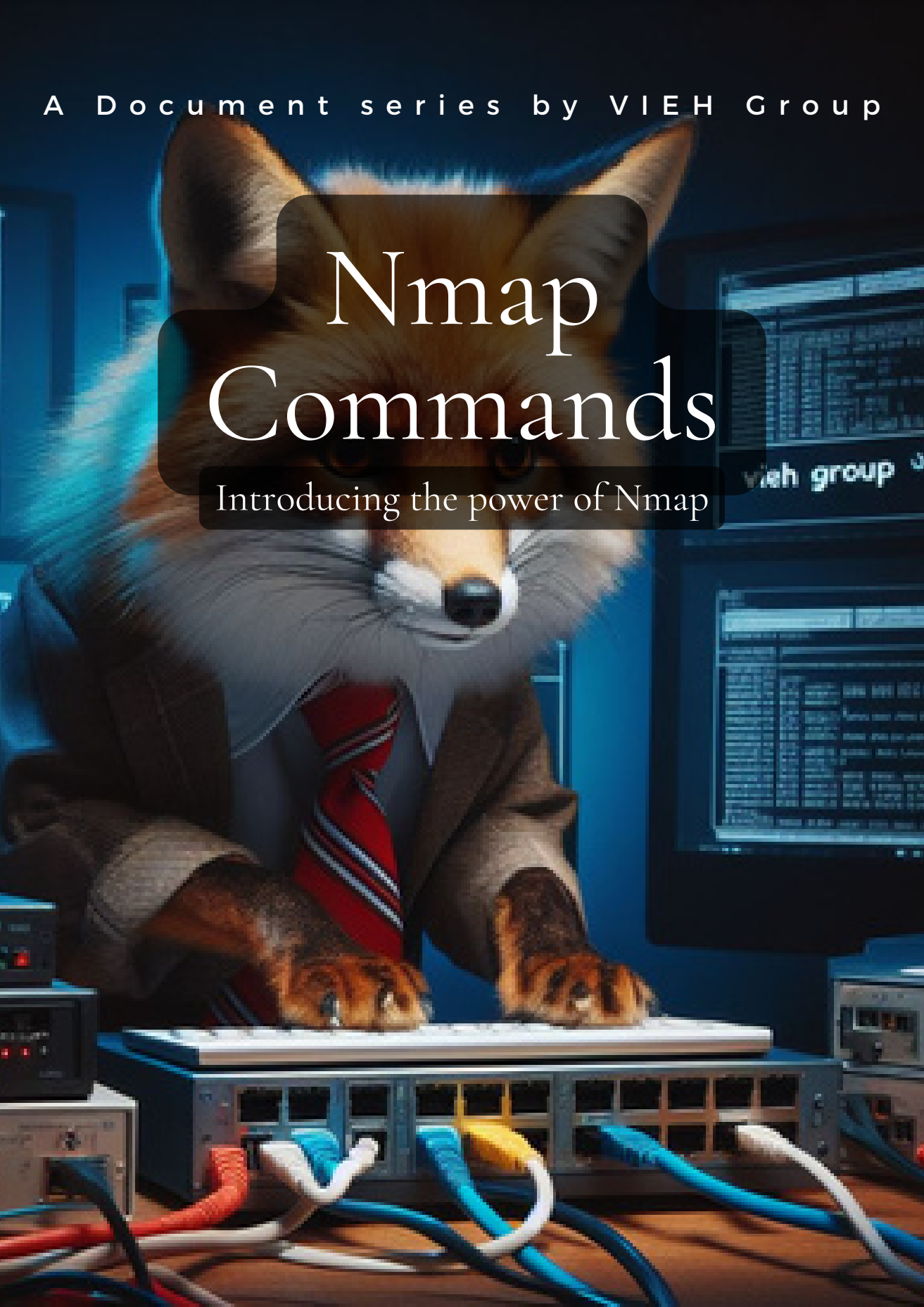
A Document series by VIEH Group

# Nmap Commands

## Introducing the power of Nmap



# Disclaimer

Dear readers,
This document is provided by VIEH Group for educational purposes only. While we strive for accuracy and reliability, we make no warranties or representations regarding the completeness, accuracy, or usefulness of the information presented herein. Any reliance you place on this document is at your own risk. VIEH Group shall not be liable for any damages arising from the use of or reliance on this document. We acknowledge and appreciate the contribution of the source person.

also,
This document is not created by a professional content writer so any mistake and error is a part of great design

Happy learning !!!

