William Adoukonou

[Company name]  [Company address]

Ethical Hacking assignment

Contents

[Introduction 2](#_Toc167265196)

[Task 1 - Create a short portfolio to analyze reflect attacks and hacking techniques 3](#_Toc167265197)

[Recent Attacks 3](#_Toc167265198)

[Common hacking techniques 4](#_Toc167265199)

[Malware 4](#_Toc167265200)

[DDOS/ Distributed Denial of Service attacks 5](#_Toc167265201)

[Social Engineering 5](#_Toc167265202)

[How to combat these threats 7](#_Toc167265203)

[How PlayStation could have combatted the attack 8](#_Toc167265204)

[How to combat Malware Attacks 8](#_Toc167265205)

[How to combat DDoS Attacks 8](#_Toc167265206)

[Task 2 - Deploy A virtual machine 9](#_Toc167265207)

[Step 1 –Microsoft Azure home Page 9](#_Toc167265208)

[Step 2- Virtual Machine Home Page 9](#_Toc167265209)

[Step 3 – Configuration Page for the Virtual Machine 10](#_Toc167265210)

[Alternative Virtual Machine Creation Tool 12](#_Toc167265211)

[Creating and naming the system 12](#_Toc167265212)

[Selecting the Virtual Hardware 13](#_Toc167265213)

[Server Fully set up and running 14](#_Toc167265214)

[Task 3 – Deploy a 2nd and 3rd virtual machine 15](#_Toc167265215)

[Step 1 – Configure VM settings 15](#_Toc167265216)

[Step 2 – enable communications on each virtual machine 16](#_Toc167265217)

[Testing Log 17](#_Toc167265218)

[Attack 1- Phishing attack 18](#_Toc167265219)

[Combat Social Engineering attacks with employee training 22](#_Toc167265220)

[Attack 2 – ARP Poisoning using Ettercap 23](#_Toc167265221)

[How to combat sniffing attacks 25](#_Toc167265222)

[Conclusion 26](#_Toc167265223)

# Introduction

A cyber security company called Cyber R Us has asked for assistance in investigating the security implications of designing a financial platform for users to send money all around the world. To complete this I will firstly create a portfolio create a short portfolio to analyze reflect attacks and hacking techniques, these will be based on 2 different attacks that are familiar in the cyber security space to help the client understand what happened. I will also include some countermeasures which the companies who were attacked could have used to prevent the amount of damage caused. This is useful as it shows Cyber R Us as well as the financial company the various procedures required to deal with any cyber threat.

The second task will be for me to deploy three virtual machines. I will also provide a summary of the configuration steps on the server and client. To help the client understand the process, I will Include step-by-step screenshots with reasoning for my design choices. Taking a more realistic approach, I will also demonstrate 2 attacks which I feel the company could easily fall victim to whilst critically reflecting on the countermeasures and prevention mechanisms that can be applied.

# Task 1 - Create a short portfolio to analyze reflect attacks and hacking techniques

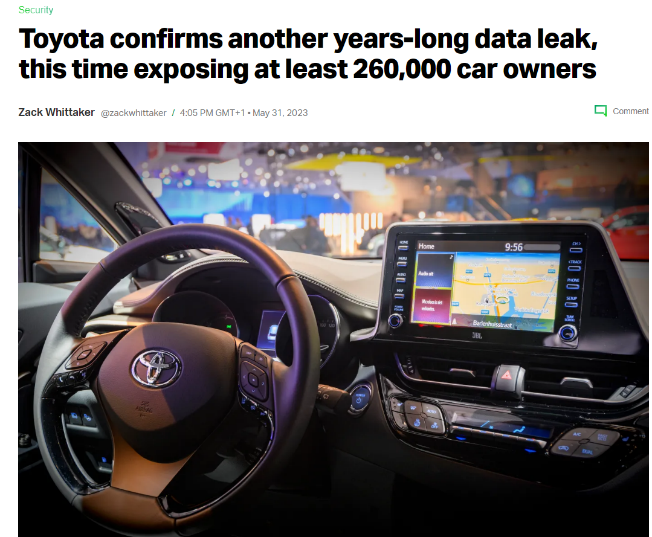
## Recent Attacks

More and more companies are falling victim to cyber-attacks as cyber criminals are becoming more and more advanced with the ways they gain access to your system. A poorly secured command line prompt can allow hackers to get access to things such as a person’s IP address and current network status. The infamous PlayStation Network Hack (2011) and the Toyota Data leak (2023) are two good examples of what hackers can achieve once they have access to key information about your system. Arcserve says that 39 % of businesses experienced a data breach last year and 40% of the data was sensitive info (passwords, banking details etc.). *(Arcserve, 2023)*. Cyber R Us can easily fall victim to either of these attacks which would be worse since they handle banking and payment information from all their customers.

A newspaper with a person walking in front of a door

Description automatically generatedWhat exactly happened in the PSN hack? Around 77 million PlayStation users logged in to notice their accounts were compromised. As well as accounts, banking information may have also been included in the data. *(WSSwired, 2021).* They then had to announce that they had a net loss of around $140 Million which was the greatest loss for a company due to a cyber-attack at the time. Worldwide news of the attack spread, causing various newspapers to publish articles on the event, further damaging their reputation.

*Figure 1, Newspaper Article alerting the public about the hack*

In terms of the Toyota Hack, It was caused by an incorrectly configured cloud storage location, allowing hackers to steal the vehicle information of around 200,000 users. Data such as “In-vehicle device ID, map data updates, updated data creation dates, and map information” were externally accessed *(CSOonline, 2023)*. Despite not releasing the figures of the financial damage they ensured, it’s safe to say they would have received: reputational damage causing them to lose customers, extra costs to increase their security and fines due to the violation of certain data laws.

