

Nmap -v -p 1-1024 <hostname>

-v

The "-v" flag in nmap stands for "verbose" mode. When used with nmap, it increases the amount of information that nmap outputs about its scanning and detection process.

By default, nmap outputs only basic information about the scan, such as the open ports and the operating system running on the scanned host. However, when you add the "-v" flag to your nmap command, nmap will output more detailed information about the scanning process, such as the status of each port, the progress of the scan, and any errors encountered during the scan.

Adding multiple "-v" flags increases the level of verbosity even further, up to a maximum of 5 levels of verbosity. However, using too much verbosity can slow down the scanning process and make the output difficult to read.

Scanning-target without firewall – results

```
eda491@kali: ~  
File Actions Edit View Help  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 4.47 seconds  
Raw packets sent: 2052 (90.252KB) | Rcvd: 703 (28.132KB)  
  
(eda491@kali)-[~]  
$ sudo nmap -v -p 1-1024 10.0.0.2  
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-17 09:37 CEST  
Initiating ARP Ping Scan at 09:37  
Scanning 10.0.0.2 [1 port]  
Completed ARP Ping Scan at 09:37, 0.08s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 09:37  
Completed Parallel DNS resolution of 1 host. at 09:37, 0.00s elapsed  
Initiating SYN Stealth Scan at 09:37  
Scanning 10.0.0.2 [1024 ports]  
Discovered open port 21/tcp on 10.0.0.2  
Discovered open port 111/tcp on 10.0.0.2  
Discovered open port 445/tcp on 10.0.0.2  
Discovered open port 23/tcp on 10.0.0.2  
Discovered open port 25/tcp on 10.0.0.2  
Discovered open port 53/tcp on 10.0.0.2  
Discovered open port 22/tcp on 10.0.0.2  
Discovered open port 139/tcp on 10.0.0.2  
Discovered open port 80/tcp on 10.0.0.2  
Discovered open port 513/tcp on 10.0.0.2  
Discovered open port 514/tcp on 10.0.0.2  
Discovered open port 512/tcp on 10.0.0.2  
Completed SYN Stealth Scan at 09:37, 0.13s elapsed (1024 total ports)  
Nmap scan report for 10.0.0.2  
Host is up (0.00016s latency).  
Not shown: 1012 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
MAC Address: 08:00:27:DA:1B:B2 (Oracle VirtualBox virtual NIC)  
  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds  
Raw packets sent: 1025 (45.084KB) | Rcvd: 1025 (41.036KB)  
  
(eda491@kali)-[~]  
$
```

Port 21 can be used both for unencrypted FTP and encrypted FTPS (FTP over SSL/TLS) connections. However, it is generally recommended to use SFTP (SSH File Transfer Protocol) instead, which uses port 22 and provides secure encrypted file transfer.

Port 111 is a well-known port number used for the Remote Procedure Call (RPC) protocol. RPC is a protocol that enables one program to execute a procedure on a remote system without needing to understand the network details, as if the procedure was running locally.

It is important to note that port 111 and the RPC protocol have been found to be vulnerable to several types of attacks, such as buffer overflow attacks and denial-of-service attacks. As a result, it is recommended to use secure alternatives to the RPC protocol, such as SSH (Secure Shell) for remote access and NFSv4 or Kerberos for file sharing.

Port 445 is a well-known port number used for the Server Message Block (SMB) protocol, which is a network file sharing protocol used by Microsoft Windows operating systems. This port is used for both SMB over TCP and SMB over NetBIOS.

Port 445 has been associated with several security vulnerabilities, particularly related to SMB protocol implementation issues, which can allow attackers to gain unauthorized access to a system, execute remote code, or cause a denial-of-service (DoS) attack. Some of the most significant vulnerabilities associated with port 445 include:

1. **EternalBlue:** A vulnerability in SMBv1 implementation that allowed the WannaCry ransomware attack to spread across the internet in 2017.
2. **SMBv3 Remote Code Execution:** A vulnerability in the Microsoft SMBv3 protocol that could allow an attacker to execute code remotely on vulnerable systems.
3. **SMBv1 Null Session Authentication:** A vulnerability that could allow anonymous access to file shares on systems running SMBv1.

Port 23 is a well-known port number used for the Telnet protocol. However, Telnet is considered insecure because it does not encrypt the data that is transmitted over the network, including login credentials and other sensitive information. This makes it vulnerable to eavesdropping, sniffing, and other types of attacks.

Port 25 is a well-known port number used for the Simple Mail Transfer Protocol (SMTP). SMTP is a protocol used for email transmission over the Internet or other TCP/IP-based networks.

