What did you do?

ShieldsUp

1. Visited https://www.grc.com/x/ne.dll?bh0bkyd2
2. Clicked on the proceed button
3. Clicked on the Common Ports button
4. Printed results to pdf “ShieldsUp\_Common Ports”
5. Clicked on text summary
6. Printed results to pdf “ShieldsUp\_Common Ports-Text”
7. Clicked on the All Service Ports button
8. Printed results to pdf “ShieldsUp\_All Ports”
9. Clicked on text summary
10. Printed results to pdf “ShieldsUp\_All Ports-Text”
11. Ran nslookup on 173.218.9.135
12. Searched unfamiliar IPv4 on web search engine
13. Discovered geographical location based on IP address (Private IP vs Public IP)

ShieldsUp is a web-based software that scans port status of TCP system ports 1-1056 on the device you run the scan from. It probes to see if these ports are open, closed or in stealth mode. These are in reference to when your PC is “listening.” A necessary port will allow data to pass past a LAN given it hasn’t been closed. These well-known ports are for destinations whereas a higher number of ports are used for source traffic. Closed ports will not allow any traffic to pass through that port. Open ports will allow all traffic to pass through that port. Stealth ports will allow traffic to pass through that port given a request was sent and response is anticipated.

ShieldsUp is an automated process once you visit the website, agree to the terms, and choose which type of scan to conduct. There is variety on what to scan: popular ports, all ports, specific ports, etc. A colored chart of all 1056 ports is provided with simple a simple corresponding legend: Green = Stealth, Red = Open, Blue = Closed.

This color coded “chicklet chart” made analyzing port status beyond easy. Interestingly, ShieldsUp specificially added ports 1024-1056 because Microsoft Windows “has a tendency to establish globally available listening services on the first few ports in the ‘client port’ range…”¹

Nessus

1. Visited https://www.tenable.com/products/nessus/nessus-essentials
2. Registered with WTAMU student details
3. Stopped process when received license activation code
   * I think this needs to be done on business computer (host on network to be scanned)
4. Struggled to get permission on an organization’s network, proceeding with home network
5. Downloaded Nessus-10.5.3-x64.msi
6. Ran Install Wizard on Nessus
7. Connected via SSL
   * Had to proceed past localhost warning
8. Registered for Nessus Essentials
9. Entered license activation code
10. Created Username and password for Nessus user account
11. Downloading plugins………….
12. Compiling plugins…………….
13. Created a Folder
14. Created a new scan targeting 192.168.1.0/24
    * 192.168.1. 🡪 1, 15, 104, 110, 129, 187, 211, 252
15. Run Scan
16. Generated Complete List of Vulnerabilities by Host Report
17. Saved to pdf “Nessus\_Network Scan Report”

Nessus is a remote security scanner that discovers vulnerabilities of all devices connected to a network. It probes and tests to discover weak links in device cybersecurity. Nessus utilizes TCP/UDP packets and sends probes to device IPs on the network. Nessus exposes vulnerabilities but stops there. It is a scanner yet does not initiate patches or fixes to vulnerabilities. Nessus does a superb job at being up to date; they habitually update known vulnerabilities to reduce nefarious actors’ opportunity.

“As an open-source network vulnerability scanner, Nessus uses the Common Vulnerabilities and Exposures architecture to make it easy for compliant security solutions to cross-link. The Nessus Attack Scripting Language (NASL), a straightforward language used by Nessus, is used to specify specific threats and potential attacks…It does this by checking a machine more than 1200 times to see if malicious actors could use any such attacks to get into the system or do other harm.”²

Analyzing the output is straightforward and intuitive due to Nessus’ generation of reports, graphs, and remediations. I dived into the analysis by looking at each device IP and the specific vulnerability and remedy. Nessus does an excellent job of breaking down each individual vulnerability and specifying the way ahead. A final product generating software on the tail end of a vulnerability scan makes sense given the annual membership of the software of $5,000+.

