A case study into penetration testing for a virtualised and simulated company website, and research into a cyber security incident and defensive technique case study.

Matthew Cragg
Cyber Security and Networking (of MSc Year 1)
Security Analysis Techniques and Procedures
University of Wales Trinity St.Davids
Swansea, Wales
Student ID 2207432

CONTENTS

I Part One 2
- I-A Introduction 2
- I-B Server Infrastructure 2
- I-C Contingency Plan 2
- I-D Penetration Testing Framework of Choice 2
- I-E Penetration Testing Tools of Choice 3
- I-F Types of Attacks Used 3
- I-G Effects and Details of Attacks 3
  - I-G1 XML External Entity Payload 3
  - I-G2 SQL Injection 4
  - I-G3 XSS Payloads 4
  - I-G4 Direct Denial of Service 5
  - I-G5 Man In The Middle Attack 5
- I-H Recommended Solutions 6
  - I-H1 SQL Injection 6
  - I-H2 Direct Denial of Service 6
  - I-H3 XML External Entity 6
  - I-H4 XSS 6
  - I-H5 Man In the Middle 7
- I-I Cost of Solutions 7

II Part Two 8
- II-A Introduction 8
- II-B Research 8
- II-C Recovery of Files 8
  - II-C1 Metadata 9
- II-D Forensics Report 9
- II-E Invoice 9

III Terminology 9

IV Reference List 9

LIST OF FIGURES

1 An assumed model of the HPC Companies Infrastructure. 2
2 A view at the website that will be attacked. 4
3 Burp Suite's view of the initial POST packet received from the store.. 4
4 The XML Payload that is entered into the POST Packet. 4
5 Burp Suite showing the Request and Response packets between the attacker and host website. 4
6 A dump file of all user names, credit cards and password hashes received in the POST packet. 5
7 The revealed password after being converted from an MD5 hash. 5
8 The SQL code required to select the columns that contain the passwords from the staff_users database. 5
9 A part of the website that was intended to be hidden from view. 5
10 SQL Query that always return true. 6
11 A demonstration of an XSS pop-up. 6
12 A CMD view of various packets being sent at once to a host machine, overwhelming the network. 6
13 Various packets being sent and received from the host machine 'Eve'. 6
14 Kali Linux command for saving TCPDump packets. 7
15 The packets being captured through TCPDump. 7
16 An attacker using Wireshark to monitor traffic through a network. 7
17 A demonstration of the EaseUS Data Recovery Wizard start screen. 8
18 EaseUS Data Recovery Wizard recovering the lost file. 9
19 The recovered documents displayed within the Windows Explorer. 9

***Abstract*—Cyber Security as a concept incorporates a vast variety of tools, ideologies and concepts that all combine with the same intention of minimising loss of data and that information is kept private to only those that are meant to see it. With the proliferation of automation within large companies' and an ever-increasing number of computers are being used to hold sensitive information, Cyber Security is imperative to the longevity of a companies life. With tools becoming more advanced, hackers find it easier to break into company computers by the day, all in the name of financial gain. Therefore, it is crucial for companies to ensure their security and protection is strong and cutting-edge. Penetration Testers are commonly hired by companies with the intention of hacking and breaking through the security systems in place, allowing the flaws to be fixed and security to grow stronger.**

I. Part One

A. Introduction

Every company in the modern day must be prepared for the threat of a cyber attack happening at any moment. While a company may be able to prepare in advance and secure files behind firewalls, secure servers, blocking certain links on employee computers and running daily backups, it can never be enough to truly be impregnable. Attackers are always one step ahead with their tools and penetration software, as they have access to the defensive hardware and software used. This allows them to constantly develop and test their attacks, finding and developing vulnerabilities in industry standard software. Within a company such as HPC, it becomes crucial to maintain both hardware and software to the industry standard, and ensure that a plan is in place should an attack be made on the company. This plan is called the Contingency Plan.

Various attacks will be developed and carried out against HPC's current network Infrastructure with the purpose of finding vulnerabilities and weaknesses. This paper will then detail how each attack performs in detail, and how to prevent the attack from occurring in the future.

Each attack will be treated differently. While no attack will have a 'fix-all' solution, some attacks and solutions may have some overlap. The solutions for the attacks come in the form of both hardware and software, which will be detailed at the end of the report, alongside a total cost.

B. Server Infrastructure

Figure 1, page 2 shows an (Assumed) model of the infrastructure used by HPC. This model was used within all attacks, with the website hosted on the main server alongside the database. An assumed two-hundred and fifty people work on-site at HPC, classifying the company as medium -sized.

C. Contingency Plan

A well-prepared company will have a contingency plan in place at all times. The plan is designed to act as a guide for what should and will happen in the event of something going wrong within the company. Various contingency plans usually follows the same principles, but are usually modified and tailored to each company and their needs.

