Megan Moore
Buff ID: 1014735

Research Report 3 – Shields Up and Nessus

Question 1: What did you do?

For this assignment, I again was unable to perform any testing on my organization's networks due to security constraints. Thus, I scanned my personal system for vulnerabilities in a variety of ways. The first part using Shields Up is to see how well my system is protected with its existing firewall. Shields Up was developed by Gibson Research Corporation (GRC) and it is designed to asses the security of a network (home, organization, etc.) by identifying potential vulneraries which could be exploited by attackers.

Shields Up works by performing port scanning and stealth testing to determine paths an attack could use to exploit a system, either through open ports and system responses to packets. While performing these scans, the tool attempts to identify the services running through the open ports and analyzing the responses received from the target system. It then compares the findings against known vulnerabilities and security flaws. The final result is a handy report listing all the details for the findings along with recommendations on how to address each item.

The number of methods hackers can use to gain entry into your own personal system are much greater than I ever expected. Working from home has been a wonderful blessing since the start of the pandemic but I can see how a company would have high concerns of how they could best protect their IP or system data. Now more than ever, cybersecurity is of front and center importance for both personal and business-related assets.

The second part of this research report involves using Nessus to perform a vulnerability scan. This tool also aids in helping to identify security weaknesses in systems, networks and even applications. The tool can also be used by organizations to assess the security posture of their infrastructure before attackers find weak points to exploit. A high-level explanation of how the tool works is the user configures Nessus with the proper parameters (target system or network, type of scan, requirements and any exclusions) leading to discovery and creation of a system and service inventory. After all the systems are identified a comprehensive vulnerability assessment occurs. Nessus has a vast database of types of security checks to compare any detected configurations against known security flaws. One note about the tool is it does not perform any actual attacks or cause damage to the targeted system. When using Nessus, I selected a few scan templates to try and these templates simplify the process by determine which setting are configurable and how they can be set up. For getting started and each scan thereafter, I selected my specific IPv4 and IPv6 as the Targets.

Question 2: What were the results?

First of the results were the two GRC Shields Up vulnerability scans done on my personal laptop and a Browser scan. These are seen below with Common Ports followed by All Service Ports displayed first.

<u>Common Ports</u>

Post scanning involves the tool sending network packets to each port on your system in order to determine which ports are open, closed or filtered. Open ports are the high focus as those are potential entry points for attackers. A closed port however is generally considered secure. If your system is unprotected, without any personal firewall or NAT router, any ports showing as stealth are being blocked

somewhere between your computer and the public Internet. This is probably being done by your ISP. Internet traffic directed to your computer at the stealth ports will be dropped before reaching your machine.

In good news, no ports were found open or closed on either scan. All received the Stealth label. This was good to see as a stealth port is one that basically ignores and drop any incoming packets of information without responding to the sender the actual open or closed status of the port. Seeing as all my system ports are stealth, my system should be invisible to the random scans I might encounter over the internet.

```
---------------------------------------------------------------------

GRC Port Authority Report created on UTC: 2023-08-02 at 02:15:30

Results from scan of ports: 0, 21-23, 25, 79, 80, 110, 113,
                            119, 135, 139, 143, 389, 443, 445,
                            1002, 1024-1030, 1720, 5000

    0 Ports Open
    0 Ports Closed
   26 Ports Stealth
----------------------
   26 Ports Tested

ALL PORTS tested were found to be: STEALTH.

TruStealth: FAILED - ALL tested ports were STEALTH,
                   - NO unsolicited packets were received,
                   - A PING REPLY (ICMP Echo) WAS RECEIVED.

---------------------------------------------------------------------
```

All Service Ports

My system did however fail the TruStealth portion on each scan. This is due to the system replying via a ping which would make it visible. While not severe, a corrective action that would be best is to update my system firewall so it was configured to block, drop or ignore the ping requests so it could better hide from being hacked. Most personal firewalls can be configured to block, drop, and ignore such ping requests in order to better hide systems from hackers. This is highly recommended since "Ping" is among the oldest and most common methods used to locate systems prior to further exploitation.

