Cybersecurity Incident Report

Ifeanyi Uzoukwu

CST 630

University of Maryland, Global Campus

April 30th, 2021

***Executive Summary***

Since the installment of GCI’s bring your own device (BYOD) policy, there has been a number of vulnerabilities detected within GCI’s IT infrastructure. Currently, our policy supports Apple, Android, Windows mobile devices. Our policy also supports computers running Windows, Mac, and Linux operation systems. GCI uses the Scalefusion Mobile Device Management (MDM) software. Scalefusion MDM is an Enterprise mobility manager, meaning that GCI can utilize it to give our employees a viable interface to conduct their tasks on. Upon the installment of the BYOD plan, GCI had also erected a rule that forbid employees from jailbreaking, or altering the operating system software on their devices. This rule was created because while jailbroken devices are easier to modify, they also are more prone to vulnerabilities, that if left unchecked, could infect the IT infrastructure of a company.

As the new Cybersecurity Incident Manager at Genesis Communications Incorporated (GCI), I have taken it upon myself to conduct an audit of our IT infrastructure. During my audit, I found that some of our servers have been performing at less-than-optimal speeds. I also noticed that this calamity had begun around the time GCI implemented a bring your own device (BYOD) policy. I have created the following Cybersecurity Incident Report (CIR) detailing the specific steps that GCI should take as a response to the incident and methods that GCI can employ to better protect itself from similar attacks in the future. This report will also feature plans on Wireless BYOD and Continuous Improvement in addition to information on the Cyber Kill Chain framework and how to apply it to GCI’s own IT infrastructure. The BYOD security plan will address measures that need to be taken to prevent similar attacks in the future, how to secure wireless access points, enterprise threats, and ways to improve incident responses. I will also offer suggestions on how to handle employee misconduct, manage remote client software and monitor suspicious behavior. Ultimately, my suggestion is to have management regularly schedule information sessions on our BYOD policy, which would include detailed rules and regulations that all GCI employees must use while they are at work.

**Wireless/BYOD Security Plan**

To cut costs in the midst of the pandemic, GCI implemented a BYOD policy that allowed our employees to use their own laptops, workstations, and mobile devices as long as they used our client whilst doing so. Unfortunately, as the number of devices using our system increased, so did the number of vulnerabilities. The range of different devices that were using our systems invited added risk to our systems since they all had access to our sensitive information. Problems such as unauthorized website access and unpatched vulnerabilities. While the BYOD security plan was a great initiative to cut costs, certain amendments need to be made for the plan to decrease the likelihood of another significant incident.

There needs to be a company-wide **standard** for the devices that are using our systems. One recommended change to the BYOD plan is for our program to only support Android, Apple, and PC devices made in the last five years. Patches for devices made before this period are already out of date, and those devices are phased out from newer and recommended patches. My second recommendation would be to review the defenses for our network that are in place. Anti-virus software, Firewalls, and intrusion detection systems (IDS) are some of the best ways to boost our network defenses. When a company has a network infrastructure that is not protected well enough because they refuse to update, upgrade, or acknowledge that need for network defenses, then that company leaves themselves open to a potential data breach. Systems that are infiltrated by attackers can be prone to communications between devices on the same network being monitored, passwords being stolen, and the creation of rouge access points.

Rogue access points are the result of devices accessing the network that do not have the proper authorization. Rogue access points can be detrimental to a system if left unchecked. Rogue access points allow for wireless backdoor access into a network which outsiders near the Rogue access point can use if they are close enough to it. Rogue access points can be used maliciously to leak private data, such as passwords and personally identifiable information. These access points can be installed by cyber threat actors intent on launching an attack. (Shah, n.d.) Rogue access points can intercept data passively or actively. In passive interception, rogue access points read information shared between devices but does not edit or alter it. This method is most commonly used for collecting data. In active interception, the attacker can alter the information being sent or the destination in which it is supposed to go. Rogue access points can be detected by a wireless network scanning tool, such as an intrusion detection system (IDS) or intrusion prevention system (IPS). Once an IDS or IPS is acquired, a scan which would show all access points connected to the network can be conducted. The results of this scan would reveal which access points are considered to be rogue. To further alleviate this matter, the IDS scan should be scheduled regularly to prevent future rogue access points from afflicting our network. Using virtual private networks (VPN) or Hypertext Transfer Protocol Secure (HTTPS). Both VPN’s and HTTPS scramble the communications between computers so that they are unintelligible even if it is captured.

