Megan Moore
Buff ID: 1014735

Research Report 4 - Ransomware Recovery

Question 1: What did you do?

Ransomware attacks are a significant and growing threat in our current digital landscape. Individuals and organizations alike must be proactive in preparation for such attacks to minimize the potential damage and ensure a smoother recovery process.

For this assignment, we were to identify decencies and vulnerabilities in our systems and networks and determine a backup and recovery list for the most critical items and assets. Additionally, we were to review our system and determine what devices or components would need updates while also reviewing how roles or passwords used need backups as well. Assets which are part of a system come in many forms from processes to physical hardware to digital data. Each asset should reflect both a sensitivity as well as security priority. Overall, the assignment is to determine one's one attack surface and the risk it introduces. Managing risk is an important process of first assessing the risks to yourself or the operations of an organization you are associated with and then systematically determining how best to control or mitigate the risks you identify. Not all risk can be mitigated so part of the assessment is also figuring out how best to lower the risk of a particular threat or at the least, bring the risk of the threat to an acceptable level.

As I completed my NMAP scans in Assignment 1, I read more of the support readings and NMAP reference information online to gather a better understanding for what each scan sought to achieve and how the information gathered would help build a strategy towards reducing my attack surface and plan a proactive approach towards network security. My background is not in IT so I found the results and knowledge gained to be very enlightening. Separately I also found reaching out to IT security colleagues in my organization to be even more rewarding as they shared real world examples of situations and remedies put in place to protect users.

The course provided reference of Dzimiela and Jennex (2023) is a case study on the recovery of a small municipality from a ransomware attack and the steps taken. Best practices for preparing for a recovery from a ransomware attack were covered and included backups, software updating, passwords, asset inventories, and response procedures. The first and most obvious preparation step is to backup your data. A regularly backed up system or important data is best practice. Ideally the backup would be an offline or cloud-based solution. Having multiple copies will safeguard against a ransomware encryption or deletion. Second, robust security measures, either for home or an organization, should be implemented. A multilayered approach is recommended along with updated anti-malware software. This should involve regular patches and updates to all software and operating systems to address vulnerabilities. Training is next and key to raise awareness and encourage best practice behavior for yourself or that of colleagues in a firm. Finally, routine testing of your defenses is helpful so weak points can be addressed immediately. This aids to build a proper incident response plan should an attack occur.

