**Research Report ShieldsUP/Nessus**

Adrian Varela

WTAMU

CIDM 6340-70: Network Management and Information Security

Professor Murray Jennex

August 3, 2023

WHAT DID YOU DO

For this exercise I started with the software of ShieldsUP. This software was easy to use through the link, making it very convenient for users to view the product of ShieldsUP. This software works as a port scanner looking for the anything that can respond back to the network or devices making it accessible if ports are left unsecure. The use of ports can enable the communication with a host and destination. By port scan, it can show whether these ports are open closed or in stealth mode. This test is accomplished through your first 1056 ports since these ports are popular for any hacker. The user can view the results of the stealth test with running the port scan. If the ports are open and vulnerable, they will return red. If they are closed, they return blue meaning there is still a response from a scan. If these return green, it means it’s in stealth mode most likely from the use of a firewall or Internet Service Provider. The way I analyzed the output was by hovering over the blocks showing specific ports and their names giving me the details back with All Service Ports option. The way I also analyzed the output was through the common ports option giving me my results. The all-service ports option gave a better in depth look on all ports throughout my network. I would go through some of the blocks to review the specific information on that port and the result of the grid scan. The other way I viewed the results was the text summary giving me the results in text return of what ports where open, closed and in stealth.

For the second part of the exercise, I utilized the Nessus software. This software was a bit different than utilizing the ShieldsUP software. When installing the software, Nessus had to be downloaded through the website giving it permission to be installed to my device. Once installed properly this gave Nessus the ability to scan my network or devices easily. I opened the application, and it went through my Google Chrome application to begin the scans. There was more in-depth knowledge making the scan return with a lot more informative as the scans gave options of what you wanted to look for through your network. I chose the basic network scan to see the basic vulnerabilities as I was unfamiliar with the software in the beginning. During the evaluation portion I had to create a new scan for my network, giving the IP Address. Once the basic information was distributed, I had to go through launch which would then evaluate my ports that were connected from the IP address and give me my report back. This report was very informative explaining in detail the vulnerabilities the host had ranging from info to critical. The software looked for the host and destination’s information and communication ensuring there was no suspicious activity. Another way I viewed the vulnerabilities was through a folder that was created showing the names and counts of vulnerable objects are within each file. When looking through this information I would evaluate what was being relayed through the software with the settings of the device I was connected on with Terminal from MacBook as well.

WHAT WERE THE RESULTS

The results displayed for ShieldsUP were what I expected from my network which was that all 26 common ports were in stealth mode. This result was the same for the first 1,056 ports that were tested meaning they did not solicit packets, or a ping was received. This is helpful for the attack surface due to people not being able to even solicit my device for a response.

Through Nessus the results were more in depth and showed the vulnerabilities that my network were displaying by network basic scan which resulted in 86% secure. The high vulnerability was the DNS (Doman Name System) Server spoofed request amplification of a (Distributed denial of service) DDOS. This is huge because of the query response being much longer than the requested response. The port that was displayed was port 53 UDP. If the DDOS happens from an attack service view, a malicious hacker can send an influx of attack traffic interrupting my network. To mitigate this issue, I would need to restrict access to my DNS server from public network. To do this I need to update my firewall rules to ensure I restrict access to my devices only. This was the only vulnerability displayed through Nessus giving me security for the rest of the network scan to meet compliance for security.

WHAT DID YOU LEARN

Through this exercise I learned the importance of why securing ports need to maintain a priority for any business. I saw how simple it was to gain access to view what ports were open to a network with the utilization of scans. When it comes to scanning ports, it is critical to ensure they are only accessible to people who are in the need to know. To do this I learned that ports should remain in stealth mode. If displayed in closed, I learned that there is still a response in which an attacker now has a destination for an attack. If not done properly any malicious user whether that’s an inside source for a company or a hacker can easily attack the network slowing that organization down. A huge part I learned from the vulnerability scan was with the Nessus software. This software helped provide me with in-depth information about solutions for most issues I viewed. The solutions being simple can go a long way with protecting assets. The other portion I learned from the ShieldsUP scan was the common ports scan. For anyone that has network administrator access I would recommend this scan for the safety of their organization. The information I learned when just going through my ports that were not a vulnerability, provided me detailed ways to keep my network even more secure. A source I found notified me of the real-world scenarios of an example of recent attacks. This attack was one from a community college in Michigan, you’ll notice that it was suspicious activity that shut down online classes for weeks. This displays why the attack surface needs to be as minimal as possible for any large organization. If the attack surface remains large, I notice the more vulnerable the organization becomes to malicious hackers.