The Cyber Kill Chain Framework is another method for managing network security. Originally developed by Lockheed Martin to better predict the events of a cyberattack, the Cyber Kill Chain has become a trusted method for recognizing insider threats, social engineering, and advanced ransomware attacks. (Hospelhorn, 2020) The Cyber Kill Chain process assimilates the structure of Cyber attacks and helps large companies and organizations develop an in-depth understanding of how the attacks were implemented. The Cyber Kill Chain Framework has eight stages, Reconnaissance, Intrusion, Exploitation, Privilege Escalation, Lateral Movement, Anti-Forensics, Denial of Service, and Data Exfiltration Adding this framework will enable a stronger threat response from GCI in regards to detecting future threats to the infrastructure.

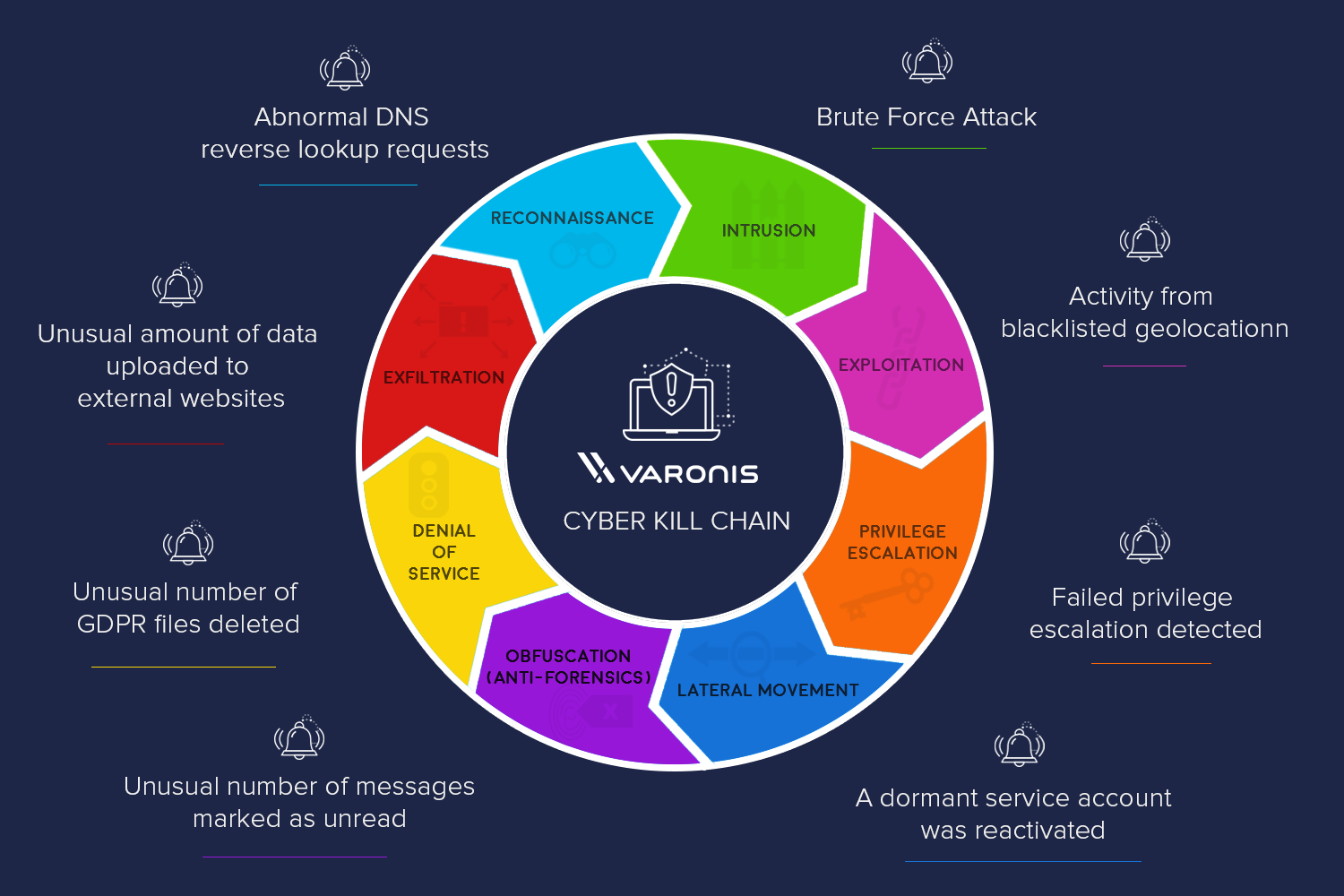


Figure : The Cyber Kill Chain (Hospelhorn, 2020)