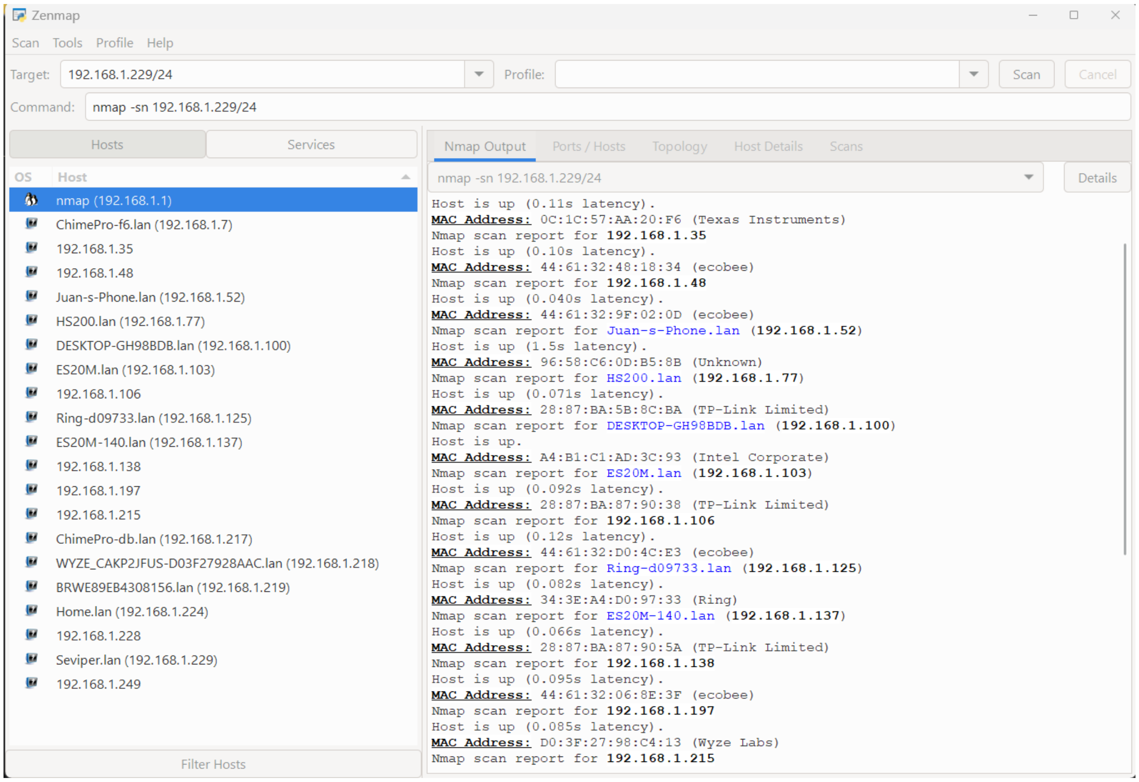
Megan Moore
Buff ID: 1014735

Research Report 4 - Ransomware Recovery

Question 2: What were the results?

When prioritizing a list of network devices which could be impacted by a ransomware attack, it is important to consider the criticality of the device, potential impact on the connecting network and the value of the data or services the device and network provide.

Used in the first assignment, Nmap provides a comprehensive view of network infrastructure, helping users understand the relationships between hosts, subnets, and routers. Nmap can be utilized to diagnose network connectivity problems, identify network bottlenecks, and troubleshoot network issues by examining the reachability and responsiveness of hosts and services. Through using Nmap, users can gain valuable insights and information about network infrastructure and security. Understanding what items could be impacted by a security attack, also referred to as your attack surface, is crucial.



Target: 192.168.1.229/24

Command: nmap -sn 192.168.1.229/24

```
nmap (192.168.1.1)
ChimePro-f6.lan (192.168.1.7)
192.168.1.35
192.168.1.48
Juan-s-Phone.lan (192.168.1.52)
HS200.lan (192.168.1.77)
DESKTOP-GH98BDB.lan (192.168.1.100)
ES20M.lan (192.168.1.103)
192.168.1.106
Ring-d09733.lan (192.168.1.125)
ES20M-140.lan (192.168.1.137)
192.168.1.138
192.168.1.197
192.168.1.215
ChimePro-db.lan (192.168.1.217)
WYZE_CAKP2JFUS-D03F27928AAC.lan (192.168.1.218)
BRWE89EB4308156.lan (192.168.1.219)
Home.lan (192.168.1.224)
192.168.1.228
Seviper.lan (192.168.1.229)
192.168.1.249
```

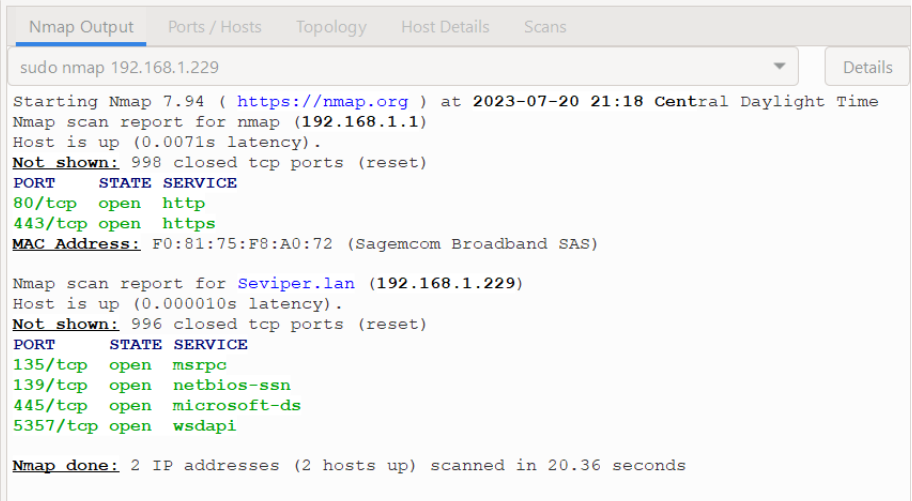
```
nmap -sn 192.168.1.229/24
Host is up (0.11s latency).
MAC Address: 0C:1C:57:AA:20:F6 (Texas Instruments)
Nmap scan report for 192.168.1.35
Host is up (0.10s latency).
MAC Address: 44:61:32:48:18:34 (ecobee)
Nmap scan report for 192.168.1.48
Host is up (0.040s latency).
MAC Address: 44:61:32:9F:02:0D (ecobee)
Nmap scan report for Juan-s-Phone.lan (192.168.1.52)
Host is up (1.5s latency).
MAC Address: 96:58:C6:0D:B5:8B (Unknown)
Nmap scan report for HS200.lan (192.168.1.77)
Host is up (0.071s latency).
MAC Address: 28:87:BA:5B:8C:BA (TP-Link Limited)
Nmap scan report for DESKTOP-GH98BDB.lan (192.168.1.100)
Host is up.
MAC Address: A4:B1:C1:AD:3C:93 (Intel Corporate)
Nmap scan report for ES20M.lan (192.168.1.103)
Host is up (0.092s latency).
MAC Address: 28:87:BA:87:90:38 (TP-Link Limited)
Nmap scan report for 192.168.1.106
Host is up (0.12s latency).
MAC Address: 44:61:32:D0:4C:E3 (ecobee)
Nmap scan report for Ring-d09733.lan (192.168.1.125)
Host is up (0.082s latency).
MAC Address: 34:3E:A4:D0:97:33 (Ring)
Nmap scan report for ES20M-140.lan (192.168.1.137)
Host is up (0.066s latency).
MAC Address: 28:87:BA:87:90:5A (TP-Link Limited)
Nmap scan report for 192.168.1.138
Host is up (0.095s latency).
MAC Address: 44:61:32:06:8E:3F (ecobee)
Nmap scan report for 192.168.1.197
Host is up (0.085s latency).
MAC Address: D0:3F:27:98:C4:13 (Wyze Labs)
Nmap scan report for 192.168.1.215
```