*Figure 2, web article on Toyota hack, TechCrunch, 2023*

## Common hacking techniques

### Malware

A screenshot of a web page

Description automatically generatedMalware is simply malicious software that is designed to cause harm to a computer system. There are many versions of malware such as Viruses, Trojans, and WORMs but an organization like Cyber R Us is more likely to fall victim to something called ransomware. This is when hackers gain access to the system and lock the user’s files behind a paywall to release them. This was the case with the National Health Service (NHS) in 2017 with the infamous ransomware attack named “WannaCry”.

*Figure 3, web article on WannaCry damage, nhe, 2018*

### DDOS/ Distributed Denial of Service attacks

A screenshot of a website

Description automatically generatedWhen data traffic goes through a network, it is sent in packets. The aim of a DDOS attack is to flood it with traffic by using “fake” packets. This slows down performance on the site and if it is more than the network can handle, it will crash. This doesn’t seem very harmless for the average person as it can be solved with a reboot after a certain amount of time but imagine Cyber R US has customers who rely on their services for day-to-day activities. This was the case for six American banks in March 2012

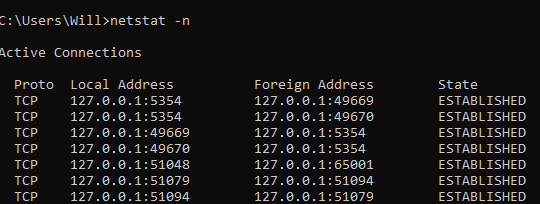
*Figure 4, A10 networks large DDoS attacks report, 2022*

### Social Engineering

A diagram of a computer virus

Description automatically generatedThis is by far the most dangerous example of physical cyber threats. This is because it relies on how each person would react in the situation. Social engineering simply means using standard “social techniques” to gain unwanted information for someone. To make matters even worse, there are many examples of social engineering which work on different users.

*Figure 5, spear fishing explained, medium.com, 2021*

As mentioned before, hackers can take advantage of the Command Prompt in windows to execute lines of code which can reveal information about a system. One of the most useful things hackers can look for is a computer's IP address. This is essentially like your home's street address. It's an ID that helps computers find and talk to your specific device. Hackers can obtain an IP address by first establishing a direct connection with the victim, then using the “netstat -n” command to reveal the IP of the connected devices. Here is an example:

*Figure 6, netstat –n command on a local machine using CMD*

In figure 3, I have entered netstat -n which then returned the local and foreign addresses of each active connection on the system. It also shows weather the connection is established or not

Another way of achieving this is through the nslookup command. Nslookup can find the real address (IP address) behind a website name, or it can do the opposite and figure out the website name connected to a specific IP address. Here is an example:

A screenshot of a computer

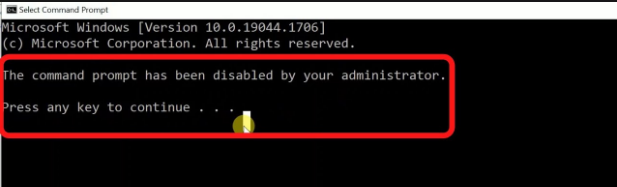
Description automatically generated

*Figure 7: used CMD to look up IP address by ‘nslookup’ command*

In figure 4 I used nslookup to reveal the IP address of the system, I then entered my target website (youtube.com) which then revealed the IP of that website.

## How to combat these threats

Despite how easy it is for hackers to gain access to your system via Command Prompt, there’s a few simple tricks to avoid this happening. The first technique used is to disable the command prompt on the system. Let's say Cyber R Us wanted to secure their company systems, all they would have to do is follow a simple guide in the administrator settings which would disable all commands from running in CMD.

In the image, the Administrator has disabled CMD for the system. This means staff cannot enter any commands into it and the window immediately closes.

### How PlayStation could have combatted the attack

Since the PSN hack was directed at the network, one technique they could have used was an intrusion detection system device. An IDS monitors the traffic on the network for any suspicious activity. An IDS could have identified the attack earlier, allowing Sony to react faster and maybe prevent the breach of millions of user's data. They could have also used regular security audits. All they would have to do is regularly assess the security posture of their systems by ethical hackers or security professionals to identify vulnerabilities before attackers exploited them.

### How to combat Malware Attacks

The most severe external threat mentioned was Malware. It can singlehandedly destroy a business financially, reputationally, or even operationally. Therefore, it’s crucial that every business that holds any type of secured data needs to invest in a good Anti-Virus. They work by performing system scans on every directory, searching for any files that seem out of place. If a file is found, it alerts the user and gives them the option to “quarantine” and then delete the file. Some examples of good antiviruses include Avast, Malwarebytes and Norton365.

### How to combat DDoS Attacks

For networking threats, the worst threat was a DDoS Attack. this Is because it has the most operational impacts. If Cyber R Us’ services are offline. They can’t profit from any transactions because nobody can access the site. This is where it becomes important for to invest in a firewall. Firewalls set a controlled barrier around your connection to the internet. Every inbound and outbound connection must be accounted for. This a good prevents viruses from automatically sending information to and from your computer system over the internet.

# Task 2 - Deploy A virtual machine

## Step 1 –Microsoft Azure home Page

A screenshot of a computer

Description automatically generated*(figure 9 Microsoft azure homepage)*

In this screenshot the Microsoft azure portal is being shown. This is the where the user has options to create and deploy a virtual machine.

## A screenshot of a computer Description automatically generatedStep 2- Virtual Machine Home Page

*(figure 10 Microsoft azure virtual machine page)*

In this screenshot the Microsoft azure virtual machine page is being shown. This is the where the user has options to add a virtual machine to their current list. They can also manage their current machines and diagnose any issues.

