A green chameleon logo

Description automatically generated

Port Scanning Chameleon Website (old version)

Contents:

Introduction:

Port scanning is a technique used in computer networking and cybersecurity to discover open ports on a computer or network device. Ports are virtual endpoints for communication in a network, and they are associated with specific services or protocols. Port scanning is typically performed for various reasons, including network administration, security assessments, and troubleshooting. Here's an overview of port scanning:

Usages:

Legality and Ethics: Port scanning can be used for both legitimate and malicious purposes. When used for security assessments, it's typically legal and ethical, if proper authorization is obtained. Unauthorized and malicious port scanning is illegal and unethical.

Countermeasures: To protect against unauthorized port scanning and potential security threats, organizations implement various security measures, including firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

Purpose:

Port scanning can serve multiple purposes:

Network Administration: Network administrators use port scanning to check which services are running on their network devices, ensure they are properly configured, and identify any potential issues.

Security Assessment: Ethical hackers and security professionals use port scanning to identify vulnerabilities in a network's security. They can discover open ports that may be targets for exploitation.

Troubleshooting: When network services are not functioning correctly, port scanning can help identify if a specific port is closed, blocked, or misconfigured.

Steps:

Tutorials of these types of attacks are available on website and YouTube videos.

Tools Used: Nmap (VM and local computer), Wireshark and Kali Linux VM:

nmap: This is the command itself, indicating that you want to run the nmap tool.

-sS: This option specifies a TCP SYN scan, which is a type of port scanning technique used to determine which TCP ports are open on the target host. It sends SYN packets to each port and analyzes the response to determine if the port is open or closed.

-T4: This option sets the timing template to "Aggressive," which determines how fast the scan runs. It's a relatively fast timing template.

-v: This option enables verbose output, providing more detailed information about the scan as it progresses.

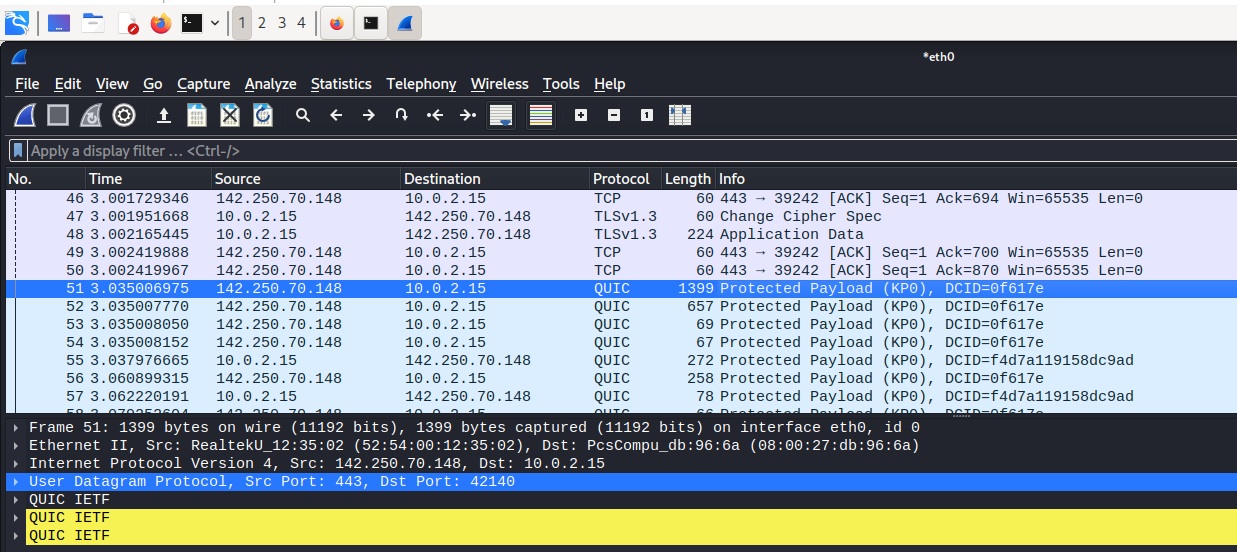
-n: This option tells nmap not to perform DNS resolution on IP addresses and hostnames. This can speed up the scan and is useful when you only care about IP addresses.

--max-parallelism 10: This option specifies the maximum number of parallel probes to send during the scan. In this case, it's set to 10, meaning that nmap will send up to 10 probes at a time.

-Pn: This option disables host discovery. It assumes that the host is up, even if it doesn't respond to host discovery probes. This can be useful when you want to scan a host that may not respond to standard discovery techniques.

--top-ports 100: This option specifies that you want to scan the top 100 most common ports. nmap maintains a list of common ports, and this option simplifies the scan by focusing on the most frequently used ones

To find the IP address for VM and website, we used Wireshark



For IP address 10.0.2.15 is private IP address for using the virtual machine of Kali Linux and 142.250.7.148 is the IP address for the old Chameleon website.

Command line is ‘nmap -sS -T4 -v -n --max-parallelism 10 -Pn --top-ports 100 142.250.70.148’ in which the options and its definition:

nmap: This is the command itself, indicating that you want to run the nmap tool.

-sS: This option specifies a TCP SYN scan, which is a type of port scanning technique used to determine which TCP ports are open on the target host. It sends SYN packets to each port and analyzes the response to determine if the port is open or closed.