In the case of Healios Pharmaceutical Company (HPC), a unique contingency plan will be required to be tailored and

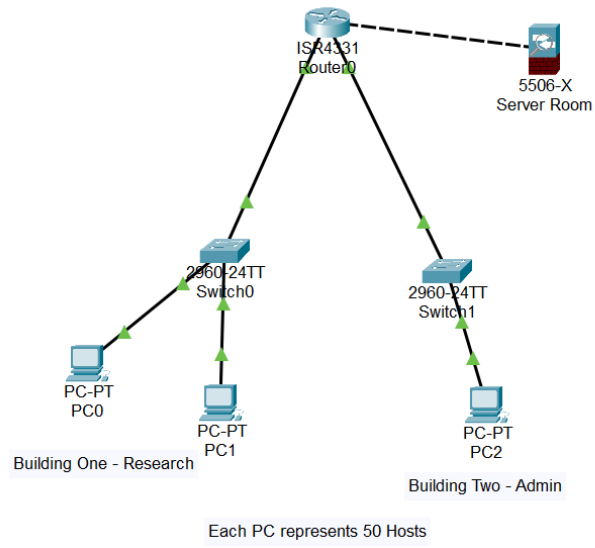

Fig. 1. An assumed model of the HPC Companies Infrastructure.

implemented. While each attack is different, it is vital to ensure the contingency plan remains the same. This is to ensure that the employees know what to do, and every step is prepared for in advance as a precaution that the attack is severer than first thought.

HPC should already be performing weekly, or even daily backups. This reduces the risk of data being lost if there needs to be a rollback due to injected software.

For HPC, in the case of attack, it is vital that all connections in and out of the company are cut. This reduces the risk of the attack from continuing, as most attacks happen remotely. While the connection has been severed, perform an internal back-up of all systems and servers to a local server. This new, separate backup, can be used to compare files and programs with the daily backups. With this comparison, it will be easier to find where the attack came from. The cut connection to the cloud will also prevent loss of intellectual property from being stolen and transferred.

With all the routers, switches, servers and hosts isolated, work can begin on locating the threat. Once found and properly dealt with, surrounding hosts and routers need to be check to ensure that a virus has not spread. Depending on the threat, a mass email or lecture may be required (For example, if the threat came from a phishing link). This reduces the risk of it happening again in the future.

Once the threat has been removed and the vulnerability has been fixed, the company systems can be rebooted and begin to perform as normal.

D. Penetration Testing Framework of Choice

The framework that this document will be following is the regularly-updated and maintained report that focuses upon ten critical threats that companies are required to be aware of, and defend against on a daily basis. The OWASP report lists ten

security risks that are vital to remember and be cautious of when developing a network, or even any form of company.

The risks that OWASP reports are as the following:

- SQL Injection - The most common form of Injection attacks are SQL attacks, also known as Standard Query Language injections. This form of attack occurs when unknown or untrusted data is submitted through fields that often require data input, such as forms.
- Broken Authentication - Login systems are used to validate that the user is who they claim to be. However, this can also be used by attackers to either break the login system either intentionally, or crack a users password to pretend to be another user.
- Sensitive Data Exposure - This form of attack is made when a website or company submits or receives sensitive information such as a users login session, password, username and other information. If the data has not been encrypted, attackers are able to copy the packets being sent and see what information is being sent back and forth.
- XML External Entities - This attack is often abbreviated as XEE. This attack is used against web applications, and attacks to trick the web application into sending data to the wrong device.
- Broken Access Control - This attack is a method used to bypass authorization programs and systems in an attempt to escalate their own privileges, and to access other hidden information or tools.
- Security Misconfiguration - This form of attack is likely the most common and known method of attacking a vulnerable system. It consists of taking advantage of vulnerabilities and settings not correctly configured.
- Cross-Site Scripting - This method of attacking is used by inputting custom code into a URL path that can be visible to customers or users. This can place false trust into the users, and may click on the link thinking that it is an authentic link, when it is actually fake.
- - Insecure Deserialization - Serialization is a term used by web applications taking objects from code and converting them into another format that may be used in another purpose. This attack is used to access the objects, and attackers can add or change information.
- - Using Components with Known Vulnerabilities - Most applications, browsers and websites are built using many various libraries and frameworks. These are used to assist developers in not repeating the same task over and over to build a new button on a website, for example. This however can have consequences when libraries or frameworks have a vulnerability in the code that attackers know, and can abuse when the website is live.
- Insufficient Logging and Monitoring - Logging is the term used to monitor activity within an application. If a website has been attacked for example, and there is no logging system in place on the server, then the company will have no way of knowing when exactly the attack happened, and will struggle to investigate further.

E. Penetration Testing Tools of Choice

- CMD - Command Prompt.
- Crackstation.
- Google Chrome.
- Gruyere.
- Burp Suite.
- Wireshark.
- Kali Linux.
- Ettercap.
- TCPDump.

F. Types of Attacks Used

Following the OWASP framework, four attacks were deployed onto the network. The following attacks were used:

- SQL Injection.
- XML External Entity Payload.
- XSS Cross-Site Scripting Payload.
- DDOS.
- Man In The Middle Attack/ARP Spoofing.

G. Effects and Details of Attacks

1) XML External Entity Payload: According to tryhackme.com, [1] 'XML (eXtensible Mark-up Language) is a mark-up language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. It is a mark-up language used for storing and transporting data.' This allows XML to be used on any system and any language, and can simplify data sharing between devices and systems.