## Step 3 – Configuration Page for the Virtual Machine

A screenshot of a computer

Description automatically generated

*(figure 11 Microsoft azure config page)*

This screenshot is from the configuration page for the virtual machine. It allows you to set the specifics for your virtual machine, including the level of security, the virtual hardware included and the operating system it will run on. Here is the full configuration for the virtual machine I made

A screenshot of a computer

Description automatically generated

## Alternative Virtual Machine Creation Tool

A screenshot of a computer

Description automatically generatedDue to constraints with the hardware available at Cyber R Us, I was unable to use Microsoft Azure to create a virtual machine. Fortunately, there was an alternative option to use Oracle VM VirtualBox to create a Windows 2019 Server. Here is what the main interface looks like:

### Creating and naming the system

A screenshot of a computer

Description automatically generated

### Selecting the Virtual Hardware

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

### Server Fully set up and running

A screenshot of a computer

Description automatically generated

A screenshot of a computer

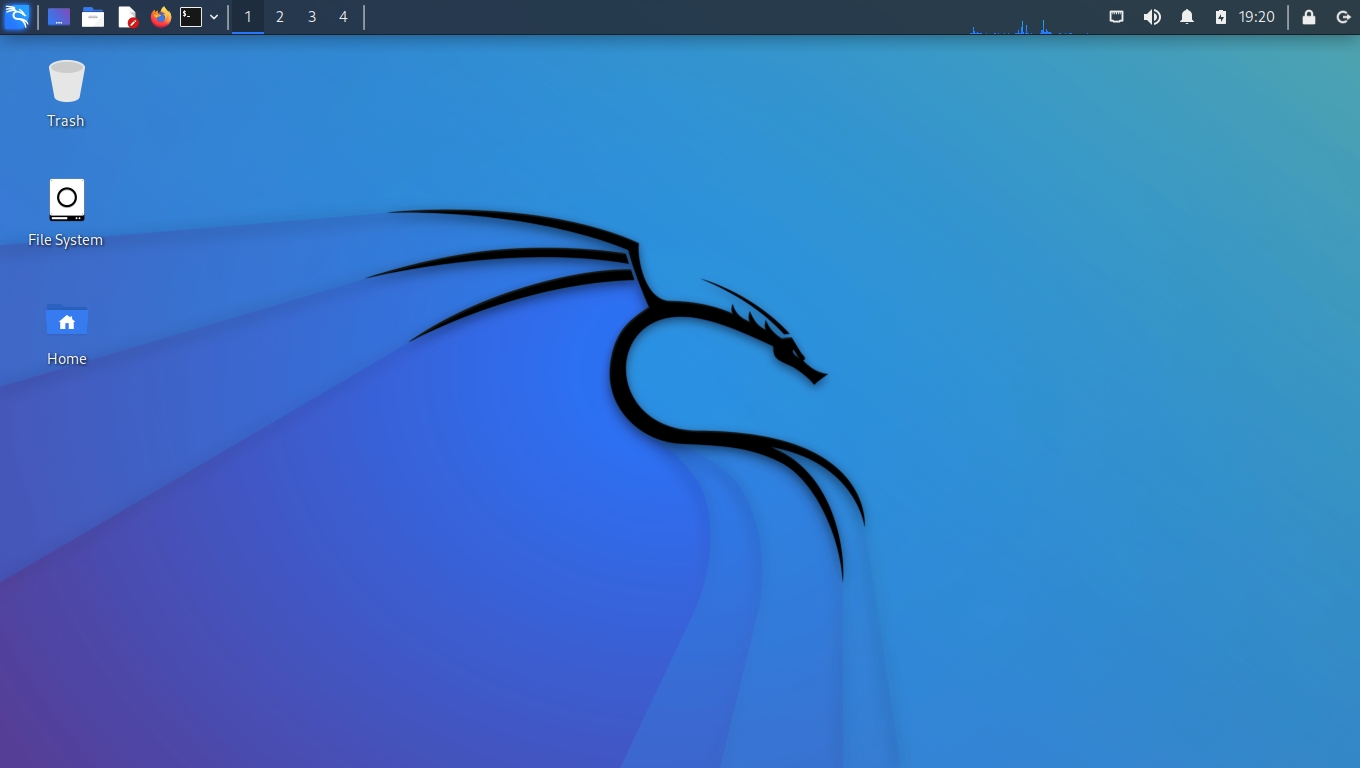
Description automatically generated

As you can see from image above, the virtual machine is active and on the windows 10 desktop. Now we need to create an additional machine to be able to communicate with the 1st one

# Task 3 – Deploy a 2nd and 3rd virtual machine

The steps from task 2 have been repeated in order to create 2 more virtual machines. Through some configurations, we can get 2 of them to communicate with each other.