**Tracking Suspicious Behavior**

Although the BYOD security plan we enacted comes with obvious amenities, it also has its own drawbacks. It has come to our attention that an employee at GCI is the owner of a device that has been involved in relatively suspicious behavior. After noticing this, I scheduled a meeting with him and informed him of our findings. When our employee denied any involvement in these developments, we believed him but decided to monitor the device in question. One way to go about this would be to collect the IP and MAC addresses of each employee and associate that information with their owners. At that point we could track their location by tracking their IP address. (Glover, n.d.) Monitoring the Bandwidth of our employees is also a good method to track their internet habits during work hours. Devices that eat up large portions of our bandwidth can be infected with malware, or could be utilizing video streaming services such as Netflix or Hulu. Devices that are found to be using a large amount of bandwidth would be obvious anomalies.

There is a chance that our employee could be the victim of an identity theft attack. In certain cases, employees are forced to conduct their work duties in public spaces and connect to public wi-fi. Places such as libraries and coffee shops are prime targets for hackers to pilfer data. If that is the case, an attacker could easily infiltrate our unsuspecting employee’s device. If cyber-attack victims are lackadaisical when it comes to protecting their device, for example if they leave their device unattended in a public setting, download unsafe applications or files, and visiting unsafe websites, then the chances of their device being infected increase exponentially.

MAC addresses can be used to track a certain device, but attackers can also find a way around this. Attackers can alter their network interface controller card to change their MAC address to that of another device, allowing them to assume the identity of the stolen MAC address user. (Upadhyay, 2020) This process is known as MAC spoofing. If this is the case as it relates to our employee, then there is reason to exonerate him from these alleged accusations. After all, as long as this employee has worked at GCI, he has been an example to follow, and turns in satisfactory work. The IT department at GCI will need to conduct a scan on the device in question to determine if it has been involved in any nefarious activity. Before the device scan, GCI needs to be sure that it has identified all of the access points into the GCI network. Each access point needs to be authorized, and there must be added security on any access point that is open. In addition to this, it would be wise to take this opportunity to create a list of verified computers, routers, firewalls, and other devices by getting the MAC address of each device used to interact with GCI’s network. Only the devices on this list that can be identified should have access to the GCI network. This is known as a whitelist. Creating a whitelist would block out unauthorized devices from accessing our network.

The other hurdle that would have to be overcome to conduct the scan is the issue with the invasion of privacy of our employees. It is not just enough that the IT department at GCI must do their due diligence to report the incident, but they must respect the privacy of our employees. An acceptable compromise is requiring our employees to sign a “form of consent” allowing the IT team to search for any correlation between the data that was compromised and their hard drive. The form of consent will also feature insight into the procedures GCI is taking to ensure their rights are not violated.

**Continuous Improvement Plan**

Since its inception, GCI has been committed to protecting our data; that of the customer and our employees own personally identifiable information (PII). When GCI started out in the late 1990’s, we were using Wired Equivalency Privacy (WEP) as our main wireless capability. WEP was created at that time as the first method of encrypting the 802.11 standard. WEP’s design was meant to promote data confidentiality which could compare to a traditional wired network. WEP was also meant to stop Man-In-The-Middle attacks. WEP has a fault in the fact that its values of initialization vectors (IV) are much too small. This weakness persists no matter which encryption standard is used with WEP because it uses a 24-bit IV. WEP encrypted everything in a static key, which was its main weakness as all information was encrypted using the same key. (Section, 2020) Because the situation with WEP was not going to drastically improve, Wi-Fi protected access (WPA) was created in 2003, and used Temporal Key Integrity Protocols (TKIP), which featured encryption key length to add an extra layer of security, as well as allowing for each packet to have its own key. WPA was more secure than WEP, but it still had its own faults that rendered it unsafe to use over an extended period of time. This brought forth the implementation of Wi-Fi Protected Access 2 (WPA2). WPA2 was introduced in 2004, and uses Advanced Encryption Standard (AES) instead of TKIP. This is a crucial advantage for WPA2, as AES is able to secure top-secret government information. WPA2 is not without faults though. An attacker that gains access to the network, can attack the devices that are connected to it. This vulnerability would apply to organizations or companies that have internal threat actors, such as unhappy or recently fired employees. (Panda Security, 2021) WPA2 also requires more processing power to run than WEP. The upgrade to WPA2, WPA3, has been in the works since 2018. WPA3 seeks to be the answer to many of the vulnerabilities that are present in WPA2. WPA3 has not been implemented at most large-scale companies. WPA2 supports both TKIP and AES, is used by most newer device models, and requires lengthier passwords, which further complicates the task of infiltrating networks that use it. WPA2 also has more security features and has options that cater to Enterprise-level organizations. Therefore, WPA2 should be the least secure security standard used at large scale companies.