NMAP gave me a roadmap of my network devices and connections. Once I really saw the list of what assets were touched and when, this helped me to frame better methods to address threats. The very first step which I had already taken was a locked network. Keeping my personal network closed from being open to access by all protects all of my information assets. For most of my important annual routines that handle information assets like tax returns, I changed from a software only asset to having backups – physical data backups stored on USB drives as well as cloud-based network backups of key files.

Megan Moore
Buff ID: 1014735

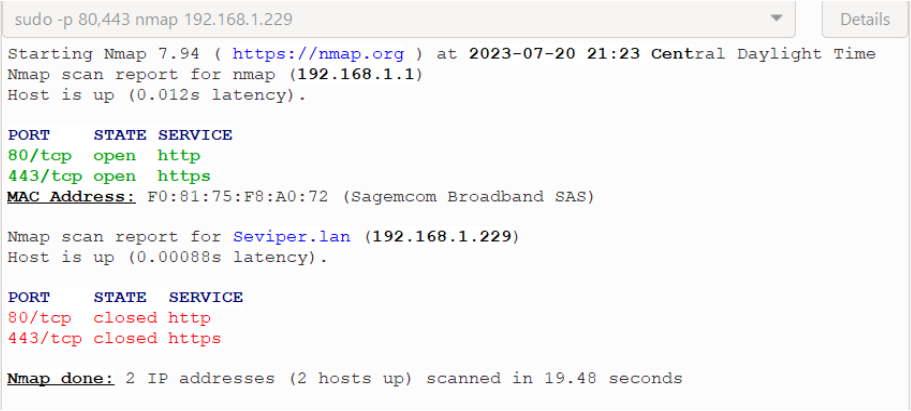
Research Report 4 - Ransomware Recovery

Below are the results of the Port tests performed in NMAP.



