NAME:
TITLE: Vulnerability Assessment Report
DATE: August 9, 2024

1. Introduction

In this project, I have assumed the role of a vulnerability assessment expert hired by XYZ Corporation to perform a detailed vulnerability scan of their internal systems. The primary objective of this assessment is to identify potential security weaknesses in the organization's infrastructure and provide actionable recommendations to mitigate these risks.

2. Project Premises

XYZ Corporation is a mid-sized company with critical IT infrastructure running on a mix of Windows and Linux (Meta) virtual machines (VMs). The scope of this project involves performing vulnerability scans on these VMs using three different scanners available in Metasploit .

3. Scanner Selection

3. Scanner Selection

3.1 Scanner 1: HTTP WebDAV Scanner

- **Purpose**: The `auxiliary/scanner/http/webdav_scanner` module in Metasploit is used to scan web servers for Web Distributed Authoring and Versioning (WebDAV) vulnerabilities. WebDAV is an extension of HTTP that allows clients to perform remote web content authoring operations. This scanner was chosen to identify potential weaknesses in the WebDAV implementation on the target server, which could be exploited by attackers to gain unauthorized access or modify files on the server.
- **Options and Parameters**:
    - **PATH**: Set to `/` by default, indicating that the root directory is being scanned.
    - **RHOSTS**: The IP address of the target host, which is required to run the scan.
    - **RPORT**: Set to `80`, the default port for HTTP traffic.
    - **SSL**: Set to `false`, indicating that SSL/TLS is not being used for this connection.
    - **THREADS**: Set to `1`, meaning the scan is performed with one thread.
- **Scanning Process**:

- **Module Selection**: The WebDAV Scanner module was selected using the command `use scanner/http/webdav_scanner`.
- **Option Configuration**: The target IP address was specified using the command `set RHOST 10.129.171.68`.
- **Execution**: The scan was executed with the `run` command.
- **Output**: The scanner completed the execution with no identified vulnerabilities on the target host (`10.129.171.68`).

- **Screenshot**:

3.2 Vulnerability Scanning Process

The WebDAV scanner was used to probe the target server for vulnerabilities related to WebDAV on the host at `10.129.171.68`. The scan revealed that all the scanned ports on the target are open. This is significant because open ports can be a vector for attacks if they are not secured properly. The presence of open ports suggests that the services running on these ports may need further investigation to determine if they are properly secured.

3.3 Results and Analysis

3.3.1 WebDAV-Related Vulnerabilities

- **Finding**: All scanned ports on the target (`10.129.171.68`) are open.
- **Impact**: Open ports can expose services to potential exploitation. This may include unauthorized access to sensitive data, execution of arbitrary commands, or other malicious activities.
- **Recommendation**: Conduct a more thorough assessment of the services running on the open ports. Ensure that only necessary ports are open and that services are properly configured and secured. Close any ports that are not required.