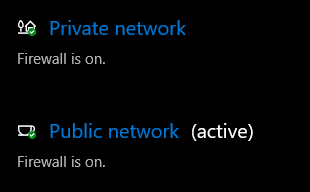
## Step 1 – Configure VM settings

Repeated task 2 process for a Kali Linux Machine

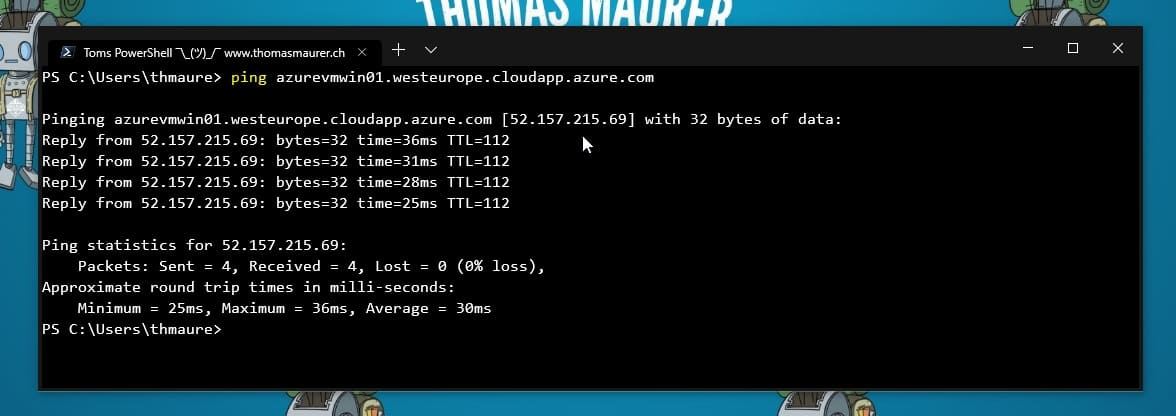
## Step 2 – enable communications on each virtual machine



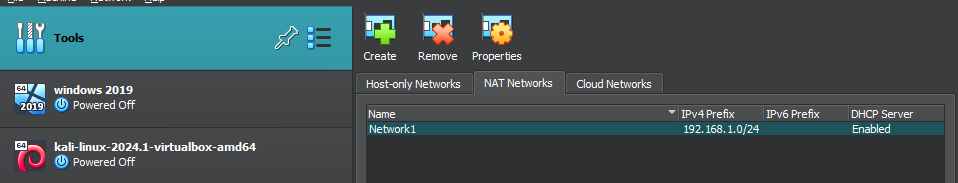
Press windows key and search for firewall

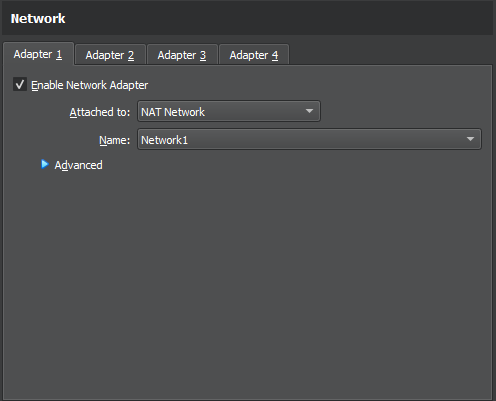


Click on private and public network and disable them both. Repeat the same steps on the 2nd virtual machine.



Using PowerShell, type “ping [virtual machine name]”

This screenshot shows the network created in VirtualBox. Any virtual machines can now be connected to the network called Network1 using the tab in the VM settings.

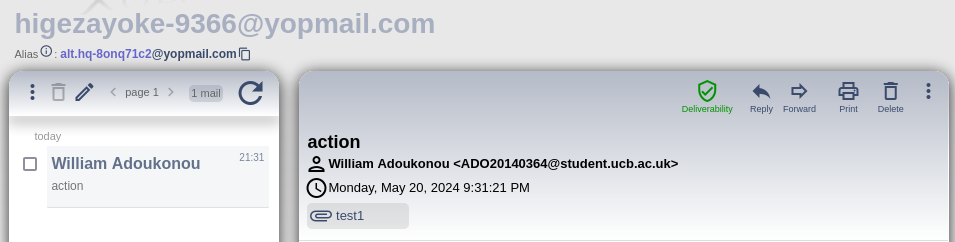


As you can see in the screenshot above. The Kali Linux server is now using adapter 1 to connect to the network that was just created with the prefix 192.168.1.0

# Testing Log

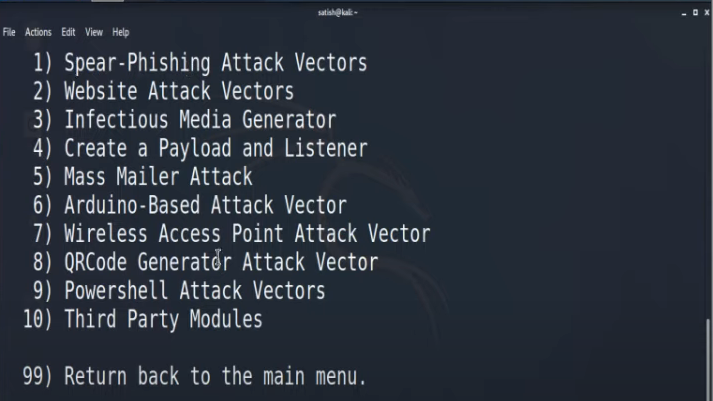
|  |  |  |  |
| --- | --- | --- | --- |
| Attacks Detected | Attack Nature | attack origin | Damage caused |
| Phishing Attack | High Risk, Medium Detection | HTML file on attacker machine. Made using SEToolkit | All emails and passwords entered will be harvested |
| Sniffing Attack | High Risk, Very Low detection | ARP packets being flooded from attacker machine | All traffic can be seen by hacker |

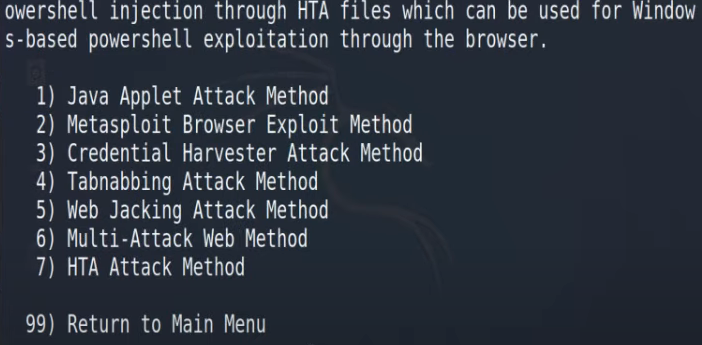
## Attack 1- Phishing attack

Using an application on Kali Linux machine called Social Engineering Toolkit, I was able to create a small file that can be sent to the victim machine via email. Once installed it will allow the user to login to a website, however the credentials entered will be stolen and saved on the attacker machine in a separate file. Here is how I achieved this.