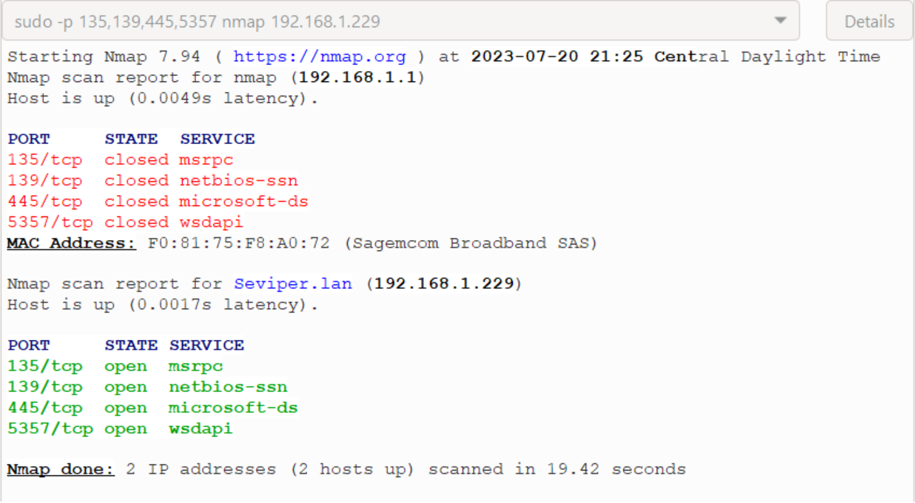
```
sudo nmap 192.168.1.229
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 21:18 Central Daylight Time
Nmap scan report for nmap (192.168.1.1)
Host is up (0.0071s latency).
Not shown: 998 closed tcp ports (reset)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)

Nmap scan report for Seviper.lan (192.168.1.229)
Host is up (0.000010s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 2 IP addresses (2 hosts up) scanned in 20.36 seconds
```



```
sudo -p 80,443 nmap 192.168.1.229
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 21:23 Central Daylight Time
Nmap scan report for nmap (192.168.1.1)
Host is up (0.012s latency).

PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)

Nmap scan report for Seviper.lan (192.168.1.229)
Host is up (0.00088s latency).

PORT    STATE  SERVICE
80/tcp  closed http
443/tcp closed https

Nmap done: 2 IP addresses (2 hosts up) scanned in 19.48 seconds
```



```
sudo -p 135,139,445,5357 nmap 192.168.1.229
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-20 21:25 Central Daylight Time
Nmap scan report for nmap (192.168.1.1)
Host is up (0.0049s latency).

PORT     STATE  SERVICE
135/tcp  closed msrpc
139/tcp  closed netbios-ssn
445/tcp  closed microsoft-ds
5357/tcp closed wsdapi
MAC Address: F0:81:75:F8:A0:72 (Sagemcom Broadband SAS)

Nmap scan report for Seviper.lan (192.168.1.229)
Host is up (0.0017s latency).

PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 2 IP addresses (2 hosts up) scanned in 19.42 seconds
```

Megan Moore
Buff ID: 1014735

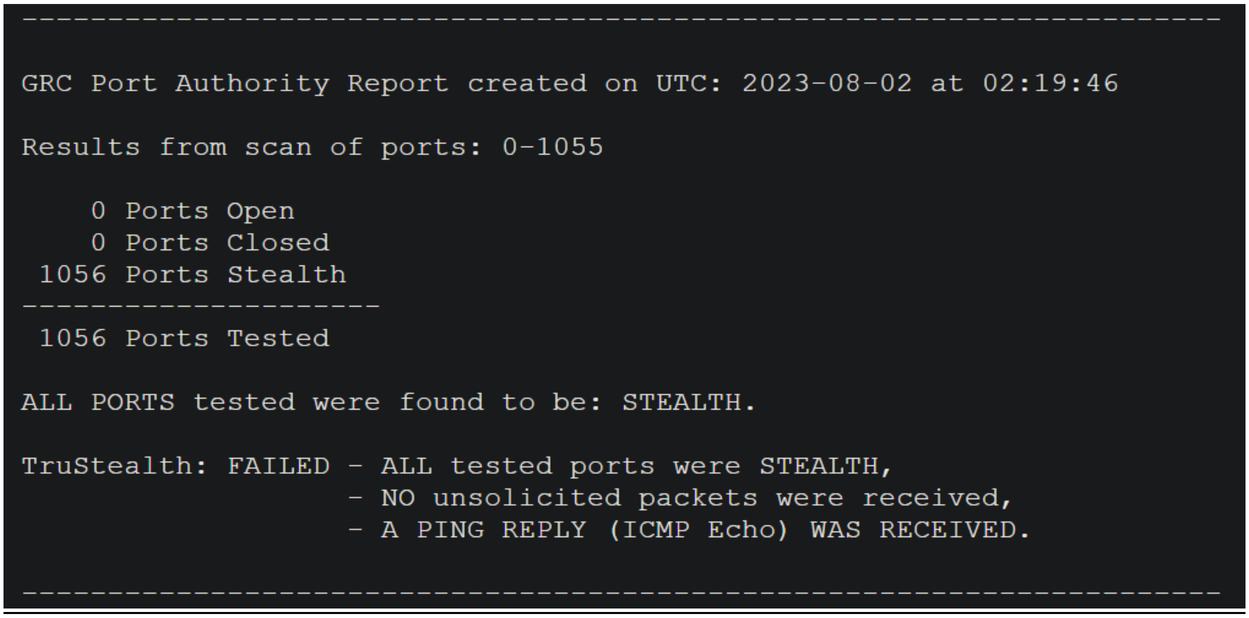
Research Report 4 - Ransomware Recovery

Reflecting over the course readings and internet review, there is a standardized approach for determining the order in which devices should be backed up and recovered. First, any kind of Domain Controllers is top priority followed by servers. I have no servers in my device list to backup so I can skip this particular critical backup. If I did, I would ensure a backup was readily done and able to be performed in the event of an attack.

