**Ransomware Recovery**

Miguel Sanchez

West Texas A&M University

CIDM-6340-70, NTWK MGT & INFO SEC

Summer 2 2023

Professor Murray E. Jennex

August 10, 2023

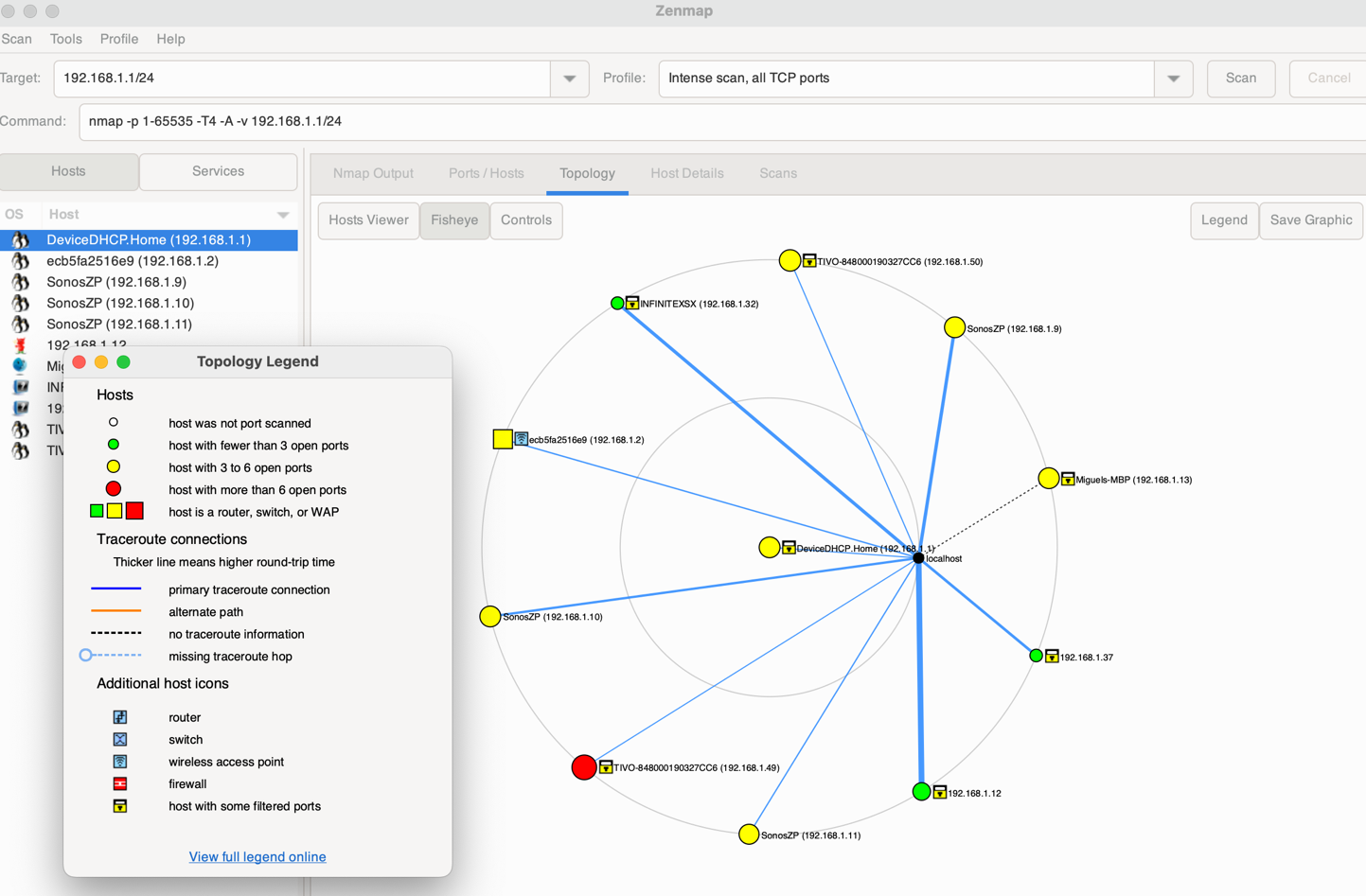
**Ransomware Recovery**

1. **What did you do – in this section tell me what you did to generate the above outputs, be specific. This section is all about how you are doing things, do not put results or outcomes here, just how you did it.**