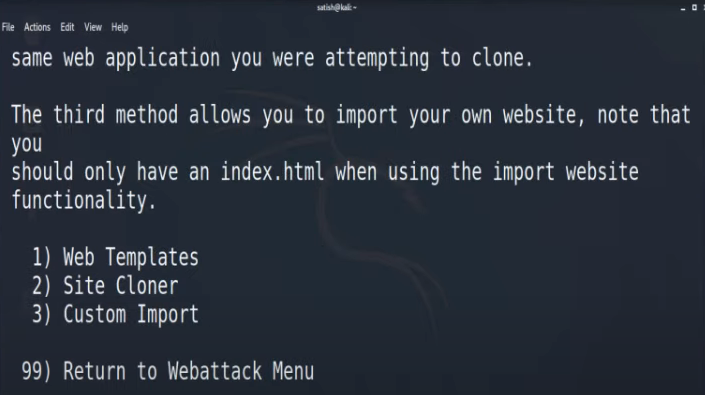


Here we have the interface for the app. Since we want to perform a social engineering attack, we need to press 1.

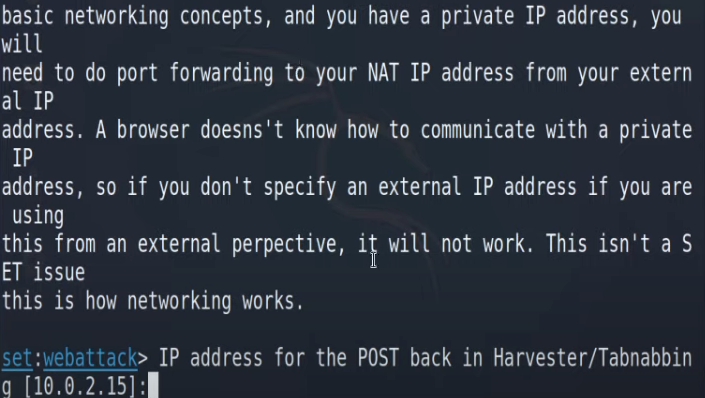
We are now taken to this menu which shows several methods of Social Engineering. The one needed for a password harvester is option 2.

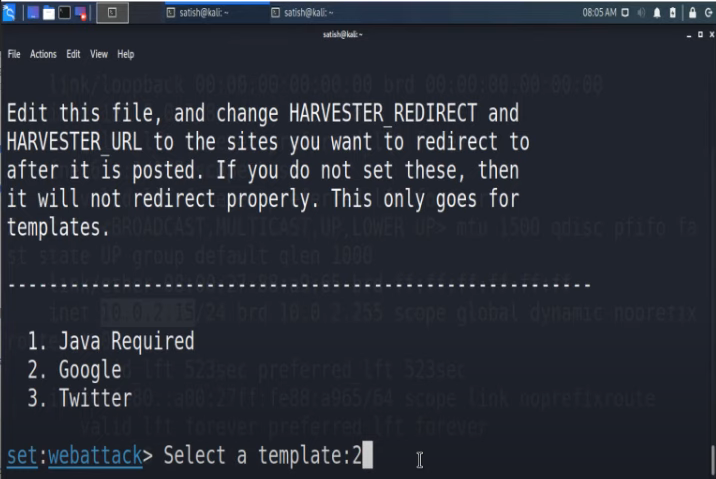


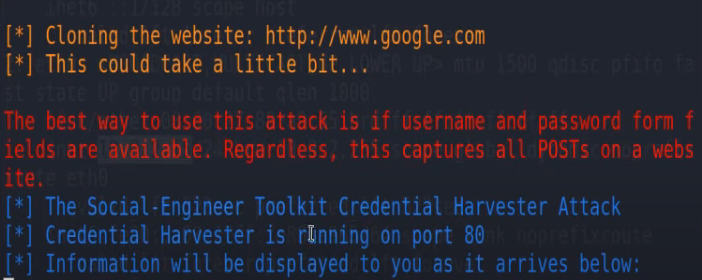
Now we have selected the website specific attacks, we need to enter option 3 for the Credential harvesting method.



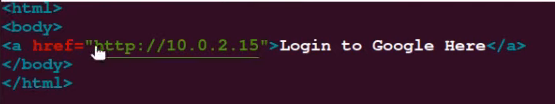
After this we get the choice of how we want to use a custom site, whether it is cloned from another site or a basic template. For this we need option 2.

The user now needs to enter the IP address of their machine to connect their computer to the malicious site.

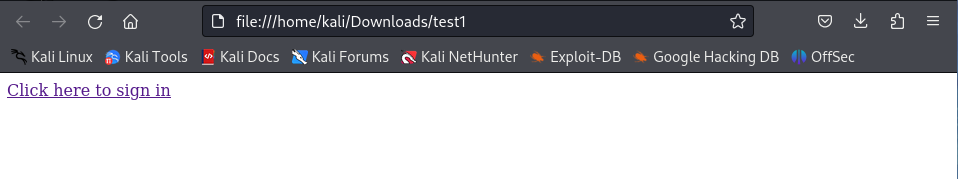
This is where the user decides what template the site should have. For this test I have chosen to use Google.