Megan Moore
Buff ID: 1014735

Research Report 3 – Shields Up and Nessus

```
--------------------------------------------------------------------------

GRC Port Authority Report created on UTC: 2023-08-02 at 02:19:46

Results from scan of ports: 0-1055

    0 Ports Open
    0 Ports Closed
 1056 Ports Stealth
----------------------
 1056 Ports Tested

ALL PORTS tested were found to be: STEALTH.

TruStealth: FAILED - ALL tested ports were STEALTH,
                   - NO unsolicited packets were received,
                   - A PING REPLY (ICMP Echo) WAS RECEIVED.

--------------------------------------------------------------------------
```

Solicited TCP Packets: **PASSED** — No TCP packets were received from your system as a direct result of our attempts to elicit some response from any of the ports listed below — they are all either fully stealthed or blocked by your ISP. However . . .

Unsolicited Packets: **PASSED** — No Internet packets of any sort were received from your system as a side-effect of our attempts to elicit some response from any of the ports listed above. Some questionable personal security systems expose their users by attempting to "counter-probe the prober", thus revealing themselves. But your system remained wisely silent. (Except for the fact that not all of its ports are completely stealthed as shown below.)

Ping Reply: **RECEIVED (FAILED)** — Your system REPLIED to our Ping (ICMP Echo) requests, making it visible on the Internet. Most personal firewalls can be configured to block, drop, and ignore such ping requests in order to better hide systems from hackers. This is highly recommended since "Ping" is among the oldest and most common methods used to locate systems prior to further exploitation.

Browser Headers

Another scan offered by Shields Up is a browser header scan. This scan uses the web browser to send a request to a remote server and determine if it may contain information about the user and the computer system running the browser. It is important to note that the user's web browser can send any sort of information at will and the typical web surfer usually has no idea this is occurring. The Information which is shared could range from things like cookies, the URL of the web page which referred the browser to the remote server potentially causing concern for tracking, the version of the browser itself and even the

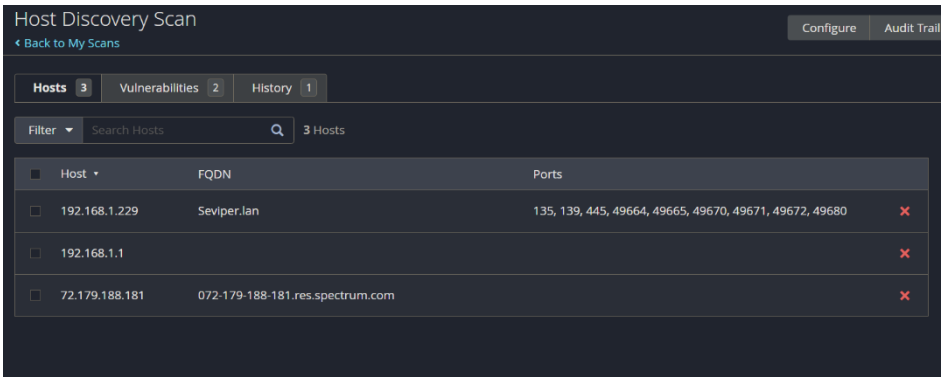
format of information. As security concerns increase and privacy continually seems to be rapidly declining, knowing what your browser is disclosing is an important vulnerability to be aware of. Reading the output of the scan, I found the detail extraordinary as I never knew this much was transmitted previously. My browser and system details were present along with what cookies types were accepted, my operating platform (Windows), and if my device was mobile or not. Knowing this data is transmitted is key to understanding my attack surface and how an attack could be planned.

```
Cache-Control: max-age=0
Connection: keep-alive
Content-Length: 32
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Language: en-US,en;q=0.9
Cookie: tpag=efq2mvpw1ne5r; ppag=efq2mvpw1ne5r; tcss=fij0vj54pipvs; pcss=fij0vj54pipvs; tico=4axyu3343fdf5; pico=4axyu3343fdf5
Host: www.grc.com
Referer: https://www.grc.com/x/ne.dll?rh1dkyd2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
sec-ch-ua: "Not/A)Brand";v="99", "Google Chrome";v="115", "Chromium";v="115"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://www.grc.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
FirstParty: https://www.grc.com
ThirdParty: https://www.grctech.com
Secure: https://www.grc.com
Nonsecure: http://www.grc.com
Session: vggjxnfssovih
```

Now shifting to Nessus, first a host discovery scan was performed. Knowing what hosts are on your network is the first step to any vulnerability assessment. This scan details out information such as the type of scanner (Nessus or Nessus Home), version of the Nessus Engine, port scanner(s) used, port range scanned, ping round trip time, credentialed or third-party patch management checks, enablement of superseded patches, date and duration of scan, number of hosts and number of checks done in parallel.