To improve upon our current network defenses that already use WPA2, the use of pre-shared keys is also recommended. Pre-Shared keys transfer private shared keys between the sender and receiver, for the purpose of authenticating users. (UMGC, 2021) Generation of encryption keys for our end users by using the Service Set Identifier (SSID), with strings of hexadecimal digits and TKIP to configure access points can be achieved with PSK. (Juniper Networks, 2019) The PSK authenticates users when they type in their username and password. PSK can be immensely helpful when processing power is limited.

Our improvement plan must be in compliance with the Federal Information Processing Standard (FIPS) 140-2, which details the security requirements for cryptographic modules. Created in 2001, FIPS 140-2 is a set of standards that describe document processing, encryption algorithms and other information technology processes for use within non-military federal government agencies and by government contractors and vendors who work with these agencies. FIPS 140-2 lists the cryptography modules that are approved by federal agencies. (McAfee, n.d.) The Institution of Electrical and Electronic Engineers (IEEE) 802.11i standard allows for the continued use of both WPA2 and PSK, as they are complaint with the standard. However, the testing of cryptographic modules against FIPS 140-2 is supposed to end on September 22nd, 2021. At that point, GCI must be prepared to replace their current data encryption methods to conform to the new standard when the time comes.

We consider Bluetooth to be a vital innovation that people use on a regular basis. Bluetooth enables devices such as apple watches, wireless headphones, and vehicular audio interfaces that people, including our employees use on a regular basis. Despite that, GCI is recommending employees to limit their use of Bluetooth during work hours, as it pertains to the “discovery mode” that is required for Bluetooth devices to set up initial connections with each other. GCI has been made aware of a vulnerability that stems from laptops, phones, and other devices being left in discovery mode for far too long. When left in this mode, there is substantial risk of information loss, and this also increases the risk of our data being compromised by an attacker. This specific risk can be mitigated by remembering to shut off discovery mode on a regular basis.

The advantages and disadvantages of other commonly used protocols; such as Hyper Text Transfer Protocol (HTTP), User Datagram Protocol (UDP), Transmission Control Protocol/ Internet Protocol (TCP/IP), and Internet Control Message Protocol ICMP). HTTP is the data transfer protocol used on the Internet. HTTP is the portion of Internet Protocol (IP) that defines which services and commands shall be used to transmit webpage data. HTTP works in conjunction with web hosts that run web service software such as Microsoft Internet Information Services (IIS). HTTP offers lower CPU and memory usage due to less connections. Offers less network congestion as a result of fewer TCP connections. HTTP has no encryption methods, leaving those that use it prone to potential tampering of data. (Roomi, 2020) ICMP is a supporting protocol used by network devices to send error messages or successful attempts at communicating with another IP address. ICMP provides administrators with the ability to send timed requests across the network. (Branch, 2016) Examples of ICMP error messages are Source Quench, Parameter Problem, and Time Exceeded. ICMP is prone to attacks, such as Ping Sweeps, Ping Floods, Forged ICMP redirects, and ICMP tunneling. TCP/IP is the primary method for communication over the internet. Large portions of data are taken and translated into packets, then send through the other layers in the TCP/IP chain. The Layers of the TCP/IP are the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer. (Computer Science, 2011) As an open protocol suite, it is not owned by any particular institute and so can be used by any individual or organization. TCP/IP doesn’t distinguish between the data link and the physical layers, which has very different functionalities. (Fendadis, 2018) UDP is a communication protocol that is primarily used for establishing low-latency and loss-tolerating connections between applications on the internet. UDP is relied on for communication, and operates by sending messages known as datagrams to and from devices. UDP provides port numbers which help in differentiating between user requests. UDP’s Datagram boundaries are respected, you can broadcast, and it is fast. However, UDP is an Unreliable protocol. There is no guarantee that datagrams will be sent to the intended party.

**Remote Configuration Management**

Remote Configuration Management allows for system configuration changes to be performed through the network without needing access to the console of the system being configured. Software is installed directly to the system which allows it to be controlled at any location that can access the program. Administrators are notified each time an attempt to remotely access the system is made. The administrator can assign permission levels to users allowed to access the system. Management tools are known targets for attackers to attempt to gain access into the networks of corporations and organizations. Microsoft's remote desktop protocol, port 3389, was maliciously used by hackers to trick users into allowing the hacker into their machines by posing as Microsoft personnel. Hackers would encrypt the user's machine, which locked the user out of their machine, and would then demand money to unlock the device. This vulnerability was mainly exploited on older versions of Windows such as Windows XP (UMGC, 2017). Using enterprise-level VPN software, such as Perimeter 81 Enterprise VPN, is recommended to log on to the system from here on.