-T4: This option sets the timing template to "Aggressive," which determines how fast the scan runs. It's a relatively fast timing template.

-v: This option enables verbose output, providing more detailed information about the scan as it progresses.

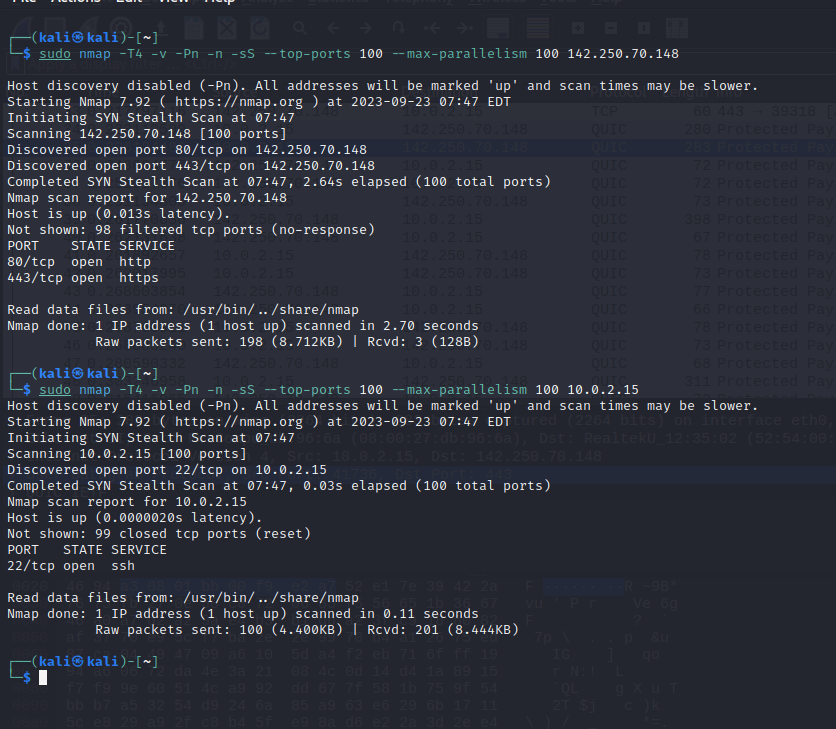
-n: This option tells nmap not to perform DNS resolution on IP addresses and hostnames. This can speed up the scan and is useful when you only care about IP addresses.

--max-parallelism 10: This option specifies the maximum number of parallel probes to send during the scan. In this case, it's set to 10, meaning that nmap will send up to 10 probes at a time.

-Pn: This option disables host discovery. It assumes that the host is up, even if it doesn't respond to host discovery probes. This can be useful when you want to scan a host that may not respond to standard discovery techniques.

--top-ports 100: This option specifies that you want to scan the top 100 most common ports. nmap maintains a list of common ports, and this option simplifies the scan by focusing on the most frequently used ones.

Screenshot of Port being scanned on Virtual Machine:



Screenshot of port of website scan at local computer:

A screenshot of a computer

Description automatically generated

Port Scan result explanation:

Here are some possible vulnerable risks that are associated with these open and closed ports:

Port 80/tcp (HTTP):

Service: HTTP (Hypertext Transfer Protocol)

Vulnerability Risk: Port 80 is commonly used for serving web content over HTTP. While having port 80 open itself is not necessarily a vulnerability, the risk depends on the web server's configuration and the software running on it. Potential risks may include:

Outdated or unpatched web server software: Vulnerabilities in web server software can lead to security issues. Ensure that the web server software is up to date with security patches.

Misconfigured server: Poorly configured web servers may expose sensitive information, directories, or have weak security settings.

Vulnerable web applications: If the web server hosts web applications, vulnerabilities within those applications could be exploited by attackers.

Port 443/tcp (HTTPS):

Service: HTTPS (HTTP Secure)

Vulnerability Risk: Port 443 is used for secure web traffic over HTTPS, and like port 80, the risk depends on the web server's configuration and software. Some considerations include:

SSL/TLS vulnerabilities: SSL/TLS configuration issues can lead to security vulnerabilities. Ensure that the server uses up-to-date and secure SSL/TLS protocols and ciphers.

Certificate issues: Improperly configured SSL/TLS certificates or self-signed certificates could pose a security risk.

Vulnerable web applications: If the web server hosts web applications over HTTPS, vulnerabilities within those applications could be exploited.

Port 113/tcp (Ident):

Service: Ident

Vulnerability Risk: Port 113 is typically associated with the Ident protocol, which is used for identifying the user of a particular TCP connection. While this port is closed in your scan results (not open)[not shown in the VM], it's generally considered a low risk, and there should be no vulnerability associated with it as long as it remains closed.

Mitigation when developing the code for the new website:

Web Application Security:

If the website includes web applications, follow secure coding practices to prevent common web vulnerabilities such as SQL injection, cross-site scripting (XSS), and CSRF (Cross-Site Request Forgery). Use web application firewalls (WAFs) to help protect against these attacks.

Error Handling:

Implement custom error handling to avoid exposing sensitive information in error messages. Provide generic error messages to users and log detailed error information securely.