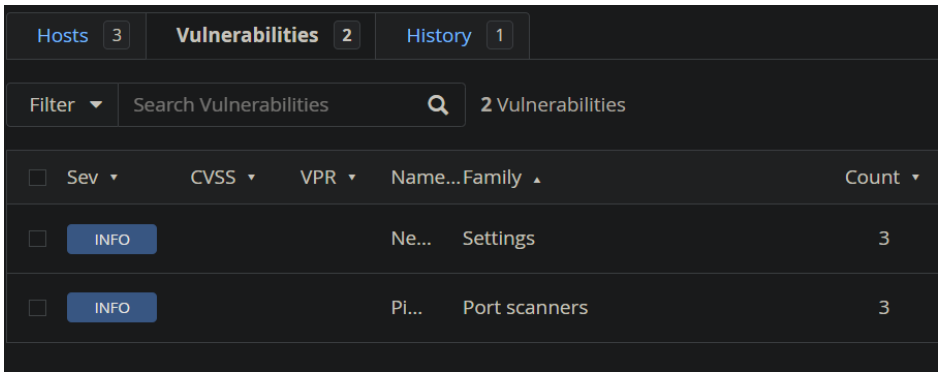
Host Discovery Scan

Results returned showed 3 Hosts, 2 Vulnerabilities and History of 1. Vulnerabilities were divided by Nessus Scan Information and Pinging of the Remote Host. The first type showed the results mentioned previously for each Target. A good thing to learn is that using vulnerability scan templates is best for most of your home or organization's standard, day-to-day scanning needs.



Megan Moore
Buff ID: 1014735

Research Report 3 – Shields Up and Nessus



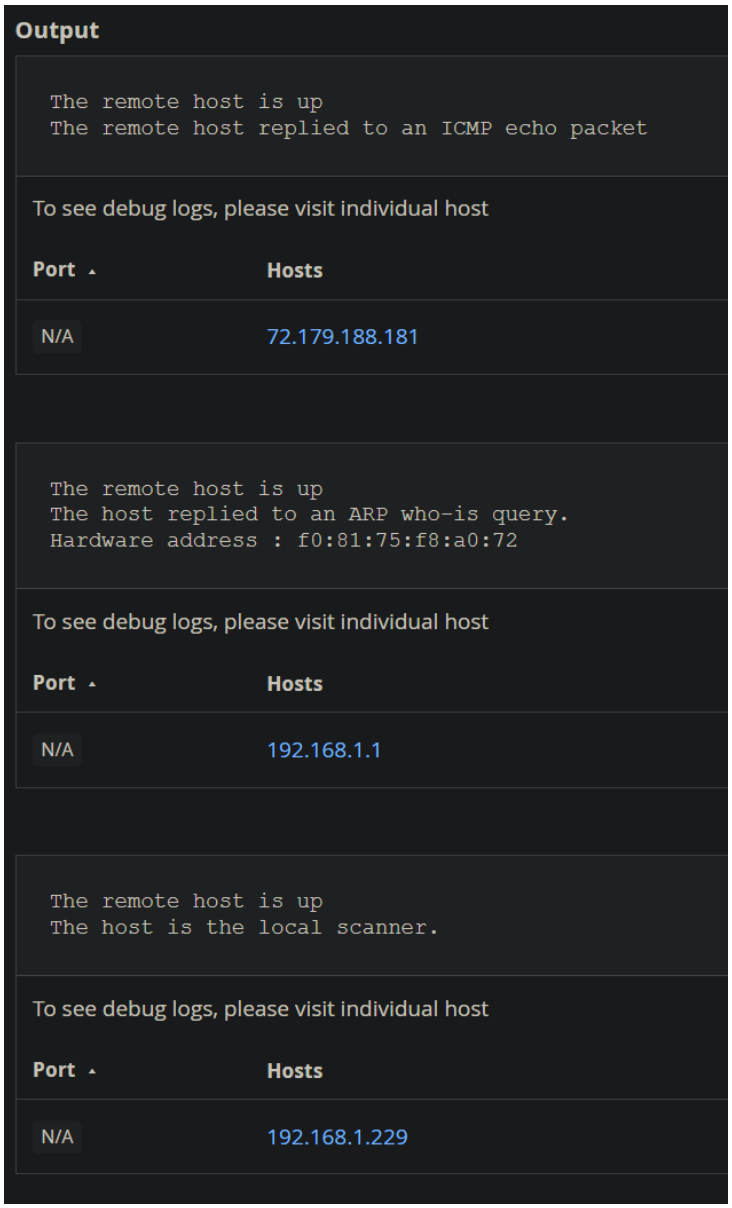
First an example of the Scan Information for one of my Targets. I didn't feel too alarmed by this.

```
Information about this scan :

Nessus version : 10.5.4
Nessus build : 20013
Plugin feed version : 202308030804
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : Host Discovery Scan
Scan policy used : Host Discovery
Scanner IP : 192.168.1.229

WARNING : No port scanner was enabled during the scan. This may
lead to incomplete results.

Port range : default
Ping RTT : 43.145 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 256
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/8/3 9:43 Central Standard Time
Scan duration : 37 sec
Scan for malware : no
```