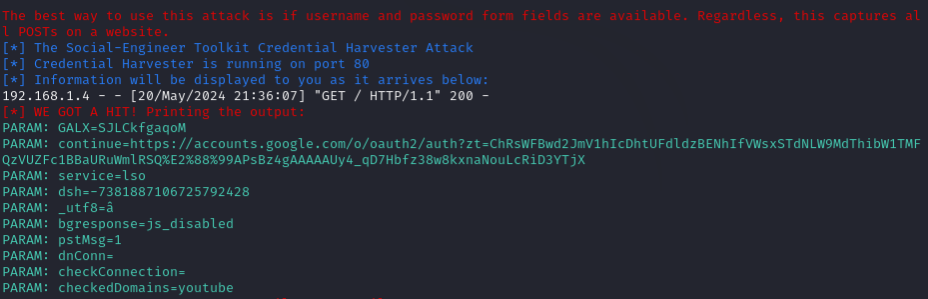
The harvester is now configured and is waiting for hits of data when a user connects to the IP address.

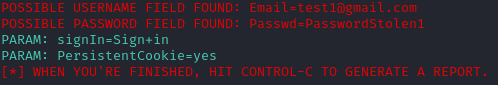


To make the attack more advanced, you can enter the link into an HTML file and send it as an email, further reducing suspicions.

When the victim on the 2nd machine downloads and opens the file in the email shown earlier, they are presented with this link.

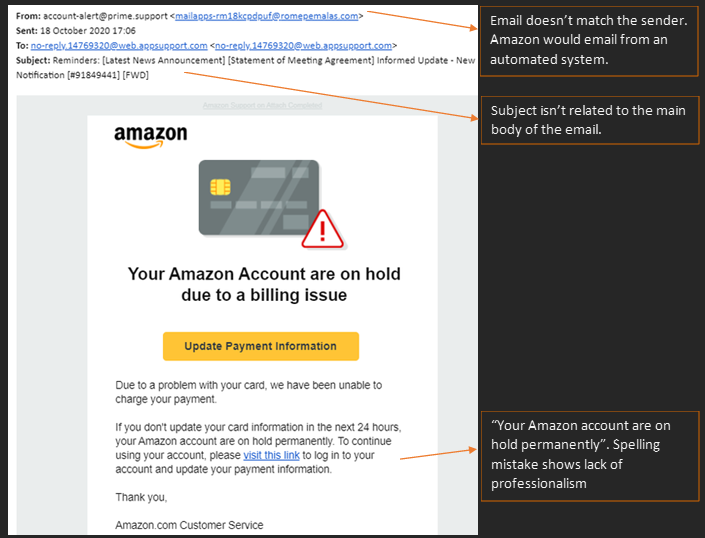
They are then taken to (what looks like) the Google sign in page. Anything they type in here will automatically be stolen and saved.

The harvester has found the connection to the other machine and gotten a hit on the data entered the file.

  
It has found the entries and saved them for the attacker.

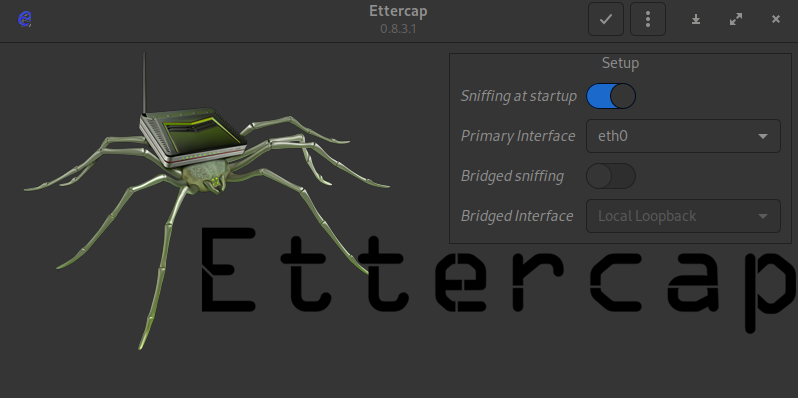
### Combat Social Engineering attacks with employee training

Cyber R Us employees need to be more aware on the tell-tale signs of a phishing attack. Most hackers make small errors when contacting the victim that all employees need to be able to pick up on quickly. Here is an example of a phishing email that any one of the employees could receive.

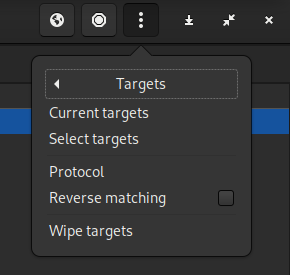
Most of these scam emails share the same traits but training Cyber R Us staff to be vigilant about them can prevent the company from losing their reputation and many of their customers.