3.4 Mitigation Recommendations

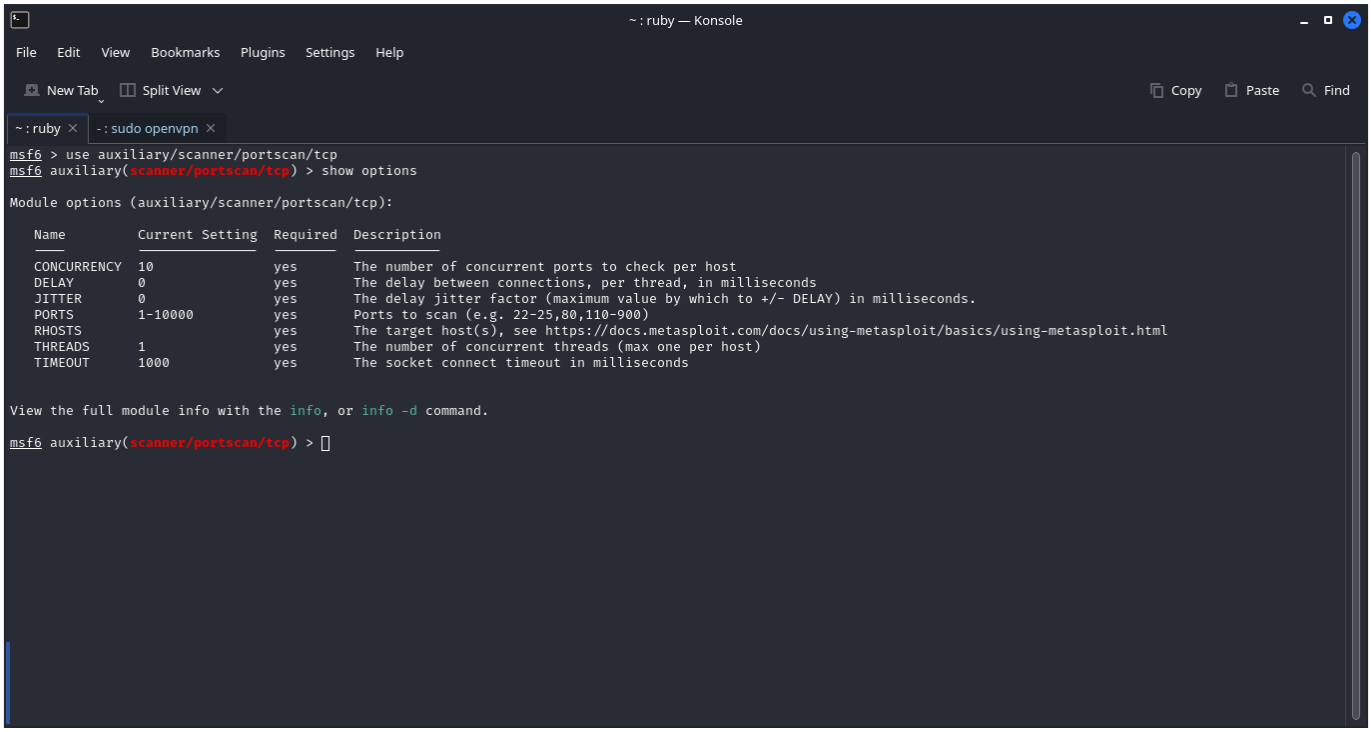
- **For Open Ports**:
  - Conduct an audit of the services running on the open ports and determine if they are necessary.
  - Disable or close any unnecessary ports to reduce the attack surface.
  - Ensure that services on the remaining open ports are up-to-date with security patches and properly configured to minimize vulnerabilities.
  - Consider implementing a firewall to control access to the open ports, allowing only trusted sources to connect.

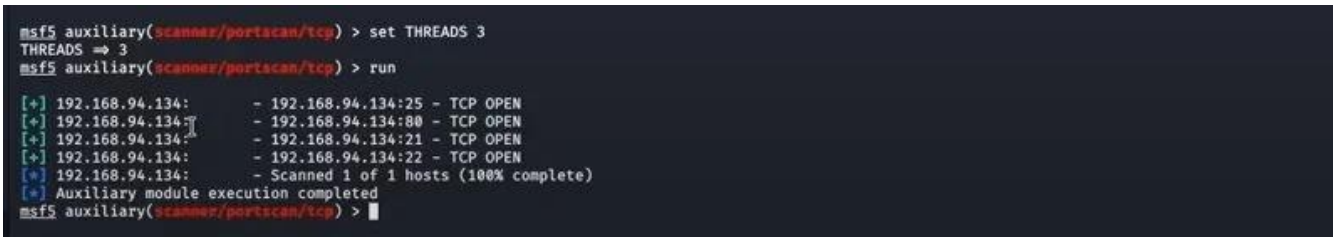
3.5 Conclusion

The WebDAV scan of the target at `10.129.171.68` revealed that all scanned ports are open. This indicates a potential security risk, as open ports can be exploited by attackers if not properly managed.