Next in prioritization would be Network infrastructure devices like routers, switches, firewalls, etc. which form the backbone of a network. For my personal network that would involve the third party supplied router and built in firewall in that device. I do not have much influence over these devices but an organization would. These would be vital to have backups and ability to be restored.

Third would be endpoint devices like my laptop, cell phones, tablets, etc. as these are all common targets in a ransomware attack. These types of devices typically can have multiple entry points for attackers to gain access to a network. I own many devices like this throughout my home, and when one considers an organization and the levels of devices which easily span into thousands for large corporations, this is quite a lengthy undertaking. For my laptop, the Shields Up exercise taught me to check all my ports and ensure they were either closed or Stealth. I confirmed all open ports were closed or set as stealth. The final piece which still needs to be updated on my end is to remedy the fact my system fails the ping test. I see myself addressing this in the near future through utilizing an additional firewall or anti-malware type of program.

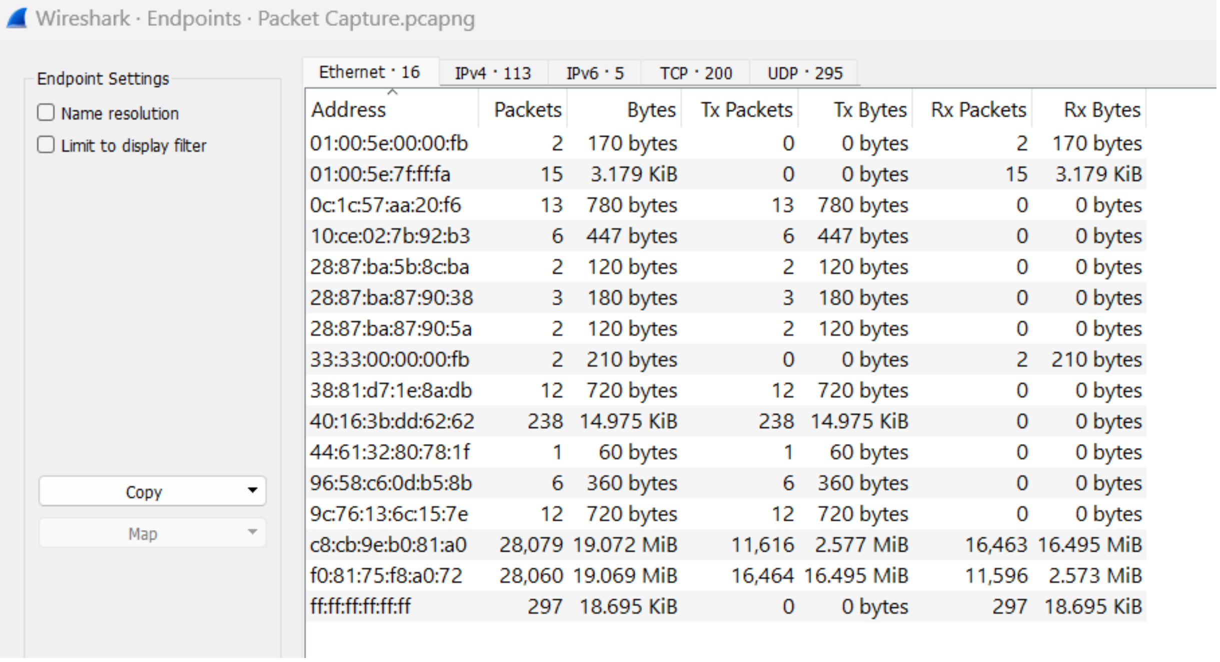
Shields Up output seen below.



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

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.

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

Another way to search for weak points is reviewing your network Endpoints.

Endpoints results from Wireshark in Assignment 2 shown below.



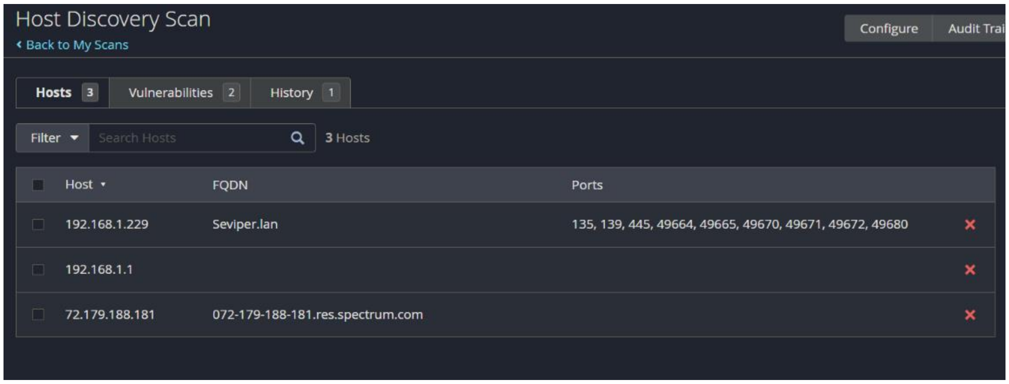
Wireshark · Endpoints · Packet Capture.pcapng

