Research Report 3 Vulnerability Scanning with Shields Up and Nessus

Analyze the results of both parts of this assignment. Determine what vulnerabilities (if any are found) are the most severe and what corrective action should be taken.

1. What did you do?

I began with the Shields Up scan. I followed this link to the vulnerability scanner: <https://www.grc.com/x/ne.dll?bh0bkyd2> I proceeded to the shields up scan. Nothing was loading when I got to the page. I disabled my ad-block extension in Firefox and refreshed the page. This allowed everything to load correctly. I selected the “Common Ports” scan, and I allowed it to run. Once it was done, I saved the results to a text document. I then went back and did a “All Service Ports” scan. I allowed it to run and saved the results similar to the first scan.

Shields Up “Common Ports” Scan works by attempting to establish a TCP Internet connection with a collection Common Ports often used in vulnerabilities. This is done from Shields Up’s servers so when a successful connection is made it demonstrates which ports are "open" or visible to the Internet. The “All Service Ports” scan works similarly but instead it targets ports 1-1056.

After running the two scans I then moved onto Nessus. I followed this link to there site: <https://www.tenable.com/products/nessus/nessus-essentials> I requested an educational license. After receiving my license, I downloaded Nessus Essentials. I Installed it and activated it with my educational license. I launched it in a browser. I setup the local admin account and waited for Nessus to finish setting up plugins. Once it was done I setup a Basic Scan. I allowed it to search for hosts. I selected 16 hosts and allowed the scan to be completed. After it was completed I setup an advanced scan to the same hosts.

Nessus is a vulnerability scanner developed by Tenable, Inc. Nessus is an open-source tool that scans for network vulnerabilities. Nessus tests each port on a computer to see what services are running. It then tests the service to make sure there are no vulnerabilities that could be used to carry out an attack.

After saving all the scans I began reviewing them. I began with the Shields Up scans and reviewed the Nessus Scans second.

1. What are the results?

The first scan Shields Up “Common Ports” scanned ports 0, 21-23, 25, 79, 80, 110, 113, 119, 135, 139, 143, 389, 443, 445, 1002, 1024-1030, 1720, 5000. It found 0 ports open, 2 ports closed, and 24 stealth ports. The closed ports are 80 and 443. The TruStealth test failed because of the following: NOT all tested ports were STEALTH, NO unsolicited packets were received, NO Ping reply (ICMP Echo) was received.

A white paper with black text

Description automatically generated

A "Stealth" port is one that will ignore and drop any incoming packets without informing the sender about the port being "Open" or "Closed". "Closed" is the best option without a stealth firewall or NAT router in place. The port is not "Open" and accepts connections from the probes which are sweeping the Internet searching for vulnerable systems. Open ports are caused by something in a system or network accepting any unsolicited incoming connections from unknown and anonymous machines on the Internet.

I have setup rules in my router specifically blocking 443 and 80. I have a domain setup and I noticed that my router was accessible over the internet and default ports. I never wanted this function, so I simply created block rules in my router. The only downside is someone would see that there is device responding. This could cause a target attack but since I have a few devices I want to access over the internet there is no way to resolve the TruStealth test.

A green and blue squares with white text

Description automatically generatedA white paper with black text

Description automatically generated The “All Service Ports” scan was next. It scanned ports 0-1055 and had very similar results. It found 0 ports open, 2 ports closed, and 24 stealth ports. The closed ports are 80 and 443. The TruStealth test failed because of the following: NOT all tested ports were STEALTH, NO unsolicited packets were received, NO Ping reply (ICMP Echo) was received.

For the Nessus Vulnerability scan I had it scan 16 host. These are the 16 hosts 10.0.0.1, 10.0.0.10, 10.0.0.39, 10.0.0.40, 10.0.0.41, 10.0.0.42, 10.0.0.46, 10.0.0.47, 10.0.0.51,10.0.0.55, 10.0.0.61, 10.0.0.111, 10.0.0.131, 10.0.0.132, 10.0.0.137, and 10.0.0.198. The scan found 36 mixed severity SSL, 12 mixed TLS, 2 IP forwarding, 2 SMB Signing not required, 1 RDP, 1 DHCP sever detection, and 20 SMB vulnerabilities.

The highest severity issue is an SSL Medium Strength Cipher Suites Supported (SWEET32). Nessus’ description of this issue is “The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.” It specifically called out port 3389 on 10.0.0.51. Port 3389 is the default Windows Remote Desktop Protocol. This vulnerability is around the encryption on the passwords is weak and could be decrypted easily. Nessus recommends “Reconfigure the affected application if possible, to avoid use of medium strength ciphers.” Basically, increase the encryption level.

One of the other vulnerabilities found was SMB Signing not required. Nessus’ description of this issue is “Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.” There solution is “Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.” This issue centers around Samba based file shares. Specifically, there is no signing required from the server. The solution is to enable signing on the server.

1. What did you learn?

For Shields Up I have used it before and was aware of what it could do in terms of port scanning. An open port on a firewall is a big deal because just anyone could come through it into your network. Blocking ports is risky since it confirms that there is a device on the other side. Ideally no confirmation, blocking or not, is sent back. My new job is to perform technical alignments on our customers. One of the assessment questions is around open ports. Because of this I will continue to use Shields Up.

For Nessus, I was aware of Tenable but not Nessus specifically. When I was at Happy State Bank I knew they talked about using Tenable to do vulnerability scans but beyond that I was unaware of what it was and could do. At my current job we do install similar software that does proactive scanning of workstations. The perk of Nessus is it can catch new devices on the network and also it can scan non-workstations. I could see this being useful for some of our clients.

References

Shields UP!! — System Error. (n.d.). Www.grc.com. <https://www.grc.com/x/ne.dll?rh1dkyd2>‌

Tenable Nessus Vulnerability Scanner: Product overview. (n.d.). SearchSecurity. <https://www.techtarget.com/searchsecurity/feature/Tenable-Nessus-Vulnerability-Scanner-Product-overview>

Itperfection. (2021, January 18). What is NESSUS and How Does it Work? ITperfection - Network Security. https://www.itperfection.com/network-security/network-monitoring/what-is-nessus-and-how-does-it-work-network-munitoring-vulnerabilit-scaning-security-data-windows-unix-linux/

Jennex, M. (2023). MgmtOfInfoSec\_6e-Ch01\_pr [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646253-dt-content-rid-51650746\_1/xid-51650746\_1

Jennex, M. (2023). Why Computers Are Vulnerable r3 [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646253-dt-content-rid-51650747\_1/xid-51650747\_1

Jennex, M. (2023). CIDM6341 Introduction [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646253-dt-content-rid-51650748\_1/xid-51650748\_1

Jennex, M. (2023). MgmtOfInfoSec\_6e-Ch12\_pr [PowerPoint slides]. https://wtclass.wtamu.edu/bbcswebdav/pid-2646267-dt-content-rid-51650758\_1/xid-51650758\_1