This document is credited to **Mohammed AlSubayt ,** whose exceptional insights elevate its value. Their contribution is deeply appreciated, underscoring their significant role in its creation.

Our newsletter: **Cyber Arjun**

**Scan QR:**

# Introduction

**Purpose**

Nmap (Network Mapper) is a powerful open-source tool used for network exploration and security auditing. It allows users to discover hosts and services on a computer network, thus creating a map of the network. Nmap commands are used to perform various network scanning tasks, such as port scanning, OS detection, version detection, and vulnerability scanning.

**Functionality**

Nmap commands provide a wide range of functionality for network scanning and security assessment. Some of the key features include:

•Port Scanning: Nmap can scan for open ports on a target host, helping to identify potential vulnerabilities.

•OS Detection: Nmap can determine the operating system running on a target host by analyzing network packets.

•Version Detection: Nmap can identify the versions of services running on a target host, helping to identify outdated or vulnerable software.

•Scripting: Nmap provides a scripting engine that allows users to write custom scripts for advanced scanning and automation.

In the following sections, we will explore some of the most commonly used Nmap commands and their functionalities.

# Nmap Brute Force Attacks

**Best Practices**

1. Use Nmap's built-in brute force options, such as -b and -t, to avoid manual input and reduce the risk of errors.
2. Avoid using brute force attacks on systems that are not authorized to access, as it can be illegal and unethical.
3. Use a strong password and enable two-factor authentication to prevent unauthorized access to systems.
4. Keep your software and systems up-to-date with the latest security patches and updates.

**Example Brute Force Attack**

To launch a brute force attack using Nmap, you can use the following command:

WordPress brute force attack:

- nmap -sV --script http-wordpress-brute --script-args 'userdb=users.txt,passdb=passwds.txt,http-wordpress-brute.hostname=domain.com, http-wordpress-brute.threads=3,brute.firstonly=true' 192.168.1.105

Brute force attack against MS-SQL:

•nmap -p 1433 --script ms-sql-brute --script-args userdb=customuser.txt,passdb=custompass.txt 192.168.1.105

FTP brute force attack:

•nmap --script ftp-brute -p 21 192.168.1.105

## Ping Scan

**Description**

Ping scan is used to check if a target host is online.

**Command**

`nmap -sn [target]`

**Usage**

- Use the `-sn` flag to specify a ping scan.
- Replace `[target]` with the IP address or hostname of the target host.

**Example**

`nmap -sn 192.168.0.1`

This will perform a ping scan on the host with the IP address `192.168.0.1` to check if it is online.

## Detecting malware infections on remote hosts using Nmap

Nmap is able to detect malware and backdoors by running extensive tests on a few popular OS services like on Identd, Proftpd, Vsftpd, IRC, SMB, and SMTP. It also has a module to check for popular malware signs inside remote servers and integrates Google's Safe Browsing and VirusTotal databases as well.

A common malware scan can be performed by using:

```
nmap -sV --script=http-malware-host 192.168.1.105
```

Or using Google's Malware check:

```
nmap -p80 --script http-google-malware infectedsite.com
```

Output example:

80/tcp open http|_http-google-malware.nse: Host is known for distributing malware.