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
01:00:5e:00:00:fb	2	170 bytes	0	0 bytes	2	170 bytes
01:00:5e:7f:ff:fa	15	3.179 KiB	0	0 bytes	15	3.179 KiB
0c:1c:57:aa:20:f6	13	780 bytes	13	780 bytes	0	0 bytes
10:ce:02:7b:92:b3	6	447 bytes	6	447 bytes	0	0 bytes
28:87:ba:5b:8c:ba	2	120 bytes	2	120 bytes	0	0 bytes
28:87:ba:87:90:38	3	180 bytes	3	180 bytes	0	0 bytes
28:87:ba:87:90:5a	2	120 bytes	2	120 bytes	0	0 bytes
33:33:00:00:00:fb	2	210 bytes	0	0 bytes	2	210 bytes
38:81:d7:1e:8a:db	12	720 bytes	12	720 bytes	0	0 bytes
40:16:3b:dd:62:62	238	14.975 KiB	238	14.975 KiB	0	0 bytes
44:61:32:80:78:1f	1	60 bytes	1	60 bytes	0	0 bytes
96:58:c6:0d:b5:8b	6	360 bytes	6	360 bytes	0	0 bytes
9c:76:13:6c:15:7e	12	720 bytes	12	720 bytes	0	0 bytes
c8:cb:9e:b0:81:a0	28,079	19.072 MiB	11,616	2.577 MiB	16,463	16.495 MiB
f0:81:75:f8:a0:72	28,060	19.069 MiB	16,464	16.495 MiB	11,596	2.573 MiB
ff:ff:ff:ff:ff:ff	297	18.695 KiB	0	0 bytes	297	18.695 KiB

List 4 Use assignment 2 – identify components/devices to be updated (vulnerabilities)

When searching for vulnerabilities in my network, I performed a Host Discovery Scan as well as a Network Scan using Shields Up.

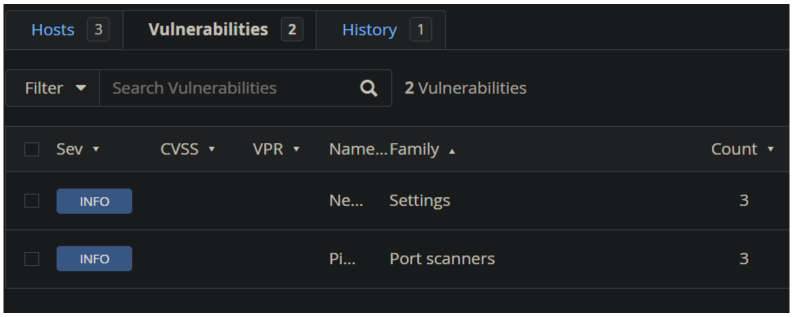
Host Discovery results shown below.



Host Discovery Scan

3 Hosts

Host	FQDN	Ports
192.168.1.229	Seviper.lan	135, 139, 445, 49664, 49665, 49670, 49671, 49672, 49680
192.168.1.1		
72.179.188.181	072-179-188-181.res.spectrum.com	



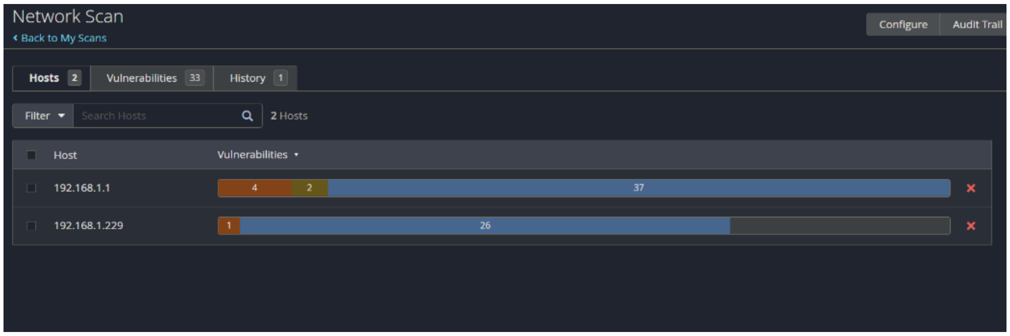
2 Vulnerabilities

Sev	CVSS	VPR	Name...	Family	Count
INFO			Ne...	Settings	3
INFO			Pi...	Port scanners	3