Next was the ping results. Each of my targets replied which was not surprising as this also happened with Shields Up. Again not a severe attack point, but a corrective action that would be best is to update my system firewall so it was configured to block, drop or ignore the ping requests so it could better hide from being hacked on a network.

Megan Moore
Buff ID: 1014735

Research Report 3 – Shields Up and Nessus

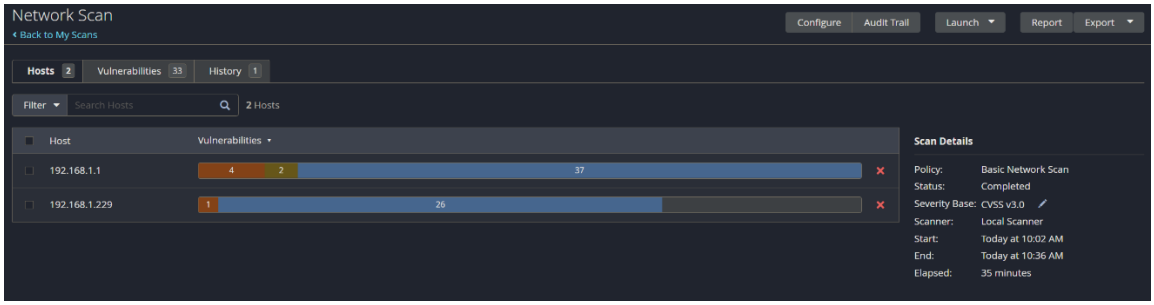


Network Scan

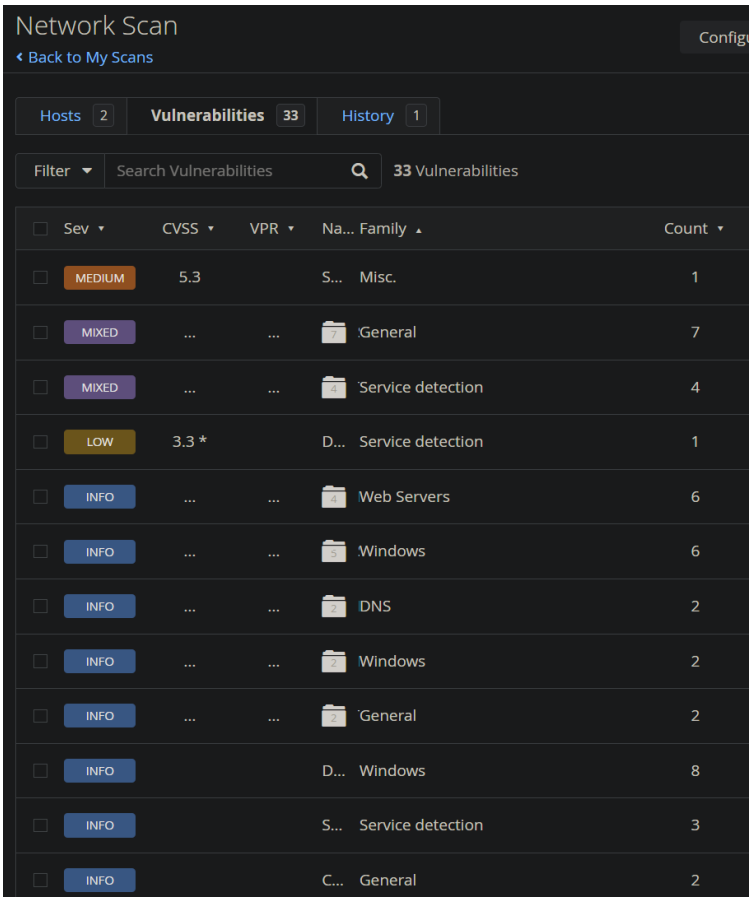
Next, I completed a Network Scan on my same Targets. This scan performs a full system scan that is suitable for any host. People can use the basic template to scan an asset or assets with all of Nessus's plugins enabled. For example, you can perform an internal vulnerability scan on your organization's systems as well as your own.