# Nmap for OS and Service Detection

**Best Practices**

1. Use the -A option to scan for all available ports and services.
2. Use the -sS option to scan for services only, and avoid scanning for OS detection.
3. Use the -p option to specify the port number, and avoid using the default port number (1-65535).
4. Use the -T option to scan for open ports, and avoid using the -t option to scan for closed ports.
5. Use the -D option to detect the operating system and service, but be aware that false positives can occur.
6. Use the -v option to display the scan results in a detailed format.
7. Use the -o option to save the scan results to a file, and avoid using the -o option to save the scan results to a file with a .nmap extension.
8. Use the -i option to specify the input file, and avoid using the -i option to specify the output file.

**Example**

To scan for open ports and services on a target machine, use the following command:

•nmap -sS -p 80 -o output.nmap

This command will scan for open ports on port 80, and save the scan results to a file named output.nmap.

# TCP Connect Scan

**Overview**

TCP connect scan is used to determine if a specific port is open on a target host.

**How it Works**

•The scan sends a TCP SYN packet to the target host's specified port.

•If the target host responds with a SYN/ACK packet, it means the port is open.

•If the target host responds with a RST packet, it means the port is closed.

•If the target host does not respond, it means the port is filtered or blocked by a firewall.

**Usage**

•Use the -sT flag with the Nmap command to perform a TCP connect scan.

•Specify the target host and port number to scan.

**Example**

nmap -sT <target_host> -p <port_number>

# SYN Scan

**What isSYN Scan?**

SYN scan is a type of port scanning technique used to determine if a specific port is open on a target host. It works by sending SYN packets to the target host and analyzing the response.

**How does SYN Scan work?**

When a SYN packet is sent to a port on a target host, the host responds with a SYN/ACK packet if the port is open and available. If the port is closed, the host responds with a RST packet. By analyzing the response, the SYN scan can determine if the port is open or closed.

**When to use SYN Scan?**

SYN scan is commonly used in network security assessments and vulnerability testing to identify open ports on a target host. It can help identify potential security vulnerabilities and misconfigurations.

**Example Command**

nmap -sS <target_host>

**Limitations**

•SYN scan requires raw socket access, which may not be available on all systems.

•Some firewalls and intrusion detection systems (IDS) may detect and block SYN scan attempts.

## UDP Scan

UDP scan is atype of network scanning technique that is used to determine if a specific port is open on a target host using UDP packets. Unlike TCP scanning, which relies on a three-way handshake, UDP scanning does not establish a connection with the target host. Instead, it sends UDP packets to the target port and analyzes the response to determine if the port is open, closed, or filtered.

# ACK Scan

The ACKscanisused to determine if a specific port is filtered or unfiltered on a target host.

### How it Works

The ACK scan sends TCP ACK packets to a target host with a specific port number. The response received from the target host can provide valuable information about the state of the port.

•If the target host responds with an RST packet, it means the port is unfiltered.

•If the target host responds with no packet or an ICMP unreachable message, it means the port is filtered.

### Usage

The ACK scan can be used for various purposes, such as network troubleshooting, firewall testing, and vulnerability assessment.

### Example Command

$ nmap -sA <target>

### Limitations

It's important to note that the ACK scan does not provide information about open or closed ports. It only determines if a specific port is filtered or unfiltered.

# Window Scan

**Description**

Window scan is used to determine if a specific port is open on a target host by analyzing the TCP window size.

**How it works**

•Sends a TCP SYN packet to the target port.

•If the port is open, the target will respond with a TCP SYN/ACK packet.

•If the port is closed, the target will respond with a TCP RST packet.

•If the port is filtered, the target will not respond.

**Command**

nmap -sW <target>

**Example**

nmap -sW 192.168.0.1

# Maimon Scan

**Description**

Maimon scan is used to determine if a specific port is open on a target host by sending malformed packets.

**Syntax**

```
nmap -sM <target> -p <port>
```

**Example**

```
nmap -sM 192.168.0.1 -p 80
```

# Xmas Scan

The Xmasscanisused to determine if a specific port is open on a target host by sending a combination of flags.

### How it Works

During an Xmas scan, the Nmap tool sends TCP packets to the target host with the FIN, URG, and PUSH flags set. If the target port is open, the host's response will differ depending on how it handles these packets. If the port is closed, the host will typically respond with a TCP RST packet.