An incident was brought to GCI’s attention about an unauthorized device being logged onto the system. Since this device is not authorized, it must be removed from the network before it can possibly hack into other systems on the network. I will have our team obtain the MAC address of the device in question and add it to a blacklist, which is a list of computers and other devices that are not allowed to access the network under any circumstances. Using our directory, users on the network’s whitelist, will be promoted to maintain their access to the network. Scanning all the VPN users using our Perimeter 81 and a network scanning tool such as WireShark, will detect the users that are on the network. If the attacker still remains on the network, GCI can collect information on the attacker and alert the police.

**Employee Misconduct**

GCI has been alerted of an employee logging into the network after business hours, without the proper authorization. The Employee Device accessed the network using an ad-hoc wireless network. Ad-hoc Wireless networks are decentralized wireless networks that do not rely on pre-existing structures, such as routers, or access points. The ad-hoc wireless network functions by having each node rout information by forwarding data to other nodes, which makes the determination of which nodes that forward data dependent on the routing algorithm in use. The appearance of ad-hoc networks in the GCI network is especially troubling because they can lead to various vulnerabilities such as device cloning, MAC address spoofing, and the chance of data on a user end node being compromised by the ad-hoc network. One method to circumvent access being enabled for an ad-hoc wireless network is to a mechanism the employs authorization at the application level. Although Ad-hoc networks are quickly set up, they tend to have large gaps in their security which is why they should not be allowed to ever remain on the network. In addition to having large security gaps, ad-hoc networks can be disrupted very easily. All connections made with the ad-hoc network must be removed and blacklisted immediately. Ad-hoc networks are prone to attacks such as resource consumption attacks and attacks on data traffic. Resource consumption attacks work by having the attacker send route request (RREQ) packets to degrade the overall network performance. (Adbelhaq, 2014) Attacks on data traffic attack computer nodes and incorrectly routes data.

I recommend that GCI also consider the use of a self-configuring dynamic network. This kind of network creates changes that can be programmed based upon the policies of its organization. Self-configuring dynamic networks come with their own drawbacks. These networks can cause issues with the implementation of the policies in question, and can also cause nodes to not function as they should. Linking networking tools to policy configuration tools can potentially mitigate this issue.

The Service Set Identifier (SSID), more commonly referred to as the Wi-Fi network name, can be hidden with a method known as signal hiding. As its name implies, Signal hiding hides the Wi-Fi network so it does not appear on the discovery list. This is useful because people who pass by a user’s laptop casually would not have the chance to see the SSID of the network that the user is on. This method would also prevent potential threats from cloning the network. Connecting to an SSID that is hiding its signal would require the user to know that specific network’s name. This method is not impenetrable, as there as programs that can still get into a network hiding its signal.