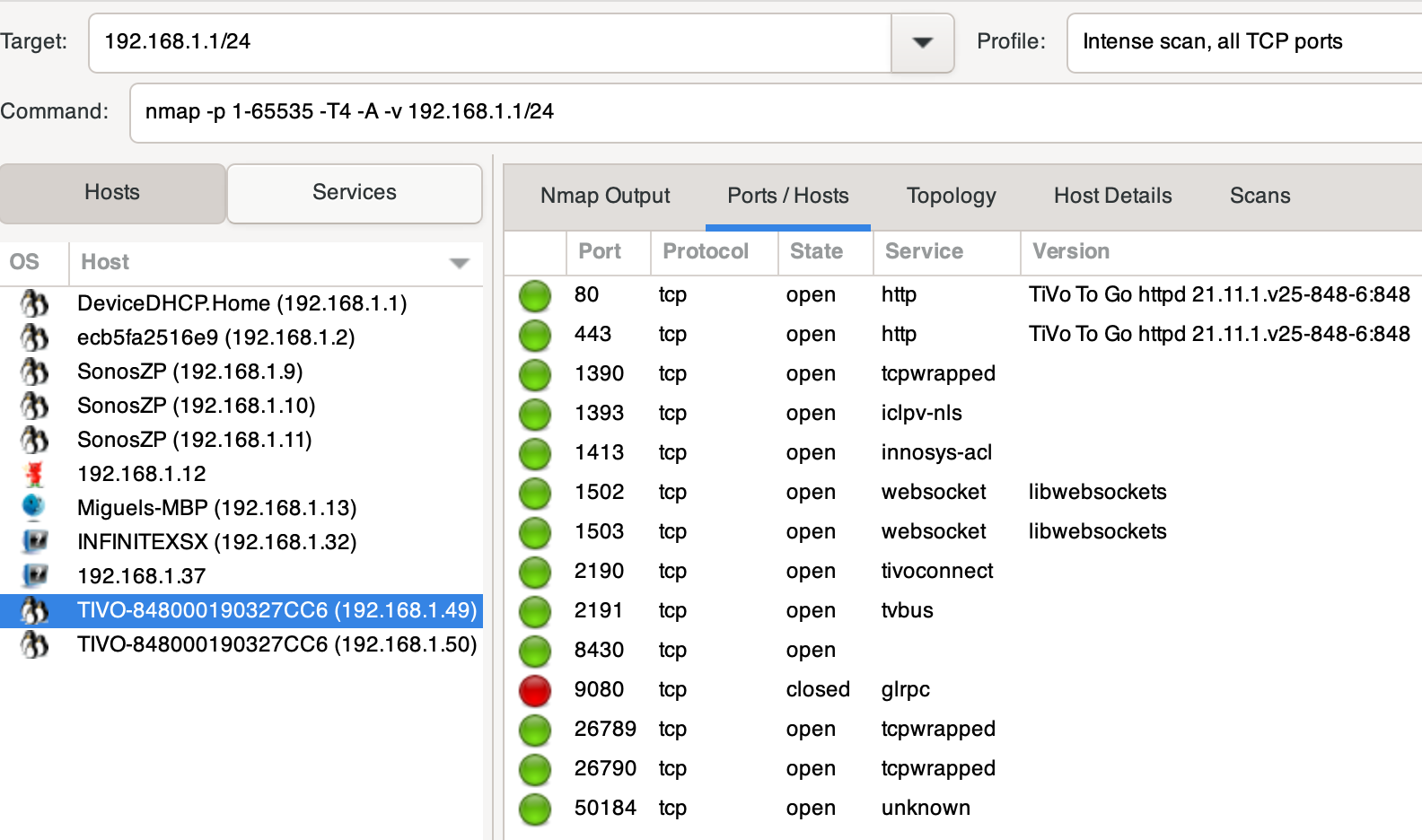
First and foremost, I had to prepare an inventory of network devices, so I ran a basic scan within NMAP. I executed the command nmap-sn 192.168.1.1/24 to scan my network and was able to get a list of all the hosts that were live (during the time of the scan). When I analyzed the list of devices there were no unknown hosts connected to the network except for one active host that concerned me “Cloud Network Technology Singapore PTE”. I began to create a repository of devices with a breakdown of each device name, MAC address, criticality of the device, device categorization (switch, router, etc.) and possibly the count of open ports (but this may not be necessary). My thought process was based on the number of ports that are open it would essentially help me identify which hosts are the most susceptible to attack and identify the method of entry. Criticality allows me to know which devices need to be brough up first and avoid losing precious data within the most critical hosts. I identified criticality by figuring out which hosts needed to be online first to be able to complete my basic daily tasks that “keep the lights on” both literally and figuratively. Once these core assets were identified ranking them became simpler because we would focus on bringing those up first because in essence they would be the “root” or the “brain” to have all the other devices “provisioned” for future access and configuration.