### Usage

To perform an Xmas scan using Nmap, you can use the following command:

nmap -sX [target]

Replace [target] with the IP address or hostname of the target host.

### Example

Here is an example of an Xmas scan command:

nmap -sX 192.168.0.1

This command will perform an Xmas scan on the host with the IP address 192.168.0.1.

### Considerations

It's important to note that some firewalls and security systems may detect and block Xmas scans, so it's recommended to use this scan method with caution and ensure that you have proper authorization before scanning any target hosts.

# FIN Scan

**Description**

A FIN scan is used to determine if a specific port is open on a target host by sending FIN packets. FIN packets are typically used to gracefully close a TCP connection. If a target port is closed, it should respond with a TCP RST packet. However, if the port is open, it should ignore the FIN packet and not respond.

**Usage**

To perform a FIN scan using Nmap, you can use the following command:

```
nmap -sF <target>
```

**Example**

Here is an example of a FIN scan command:

```
nmap -sF 192.168.0.1
```

# Null Scan

### Description

A null scan is used to determine if a specific port is open on a target host by sending packets with no flags set.

### How it works

A null scan takes advantage of the fact that some systems respond differently to different types of packets. When a null packet is sent, a system that has a closed port will respond with an RST (reset) packet, indicating that the port is closed. However, if the port is open, the system will not respond at all, indicating that the port is open.

### Usage

To perform a null scan, use the following command:

```
nmap -sN <target>
```

## Idle Scan

Idlescan is a technique used to determine if a specific port is open on a target host by using an indirect method. It involves using a third-party host, known as an idle zombie, to send packets to the target host and analyze the responses. This allows the attacker to remain anonymous and avoid detection.

To perform an idle scan, the following Nmap command can be used:

nmap -sI <zombie host> -p <port> <target host>

•<zombie host>: The IP address of the idle zombie.

•<port>: The port number to scan.

•<target host>: The IP address or hostname of the target host.

Idle scan can be useful in scenarios where the attacker wants to hide their identity or evade detection by using a trusted third-party host.

# FTP Bounce Scan

FTP bounce scan is atechnique used to determine if a specific port is open on a target host by using an FTP server as a proxy. This type of scan can be useful in situations where direct scanning is not possible or when you want to hide your true identity by using an intermediary FTP server.

**FTP Bounce Scan Commands**

| Command | Description |
| --- | --- |
| nmap -p <port> -b <FTP server> <target> | Performs an FTP bounce scan by specifying the target port, the FTP server to use as a proxy, and the target host. |
| nmap -p <port> --proxy <FTP server> <target> | Performs an FTP bounce scan by specifying the target port, the FTP server to use as a proxy, and the target host. |
| nmap -p <port> --proxies <FTP server> <target> | Performs an FTP bounce scan by specifying the target port, the FTP server to use as a proxy, and the target host. |

## DNS Scan

ADNSscan is atype of network scan that is used to determine information about DNS servers and associated hostnames. It allows you to gather valuable information about the DNS infrastructure of a target network.

**Common Nmap DNS Scan Commands**

| Command | Description |
| --- | --- |
| nmap -sn <target> | Performs a simple ping scan to discover live hosts on the network. |
| nmap -sL <target> | Lists all IP addresses that are associated with the target domain. |
| nmap -sP <target> | Performs a ping scan on the specified target to determine if it is online. |
| nmap -sU -p 53 <target> | Performs a UDP scan on port 53 to identify open DNS servers. |
| nmap --script dns-brute <target> | Performs a brute-force DNS scan to discover subdomains of the target domain. |

## SMB Scan

SMB scan is acommand used in Nmap to gather information about SMB (Server Message Block) services and shares on a target host. It allows users to identify open SMB ports, enumerate shares, and gather information about the SMB version and configuration.