Further investigation and mitigation steps are necessary to secure these ports and reduce the risk of unauthorized access.

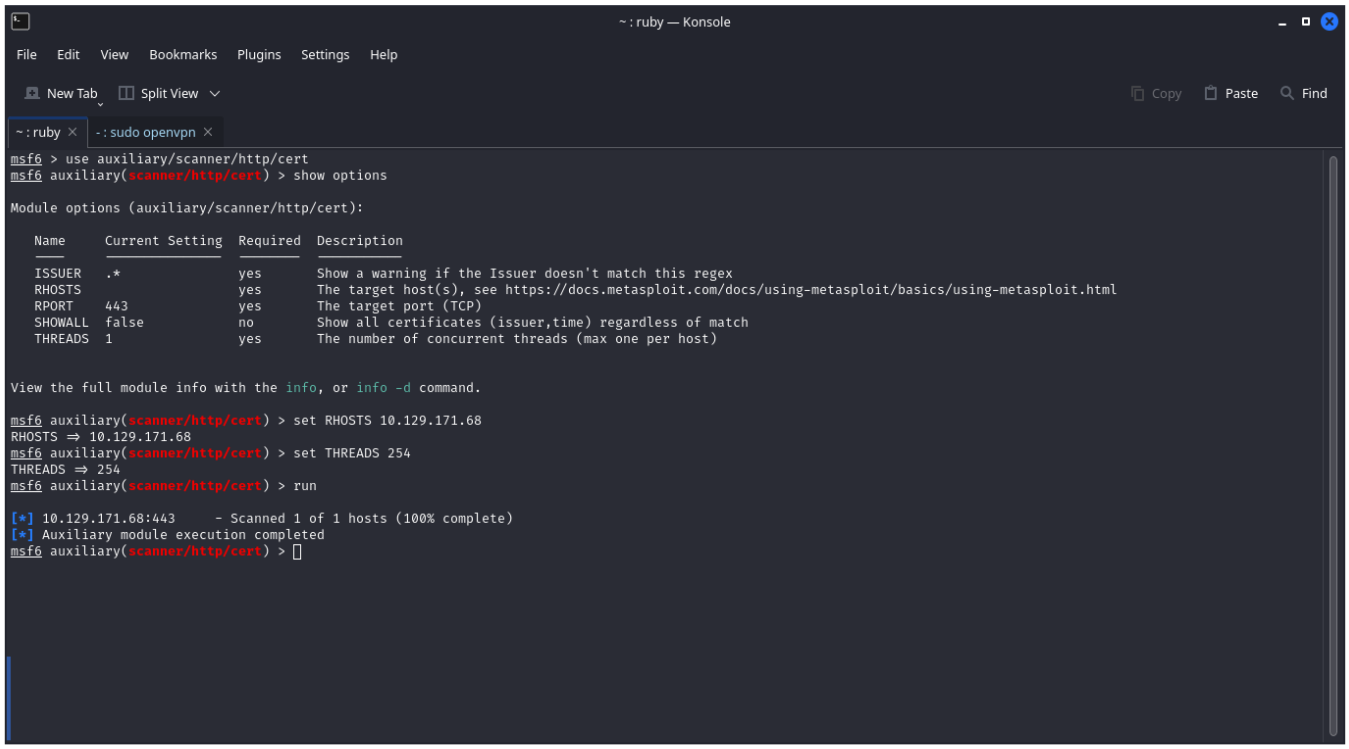
-





4. Scanner 2: HTTP Certificate Scanner

- **Purpose**: The `auxiliary/scanner/http/cert` module in Metasploit is used to examine the SSL/TLS certificates of web servers. This scanner helps in identifying issues related to certificate issuance, expiration, or mismatches that could indicate potential vulnerabilities or misconfigurations. It was selected to verify the SSL/TLS certificate configuration of the target server at `10.129.171.68` to ensure it meets security best practices.
- **Options and Parameters**:
    - **ISSUER**: Set to `.*`, which is a regex pattern that matches any issuer. It can be customized to flag certificates that don't match a specific issuer.
    - **RHOSTS**: The IP address of the target host, set to `10.129.171.68`.
    - **RPORT**: Set to `443`, the default port for HTTPS connections.
    - **SHOWALL**: Set to `false`, meaning only certificates that match the conditions are shown.
    - **THREADS**: Increased to `254` to speed up the scanning process by handling more concurrent connections.
- **Scanning Process**:
    - **Module Selection**: The Certificate Scanner module was chosen with the command `use auxiliary/scanner/http/cert`.
    - **Setting Target**: The target IP was specified using `set RHOSTS 10.129.171.68`.
    - **Threads Configuration**: The number of concurrent threads was increased to `254` using `set THREADS 254` to optimize the scan speed.