When an email is sent, the SMTP client (usually a mail user agent or MUA) sends the message to an SMTP server on port 25, which is responsible for forwarding the message to its intended recipient. The SMTP server uses a series of commands and responses to communicate with the client and other SMTP servers in order to deliver the email to its final destination.

Port 25 is used for both unencrypted SMTP and encrypted SMTP with STARTTLS. However, it is recommended to use encrypted SMTP with STARTTLS or SMTPS (SMTP over SSL/TLS) to ensure the confidentiality and integrity of the email content and prevent interception or modification of the message.

Port 25 is also a popular target for spammers and hackers who attempt to abuse SMTP servers for sending spam or conducting phishing attacks. To prevent abuse, many ISPs and email providers block outgoing connections to port 25, requiring users to use their designated email servers or alternate ports, such as 587 or 465. Additionally, SMTP servers should be configured with appropriate security measures, such as access control, rate limiting, and authentication, to prevent unauthorized access or abuse.

Port 53 is a well-known port number used for the Domain Name System (DNS) protocol. DNS is a protocol used for translating human-readable domain names, such as `www.example.com`, into machine-readable IP addresses, such as `203.0.113.10`, which are used to route traffic over the Internet.

When a DNS client requests a domain name resolution, it sends a query to a DNS server on port 53. The DNS server responds with the corresponding IP address, which the client then uses to establish a connection to the requested server or service.

DNS is a critical part of the Internet infrastructure and is used by almost every network-connected device. However, port 53 is also a common target for attackers, who can use DNS to conduct various types of attacks, such as DNS cache poisoning, DNS amplification attacks, and domain hijacking.

To prevent DNS-related attacks, it is recommended to implement appropriate security measures, such as:

1. Configure DNS servers with proper access control and authentication mechanisms to prevent unauthorized access and modification.
2. Use DNSSEC (DNS Security Extensions) to add a layer of security to DNS by providing authentication and integrity verification for DNS queries.
3. Implement DNS over HTTPS (DoH) or DNS over TLS (DoT) to encrypt DNS traffic and prevent eavesdropping or tampering.
4. Use firewalls and intrusion prevention systems to monitor DNS traffic and detect and block malicious activity.

Port 22 is a well-known port number used for the Secure Shell (SSH) protocol. SSH is a secure network protocol that allows encrypted communication between two networked devices, typically a client and a server.

When an SSH client establishes a connection to an SSH server, it connects to port 22 by default. Once the connection is established, the SSH protocol provides a secure channel over which the client can send commands and receive responses from the server.

SSH is widely used for remote command-line access, file transfer, and tunneling, and is considered a more secure alternative to other remote access protocols such as Telnet or FTP. The SSH protocol provides strong encryption and authentication, which makes it resistant to eavesdropping, password sniffing, and other types of attacks.

Port 139 is a well-known port number used for the NetBIOS Session Service, which is part of the NetBIOS protocol suite used by Windows operating systems for file sharing and communication between networked devices.

NetBIOS stands for Network Basic Input/Output System, and it provides a way for applications on different computers to communicate with each other over a local network. The NetBIOS Session Service is responsible for establishing and maintaining connections between networked devices and allows for the transfer of data between them.

However, port 139 is also known to be a security vulnerability because the NetBIOS protocol suite was not designed with security in mind. This can allow attackers to gain unauthorized access to network resources, intercept sensitive data, or launch denial-of-service attacks.

To secure NetBIOS-based file sharing and communication, it is recommended to take the following security measures:

1. Disable NetBIOS over TCP/IP or use a firewall to block access to port 139 from the Internet.
2. Use SMB (Server Message Block) version 2 or later instead of NetBIOS for file and printer sharing.
3. Use IPsec (Internet Protocol Security) to encrypt NetBIOS traffic and protect against eavesdropping and tampering.
4. Apply security patches and updates to operating systems and networked devices to address known vulnerabilities.
5. Monitor network activity for signs of suspicious or malicious activity, and set up intrusion detection and prevention systems to prevent attacks.

Port 445 is a well-known port number used for the Server Message Block (SMB) protocol, which is a network file-sharing protocol that allows communication between networked devices. SMB is widely used on Windows-based systems for sharing files, printers, and other resources.

Port 445 is a critical port for SMB-based file sharing, and it is also a common target for attackers. There have been several high-profile attacks that have exploited vulnerabilities in the SMB protocol, including the WannaCry ransomware attack in 2017, which affected thousands of systems worldwide.