To analyze the vulnerability data, Nessus’ framework of risk must be understood. Vulnerability Priority Rating (VPR) is the output of predictive prioritization, showing the remediation priority. VPR deals with actual cyber risks. “Tenable uses and displays third-party Common Vulnerability Scoring System (CVSS) values retrieved from the National Vulnerability Database (NVD) to describe risk associated with vulnerabilities. CVSS scores power a vulnerability’s Severity and Risk Factor values.”³ CVSS calculates theoretical risk and can be dramatically different than the VPR rating.

|  |  |  |
| --- | --- | --- |
| Severity | CVSS V3.0 Range | VPR Range |
| Critical | 9.0-10.0 | 9.0-10.0 |
| High | 7.0-8.9 | 7.0-8.9 |
| Medium | 4.0-6.9 | 4.0-6.9 |
| Low | 0.1-3.9 | 0.1-3.9 |
| Info | 0 | N/A |

What are the results?

ShieldsUp

Ports 1-1056 are in stealth. Interestingly Port 0 was closed due to being a reserved port that can’t be used. With only one port “visible” my home network has a reduced attack surface. Even with the response showing the port is closed, it only makes it known there is a device at this IP. This resulted in what seems like a quirk of the scan: “TruStealth” failed due to Port 0 being closed. No unsolicited packets nor ping replies (ICMP Echo) were received.¹

None of the first thousand ports were “listening” given there was not a request for data. This is an effect of my ISP’s firewall. Traffic does not enter my home network unsolicited. In running nmap -p (port number) against my Public IP 173.218.9.135, I found most ports were closed. Meaning my nmap sent a SYN and I received an RST. There were a few such as Telnet (23) and HTTP (80) that came back as filtered, so no RST. DNS (53) and HTTP-ALT (8000) were open.

I suspect the difference between nmap showing a port as closed and ShieldsUp showing the same port as filtered is caused by which side the port scan is happening from. With nmap, the TCP/IP port probes are sent from within the Gateway router and on my home network’s side of the ISP’s firewall. This allows the RST confirming a closed port because the probe was requested. With ShieldsUp, the TCP/IP port probes are sent from the ShieldsUp IP 4.79.142.206 on the WAN side of my home network and ISP firewall. My ISP firewall probed ports and all were found in stealth to stay hidden. No ports were confirmed to exist because a SYN was not pushed.

Nessus

The following IP addresses were active on my home network during the Nessus scan with varying levels of vulnerability risk. None of my devices had critical nor high vulnerability risk.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IPv4 | Name | Type | Medium | Low | Info |
| 192.168.1.1 | Docsis-Gateway | Wi-Fi Router | 5 | 1 | 31 |
| 192.168.1.15 | DESKTOP-3SHPIF1 | PC | 1 | 0 | 17 |
| 192.168.1.104 |  | iPhone | 0 | 0 | 8 |
| 192.168.1.110 |  | Tablet | 0 | 0 | 18 |
| 192.168.1.129 | Galaxy-Tab-A7-Lite | Tablet | 0 | 0 | 5 |
| 192.168.1.187 | BRW5C61999450D8 | Brother Printer | 0 | 0 | 4 |
| 192.168.1.211 | RokuPremiere | Roku | 0 | 0 | 16 |
| 192.168.1.252 | Gena-s-s10e | Samsung Cell Phone | 0 | 0 | 5 |

192.168.1.1

1. IP Forwarding Enabled (Medium)

* Vulnerability is null due to the device being a router

2. SSL Certificate Cannot Be Trusted (Medium)

* Vulnerability has three ways chain of trust can be broken
  1. Unknown public certificate authority – likely cause of self-signed certificate
  2. Outdated certificate
  3. Bad certificate signatures
* Solution is to generate a proper SSL certificate

A diagram with text on it

Description automatically generated with medium confidence3. SSL Self-Signed Certificate (Medium)

* Vulnerability is certificate chain for this service is not signed by a recognized certificate authority
* Solution is to generate a proper SSL certificate

4. TLS Version 1.0 Protocol Detection (Medium)

* Vulnerability is remote service accepts connections encrypted using TLS 1.0 which has several cryptographic design flaws
* Solution is enable support for TLS 1.2 and 1.3 and disable support for TLS 1.0

5. TLS Version 1.0 Protocol Deprecated (Medium)

* Vulnerability is remote service accepts connections encrypted using TLS1.1 which lacks support for current and recommended cipher suites
* Solution is enable support for TLS 1.2 and 1.3 and disable support for TLS 1.0