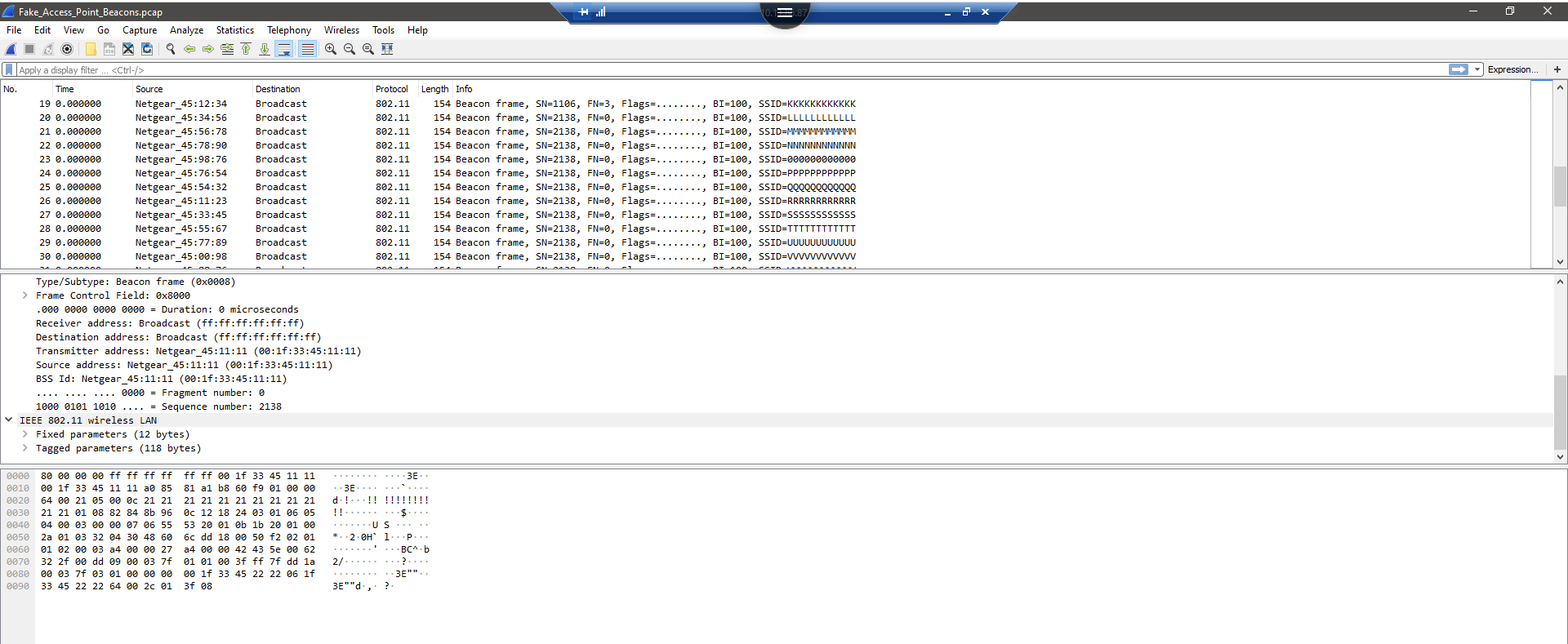
Using Security information and event management (SIEM) tools can provide GCI with the chance to analyze, detect, and respond to problematic occurrences on the network. The SIEM tool can alert GCI’s administrators when an employee is accessing the network at odd hours.

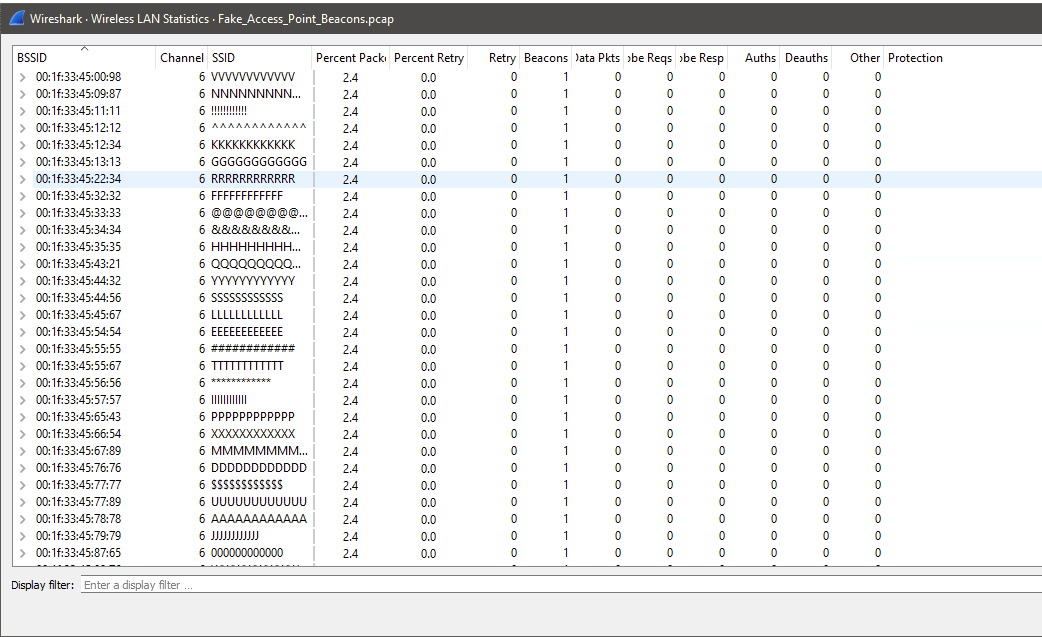
**Wireless Traffic Analysis**

GCI conducted a network scan to find all rogue access points and disturbances to the network. The results of that scan are as follows. For our analysis, I took a look into the following BSSID’s and MAC addresses.