Once we broke down the devices next was identifying if there were any backup files of the hosts, so we have a way to restore the devices to a state prior to the ransomware attack. We then must identify (prior to restoration of an older software version) if any vendor support is needed prior to restoration and if we can still upgrade to a newer version after restoration. Essentially, we need to identify the impact of “backtracking” the software on the hosts and see if any services or functionality is lost by doing this. If anything is impacted, we would need to see if the vendor would be willing to work with us directly to resolve the issues. Once we created our asset inventory and backup statuses our next step was capturing the software upgrades, we could make to move along the restorative process. Finally, we would need to capture the passwords for each host and user accessing the hosts to have users provisioned again and gain access to their specific host devices. All the aforementioned steps are part of the basic response procedures I would typically take to recover from a ransomware attack.

1. **What are the results – in this section tell me what the specific deliverables are. Also, identify any deficiencies in your deliverables and what should be done to resolve the deficiencies.**

After completing the SYN scan (from nmap), I noticed my entire network is susceptible to attack due to the massive number of ports that are set to “open”. I have approximately 100+ ports open and the entire scan froze my computer while ZenMap continuously crashed on my Mac. The initial scan took approximately 3 hours and the additional scan for my MacBook was going to take approximately 2.2 hour until it froze completely. I attempted to extract the information but was not able to but did capture screenshots which I will attach to this paper. The ports are not the worst part of my problem. I noticed that the Phillips Hue lights and the Sonos speakers were huge security risks on my network and this could very well have been the port of entry for the ransomware attack. According to research from Cluley ‘Bitdefender’, hackers have been working constantly with IoT devices such as these Phillips Hue lights, due to their popularity. These Phillips hue devices are prime for hackers due to the many ways of accessing these devices and manipulating first the individual light bulb. Once the hacker can manipulate the lighting a user will troubleshoot and must delete the affected bulb from the bridge that controls all the Hue devices. Once the bridge reconnects to the bulb (which is now compromised) the user will go through the process of reconnecting the bulb which gives access to the network to the hacker. The hacker will then be able to access the internal network through the compromised bulb, then bridge and proceed to wreak havoc on the network and its connected devices (similarly to a virus). That then allows the hacker to gain access to all IoT devices such as mobile phones, Bluetooth of various devices and even open ports on the router to obtain even more access. When reviewing topography map of my network I was able to identify which devices had filtered ports which provide some level of protection. Devices like the game consoles, two macbook pros and the TIVO devices all have some form of filtered ports. Seven out of 11 active devices have 3- 6 port open. Four out of eleven devices are hosts without any filters which is a huge concern in my eyes. Specifically, the devices in question are the Sonos and Phillips Hue Bridge. All of these devices are susceptible and open for an attack of some kind. 

I looked further into the Sonos devices and came across research that Trend Micro used tools like NMap to to identify Sonos speakers (and Bose) that have lax networking security requirements. According to research from Greenberg, A., the hackers would “Rick Roll” users by playing the popular Rick Ashley song ”Never Gonna Give You Up”. Luckily it was identified that through API’s the hackers can play any sounds they would like through the speakers but the most interesting hack identified from this was the Sonos and Bose Alexa “voice-controlled speakers”. Since many homes are connected by way of automation and “voice controlled” devices hackers were able to have Alexa speak to itself and even give commands such as “open doors” and etc. Since this was identified Sonos and Bose have made the necessary steps to upgrade security firmware to avoid any data leakage and “tighten” up their protocols. This just goes to show me that through convenience of human behavior and “automation” we open ourselves up to extremely risky scenarios. Once device in specific had more than 6 open ports and that is our TIVO device from Breezeline.