This, however, makes it incredibly useful for attackers. If an attacker is able to deliver a payload of their own XML, they are able to change data as they see fit.

In the attack, a store front is accessed. In the figure below, a simple listing for inflatable darts are shown. When the request is made for the available stock to be shown, the POST request is captured by Burp, a program designed and created for performing security tests for websites.

When the POST protocol request is made, it becomes visible within Burp. This can be seen in figure 3, page 4. This packet allows the HTML code to be changed, and then sent back to the website with the following changes in figure 4, page 4.

The productID is also changed to '&xxe;'. This code is placed between the XML declaration and the stockCheck element. This requests the passwd file from the website when the request is sent back.

After accessing the website password files through Burp Suite, the next logical step for an attacker will be trying to decrypt the passwords. Most records are held within SQLite, and the passwords are usually hashed using a method called MD5 Hash. MD5 is a hashing algorithm that used to be commonly used to decrypt passwords and other sensitive information. It has since been broken and decrypted, rendering the MD5 hashing algorithm useless within a security environment.

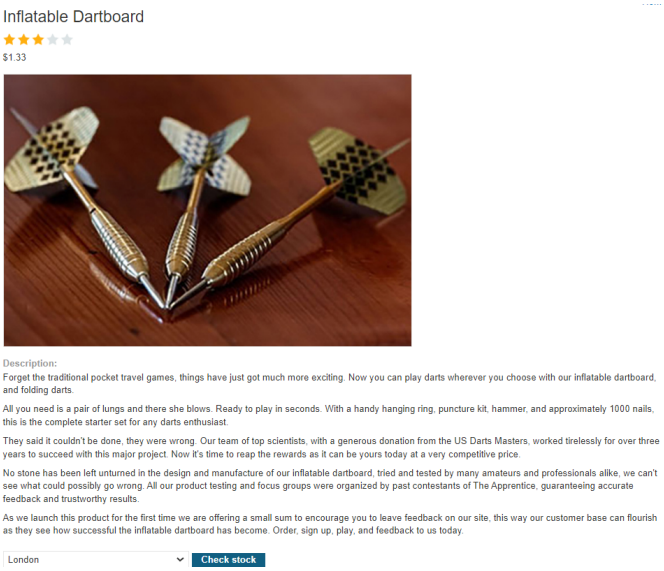

Fig. 2. A view at the website that will be attacked.

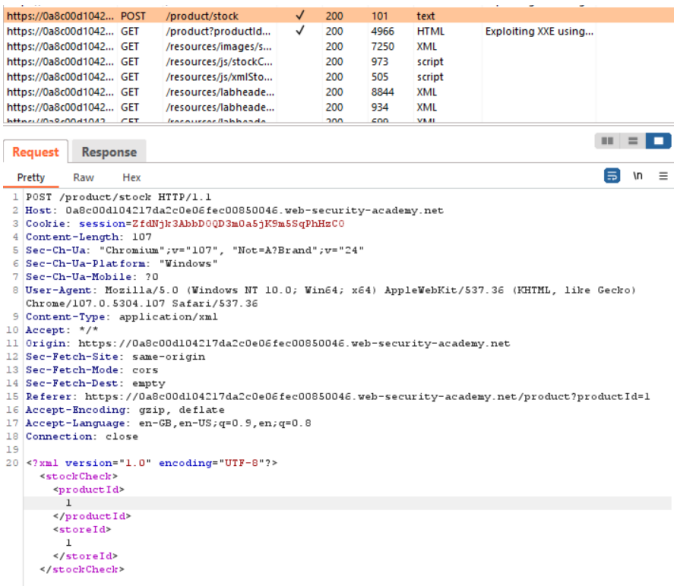

Fig. 3. Burp Suite's view of the initial POST packet received from the store..

Consequently, hashing algorithms such as Argon2 and Bcrypt are instead used by professionals.

After downloading the POST packet locally, the entries for employee names, credit cards and passwords in MD5 hash codes are on display, shown in figure 6, page 5.

SQLite is a library used by developers to embed within their applications. This creates a database that allows developers to store and hold information within a database for use within their applications.

From the entries, the following can be determined. The employee name, credit card and password. While the password is encrypted, a tool called Crackstation can be used to decrypt the password and return the true password in plain text.

With the password successfully cracked and now in plain

```
<!DOCTYPE test [ <!ENTITY xxe SYSTEM
"file:///etc/passwd"> ]>
```

Fig. 4. The XML Payload that is entered into the POST Packet.

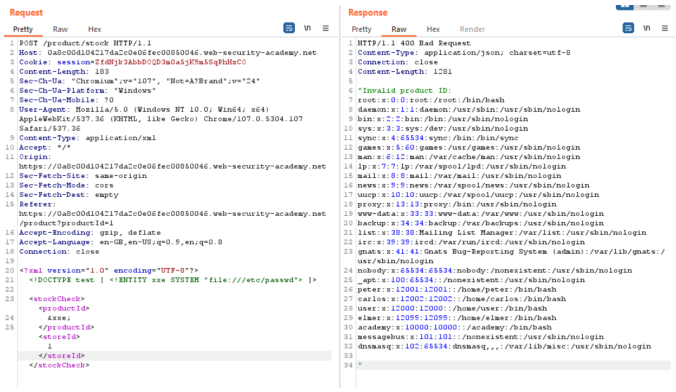

Fig. 5. Burp Suite showing the Request and Response packets between the attacker and host website.

text, shown in figure 7, page 5, the attacker is easily able to login using the victims name and password, which is 'password'.