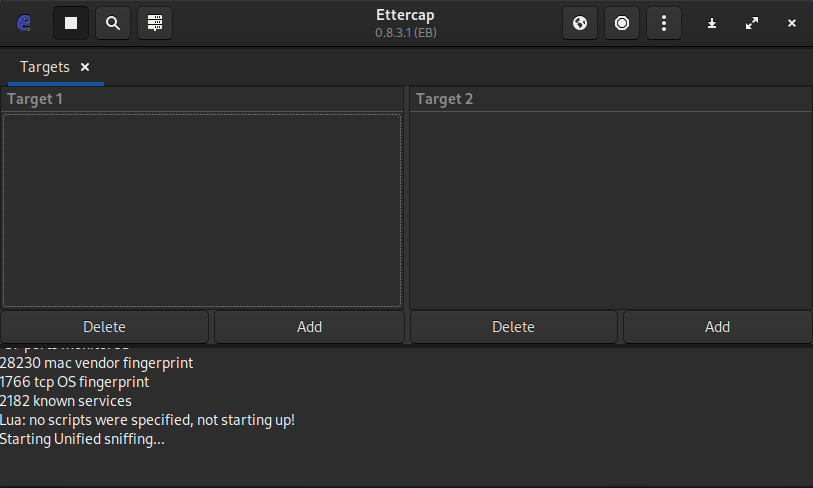
## Attack 2 – ARP Poisoning using Ettercap

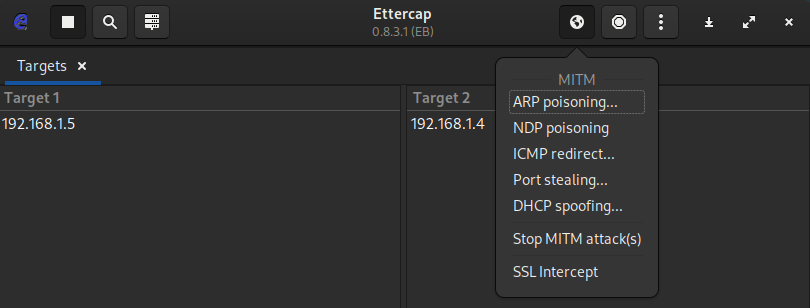
Using another program on Kali called Ettercap, I was able to insert data traffic into another system's network traffic to do a similar job as SEToolkit



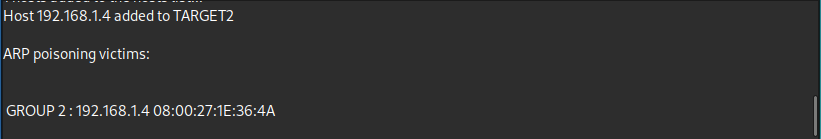
This is the Ettercap interface; to begin we just need to set the primary interface which is already configured and press the tick at the top.

It then takes us to the main page where we go to the top right and click targets, then click current target.

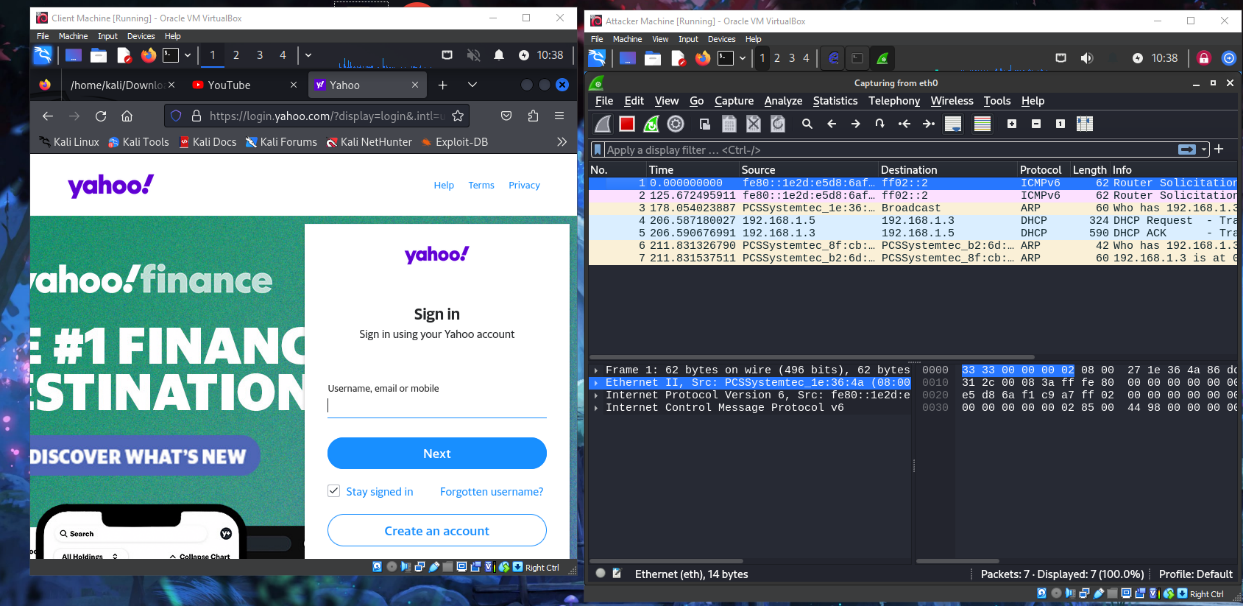
Now we are on the target page, we need to press add target for 1 and 2. Target one will be our IP address which is 192.168.1.5. Target 2 will be the victims IP address which will be 192.168.1.4

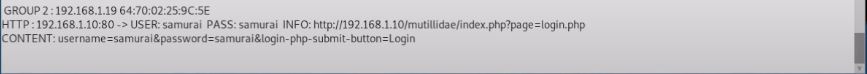


Now the target has been identified by Ettercap, we can begin with the ARP poisoning. This will flood the victims' network traffic with data using the ARP protocol and allow us to view their current network traffic.

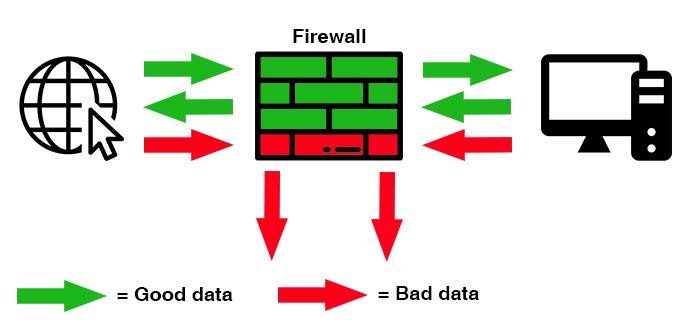
Feed now shows ARP poisoning is live and actively working. To measure this, we need to use a program like Wireshark which allows us to monitor traffic on any given network. Now when the victim makes any interactions with the network, we can spy on it through the attacker machine.