The TIVO device uses various tcp ports to run various processes for the TIVO device such as TiVoconnect (this allows multiple TiVo devices to connect to one another ‘auto discovery’. The TiVo also has three separate ports with a service called tcpwrapped. Tcpwrapped is a software solution that is Linux based which provides firewall protection. Essentially it monitors incoming packets and if an external node tries to connect the software identifies if it has authorization.

Below is the asset inventory list I was able to create after a thorough review of the network.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Device Name** | **MAC Address** | **IP Address** | **OS Version** | **Back Up Date** | **Device Category** | **Vendor** | **Password** |
| 1 | Miguels MBP | 3D:2B:J8:37:B2 | 192.168.13 | Ventura 13.5 | August 9th, 2023 | Personal Computer | Apple | ################# |
| 2 | Miguel's Ipad | 7C:1M:G8:37:4J | 192.168.22 | 16.5.1 | August 9th, 2023 | Personal Computer | Apple | ################# |
| 3 | Alissa's MB | 8C:6P:X8:37:S7 | 192.168.01 | Sierra 12.8 | February 23rd, 2023 | Personal Computer | Apple | ################# |
| 4 | Miguels iPhone | 6C:5B:G8:37:F5 | 192.168.05 | 10.6.4 | January 18,2022 | Mobile Device | Apple | ################# |
| 5 | Alissa's iPhone | 1C:2B:K8:37:K7 | 192.168.04 | 10.6.3 | September 12,2022 | Mobile Device | Apple | ################# |
| 6 | LG WebOS | 2C:4A:H8:37:I8 | 192.168.03 | 21.41 | August 8th, 2023 | Televison | LG - Best Buy (Third Party Managed) | ################# |
| 7 | BreezeLineTivo | 4Y:1M:G8:37:4J | 192.168.00 | X78.78 | N/A | ISP Router | BreezeLine | ################# |
| 8 | PS-18 | 8C:6P:X8:37:S7 | 192.168.07 | 09.23V | August 5th, 2023 | Console | Sony | ################# |
| 9 | INFINITEXSX | 7C:1M:G8:37:4J | 192.168.11 | X57.87C | August 5th, 2024 | Console | Microsoft | ################# |
| 10 | Switch | 6C:5B:G8:37:F5 | 192.168.14 | 10.3 | August 5th, 2025 | Console | NUSA | ################# |
| 11 | Sonos One | 9F:2B:K8:37:K7 | 192.168.15 | 7C.56 | N/A | Speaker | Sonos | ################# |
| 12 | Sonos Sub | 6H:1M:G8:37:4J | 192.168.16 | 7C.56 | N/A | Speaker | Sonos | N/A |
| 13 | Sonos Play | 2C:2B:J8:37:B2 | 192.168.17 | 7C.56 | N/A | Bridge | Sonos | N/A |
| 14 | Phillips Bridge | 7C:2B:J8:37:B2 | 192.168.18 | 10.44.55 | N/A | Bridge | Phillips | ################# |
| 15 | Phillips Hue | 4Y:1M:G8:37:4J | 192.168.19 | 10.44.55 | N/A | LED Light | Phillips | N/A |
| 16 | Phillips Hue | 8C:6P:X8:37:S7 | 192.168.20 | 10.44.55 | N/A | LED Light | Phillips | N/A |

I was able to leverage Nessus to identify the version of each host as well as the vulnerability of the current software. There were various red flags or issues that came about from my scan and categorization during this exercise. The most critical device on my network (the main MacBook Pro) also had a critical vulnerability coming from the application “Google Chrome”.