To secure SMB-based file sharing and prevent attacks, it is recommended to take the following security measures:

1. Apply security patches and updates promptly to operating systems and networked devices to address known vulnerabilities.
2. Disable SMBv1, which is an outdated and vulnerable version of the SMB protocol, and use SMBv2 or later instead.
3. Implement access control lists and firewalls to restrict access to SMB ports and limit the exposure to potential attacks.
4. Use encryption and authentication mechanisms such as SMB signing, IPsec, or VPN to secure SMB traffic and prevent eavesdropping or tampering.
5. Monitor network activity for signs of suspicious or malicious activity, and set up intrusion detection and prevention systems to prevent attacks.

Port 80 is a well-known port number used for the Hypertext Transfer Protocol (HTTP), which is the protocol used for transferring data over the World Wide Web. HTTP is used by web browsers to request and receive web pages, images, videos, and other content from web servers.

When a user enters a URL in a web browser, the browser sends an HTTP request to the web server, which responds with an HTTP response containing the requested content. HTTP uses a client-server architecture, where the client (the web browser) initiates the communication, and the server responds to the client's requests.

Port 80 is the default port for HTTP traffic, but it can also be used for other types of web traffic such as HTTP Secure (HTTPS) and Web Proxy Autodiscovery Protocol (WPAD).

To ensure the security of HTTP-based web traffic, it is recommended to take the following security measures:

1. Use HTTPS instead of HTTP for secure communication over the web. HTTPS encrypts web traffic and provides authentication and integrity checks to prevent eavesdropping, tampering, and phishing attacks.
2. Apply security patches and updates promptly to web servers and web applications to address known vulnerabilities.
3. Use firewalls and access control lists to restrict access to HTTP ports and limit the exposure to potential attacks.
4. Implement web application firewalls and intrusion detection and prevention systems to detect and prevent attacks such as SQL injection, cross-site scripting, and denial-of-service.
5. Monitor web server logs and network activity for signs of suspicious or malicious activity, and set up alerts to notify security teams of potential security breaches.

Port 512 is a well-known port number used for the Remote Process Execution (RPE) protocol, which is a legacy protocol used by some versions of the Digital Equipment Corporation's (DEC) VAX/VMS operating system for remote process execution.

The RPE protocol allows a user to execute a command on a remote system running the VAX/VMS operating system. The user sends a request to the remote system, which executes the requested command and returns the result to the user.

However, port 512 is also known to be a security vulnerability because the RPE protocol was not designed with security in mind. This can allow attackers to gain unauthorized access to remote systems, execute arbitrary commands, and take control of the system.

To secure the RPE protocol and prevent attacks, it is recommended to take the following security measures:

1. Disable the RPE protocol or use a firewall to block access to port 512 from the Internet.
2. Use secure remote access protocols such as SSH or VPN to access remote systems securely.
3. Apply security patches and updates to operating systems and networked devices to address known vulnerabilities.
4. Monitor network activity for signs of suspicious or malicious activity, and set up intrusion detection and prevention systems to prevent attacks.

Port 513 is a well-known port number used for the Remote Execution and Distributed Computing Environment (REXEC) protocol, which is a legacy protocol used for remote command execution on UNIX-based systems.

The REXEC protocol allows a user to execute a command on a remote system running a UNIX-based operating system. The user sends a request to the remote system, which authenticates the user and executes the requested command with the user's privileges.

However, port 513 is also known to be a security vulnerability because the REXEC protocol was not designed with security in mind. This can allow attackers to gain unauthorized access to remote systems, execute arbitrary commands, and take control of the system.

To secure the REXEC protocol and prevent attacks, it is recommended to take the following security measures:

1. Disable the REXEC protocol or use a firewall to block access to port 513 from the Internet.
2. Use secure remote access protocols such as SSH or VPN to access remote systems securely.
3. Implement access control lists and authentication mechanisms to restrict access to the REXEC service and limit the exposure to potential attacks.
4. Apply security patches and updates to operating systems and networked devices to address known vulnerabilities.
5. Monitor network activity for signs of suspicious or malicious activity, and set up intrusion detection and prevention systems to prevent attacks.

Port 514 is a well-known port number used for the Syslog protocol, which is a standard protocol used for collecting, transmitting, and storing log messages from network devices, servers, and applications.

The Syslog protocol allows network devices and applications to send log messages to a central Syslog server for centralized logging and analysis. The Syslog server receives the log messages and stores them in a central repository for future analysis and troubleshooting.

However, port 514 is also known to be a security vulnerability because Syslog messages are not encrypted by default, which can allow attackers to intercept and view sensitive log messages containing usernames, passwords, and other confidential information.