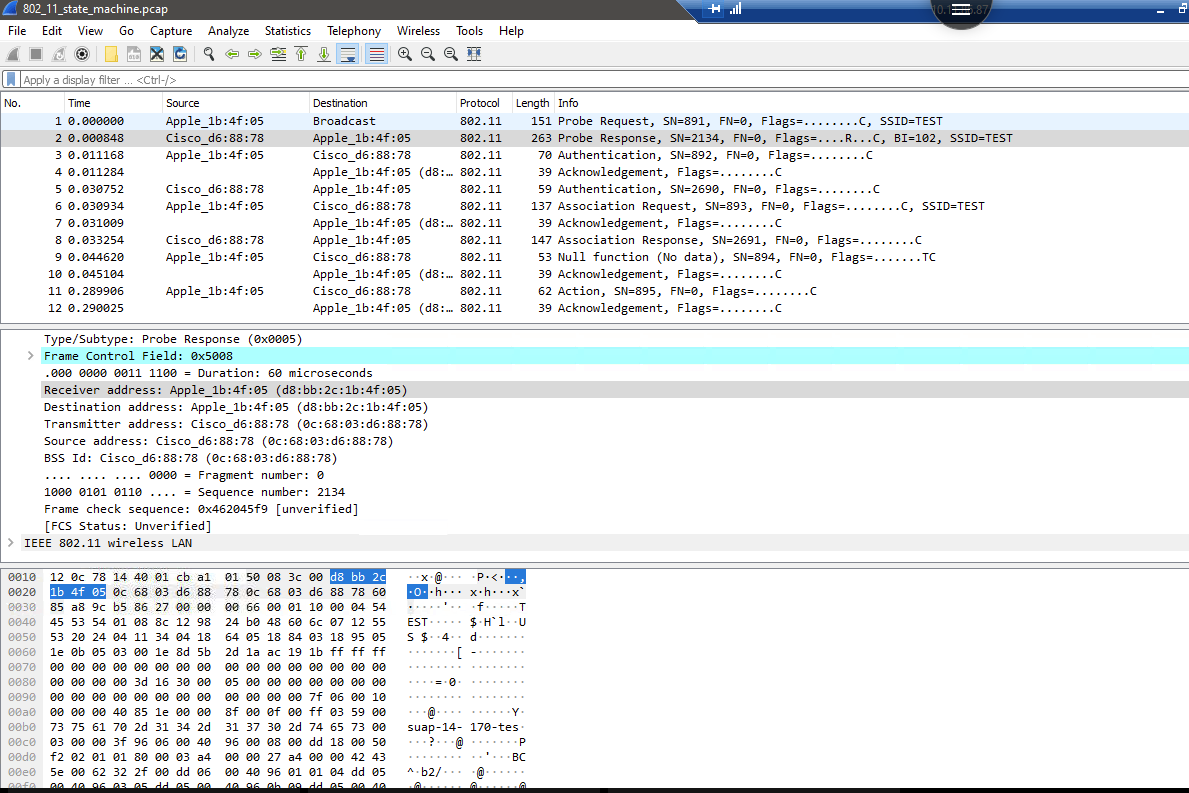
* Netgear\_45:11:11 (00:1f:33:45:11:11)
* Netgear\_45:56:56 (00:1f:33:45:56:56)
* Netgear\_45:90:90 (00:1f:33:45:90:90)
* Netgear\_45:78:78 (00:1f:33:45:78:78)
* Netgear\_45:54:32 (00:1f:33:45:54:32)
* Netgear\_45:33:45 (00:1f:33:45:33:45)

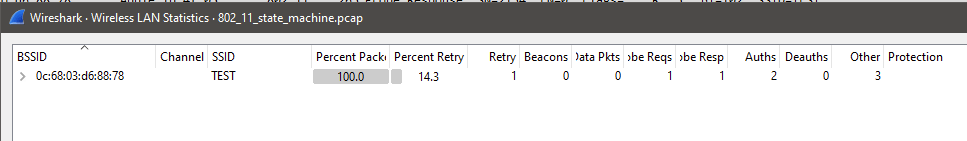
None of the 42 packets found in this file had a MAC address that was on the whitelist.



Upon examination of the BSSID’s and their corresponding SSID’s I found that the last two sets of digits relating to the BSSID of these WAP’s had an overly simplistic pattern to them. The WAPs are using channel 6. As you can see below, the SSID’s are repetitions of the same letter or character. This is both highly unusual and not compliant with the regulations of GCI’s network policy. None of these connections are approved according to the whitelist that was provided. In total, 42 rogue access points were discovered in the scan. 

Another scan of the network brought about a list of BSSID’s that a device that was approved to be on the whitelist was sending and receiving information from an unauthorized device. Apple\_1b:4f:05 (d8:bb:2c:1b:4f:05) which was not on our whitelist, but it was using channel 48, which was approved, to communicate. The source device did not match that of the devices on the whitelist. In the second frame of the 802\_11\_state\_machine.pcap file, the transmitter MAC address and the SSID were both on the whitelist.