A screenshot of a computer

Description automatically generated

Once I reviewed each device listed above in my priority list

To avoid the ransomware contaminating any backups, my plan is to take all the devices offline and roll back any devices that have backups associated to them. Once I have them offline the backups would have to come from a separate memory drive to avoid contamination and ensure they are offline. Once I “roll-back” the devices my plan would be to run an antivirus, malware, and antivirus scan to check for any remnants of the ransomware. Once the antivirus scan has completed and all scans have passed the deep scan, my next step would be to change all of the credentials on each device (in the event the passwords were captured by the ransomware). I don’t know if the ransomware was able to get into the system files and extract / decrypt the passwords embedded within the system logs. Once the antivirus scan is completed and I have changed the password on the devices I would bring the devices online with new IP addresses and avoid using the same static IP’s that were used before. I would potentially look to make a more robust networking architecture with a DMZ approach to avoid future instances of attack. Once I have the devices back online, I would like to run a “sanity check” of sorts by running nmap on the new network and identify any open ports / vulnerabilities. After nmap I would run ShieldUp! and Nessus to identify vulnerabilities in the current OS of the devices I have. Nessus will report back that the versions are outdated since they are coming from backups. Once all scans have come back clear from antivirus, malware, ransomware, and network vulnerability I would update the devices to the latest OS and include any security updates needed. After doing these steps I would run Nessus one more time to identify any new vulnerabilities after updating all the devices to their latest versions.

1. **What did you learn – discuss your takeaways from the assignment, tell me what you learned about ransomware and preparing to recover from a ransomware attack and how you can use it in the future, also discuss how this has value to the organization in the future.**

I learned that in order to handle potentially catastrophic logistical and financial effects of a ransomware attack business must create a ransomware response strategy. These attacks can be avoided by taking preventative measures such as employee training, using antivirus and endpoint protection, network and data backups, provisioning of access controls and penetrative/vulnerability tests. The need for a standard operating procedure with detailed instructions for backup plans (for both external and internal communications), severity of impact analysis, damage mitigation, malware destruction and an operational recovery plan are all critical components of a strong incident response strategy to battle ransomware attacks.

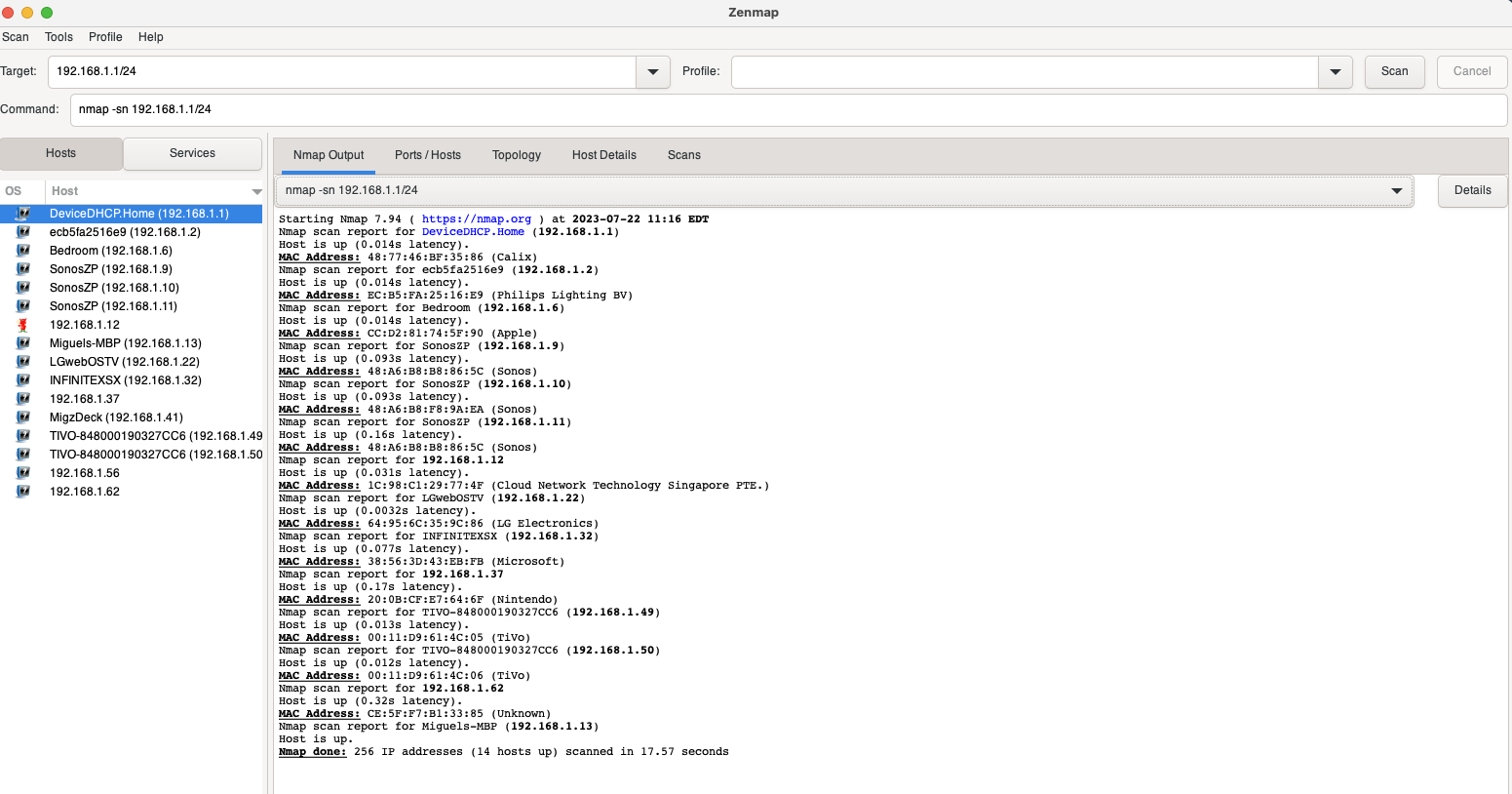
In research I came across, it was brought to my attention that ransomware is one of the biggest risks to organizations around the globe. Ransomware is known to contribute to a significant amount of Cyber Insurance claims (which I didn’t even know cyber insurance claims existed). The average cost of a ransomware incident can cost an organization over $450,000 in lost revenue and the impact to business interruption can increase exponentially to an average cost of $600,000 and more (the larger the organization the greater the impact). The greatest asset to any organization is its people but it can also be their key weakness when it comes to ransomware attack. Therefore, training of staff is critical, and a solid ransomware response plan includes training an organizations workforce. A basic training for all employees should include the following: identifying suspicious emails, updating and patching software (this can be done through a software like Nessus), securing passwords that are robust, securing personal and business data and upkeep the latest cybersecurity solutions and operations.