As you can see in the image. The client machine is trying to log onto yahoo.com. The attacker machine is on Wireshark where we can see malicious ARP packets being entered in.



With the use of a file sent to the Victim that requires a login (as seen in Attack 1 with Google clone), the attacker would be able to see the username and password entered the fields. Here is an example of what that would look like.

### How to combat sniffing attacks



*(Figure 12, demo of a firewall, ohsoit.co.uk, 2018)*

Sniffing attacks affect everyone. A researcher says he cracked 70 percent of neighbourhood Wi-Fi passwords using this method *(okta, 2022).* Networking threats have the most operational impacts. This is where it becomes important for them to install a firewall. Firewalls essentially set a controlled barrier around your connection to the internet. Every inbound and outbound connection must be accounted for. This provides a good layer of security to prevent viruses from automatically sending information to and from your computer system over the internet. It works by letting the user select what ports they want to block traffic from so not every form of connection is blocked.

It's also important to set up a VPN when specifically working with sniffing attacks. A VPN or Virtual Private Network works by taking the traffic from your device and the network and routing it through a discrete tunnel. This means anything in the tunnel like web traffic and your IP address is hidden from 3rd parties such. A hacker wouldn’t be able to target you since they wouldn’t have an address to identify where your traffic is coming from. The one tradeoff is that the connection speed is lowered since the traffic must travel further.

# Conclusion

This assignment has provided an advanced understanding of security threats that are crucial for a financial company developing a platform for international money transfers. By analyzing reflection attacks, Cyber R Us helped gain valuable insight into how attackers can exploit network weaknesses. The money transfer platform would benefit from this as they can prevent attackers from intercepting sensitive user information or manipulating transactions.

Using virtual machines gave me the chance to use a safe environment to explore tools commonly used by attackers such as SE Toolkit and Ettercap. SEToolkit on Kali Linux was just a very basic example of what hackers have available to create more chaos. Understanding these techniques allows Cyber R Us as well as the financial company to implement robust user education and authentication protocols to protect their customers from social engineering scams which are prevalent in the finance industry. Ettercap showed the need for securing network communication channels. By implementing strong encryption and access controls, you can ensure that money transfers are safe.

*References*

Arcserve. “7 Most Infamous Cloud Security Breaches.” *Arcserve*, 13 July 2022, www.arcserve.com/blog/7-most-infamous-cloud-security-breaches.

c0d3x27. “Spear Phishing and Subdomains Takeover.” *Geek Culture*, 12 Nov. 2021, medium.com/geekculture/spear-phishing-and-subdomains-takeover-a8f7086a6244. Accessed 22 May 2024.

Garcia-Alvarez, Diamond. “The 2011 PlayStation Network Hack – What Actually Happened?” *Wsswired.com*, 1 Oct. 2021, wsswired.com/4837/entertainment-3/the-2011-playstation-network-hack-what-actually-happened/.

METRO NEWS. “SINKING PLAYSTATION3 TORPEDOED AGAIN – by SONY’S OWN TECHNICAL INCOMPETENCE. 77 MILLION LIVES RUINED by IGNORANCE» UK RESISTANCE.” *Metro.co.uk*, 2012, ukresistance.co.uk/2011/04/sinking-playstation3-torpedoed-again-by-sonys-own-technical-incomptence-77-million-lives-ruined-by-ignorance/. Accessed 22 May 2024.

Morton, David. “What Is a Firewall? Why Does My Business Need a Firewall?” *Ohso Technical - IT Support Services in London*, 12 Nov. 2018, ohsoit.co.uk/what-is-a-firewall/. Accessed 22 May 2024.

National Health Executive. “WannaCry Cyber-Attack Cost the NHS £92m after 19,000 Appointments Were Cancelled.” *National Health Executive*, 12 Oct. 2018, www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled.

Nicholson, Paul. “5 Most Famous DDoS Attacks | A10 Networks.” *A10 Networks*, 21 Jan. 2022, www.a10networks.com/blog/5-most-famous-ddos-attacks/.

Okta. “Sniffing Attack: Definition, Defense & Prevention | Okta.” *Www.okta.com*, 21 Apr. 2021, www.okta.com/identity-101/sniffing-attack/.

Techcrunch. “Toyota Confirms Another Years-Long Data Leak, This Time Exposing at Least 260,000 Car Owners.” *Techcrunch.co.uk*, 31 May 2023, techcrunch.com/2023/05/31/toyota-customer-data-leak-years/?guccounter=1&guce\_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce\_referrer\_sig=AQAAAGGiM14yLOVMcMDb0oQz30NBaNb1eJ4DX\_vW-QI2-3bVxzTlRHeO9oJDplQ6EjH2RpPJm4nkLXFAPpDTdJIqEB4\_ZCxiGhHPgCm-sueJu1vgE0VC\_\_nigjhXn9I2zbQjS\_dni6SneOoZJX9VN1NFAfMv1IN6hGf\_-OyvfbMDoQqF.

Venkat, Apurva. “Cloud Misconfiguration Causes Massive Data Breach at Toyota Motor.” *CSO Online*, CSO Online, 6 June 2023, www.csoonline.com/article/575483/cloud-misconfiguration-causes-massive-data-breach-at-toyota-motor.html.