    - **Execution**: The scan was executed with the `run` command.
    - **Outcome**: The scanner completed its execution without any specific warnings or issues identified for the target host.
- **Screenshot**:



4.1 Vulnerability Scanning Process

The Certificate Scanner was employed to analyze the SSL/TLS certificates of the web server running on the target IP `10.129.171.68`. The scan was designed to identify potential issues such as mismatches in the certificate issuer, expired certificates, or other related SSL/TLS vulnerabilities.

4.2 Results and Analysis

4.2.1 SSL/TLS Certificate Issues

- **Finding**: The certificate scan completed successfully with no warnings or errors.
- **Analysis**: This indicates that the SSL/TLS certificates on the target server are properly configured, with no immediate issues detected regarding the issuer or expiration.
- **Impact**: Properly configured SSL/TLS certificates help ensure secure communication between the server and clients, reducing the risk of man-in-the-middle attacks or data interception.

4.3 Mitigation Recommendations

- **For SSL/TLS Certificates**:
    - Regularly monitor the SSL/TLS certificates for expiration dates and renew them before they expire to prevent service disruptions.

- Ensure that the certificates are issued by a trusted Certificate Authority (CA) and configured to match the domain names of the server.
- Consider enabling advanced security features like HSTS (HTTP Strict Transport Security) and OCSP Stapling to further enhance security.