**SMB Scan Command**

| Command | Description |
| --- | --- |
| nmap -p 445 --script smb-enum-shares.nse <target> | Performs an SMB scan on the specified target host to enumerate available shares. |
| nmap -p 445 --script smb-os-discovery.nse <target> | Identifies the operating system of the target host by analyzing SMB responses. |
| nmap -p 445 --script smb-vuln-ms17-010.nse <target> | Checks if the target host is vulnerable to the MS17-010 (EternalBlue) exploit, which affects SMBv1. |
| nmap -p 445 --script smb-security-mode.nse <target> | Determines the security mode of the SMB service on the target host (e.g., user, domain, server). |

## SNMP Scan

SNMP scanisusedtodetermine information about SNMP services and devices on a target host.

**Nmap Command**

To perform an SNMP scan, use the following Nmap command:

nmap -sU -p 161 --script snmp-sysdescr,snmp-netstat,snmp-processes <target>

This command will scan for SNMP services on the target host and gather information such as system description, network statistics, and running processes.

# SMTP Scan

**What isSMTP Scan?**

SMTP scan is used to determine information about SMTP services and email servers on a target host.

**How does it work?**

SMTP scan sends a series of commands to the target host's SMTP server to gather information such as the banner message, supported authentication methods, and available email addresses.

**Why is it useful?**

SMTP scan can help identify potential vulnerabilities in the email server configuration and detect open relays, which can be used for spamming or unauthorized email relay.

**Nmap Command**

To perform an SMTP scan using Nmap, use the following command:

```
nmap -p 25 --script smtp-commands <target>
```

# HTTP Scan

HTTPscanis a typeof scan performed using Nmap to determine information about HTTP services and web servers on a target host. It allows you to gather valuable information about the web server, such as the version, supported methods, and potentially vulnerable software.

**Nmap HTTP Scan Commands**

| Command | Description |
| --- | --- |
| nmap -p 80 --script=http-title <target> | This command scans port 80 (default HTTP port) and retrieves the title of the web page hosted on the target. |
| nmap -p 80 --script=http-headers <target> | This command scans port 80 and retrieves the HTTP headers of the web server, providing information such as server type, supported methods, and cookies. |
| nmap -p 80 --script=http-methods <target> | This command scans port 80 and determines the HTTP methods supported by the web server, such as GET, POST, PUT, DELETE, etc. |
| nmap -p 80 --script="http-vuln*" <target> | This command scans port 80 and checks for known vulnerabilities in the web server software. |

# HTTPS Scan

**Overview**

HTTPS scan is used to determine information about HTTPS services and secure web servers on a target host.

**Nmap Command**

```
nmap -p 443 --script ssl-enum-ciphers <target>
```

**Description**

This command is used to scan for secure web servers on a target host. It checks for the supported SSL/TLS ciphers and protocols and provides information about the server's certificate.

**Usage**

Replace `<target>` with the IP address or hostname of the target host.

**Example**

```
nmap -p 443 --script ssl-enum-ciphers example.com
```

**Output**

The command will output a list of supported ciphers and protocols, as well as information about the server's certificate.

# Telnet Scan

Telnet scan is atype of network scan used to determine information about Telnet services and remote login on a target host. It allows you to check if Telnet is enabled on a specific IP address or range of IP addresses, and gather information about the Telnet service running on those hosts.

**Telnet Scan Commands**

| Command | Description |
| --- | --- |
| nmap -p 23 <target> | Scan a single target IP address for open Telnet ports |
| nmap -p 23 --open <target> | Scan a single target IP address and only display hosts with open Telnet ports |
| nmap -p 23 -iL targets.txt | Scan a list of targets from a text file for open Telnet ports |
| nmap -p 23 --exclude <excluded_hosts> <target> | Scan a single target IP address excluding specified hosts from the scan |

# SSH Scan

SSH scan is atype of Nmap scan that is used to determine information about SSH services and secure remote login on a target host. By performing an SSH scan, you can gather important details about the SSH configuration and security of a remote system.