Preventing similar incidents such as the one above is vital to maintaining GCI’s strong IT network infrastructure. Maintaining a whitelist along with the employing a continuous network monitoring tool such as Perimeter 81 will provide the best method for GCI to protect its network and prevent incidents such as this one. Signal hiding is also a very good practice for GCI to continue.

GCI is able to maintain a solid chain of custody of our evidence of our recent attack. After the scan was completed, screen shots were taking documenting which whitelisted MAC address had been communicating with outside devices. GCI has been able to trace that MAC address to a specific employee and they will be reprimanded at GCI’s disclosure. The screen saves were moved to a private USB drive and are being held in a safe with very limited access to ensure they are not compromised.

**Conclusion**

As cybersecurity incidents are on the rise, companies around the world will have to work harder to protect their precious data from hackers and intruders. GCI was able to get off relatively easy because of a well thought out and executed plan. The BYOD policy should not be affected by these events, but restrictions on how freely our employees could access the network and the types of devices that were allowed to access the network must be enforced for our policy to remain viable.

**References**

Adbelhaq, M., Alsaqour, R., Al-Hubaishi, M., Alahdal, T., & Uddin, M. (2014, July). The Impact of Resource Consumption Attack on Mobile Adhoc Network Routing. Retrieved May 7, 2021, from https://www.researchgate.net/profile/Mueen-Uddin/publication/257353025\_The\_Impact\_of\_Resource\_Consumption\_Attack\_on\_Mobile\_Ad-hoc\_Network\_Routing/links/02e7e52fc7e5b09b3c000000/The-Impact-of-Resource-Consumption-Attack-on-Mobile-Ad-hoc-Network-Routing.pdf

Branch, D. (2016, July 19). Icmp: The good, the bad, and the ugly. Retrieved May 7, 2021, from https://blog.securityevaluators.com/icmp-the-good-the-bad-and-the-ugly-130413e56030

Computer Science. (2011, October 04). Compare and contrast the advantages and disadvantages of TCP - UDP. Retrieved May 6, 2021, from http://cs-pages.blogspot.com/2011/10/compare-and-contrast-advantages-and.html#:~:text=The%20main%20advantages%20for%20UDP,program%20at%20the%20application%20level.&text=TCP%20and%20UDP%20use%20the%20same%20addressing%20scheme.

Fendadis, J. (2018, July 13). Advantages and disadvantages of the tcp/ip model. Retrieved May 6, 2021, from https://www.tutorialspoint.com/Advantages-and-Disadvantages-of-the-TCP-IP-Model

Glover, G. (n.d.). Wireless access point Protection: 5 steps to find Rogue wi-fi networks and comply with PCI DSS Requirement 11.1. Retrieved May 4, 2021, from https://www.securitymetrics.com/blog/wireless-access-point-protection-finding-rogue-wi-fi-networks

Hospelhorn, S. (2020, March 29). What is the cyber kill chain and how to use it effectively: Varonis. Retrieved May 3, 2021, from https://www.varonis.com/blog/cyber-kill-chain/

Juniper Networks. (2019, January 9). Understanding PSK Authentication. Retrieved May 9, 2021, from https://www.juniper.net/documentation/en\_US/junos-space-apps/network-director3.0/topics/concept/wireless-wpa-psk-authentication.html

McAfee. (n.d.). FIPS 140-2 Compliance Requirements. Retrieved May 8, 2021, from https://www.mcafee.com/enterprise/en-us/about/cloud-compliance/fips-140-2-encryption-compliance-requirements.html

Panda Security. (2021, April 26). WPA vs wpa2: Which wifi security should you use? Retrieved May 7, 2021, from https://www.pandasecurity.com/en/mediacenter/security/wpa-vs-wpa2/

Roomi, M. (2020, August). 5 advantages and disadvantages of HTTP: Drawbacks & benefits of HTTP. Retrieved May 8, 2021, from https://www.hitechwhizz.com/2020/08/5-advantages-and-disadvantages-drawbacks-benefits-of-http.html

Section. (2020). Why you shouldn't use wep encryption. Retrieved May 6, 2021, from https://www.section.io/engineering-education/wep-encryption/

Shah, A. (n.d.). Rogue access points. Retrieved May 3, 2021, from https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/rogue-access-points-mitm-attacks

Upadhyay, I. (2020, October 20). MAC spoofing Attack: All you need to know in 6 important points. Retrieved May 5, 2021, from https://www.jigsawacademy.com/blogs/cyber-security/mac-spoofing-attack/#What-is-MAC-spoofing-and-why-is-it-done?