When the changes are returned to the website, the request file is returned and displayed on the right, showing the contents of the passwd file.

2) SQL Injection: To begin, the first attack deployed will target the database of the main server. This is used in an attempt to gain access to all employee usernames and passwords or enter websites usually hidden from public view. This is done through a method called SQL Injection by entering code that is usually reserved for database entries, through the website URL or other forms on the website. These forms can include login pages, post submissions or anywhere else that a user may enter text, numbers or any other form of information.

All databases contain information and data used by websites and other applications, such as passwords and usernames. But this can also extend to the ID numbers of websites, and a developer can hide a website through the database.

In figure 9, page 5, a website is shown with an article on display. Using the SQL code in figure 8, page 5 at the end of the URL, the passwords within the staff_users column of the database are displayed.

Within a standard form that uses SQL to verify passwords, it is possible to bypass the authorization fields by entering the code in figure I-G2, page 6.

This SQL query always return true, as 1=1 is a true statement. With the OR operator, this will cause the query input to always return as true, and therefore the password system will consider it a valid password, and allow the attacker to bypass having an actual password.

3) XSS Payloads: XSS, or cross-site scripting is a vulnerability within web applications that are usually deployed by an injection, similar to SQL injections.

```
0|Joy Paulson|4916 9012 2231 7905|5f4dcc3b5aa765d61d8327deb882cf99
1|John Walters|5298 0704 2379 5940|f806fc5a2a0d5ba2471600758452799c
2|Lena Abdul|5575 0248 8055 2348|23003be56f641bf9b1fbe75a851a0340
3|Andrew Miller|4716 3986 3908 1152|4b525fc7a9098015d955968c92947e80
4|Keith Wayman|5324 9581 9808 7840|277f2a7ecb7cfcd264aeb2067fb46df8
5|Annett Scholz|4716 2571 8467 6859|8c728e685ddde9f7fbbc452155e29639
```

Fig. 6. A dump file of all user names, credit cards and password hashes received in the POST packet.

Hash	Type	Result
5f4dcc3b5aa765d61d8327deb882cf99	md5	password

Fig. 7. The revealed password after being converted from an MD5 hash.

XSS injections can come in various different forms. The main three attacks used are,

- Pop-ups - These create a notification within the browser that the user must click to either dismiss or enter.
- HTML Edit - This method of injection changes the content of the HTML where the attacker can change the look and content of what is displayed.
- Keylogger - This injection logs and tracks all the users keystrokes and inputs. This is dangerous when a user is required input their username and password.

A website vulnerable to XSS will appear to be normal to begin with, and only when an attack has been made will the issues become clear.

In this attack, a website called Gruyere will be used to demonstrate the attack, and the fixes can be made to HPC's website after.

In this website, users are able to post 'Snippets', similar to messaging board. This is used within companies such as HPC, who use applications such as Slack and Teams for employees to communicate.

However, if a company has an in-house messaging board, XSS is a dangerous attack. A basic XSS attack looks like the website in figure 11, page 6.

While the snippet appears to just be a link to a cat photo website, the link is fabricated and the blue text displays the pop-up at the top when the mouse hovers over. This is immediately suspicious, but to an untrained eye, they may follow the link within the pop-up to follow the link, which could take them to an injected website.

4) Direct Denial of Service: A Direct Denial of Service attack, or DDoS, is an attack often used by attackers to prevent users from accessing websites, or to shut down a web application. This is often deployed by using multiple hosts at a time to overwhelm a network, rendering it useless for a time.

In the figure 12, page 6, a high packet count is sent to a router constantly over a long length of time, which would prevent other packets of information to be sent or received. This would render the router useless during the time of attack.

5) Man In The Middle Attack: A Man In The Middle Attack (Commonly abbreviated to MiTM) is also commonly known as ARP Spoofing. An ARP is an abbreviation for Address Resolution Protocol. This protocol's primary function is to determine an IP address into a a physical address. This is

```
0 UNION SELECT 1,2,group_concat
(username,'\;',password SEPERATOR')
FROM staff_users
```

Fig. 8. The SQL code required to select the columns that contain the passwords from the staff_users database.

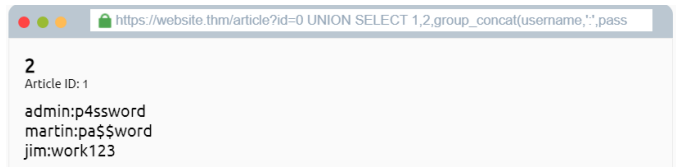

Fig. 9. A part of the website that was intended to be hidden from view.

vital to the function of the internet in the modern day, and is what allows users to transfer data and access websites.