To secure the Syslog protocol and prevent attacks, it is recommended to take the following security measures:

1. Use a secure Syslog protocol such as Syslog-NG or Syslog over TLS to encrypt Syslog messages and ensure confidentiality and integrity.
2. Use firewalls and access control lists to restrict access to Syslog ports and limit the exposure to potential attacks.
3. Implement secure authentication mechanisms and access controls to restrict access to Syslog servers and prevent unauthorized access.
4. Monitor Syslog activity for signs of suspicious or malicious activity, and set up alerts to notify security teams of potential security breaches.

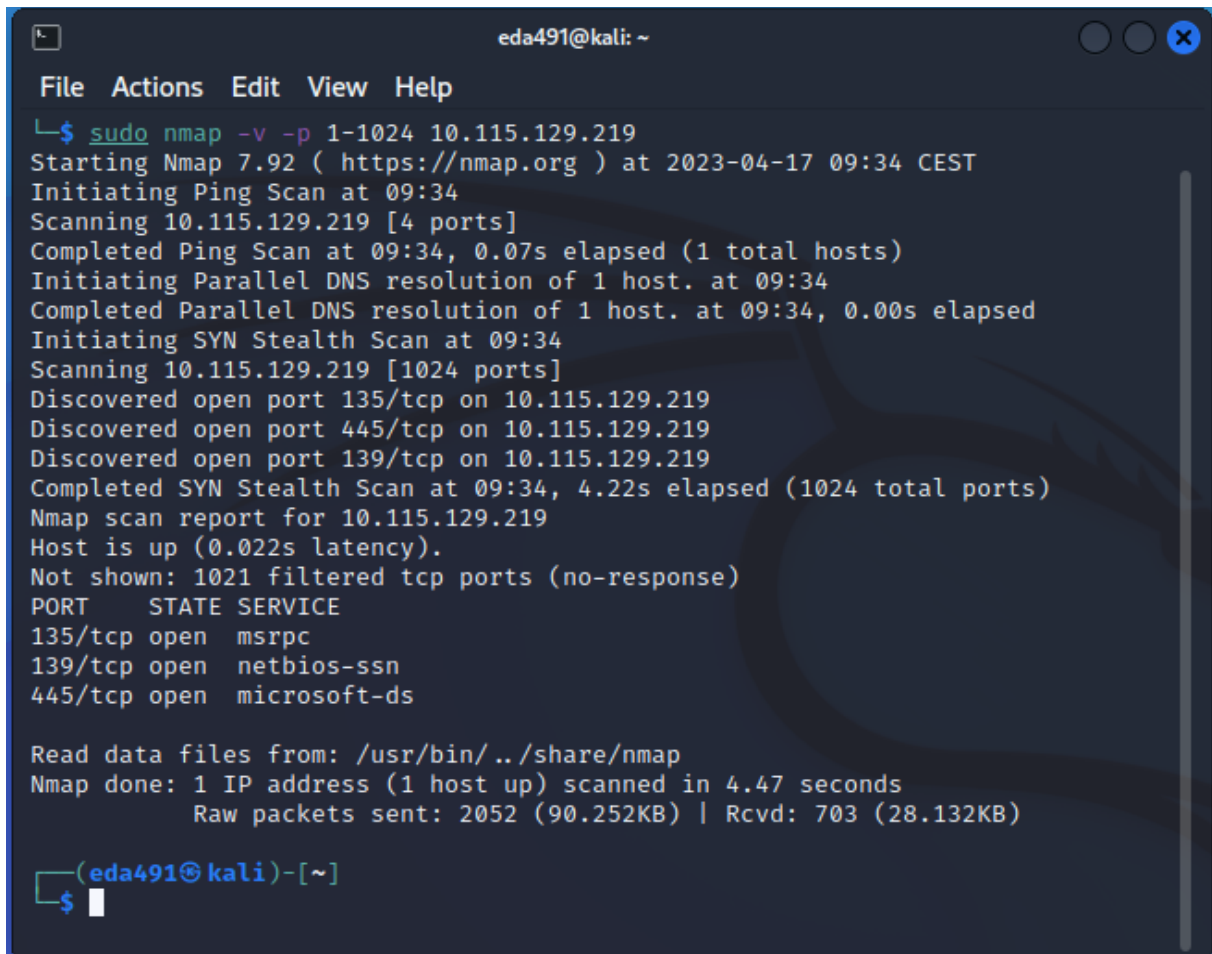
Scanning-target with firewall – results

```
eda491@kali: ~/Desktop
File Actions Edit View Help
(eda491@kali)-[~/Desktop]
$ sudo nmap -v -p 1-1024 10.0.0.2
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-17 09:41 CEST
Initiating ARP Ping Scan at 09:41
Scanning 10.0.0.2 [1 port]
Completed ARP Ping Scan at 09:41, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:41
Completed Parallel DNS resolution of 1 host. at 09:41, 0.00s elapsed
Initiating SYN Stealth Scan at 09:41
Scanning 10.0.0.2 [1024 ports]
Discovered open port 22/tcp on 10.0.0.2
Discovered open port 80/tcp on 10.0.0.2
Completed SYN Stealth Scan at 09:41, 4.68s elapsed (1024 total ports)
Nmap scan report for 10.0.0.2
Host is up (0.00034s latency).
Not shown: 1022 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:DA:1B:B2 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.91 seconds
Raw packets sent: 2049 (90.140KB) | Rcvd: 5 (204B)

(eda491@kali)-[~/Desktop]
$
```