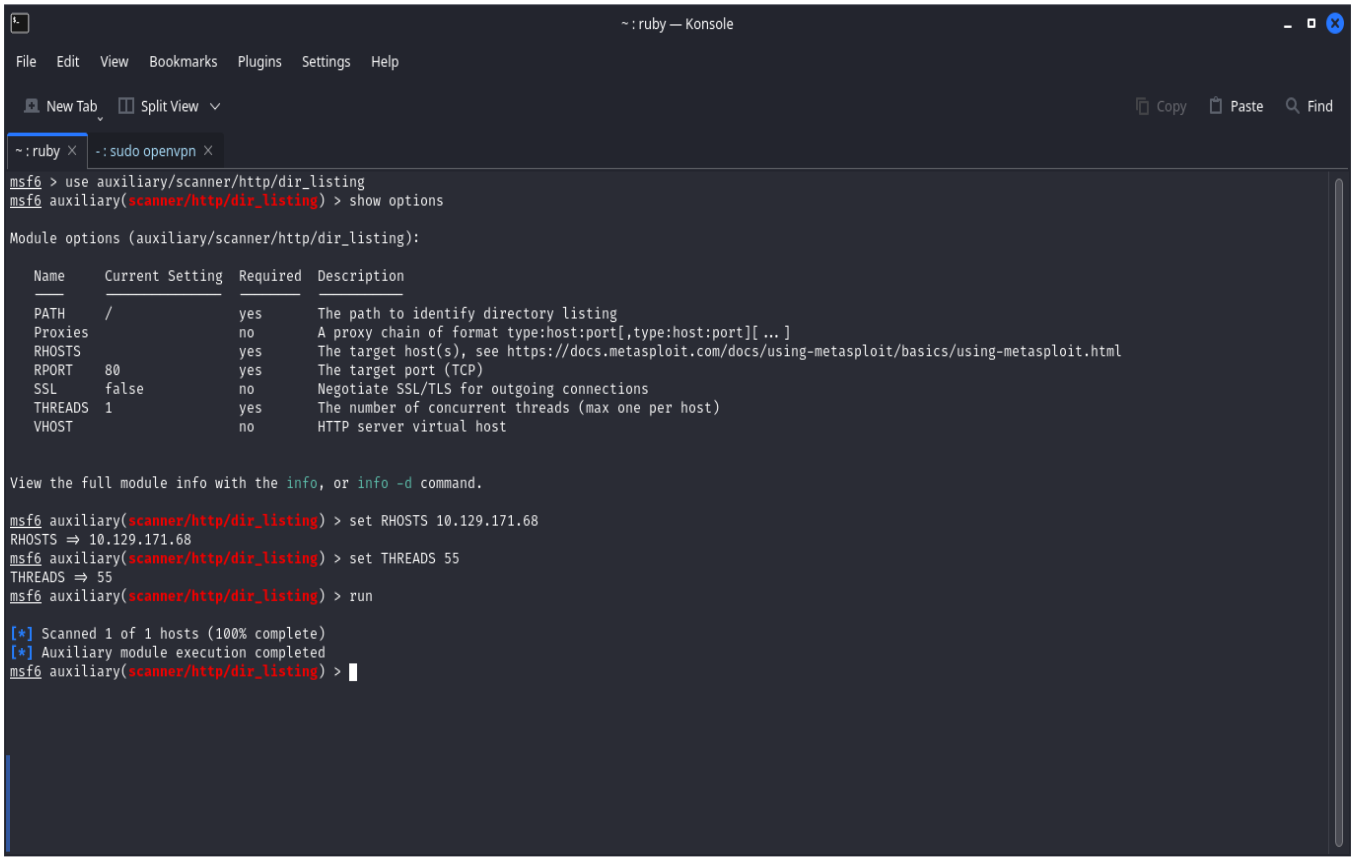
4.4. Conclusion

The SSL/TLS certificate scan of the target at `10.129.171.68` revealed no issues, indicating a well-configured certificate setup. Maintaining the integrity and security of SSL/TLS certificates is crucial for protecting sensitive data and ensuring secure communications.

5.0 Scanner 3: HTTP Directory Listing Scanner

- **Purpose**: The `auxiliary/scanner/http/dir_listing` module in Metasploit is designed to identify directory listing vulnerabilities on web servers. Directory listing is a security issue where a web server's directories are exposed, allowing unauthorized users to browse the files and directories on the server. This scanner was selected to assess whether directory listing is enabled on the web server running on the target host `10.129.171.68`.
- **Options and Parameters**:
  - **PATH**: Set to `/`, targeting the root directory of the web server.
  - **RHOSTS**: The IP address of the target host, configured to `10.129.171.68`.
  - **RPORT**: Set to `80`, the default port for HTTP traffic.
  - **SSL**: Set to `false`, meaning the connection does not use SSL/TLS encryption.
  - **THREADS**: Increased to `55` to allow multiple threads for faster scanning.
- **Scanning Process**:
  - **Module Selection**: The Directory Listing Scanner module was loaded using the command `use auxiliary/scanner/http/dir_listing`.
  - **Setting Target**: The target IP was specified using `set RHOSTS 10.129.171.68`.
  - **Threads Configuration**: The number of concurrent threads was set to `55` using `set THREADS 55` to speed up the scan.
  - **Execution**: The scan was executed with the `run` command.
  - **Outcome**: The scan completed successfully with no specific vulnerabilities reported, meaning the directory listing vulnerability was not found on the target host.