This, however, causes a crucial vulnerability when the protocol is compromised and exposed to attackers. According to Defiana Arnaldy and Audhika Rahmat Perdana from the article 'Implementation and Analysis of Penetration Techniques Using the Man-In-The-Middle Attack', [2] "The process of doing penetration testing using the MITM method results in an 85% success rate for finding security holes or vulnerabilities when testing using sniffing techniques." This statistic originates from using various forms of attacks, including SQL injection, brute force, sniffing and XSS. Only XSS failed with a 45% success rate, whereas the other forms of attacks achieved 75% or higher.

A MiTM attack is created when an attacker 'sniffs' a network for incoming or outgoing traffic. Sniffing in this context is the term used for monitoring and watching traffic on a network. When a vulnerable packet is identified, an attacker is able to intercept the packet. With the packet in the attackers possession, they are able to modify, view or copy the data within, similar to the attack made in Burp Suite earlier in the paper. Once the attacker has finished with the packet, they are able to send the packet to continue its route, finally reaching the original destination. At this point, neither the sender nor receiver will know about the attack.

For this attack, a variety of tools were used to capture packets in transmission. To begin, TCPDump began to sniff the current network for any vulnerabilities. The packets were captured through a vulnerable machine called 'Eve', where the attacker had gained control previously with the other attacks. Figure 13, page 6, shows all the various packets being sent and received as they transmitted. TCPDump also shows the type of packet being sent (In this case, ICMP, or Internet Control Message Protocol, used for instant messaging such as Whatsapp and Facebook.), the length of a packet, and what machine the packets are being sent from, which is a host machine named Bob.

With the packets identified, the attacker is able to capture the packets using TCPDump through the command in figure I-G5, page 7. This command saves all the captured packets, and

```
' OR 1=1;--
```

Fig. 10. SQL Query that always return true.

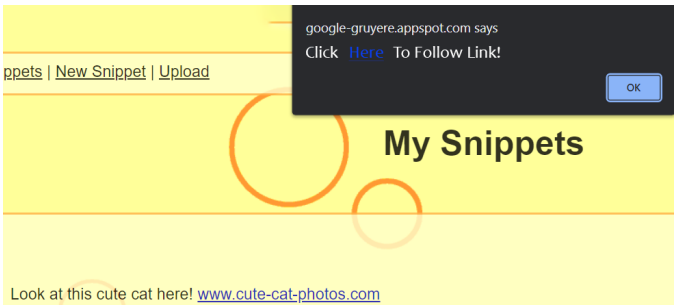

Fig. 11. A demonstration of an XSS pop-up.

allows the attacker to open them within Wireshark.

With the packets captured and saved, Wireshark can be used to further monitor and analyse the packets. From here, a similar form of attack may be made that was introduced in the XML External Entity payload.

H. Recommended Solutions

1) SQL Injection: SQL Injections are used on websites or forms that are unprepared and not configured properly. It is vital to secure the login systems and any in-house forms that may be used to reduce or even possibly eliminate any risk of an SQL Injection from allowing unwanted access.

If the database has been prepared by a developer with input validation, then the form or login page will only allow certain strings, values and parameters. This ensures that no addition data or code can be injected, and only the required type of response may be given. For example, if a question is only asking for a data of birth, it would make no sense to allow special characters or letters, and therefore only allowing numbers to be entered will reduce the risk of any additional code from being added.

Some input characters may break SQL queries as they are used in code to access the database. These characters include ' " $. A developer can either disallow these characters to be inputted by a user, or force the query to add \ before any of the characters. The backslash will allow SQL to parse the character separately from the code, similar to a comment in normal code.

2) Direct Denial of Service: During a DDoS attack, it is advised to change the IP address of the effected device or machine instantly, and other nearby devices within the VLAN. A DDoS attack can be prevented by implementing a firewall between the router and traffic being received. A firewall can provide an additional barrier between the router and attack, and will filter most unknown packets from being sent to the router, lowering the amount of pings being sent drastically.

Additionally, a Virtual Private Network, or VPN, can be used to hide your IP and prevent attackers from locating your IP with ease.

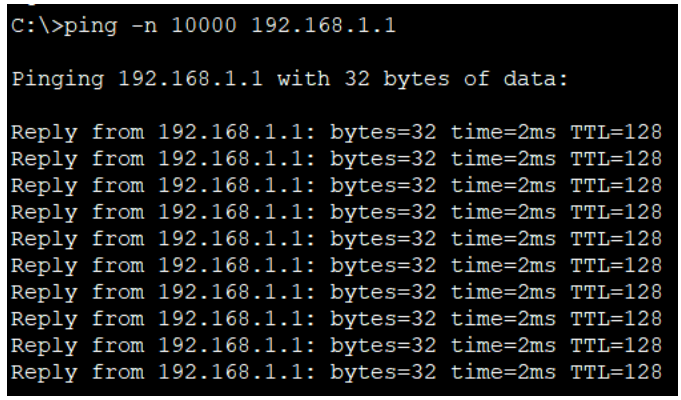

Fig. 12. A CMD view of various packets being sent at once to a host machine, overwhelming the network.

