CIDM 6340

Network Management and Information Security

Research Report 3 – Vulnerability Scanning with Shields Up and Nessus

Vernice Tanquerido

**What did you do**

The focus of this activity is to run vulnerability scans using ShieldsUp and Nessus.

ShieldsUP is a free-to-use port scanning service owned and operated by Steve Gibson. Currently, the service is limited to performing scans on only the device IP address that is running ShieldsUP. Two port scans were done for common ports and all service ports.

ShieldsUp detects vulnerabilities on a user’s computer by identifying port statuses. The service does this by attempting to establish standard TCP connections with the ports on their computer. The common ports scan inspects a collection of the most common internet ports on their computer. In our case, it scanned 26 ports. The all service ports scan, on the other hand, scans the first 1056 TCP ports of the user’s system. It then returns the status of each port if it is open, closed, or stealth. Each port was analyzed according to their status.

A stealth port does not respond or completely ignores incoming traffic. It would appear as if the port is invisible or does not exist which provides an added layer of security if hackers try to access your system.

A closed port responds to a packet but will indicate that the port is closed or not open for communication. An attacker will be still be able to identify that the port exists but it will reject requests sent its way.

An open port indicates a vulnerability to a system. This means that internet traffic requesting a connection to the machine is being accepted and connections are being created.

ShieldsUp will return a TruStealth Analysis showing how each port responded to the server’s ping requests. A perfect TruStealth rating means that your system completely ignored all ping requests sent by the server.

Nessus is a more comprehensive scanning service that can detect vulnerabilities of networks outside of the device's IP address. It first discovers hosts connected to the address that the user entered. It does this by sending ping requests to identify which hosts are responsive. The free version used for this activity can scan up to 16 hosts at a time. It then checks open ports on each of the selected hosts, identifies their OS, and performs other vulnerability checks. It then returns a dashboard that lists the hosts analyzed and their respective vulnerabilities, categorized according to their severity. Nessus classifies vulnerabilities based on Common Vulnerability Scoring System (CVSS) values from the National Vulnerability Database (NVD). They can be either be critical, high, medium, low, or info.

Our home network was used in this activity and 15 hosts were analyzed for vulnerabilities. These vulnerabilities were ranked according to the severity that Nessus assigned. The high vulnerabilities were prioritized and analyzed first, then the medium vulnerabilities, and so on.

**What are the results**

The first part of the activity is to run vulnerability checks on ShieldsUP. The common ports scan inspected 26 ports. The TruStealth Analysis on these most common ports returned a perfect “TruStealth” rating meaning that the system ignored all the ping requests sent by the server. This means that the system is hidden from attackers and reduces the likelihood of being targeted for attacks.

A white paper with black text

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A group of text boxes

Description automatically generated

Like the results for the common ports scan, the scan on all the service ports also returned a perfect TruStealth rating. All requests sent by the server were ignored and no packet was returned by the system.

A green squares with numbers

Description automatically generated

A close-up of a white background

Description automatically generated

Nessus performed a more in-depth vulnerability analysis on the network. Vulnerabilities were categorized based on their severity. In this case a total of 39 vulnerabilities were identified. Out of this, 87% are info, 2% are low, 9% are medium, 2% are high and there were no critical risks.

A high vulnerability is identified on host 192.168.1.115. The device was discovered to be running on a Microsoft Windows 10 Operating System and the high risk vulnerability associated with it is that it supports the use of SSL ciphers that offer medium strength encryption. On an attack surface perspective, this would provide an attacker an opportunity to decipher the encrypted data. To mitigate this, the server can be configured to where strong cipher suites are used instead.

A screenshot of a computer

Description automatically generated

Another vulnerability found on this host and two others (192.168.1.140 and 192.168.1.123) is that the SSL certificate cannot be trusted. This was categorized as medium. According to Nessus, this situation can occur in three ways. First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. Second, a certificate was not valid at the time of the scan. Lastly, the certificate chain may contain a signature that did not match with the certificate information. In any of these three scenarios, it would make it difficult to identify the authenticity of the web server and is a gateway to attacks. A proper SSL certificate can be generated to avoid security risks.

Similar to this vulnerability, a self-signed SSL certificate can also be mitigated through proper generation of an SSL certificate.

Another medium vulnerability identified through the scan is that the SMB signing is not required. This is associated with host 192.164.1.140. This means that an unauthenticated attacker can take advantage of this and connect to the SMB server. To prevent this, proper sign-in or authentication from the host must be enabled.

On host 192.168.1.115, there were two medium vulnerabilities identified associated with TLS versions being outdated specifically versions 1.0 and 1.1 that were identified. Version 1.0 is identified to have cryptographic design flaws and both versions no longer function properly for major web browsers. Updating TLS to version 1.2 or higher will help protect this attack surface.

One low vulnerability was detected on 192.168.1.123. The hosts responds to ICMP Timestamp requests. This would give an attacker information on the date set on the device which may allow them to breach time-based authentication protocols. This risk can be mitigated by filtering out ICMP timestamp requests and outgoing replies.

All other vulnerabilities are information identified for each host. A full list of the hosts scanned and vulnerabilities detected can be found in Appendix I and II.

**What did you learn**

In this activity, I learned about the tools that can be used to asses your device or network’s vulnerability. ShieldsUp is a great tool to use to perform a quick check of the port statuses of your device and determine potential attack surfaces. To get a more detailed analysis and perform scans on other devices as well, Nessus from Tenable is a useful service that breaks down the vulnerabilities of your desired networks. Having the vulnerabilities identified, allows you to assess your network so that you can perform necessary modifications to protect your system and improve security.

With this knowledge, regular scans can help determine its vulnerabilities and uncover security weaknesses across the network. Identifying open ports or possible attack surfaces using ShieldsUp makes way for the organization to implement measures to keep these surfaces secure and be managed accordingly.

Using the severity data provided by Nessus, the organization can assess the potential impact if a particular system is attacked. This can help in prioritization efforts to make sure that the most critical issues are addressed first thereby reducing the overall risk. By identifying and addressing these vulnerabilities, the organization can reduce the possibility of attackers infiltrating the system and thereby saving the organization its resources and other damages the attack may cause.

**Appendix I**

Hosts scanned and their vulnerabilities

A graph with blue and white lines

Description automatically generated

**Appendix II**

Vulnerabilities identified on the network

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a phone

Description automatically generated