Megan Moore
Buff ID: 1014735

Research Report 3 – Shields Up and Nessus



Reviewing the vulnerabilities gave me more ease regarding my potential for a cyber-attack. From an identified total of 33, only 1 Medium item followed by 1 Low, a few Mixed and the remaining all Info. The Medium item turned out to be “SMB Signing not required”. Nessus informed me the issue with this is an unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. What I found remarkable is Nessus actually proposed a solution. For this case, I would need to enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. Had I never ran this scan, I never would have known.



Megan Moore
Buff ID: 1014735

Research Report 3 – Shields Up and Nessus

I wanted to perform an Attack Surface Discovery scan but regrettably this scan is only available in the Expert version of the Nessus program This particular scan uses Bit Discovery to scan a list of high-level domains and extract subdomains and DNS-related data. The detail gained from that would be far greater so perhaps this is something I could consider at a later point in time.

Question 3: What did you learn?

I personally did not realize these types of websites existed to check my exposure. Now that I know what this does, I will probably routinely cheek in on that far more frequently. I discovered my system successfully has no open ports, thus been better protected than I assumed the scan would show. I would be curious if installing some kind of antivirus software would aid in further protecting my system going forward. I have only ever used what came with my system (Windows firewall) and never any additional program. Regardless of my results from the vulnerability scans, the free version of the scans is not reflective of a full system scan but only a subset. In the future, it could be worthwhile to expand into using the paid version.

Shields Up is just one tool among many available for network vulnerability scanning. This assignment helped me see how it can provide valuable insights into the security of my own network. For an organization, it could be used as part of a comprehensive security strategy which could also include patch management, secure configurations and of course, regular security audits. Nessus followed the same path as it automates many manual tasks for vulnerability scans that allows users and security professionals alike to take proactive measures to strengthen their security defenses.

As I have become more aware of how much of my own information is distributed online, I have been more cautious in what I do when connected to the internet. In the past, I did not value my information as an asset any hacker would like to steal. I assumed such things were reserved for corporations or public figures. Now these days, I realize the protection of my information is key just from dealing with a credit card being stolen from a Target data breach. Hackers don't care how big a fish is sometimes. They just want a fish they can use. Full identity theft or information extortion is not something I wish to ever experience.

Overall, I know my own personal risk can be reduced through education. As I learn more techniques I can adapt or apply for my system, the higher I raise my security against threats. Social engineering use is becoming more widespread and trickier along with phishing attacks sent in email. I know my work email is constantly tested by our IT admins along with various test phishing campaigns. While the goal is to pass these tests when work rolls them out, the real point is to make us familiar to the types of risk being connected to the internet poses and how to best protect yourself.

Finally, the time I spent researching the vulnerability scan tools for this report helped me understand the actions needed for a heightened posture when it comes to cybersecurity and protecting my own most critical assets. The same would apply to any organization.

- Reduce the likelihood of a damaging cyber intrusion through prioritizing software updates, validating access to networks and systems, disable any port or protocol not in use and for a company, ensure the IT teams have implemented strong controls.

Megan Moore
Buff ID: 1014735

Research Report 3 – Shields Up and Nessus

- If a potential attack occurs, have a plan in pace to quickly detect and respond to the situation.
- Work to increase and maximize one's home resilience or that of their organization to any kind of destructive incident through testing backup procedures and manual controls to ensure critical functions stay operational.