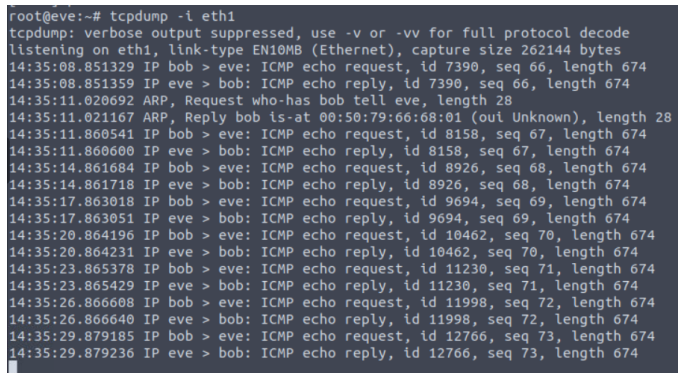

Fig. 13. Various packets being sent and received from the host machine 'Eve'.

3) XML External Entity: According to a website called cheatsheetseries, [3] "The best method to preventing XML injection attacks is to completely disable External Entities entirely." Depending on what coding language is used, there are various functions and methods to disabling External Entities. Disable External Entities also assists in preventing certain denial of service attacks.

4) XSS: Similar to SQL Injection, filtering what a user is able to input within fields can drastically reduce the chances of XSS attacks. Encoding and encrypting data when it is sent out of a users computer can prevent data from being intercepted with programs such as Burp. IBM, an industry giant who deigns and develops AI, Cloud and Enterprise Software, list three practices that will assist companies in being protected by most XSS attacks.

The list comprises of [4],

- "Escape user input. Escaping means to convert the key characters in the data that a web page receives to prevent the data from being interpreted in any malicious way. It doesn't allow the special characters to be rendered."
- "Validate user input. Treat anything that originates data from outside the system as untrusted. Validate all the input data. Use an allow-list of known, acceptable, good input."
- "Sanitize data. Examine and remove unwanted data, such

```
tcpdump -A -i eth1 -w /tmp/tcpdump.pcap
```

Fig. 14. Kali Linux command for saving TCPDump packets.

```
46 packets captured
46 packets received by filter
```

Fig. 15. The packets being captured through TCPDump.

as HTML tags that are deemed to be unsafe. Keep the safe data and remove any unsafe characters from the data."

5) Man In the Middle: Similar to most attacks, it is crucial to prepare for MiTM attacks and prevent them before they occur. However, this is easier said than done, as is most security, as established and dedicated attackers will always find a way.

Having strong WEP/WAP encryption access points on wireless routers and devices can prevent sniffing tools from accessing the packets being transmitted, and will assist heavily on preventing brute force tools.

A VPN, or Virtual Private Network, are used by casual internet users and dedicated companies. VPN's mask the users IP address and location, and can be used to hide where a person may be. This will prevent a sniffing tool from seeing the true destination or origin of a packet.

HTTPS is an advancement of the standard HTTP (Hyper-Text Transfer Protocol.) that ensures a connection between two devices is secure. This is usually done through the use of private key encryption. This protocol validates that the connection is secure and that only the persons intended to see, send and receive the packets are the ones with the correct private key.

I. Cost of Solutions

While the cost of protecting and securing a network may be high, the cost associated with an unprotected network will be greater still. This will come from the constant loss of data as it is taken, the loss of intellectual properties and fines that may be received.

Preparing for the worst is often the best case scenario, with a contingency plan in place and preparations for a fail-safe.

An industry standard server for a medium -sized business can cost anywhere between £4,000 and £10,000. As this is wide range, the following will assume the median for the total cost.

The company will require a second server to act as the fail-safe, to ensure that data is never lost and the connection for employees can remain constant for them to work. A third server will be required to act as a back-up server, where data of the first and second server is copied to every few minutes. This will prevent any major loss of data if a server was to crash, or any attack was launched.

Each router, server and switch will require a firewall tailored to match the devices requirements. Companies often apply

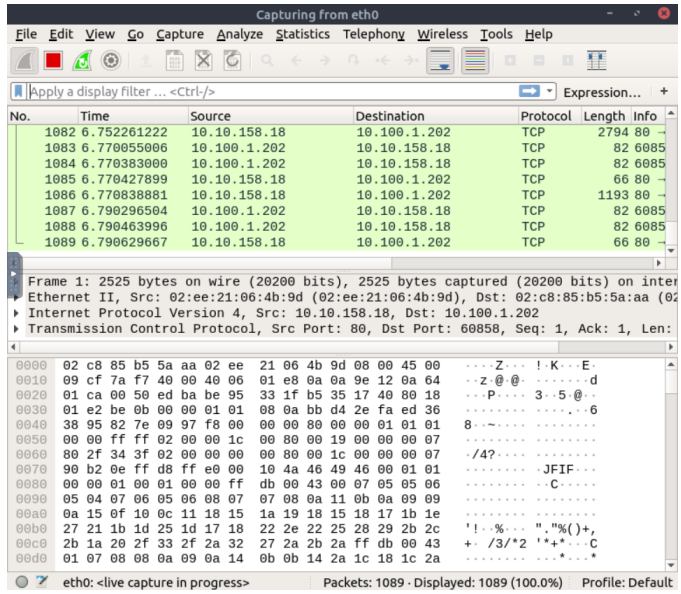

Fig. 16. An attacker using Wireshark to monitor traffic through a network.