**SSH Scan Results**

| Command | Description |
| --- | --- |
| nmap -p 22 <target> | Performs a basic SSH scan on the specified target IP address or hostname. It checks if port 22, the default SSH port, is open on the target. |
| nmap -p 22 --script ssh2-enum-algos <target> | Performs an SSH scan with the 'ssh2-enum-algos' script, which enumerates the supported algorithms for key exchange, encryption, and MAC (Message Authentication Code) on the target. |
| nmap -p 22 --script ssh-auth-methods <target> | Performs an SSH scan with the 'ssh-auth-methods' script, which enumerates the supported authentication methods for SSH on the target. |
| nmap -p 22 --script ssh-hostkey <target> | Performs an SSH scan with the 'ssh-hostkey' script, which retrieves and displays the SSH host keys of the target. This can help identify if the target's SSH keys have been tampered with or changed. |

# VNC Scan

VNC scan isatype of scan used to determine information about VNC services and remote desktop access on a target host. VNC (Virtual Network Computing) is a graphical desktop sharing system that allows users to remotely control another computer. By performing a VNC scan, you can identify if a target host has VNC services running and potentially gain remote access to the desktop environment.

**VNC Scan Commands**

| Command | Description |
| --- | --- |
| nmap -p 5900-5903 -sV -sC <target> | Performs a VNC scan on the specified target host. The -p flag specifies the port range to scan (5900-5903 for VNC). The -sV flag enables version detection, which attempts to determine the VNC server version. The -sC flag enables default script scanning. |
| nmap -p 5900-5903 --script=vnc-info <target> | Performs a VNC scan using the 'vnc-info' NSE (Nmap Scripting Engine) script. This script specifically targets VNC services and provides detailed information about the server, including supported authentication methods, screen resolutions, and more. |
| nmap -p 5900-5903 --script=vnc-brute <target> | Performs a brute force attack on VNC services using the 'vnc-brute' NSE script. This script attempts to guess the username and password combination for VNC authentication. It can be used to test the security of VNC services and identify weak credentials. |

# NFS Scan

NFSscanisacommand used in Nmap to determine information about NFS services and network file sharing on a target host.

**NFS Scan Commands**

| Command | Description |
| --- | --- |
| nmap -p 2049 --script nfs-ls <target> | Lists the directories and files available for NFS mounting on the target host. |
| nmap -p 2049 --script nfs-showmount <target> | Shows the NFS exports (shared directories) on the target host. |
| nmap -p 2049 --script nfs-statfs <target> | Displays the disk space usage and statistics for NFS mounted file systems on the target host. |
| nmap -p 2049 --script nfs-statfs2 <target> | Retrieves the disk space usage and statistics from the NFS server on the target host. |

# RPC Scan

**Description**

The RPC scan is used to determine information about RPC services and remote procedure calls on a target host.

**Usage**

To perform an RPC scan, use the following command:

nmap -p 111 --script rpcinfo <target>

This command will scan port 111, which is the default port for RPC services, and use the 'rpcinfo' script to gather information about the RPC services running on the target host.

**Output**

The output of an RPC scan will provide details about the RPC services found on the target host, including the program ID, version, and protocol used.

**Example**

Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-01 10:00 EDT
Nmap scan report for target.example.com (192.168.0.1)
Host is up (0.001s latency).

PORT STATE SERVICE
111/tcp open rpcbind
| rpcinfo:
| program version port/proto service
| 100000 2,3,4 111/tcp rpcbind
| 100000 2,3,4 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 49053/tcp mountd
| 100005 1,2,3 50780/udp mountd
| 100021 1,3,4 42395/tcp nlockmgr
| 100021 1,3,4 44839/udp nlockmgr
| 100024 1 36274/tcp status
| 100024 1 42247/udp status
|_ 100227 2,3 2049/tcp nfs_acl

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

In this example, the RPC scan reveals that the target host has several RPC services running, including rpcbind, nfs, mountd, nlockmgr, and status. The scan also provides information about the program versions and the ports/protocols used by each service.

Thank you for taking the time to read through our publication. Your continued support is invaluable.

Jai Hind!