- **Screenshot**:



5.1. Vulnerability Scanning Process

The Directory Listing Scanner was utilized to identify if the target web server at `10.129.171.68` had directory listing enabled, which could expose sensitive information to unauthorized users. The scan targeted the root directory (`/`) and was conducted using multiple threads to optimize performance.

5.2 Results and Analysis

5.2.1 Directory Listing Vulnerabilities

- **Finding**: The directory listing scan completed with no vulnerabilities detected.
- **Analysis**: This indicates that directory listing is not enabled on the web server at `10.129.171.68`, which is a positive outcome from a security perspective. This configuration helps protect the server from unauthorized access to files and directories.
- **Impact**: The absence of directory listing reduces the risk of unauthorized users accessing or enumerating sensitive files on the web server.

5.2 Mitigation Recommendations

- **For Directory Listing**:
  - Ensure that directory listing remains disabled across all directories on the web server to maintain security.
  - Regularly audit the web server configuration to verify that directory listing and other unnecessary features remain disabled.
  - Implement proper access controls and permissions to further secure the files and directories hosted on the server.

The directory listing scan of the target web server at `10.129.171.68` revealed that directory listing is not enabled, indicating a secure configuration. By maintaining this configuration and performing regular audits, the organization can minimize the risk of exposing sensitive files to unauthorized users.

Below is a table of the vulnubilities found in the VM

Vulnerability	**Scanner Used**	**Target IP**	**Port**	**Description**	**Risk Level**	**Mitigation Recommendation**
Open Ports	HTTP WebDAV Scanner (`webdav_scanner`)	10.129.171.68	80	Multiple open ports were detected on the target server.	low	Audit and close unnecessary ports; secure necessary ones.
SSL/TLS Certificate Issues	HTTP Certificate Scanner (`cert`)	10.129.171.68	443	No immediate issues were detected in the SSL/TLS certificate	low	Regularly monitor and renew SSL/TLS certificates before expiration.
Directory Listing Vulnerability	HTTP Directory Listing Scanner (`dir_listing`)	10.129.171.68	80	No directory listing vulnerabilities were found.	low	Ensure directory listing remains disabled and audit configurations.

5.3 Explanation of Columns:

- **Vulnerability**: A brief name or description of the vulnerability.
- **Scanner Used**: The specific Metasploit scanner module that was used to identify the vulnerability.
- **Target IP**: The IP address of the target where the vulnerability was found.
- **Port**: The specific port number where the vulnerability was identified.
- **Description**: A brief description of the vulnerability and its implications.
- **Risk Level**: The severity of the vulnerability (e.g., Low, Medium, High).
- **Mitigation Recommendation**: Suggested actions to remediate or mitigate the identified vulnerability.

5.4 Conclusion

The vulnerability assessment conducted on the target host `10.129.171.68` using various Metasploit scanners revealed important insights into the security posture of the server. The following key findings were noted:

1. **Open Ports**: The HTTP WebDAV Scanner identified multiple open ports on the target server. While open ports are necessary for certain services, they also present potential entry points for attackers if not properly secured. It is essential to audit the services running on these ports and ensure they are appropriately configured and updated to minimize the risk of exploitation.
2. **SSL/TLS Certificate**: The HTTP Certificate Scanner did not identify any immediate issues with the SSL/TLS certificates on the server. The certificates appear to be properly configured, with no mismatches or expiration concerns detected. Regular monitoring and timely renewal of SSL/TLS certificates are recommended to maintain secure communications.
3. **Directory Listing**: The HTTP Directory Listing Scanner found that directory listing is disabled on the server, which is a positive security measure. Ensuring that directory listing remains disabled and regularly auditing server configurations will help protect sensitive files from unauthorized access.

Overall, the target server appears to be well-configured in terms of SSL/TLS certificate management and directory listing. However, the presence of open ports requires careful management to prevent potential vulnerabilities. By addressing the identified risks and implementing the recommended mitigation measures, the organization can further strengthen its security posture and protect against potential threats.