multiple firewalls to one network, which is used to segregate various connections for extra protection. According to Alex X. Liu and Mohamed G. Gouda in 'Firewall Policy Queries' , [5] "Serving as the first line of defence against malicious attacks and unauthorized traffic, firewalls are crucial elements in securing the private networks of most businesses, institutions, and even home networks. A firewall is placed at the point of entry between a private network and the outside Internet so that all incoming and outgoing packets have to pass through it." Firewalls come in different grades, much like any piece of technology. These prices can range between £700 for a low-end firewall and £10,000 at the opposite end of the spectrum. An industrial firewall for a company the size of HPC, it would cost approximately £6,000 for a Cisco grade firewall.

A VPN would be rather cheap in comparison to the previous costs, starting at around £500 to £1,000.

The following list comprises of the various items from both the recommend solutions section and contingency plan.

- Cisco FirePOWER 1010 ASA VPN Router - £589.98
- Smart Selection PowerVault MD1420 Server Rack - £22,329.21 (Three racks, £7,443.07 each).
- Cisco ASA 5500-X Series Next-Generation Firewall - £2,782.05
- Penetration Testing and report - £1,110 (Hourly Rate of £27.75 for one week of work).

An estimate of three weeks will be required to set-up the network. In total, the required software and hardware improvements would cost approximately £26,811.24, with the additional cost of a on-site network team to monitor, develop and maintain the network.

All items include VAT. The hourly salary is calculated from the average Network Engineer salary of £41,970 per calendar year.

II. Part Two

A. Introduction

By definition, digital forensics investigations are identical to 'normal' forensic investigations, with the distinction that digital forensics is done through the use of computers and deals primarily with electronic hardware and evidence. Digital forensics is usually done through examination of common computer parts such as hard disks, RAM, and saved files.

In the case of Nera Star and Healios Pharmaceutical Company, discretion and care is required when dealing with sensitive and valuable information such as chemical research and formulae.

B. Research

When data is lost or deleted from a computer's hard disk or external disk, the sectors and bits that were used to display and hold the file's data still remain. The only difference is that the space appears to be empty to the computer's user, and the space may be overwritten in the future when that particular sector of the hard disk is required. Therefore, it is possible for deleted files to be recovered using specialized software, though the fact must be acknowledged that over time, the risk of that particular sector may have been overwritten already. This means that it would be imperative for a computer forensics investigator to begin the process of recovery as soon as they are able to, to minimize the risk of the file being overwritten and lost.

Some people use specialized software such as CCleaner to perform deep cleans on their hard drive. The program deletes all the information as standard, and and begins to fill up the drive once more with useless information, like small bytes of data that mean nothing. Once the drive is full, the data is deleted, and another pass of data is written to the drive. This process ensures that none of the original data remains on the hard drive, and it cannot be recovered - even through specialist software. Deep cleaning is a process often used by people who intend to sell their computer to another person, and don't want to risk their information being recovered. Though, this is also used by criminals to cover their tracks once they have finished their task.

There are a number of tools available for use in recovering data. Some examples include 'Recover My Files', 'UndeletePlus' and 'EaseUS Data Recovery Wizard'. For this scenario, the latter program to recover the lost PDF file, 'EaseUS Data Recovery Wizard' shall be used. Each of the programs boasts their own unique features and design, though ultimately they all strive for the same goal, to recover lost data either personally or professionally. While Recuva is known industry wide as a very reliable alternative, it is no longer recommended due to the fact the software's last update was in 2016, and has been considered abandoned, leaving severe security risks. This also creates an issue where the software is unable to support or recover modern file types that have since been created. Ultimately, 'EaseUS Data Recovery Wizard' was chosen for this scenario is that the free version allows for up to 500mb to be recovered (which is the same as other free programs.), and also allows for external and hard drives, as well as USB flash drives, memory cards and various types of storage partitions such as the boot partition, to recover any important operating system files that may have been accidentally lost. In this specific case, 500mb is more than enough for us to recover the necessary data.

C. Recovery of Files

Due to the value of the data that could be lost if not handled properly, it would be of most importance to first secure a warrant to seize and secure the perpetrator's computer. As mentioned, the sooner that the computer can be found and seized, the less risk of the data being overwritten. When the computer has been seized and safely secured by CCFL, the first action would be to document all the cables, parts and what state the computer was in. If the computer was found powered on, it is imperative that the computer remains on and cloned without being switched off. This is because turning off the computer risks the volatile data being lost. Volatile data is data stored within the RAM, and this can be used to check what programs have previously been accessed during the computers power cycle. This could hold vital information, as the perpetrator may have used software to clean the hard drive completely. While this means the data would be harder, or even impossible to recover, it would provide clear evidence that they have done this intentionally and it can be used in a court of law.