Scanning host computer IP address – results

A terminal window titled 'eda491@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The terminal shows the execution of 'sudo nmap -v -p 1-1024 10.115.129.219'. The output includes: 'Starting Nmap 7.92 (https://nmap.org) at 2023-04-17 09:34 CEST', 'Initiating Ping Scan at 09:34', 'Scanning 10.115.129.219 [4 ports]', 'Completed Ping Scan at 09:34, 0.07s elapsed (1 total hosts)', 'Initiating Parallel DNS resolution of 1 host. at 09:34', 'Completed Parallel DNS resolution of 1 host. at 09:34, 0.00s elapsed', 'Initiating SYN Stealth Scan at 09:34', 'Scanning 10.115.129.219 [1024 ports]', 'Discovered open port 135/tcp on 10.115.129.219', 'Discovered open port 445/tcp on 10.115.129.219', 'Discovered open port 139/tcp on 10.115.129.219', 'Completed SYN Stealth Scan at 09:34, 4.22s elapsed (1024 total ports)', 'Nmap scan report for 10.115.129.219', 'Host is up (0.022s latency).', 'Not shown: 1021 filtered tcp ports (no-response)', a table of open ports, 'Read data files from: /usr/bin/../../share/nmap', 'Nmap done: 1 IP address (1 host up) scanned in 4.47 seconds', and 'Raw packets sent: 2052 (90.252KB) | Rcvd: 703 (28.132KB)'. The prompt at the bottom is '(eda491@kali)-[~]' with a cursor.

```
File Actions Edit View Help
└─$ sudo nmap -v -p 1-1024 10.115.129.219
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-17 09:34 CEST
Initiating Ping Scan at 09:34
Scanning 10.115.129.219 [4 ports]
Completed Ping Scan at 09:34, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:34
Completed Parallel DNS resolution of 1 host. at 09:34, 0.00s elapsed
Initiating SYN Stealth Scan at 09:34
Scanning 10.115.129.219 [1024 ports]
Discovered open port 135/tcp on 10.115.129.219
Discovered open port 445/tcp on 10.115.129.219
Discovered open port 139/tcp on 10.115.129.219
Completed SYN Stealth Scan at 09:34, 4.22s elapsed (1024 total ports)
Nmap scan report for 10.115.129.219
Host is up (0.022s latency).
Not shown: 1021 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.47 seconds
Raw packets sent: 2052 (90.252KB) | Rcvd: 703 (28.132KB)

(eda491@kali)-[~]
└─$
```

Port 135 is a well-known port number used for the Remote Procedure Call (RPC) protocol, which is a network communication protocol used by Windows-based systems for remote procedure calls and interprocess communication.

The RPC protocol allows programs to call procedures or functions on remote systems and exchange data between different processes over the network. However, port 135 is also known to be a security vulnerability because the RPC protocol has a history of security vulnerabilities and exploits, such as the DCOM RPC vulnerability in 2003.

Attackers can exploit vulnerabilities in the RPC protocol to gain unauthorized access to remote systems, execute arbitrary code, and take control of the system. To secure the RPC protocol and prevent attacks, it is recommended to take the following security measures:

1. Keep the operating system and networked devices up-to-date with the latest security patches and updates to address known vulnerabilities.
2. Use firewalls and access control lists to restrict access to RPC ports and limit the exposure to potential attacks.

3. Implement secure authentication mechanisms and access controls to restrict access to RPC services and prevent unauthorized access.
4. Disable unneeded RPC services and protocols, such as DCOM and NetBIOS, which are vulnerable to attacks.
5. Monitor network activity for signs of suspicious or malicious activity, and set up intrusion detection and prevention systems to prevent attacks.