6. DHCP Server Detection (Low)

* Vulnerability is the script contacts the remote DHCP server and attempts to retrieve information about the network layout
* Solution is filtering to keep this information off the network and remove unused options

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Severity | CVSS V3.0 | VPR Score | Plugin |
| IP Forwarding Enabled | Medium | 6.5 | 4.0 | 50686 |
| SSL Certificate Cannot be Trusted | Medium | 6.5 | - | 51192 |
| SSL Self-Signed Certificate | Medium | 6.5 | - | 57582 |
| TLS Version 1.0 Protocol Detection | Medium | 6.5 | - | 104743 |
| TLS Version 1.1 Protocol Deprecated | Medium | 6.5 | - | 157288 |
| DHCP Server Detection | Low | 3.3 | - | 10663 |

The remainder of the vulnerabilities were all in the information category, designating there is virtually no risk.

192.168.1.15

1. SMB Signing Not Required (Medium)

* Vulnerability is signing is not required on the remote SMB server – open for man-in-the-middle
* Solution is enforcing message signing on host’s configuration – digitally sign communications

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Severity | CVSS V3.0 | VPR Score | Plugin |
| SNB Signing not Required | Medium | 5.3 | - | 57608 |

The remainder of the vulnerabilities were all in the information category, designating there is virtually no risk.

The risk to the attack surface is minimal with the TLS Version 1.0 and 1.1 Protocol vulnerabilities being the largest risk in my opinion. TLS 1.0 has been around since 1999 giving bad actors plenty of time to find the weak spots. It is largely still utilized for backwards compatibility but can be disabled easily. TLS 1.1 is in a similar vein, just an outdated Transport Layer Security. TLS 1.3 is the current version as of 2018. If TLS 1.0 and 1.1 are disabled, it will reduce the attack surface. The downside is that I won’t be able to connect to any https that support TLS 1.0 and 1.1. Microsoft took a bold step in enforcing the current TLS to start in 2020. How important is it to leave TLS 1.0 and 1.1 open? Not much. A 2021 TLS Telemetry Report found the following:⁴

A blue rectangle with black text

Description automatically generated

I have confidence these metrics are quite larger in 2023. I am not sure how big an issue the SSL vulnerabilities are. In my research, I’m led to believe this is an effect of being behind the IPS’s firewall. Incomming traffic is intercepted by the IPS firewall, and it replaces the certificate with its own self-signed certificate. Meaning the self-signed certificate is not recognized by any host outside my home network.

SNB Signing not Required is a theoretical risk, a 5.3 on CVSS V3.0. It opens my PC traffic up for man-in-the-middle attacks and is a relatively easy fix. Server Message Block signatures eliminate the possibility for a spoofed message because the true original is hashed.

What did you learn?

ShieldsUp

Steve Gibson created the Gibson Research Corporation and offers largely free software and services that help protect cyber users. ShieldsUp has been assisting attack surface mitigation since 1999. It’s impressive the ShieldsUp tool is still so useful to this day although it makes sense. With the foundation of world wide web networking being so heavily TCP/IP port based, ShieldsUp will continue to be useful unless a revisionary change occurs in transport.

ShieldsUp can be used in many facets albeit the same job. Hardware and software firewalls as well as virtual machines can all utilize the service. I think the software was much more critical prior to IPS’s including firewalls on their client routers and switches. In the end, ShieldsUp can tell me what’s blocked, what’s accessible, and what’s talking on it.

As technology is innovated, new forms of cyberattack threats emerge. When new threats emerge, we develop new technology to combat cyberattacks. I am unclear on the difference between nmap designation of filtered versus ShieldsUp designation of stealth, but suspect they are synonymous.

ShieldsUp automatically used my public IP address which led me on a rabbit hole dive into why my Gateway IP address (private) wasn’t an option. I discovered “nslookup” followed by an IP address gives all sorts of details. You can see the flow of notes below, ultimately followed by an “ah yes, that makes sense” when I arrived at public IP addresses.