Once the computer has been properly documented by both photographs and labels, it is crucial to ensure that the original data and hard disk remains untouched and as-is. Therefore, the hard disk will be cloned and all data will be copied over to a workstation. This will be done by specialized software to ensure that data is copied bit by bit, and no information or quality is lost, and that integrity is maintained. This can be done by using software such as FTK (Forensic Toolkit). Once the data image has been created and copied, the data recovery program can begin to scan the drives to attempt to find any files that have been deleted.

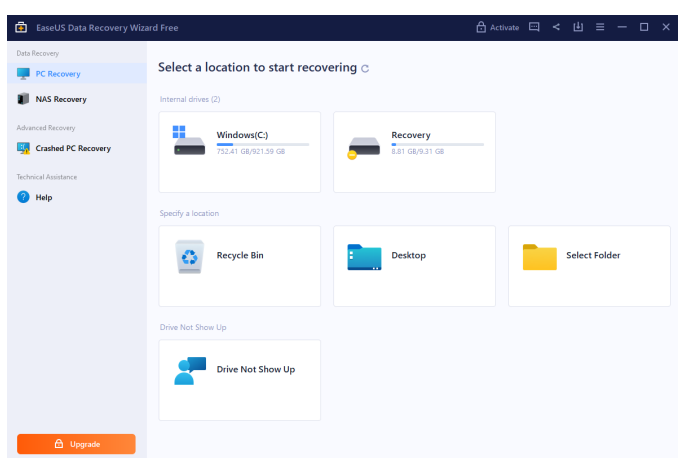

Fig. 17. A demonstration of the EaseUS Data Recovery Wizard start screen.

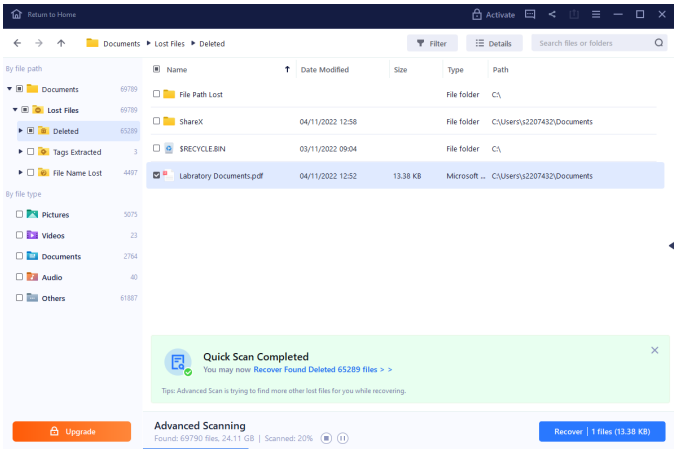

Fig. 18. EaseUS Data Recovery Wizard recovering the lost file.

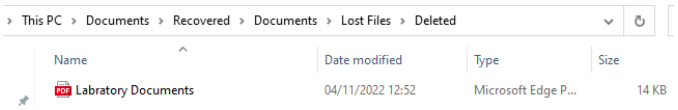

Fig. 19. The recovered documents displayed within the Windows Explorer.

1) Metadata.: While this is sufficient in some cases, some perpetrators attempt to hide crucial evidence by changing the file extension. An example of this would be changing 'Laboratory Documents.pdf' to 'HolidayPic34.jpg.'. This may fool anyone looking through the files quickly, and not give a second look to the supposed holiday photo.

Therefore, it is crucial to identify the original extensions for all files. This can be done by accessing the Metadata of a file. Metadata is a summarisation of basic information about a file, such as the file creation, the size and other information.

A tool used to find the Metadata of a program is called ApacheTika. This toolkit detects and extracts Metadata from all files within a folder and displays it within a single interface.

In this case, it confirmed that the PDF had not been modified, and is still the original PDF that was originally created.

D. Forensics Report

Alongside this report, a forensics report has been attached detailing the case summary, objective, evidence analysed (All evidence items have been assumed), investigation steps, findings and conclusion.

E. Invoice

Accompanying this report, an invoice has been generated and attached detailing the cost, deliveries and services. All costs and services have been assumed.

III. Terminology

List of terminologies used in this document:-

- mb - Megabyte.
- gb - Gigabyte.
- CCFL - Ceac Cybersecurity and Forensics Ltd.
- RAM - Random Access Memory.
- HPC - Healios Pharmaceutical Company.
- DDOS - Direct Denial of Service.
- VPN - Virtual Private Network.
- MiTM - Man In The Middle.
- MD5 - Message Digest Algorithm, Fifth Edition.

IV. Reference List

[1] "TryHackMe | OWASP Top 10." [Online]. Available: https://tryhackme.com/room/owasptop10

[2] D. Arnaldy and A. R. Perdana, "Implementation and analysis of penetration techniques using the man-in-the-middle attack," in *2019 2nd International Conference of Computer and Informatics Engineering (IC2IE)*, 2019, pp. 188–192.

[3] "XML External Entity Prevention - OWASP Cheat Sheet Series." [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html

[4] "Protect from cross-site scripting attacks - IBM Garage Practices." [Online]. Available: https://www.ibm.com/garage/method/practices/code/protect-from-cross-site-scripting/

[5] A. X. Liu and M. G. Gouda, "Firewall policy queries," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 6, pp. 766–777, 2009.