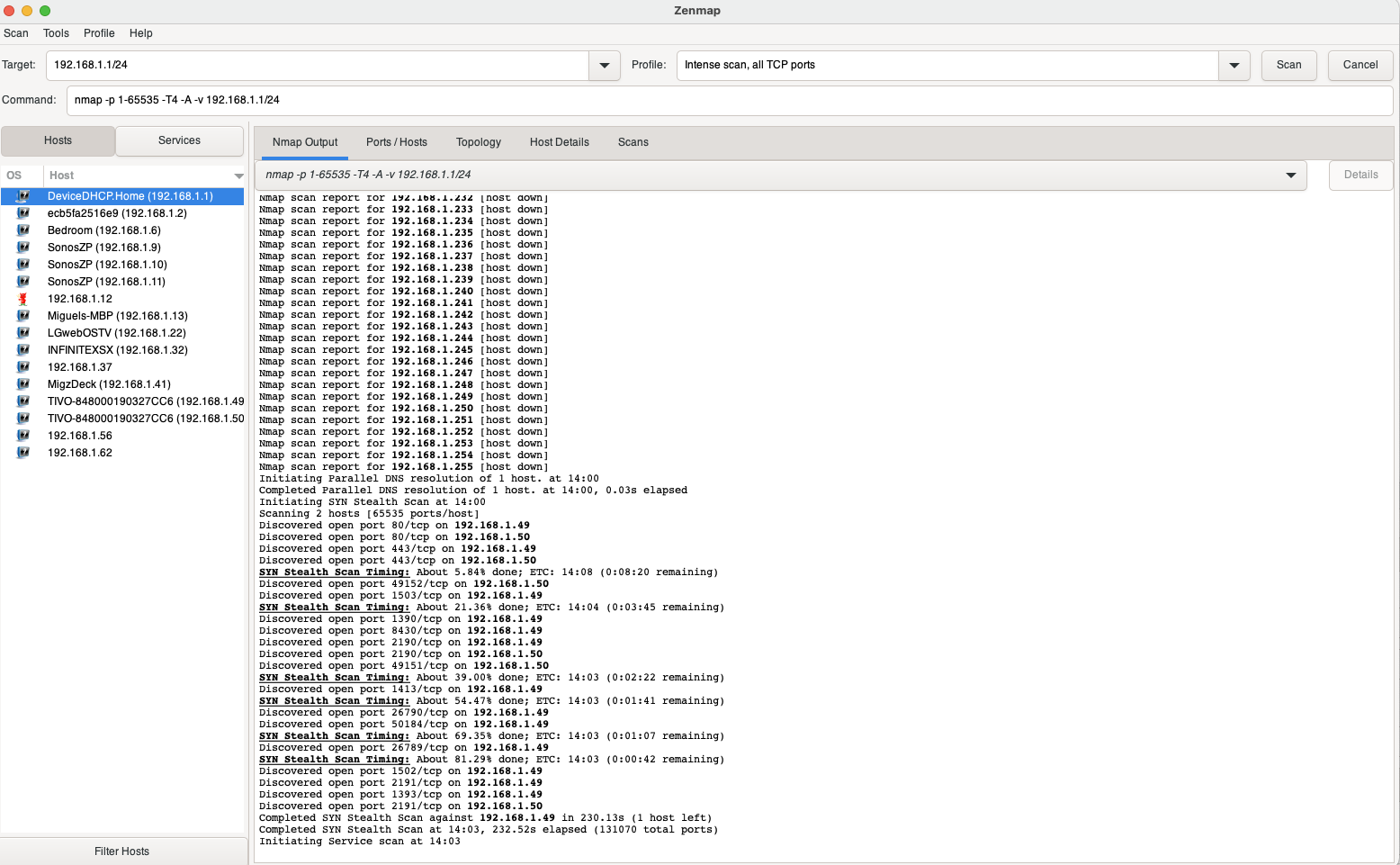
From an IT perspective the cyber security team should follow the following checklist: endpoint safety including antivirus software, identifying malicious software in real time, segmented data backups that can be located offline and on separate networks, leverage cloud backup services, DMZ / divided networks, MFA (Multi-Factor-Authentication) where administrative access is extremely limited, block remote desktop protocols, penetrative testing completed regularly and a finally a strategy to respond to a ransomware attack and implement the appropriate corrective actions.