1. ShieldsUp automatically used IPv4 173.218.9.135 – my neighborhood router? IPS device regardless. Nslookup shows name is “173-218-9-135-grvl.mid.dyn.suddenlink.net” Trace route shows this IP is only one hop away.
2. Searching 173.218.9.135 on web search engine provided ntunhs.net website that the IP range 173.218.0.0 – 173.218.255.255 belongs to Suddenlink Communications based out of Missouri.
3. Dialing into more specific, the same first three octets show 173.218.9.0 is based in Derrider, LA along with Latitude: N 30.8277 Longitude 93.24.94 and a map showing the closest town to me.
4. IP / Domain Lookup⁵
5. Private IP vs Public IP

Regarding attack surface, you really must scan every port of everything on your network. This will take a lot of computational power! Scan every TCP port to find what is open, may all the services to a device, and look for vulnerabilities in products themselves. With every batch of new products, new attack vectors open. As Steve Gibson puts it, “Each open port on a machine creates a potential point of attack for an internet intruder.”

ShieldsUp is a very quick, reliable, and free way to test port status of devices and firewalls. A downside I see is you need to test from the device you are utilizing. I didn’t see a way to port scan an exterior IP even from within a trusted network. I can see ShieldsUp being extremely useful for verification of port status after doing adjustments and configurations on host devices. It gives peace of mind and validation of the intended configurations.

Nessus

I learned most businesses and organizations are untrusting about vulnerability testing unless you are their employee or member! To protect possible exposure of vulnerabilities, the Army adamantly told me no. No, you cannot do a vulnerability scan. The network security is not your concern. I had several other businesses give me the wary look and wondering my angle gaze. Ultimately, I probed my home network.

Nessus is a tool that checks for known vulnerabilities and offers the solutions of those exposed, but it is still up to the user/network administrator to complete the fix. Depending on the severity of potential attack surface, risk acceptance will play a key role in choosing where to spend resources. This feeds into why the students of this class need to understand how to report vulnerabilities, the way ahead, and recommended priorities of effort in a clear, concise, and vernacular way. A report doesn’t help anything if no recommendations are included or the “IT speak” is so dense a translator is required. With that said, meekness doesn’t win either. If there is a problem that requires immediate action, ensure you pull up a seat at the decision maker’s table and relay the capabilities and limitations.

I was surprised that my printer was recognized and skipped. Printers react poorly when scanned by Nessus, so the software marks the device as dead and doesn’t scan it. This could create an opening of attack surface with nefarious actors knowing this avoidance. If I were a black hat probing a network and recognized a printer’s IP, it seems a likely target knowing Nessus won’t scan it.

Business/Organization networks will quickly scale upward in complexity, number of devices, and business requirements like open ports and services. The Nessus Network Scan won’t come back as simple and clean as my home network did, largely in part to my IPS firewall. I can see the need for consistent vulnerability scan monitoring to ensure patches are installed in a timely manner and more severe remediations if required. I visualize the Severity x Likelihood quadrant graph with risk being measured. Low severity & low likelihood = low risk. High severity & low likelihood / low severity & high likelihood = medium risk. High severity & high likelihood = high risk.

I can see Nessus as being an extremely helpful tool for small and large organizations. With the indefinite amount of trial versions that can be used, small organizations with 16 IPs or less can use Nessus to great effect. Large organizations will be able to afford the $5000 annual membership fee with Tenable to utilize the software, and I believe this to be a bargain given the alternative high dollar ransomware. It seems like the medium sized organizations are left flapping in the wind though. Too many devices to make the trial versions applicable and too small to afford the membership fee; the Goldie Locks zone is left out with this tool.

1. ShieldsUp!! Port Authority Edition – Internet Vulnerability Profiling

https://www.grc.com/x/ne.dll?rh1dkyd2

1. What is the Nessus Scanner? Working and Key Features

https://www.spiceworks.com/it-security/data-security/articles/what-is-nessus-scanner/

1. CVSS Scores vs. VPR

https://docs.tenable.com/nessus/Content/RiskMetrics.htm

1. The 2021 TLS Telemetry Report

https://www.f5.com/labs/articles/threat-intelligence/the-2021-tls-telemetry-report

1. IP/Domain Lookup

https://www.ntunhs.net/cgi-bin/whois20\_1\_allip3.cgi?HPLang=EN&LV=3&IP=173.218.9.0