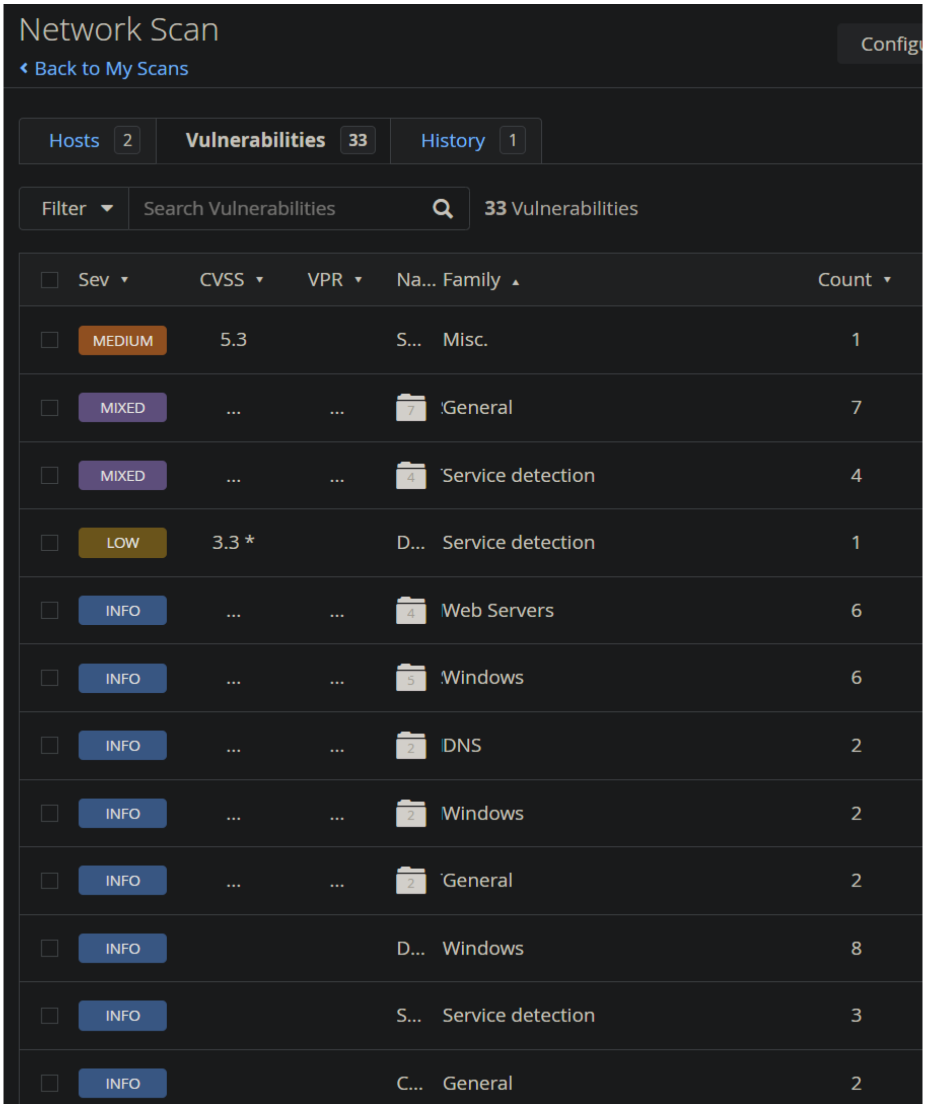
Megan Moore
Buff ID: 1014735

Research Report 4 - Ransomware Recovery

Network Scan and Vulnerability list shown below.



Host	Vulnerabilities
192.168.1.1	4 2 37
192.168.1.229	1 26



Sev	CVSS	VPR	Na...	Family	Count
MEDIUM	5.3		S...	Misc.	1
MIXED	...	...	7	General	7
MIXED	...	...	4	Service detection	4
LOW	3.3 *		D...	Service detection	1
INFO	...	...	4	Web Servers	6
INFO	...	...	5	Windows	6
INFO	...	...	2	DNS	2
INFO	...	...	2	Windows	2
INFO	...	...	2	General	2
INFO			D...	Windows	8
INFO			S...	Service detection	3
INFO			C...	General	2

Finally, part of this research assignment was to identify passwords and roles which need backups. Considering my current attack surface which is mainly across devices, best practice would be to routinely keep the software updates current followed by updating the password used to login to these items. I find myself not being the most thoughtful of cybersecurity at times as I typically work from home and am always engaged in work using my devices. I hardly ever change a login user role or password once setup the first time. Best practice would to ensure to delete old roles or permissions granted to other individuals and to also change my password to be more difficult. The frequency emails are hacked is significant, not to mention the data breaches you hear about through the news.