When creating a ransomware attack response strategy should be extremely detailed and have backup procedures. Those procedures should include also the following: 1- communication methods and guidelines for all impacted users and communicate the attack to everyone within the organization; 2- Impact analysis to identify the events that occurred, impacted networks, computers and applications; 3 – Recovery response which includes the elimination of the threat along with ways to contain the infected devices and limit the attack impact (this may include taking down specific networks, computers and even devices).

The value of a strong cybersecurity team with the expertise needed to create, implement, and adhere to the above will be critical in the success of any organization to recover from a ransomware attack. While we try our hardest to avoid these attacks, preparing for the worst, providing the necessary training, and including the appropriate cyber security professionals will be critical to mitigate the impact on an organization and prepare them for any future attacks.

NMap Output Screenshots





**References**

*What Is A Port Scan? How To Prevent Port Scan Attacks? | Fortinet*. (n.d.). Fortinet. <https://www.fortinet.com/resources/cyberglossary/what-is-port-scan#:~:text=A%20port%20scan%20is%20a,being%20used%20by%20an%20organization>.

*How your network could be hacked through a Phillips Hue smart bulb? | Cluley, Graham* Bitdefender. <https://www.bitdefender.com/blog/hotforsecurity/how-your-network-could-be-hacked-through-a-philips-hue-smart-bulb/>

Greenberg, A. (2017, December 27). Hackers can rickroll thousands of sonos and bose speakers over the internet. *WIRED*. https://www.wired.com/story/hackers-can-rickroll-sonos-bose-speakers-over-internet/

<https://www.tenable.com/sites/default/files/uploads/documents/whitepapers/Whitepaper-Nessus_Agents_0.pdf>

*GRC | Port Status Info*. (n.d.). https://www.grc.com/su/portstatusinfo.htm#:~:text=Port%20Authority%20%E2%80%93%20ShieldsUP!!%20and,or%20%22Closed%22%20for%20business.