This assignment confirmed my thought that somehow, it was possible for someone to gain access to a network and easily crack and obtain the credentials not just of one user but many. This would be an IT department's greatest fear for multiple users on a network. Using a feature called shadowing, I watched a YouTube demonstration of how an entire list of users on a network was accessed, cracked and then each user and password was saved. This would allow the hacker to return with the proper credentials and then cause much more targeted harm.

My asset inventory list feels like it could use multiple review passes to fully flush out every piece of data needing protection in my home and network however I feel far more confident in recognizing how wide spread my information assets reach and how this assignment can help me to see their value and priority and then create the appropriate controls to minimize the risk.

I can dream about creating a hacker free zone for my information assets but with how much I access cloud or network type things and how those things touch my other assets, I would just laugh at this possibility. These days, networking connects us all and is what allows us to each create multiple online accounts as well as be an active participant in social media.

<u>Question 3: What did you learn?</u>

While performing this assignment, I became aware at just how large my attack surface truly is. Until performing the steps of taking a true inventory, many information assets feel so common that one may not question or implement a best practice way to protect it. Every time I feel I have a comfortable hand on my information security, exercises like this one wake me up to the real level of threat all of my assets really face. I would say I have far more risk than I first judged for my myself. There are many different ways someone could exploit my information assets if they cracked the security on an item which touches multiple systems and routines. By understanding the attack surface, home network owners and organizations alike can enhance their security posture by taking precautions and implementing measures such as regular software updates, robust access controls, network segmentation, intrusion detection systems, firewalls and overall security awareness training. Gaining insight where a system can be vulnerable is essential in order to take the proper precautions to protect it.

Recovering from a ransomware attack is painful and require a thorough process. This week's readings and research gave me insight into the steps needed to recover. Recovery begins by isolating the infected system by disconnecting it from the network to prevent further spread. At this point, you can assess the situation by examining the impact of the attack in encrypted or compromised data. In order to understand the recovery requirements, one must first the extent of the damage. If at an organization, the incident is critical in being reported so the appropriate regulatory process can begin as it is imperative all information necessary is gathered in order to aid apprehending the attackers. The same cane be said from home but the attack surface of a corporation is far larger and more extensive so the impact is far, far greater. At this point, experts can be engaged if specialization in recovery is needed and then the restoring process from backups begin. Backups should be reviewed intensely to ensure they are free of malware before beginning the restoration process. A person or organization can then learn from the attack to review vulnerabilities which led to the attack occurring and what else might be a weak point for another attack. Security measures can then be updated from this knowledge and range from enhanced access controls, network segmentation, etc. along with a more robust backup strategy. This course and assignment thoroughly taught me that prevention is always better than recovery when it comes to attacks. By implementing a proactive security measure, participating in training and maintaining monitoring of the system the overall risk and impact from ransomware attacks is greatly reduced.

I felt this assignment was very enlightening in visualizing my own overall risk. Risk identification, which I began in the inventory piece, is crucial to being prepared, not just for personal reasons but also for the role we each play in organizations and society. In my current role as a project manager, I'm constantly reminded of the responsibility of identifying and managing risk through the life of a project. Tools like an information asset inventory are wonderful aids in that endeavor. To manage personal risk, we need to know ourselves. Knowing ourselves involves understanding how information can be collected, stored or transmitted. It also requires the ability to identify information assets which are valuable to our personal selves, classifying each of those assets and then determining how each is protected from threats. Overall, I would say my risk is moderate based on my behaviors and current controls in place. I would like to spend time reviewing how I can place additional controls to safeguard my information assets more. Some risk I am willing to accept, in the example of using a smart phone as the high usage and necessity of being connected is very important and frankly nonnegotiable.

One other thing I learned is while it may not be necessary to change passwords as often as I do, chances are passwords become exposed over time in data breaches. The best way to improve my chances of remaining protected is a complex password perhaps generated by a password manager. The stronger and more unique a password is, the less likely it will be guessed. I may need to revisit all of my logins and update those to be more complex. I don't believe I can ever reduce my risk in using my email address as it is needed in so many places. I expect it to always have some level of exposure. 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.