



L7 – Security Analysis, Techniques and Procedures (ACCA7030)

By
FATEMA NAMAZI

LECTURER: CARLENE CAMPBELL

ASSIGNMENT SUBMITTED AS PART OF THE REQUIREMENTS FOR THE
AWARD OF
MSC IN COMPUTER NETWORKS AND CYBER SECURITY

JANUARY 2023

INDEX

PART A

TOPIC	PAGE NO.
DESIGNING AND SETTING UP HPC SERVER INFRASTRUCTURE	6
POTENTIAL THREATS AND ATTACK VECTORS IDENTIFIED	7
NETWORK ATTACK TYPES	9
TECHNICAL PENTESTING REPORT	11

PART B

TOPIC	PAGE NO.
FORENSICS REPORT	29
CONCLUSION	33
COST	34
REFERENCES	35

LIST OF TABLES AND DIAGRAMS

DIAGRAM	PAGE NO.
HPC SERVER INFRASTRUCTURE	6
CONTINGENCY POLICY	16
VULNERABILITIES SEVERITY	19
REFLECTED CROSS SITE SCRIPTING	19
MEDIUM SEVERITY VULNERABILITY ISSUES	20
SMTP SERVER WITHOUT AUTHENTICATION	20
FIXATION OF SESSION	21
UPDATE FUNCTIONALITY OF WEAK ACCOUNT	21
INSECURE SOFTWARE VERSION	21
USER AND E-MAIL ENUMERATION	22
RECOMMENDED SOLUTIONS FOR THE THREATS DISCOVERED	24
TIMELINE	27
PROPOSED ARCHITECTURE	30
DISK IMAGING	31
MFT RECORD	31
FILE EXTENSION & SIGNATURE	32
FILE RECONSTRUCTION	32
ANALYSIS OF DAMAGED FILES	33
COST	34

LIST OF ACRONYMS

ASIC	Application Specific Integrated Circuit
DDOS	Distributed Denial of Service Attack
DFA	Deterministic Finite Automaton
DNS	Domain Name System
DoS	Denial of Service
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
OSHBIDS	Open-Source Host-based intrusion detection system
SPADE	Statistical Packet Anomaly Detection Engine
TCP	Transmission Control Protocol

PART A

1. DESIGNING AND SETTING UP HPC'S SERVER INFRASTRUCTURE



HPC server infrastructure

Clients

These are the users which has access to connect to the company's official website from any IP address, they are the customers of the company and can browse via any device.

External Firewall

CMG NetScaler Firewall has been used as the external firewall for the company, Here the SSL will terminate. On HTTP protocol the client's communication is forwarded to the reverse proxy server.

Reverse Proxy

The reverse proxy helps in hosting the company's websites.

Application Server

Application server is characterized as a Java Application and the is Tomcat based on the Java Servlet engine.

2. POTENTIAL THREATS AND ATTACK VECTORS IDENTIFIED.

VULNERABILITIES

When carrying out the multi-layered full scope cyberattack simulation, the following potential threats and attacks were identified, the most critical vulnerabilities were also documented along with how they can be exploited.

Networks are typically afflicted by one or all of three primary vulnerabilities [1]:

1. Technology weaknesses
2. Configuration weaknesses
3. Security policy weaknesses

These weaknesses include the TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses [1]. In terms of the configuration weakness, it is important for the network administrators or network engineers to learn what the configuration weakness are and configure their systems and devices accordingly [1]. And lastly, when it comes to the Security Policy weaknesses, If the users do not follow the security policy their network can be at security risks [1].

THREATS

There are 4 classes of threats which could cause serious damage to the security of the network. They are as follows:

1. *Unstructured Threat:*

These threats are mostly from inexperienced or unskilled hackers who use the available hacking tools such as shell scripts and password crackers to attack a system [1].

Unstructured tests like these which are only executed with the purpose of challenging and testing skills can still do serious damage to the organisation and is also considered a serious offence by the law.

2. *Structured Threat:*

These threats are from individuals who are technically competent and are experienced hackers [1]. They are well informed about the system vulnerabilities and can develop and exploit scripts and code [1]. They use sophisticated hacking techniques to penetrate unsuspecting businesses [1].

3. *External Threats:*

These threats can be from certain individuals or companies who aren't a part of the organization or company. They hold no power over the computer systems or network and have no access either. The basis of their access is mainly from internet or dialup access servers [1].

4. *Internal Threats:*

These threats are from users who are a part of the organization or company and has access to the network with either a physical access to the network or account on the server [1].

ATTACKS

There are several attacks using the internet protocols, this protocol can be exploited in number of ways [2]. There is no real authenticity protection in the default mechanism of the internet protocol suite [2].

Basically, attacks can be categorized under 4 major classes, which are as follows:

1. Reconnaissance
2. Access
3. Denial of service
4. Worms, Viruses, and Trojan Horses

1. *Reconnaissance:*

Reconnaissance in the network system means unpermitted mapping and discovery of services, vulnerabilities, or systems [1]. Another term for this could be information gathering and in recent cases, it precedes a denial of service (DoS) attack [1].

2. *Access:*

It means to gain access over the system by an unpermitted intruder, it means the ability to access devices for which they do not have a password [1]. It can be achieved by hacking, scripts or tools that are used to exploit vulnerabilities of the system being attacked.

3. *Denial of Service (DoS):*

It means the service in which the hackers corrupt or disables the network system, with the purpose to deny access to the service to the intended user [1]. It involves slowing down the system as to make it unusable or crashing it down completely or it can also be corrupting or deleting data [1].

4. *Worms, Viruses, and Trojan Horses:*

These are usually referred to as malicious software being attached to the host to damage or corrupt the system or services [1]. Or could also cause denial of access to the network, services, or systems [1]. They are also capable of accessing sensitive data of the system and copying it to other systems [1]. SYN flooding includes sending large number of SYN packets and not acknowledging its replies leading to accumulating more SYN packets than its software capabilities [2]. Trojan Horses are used to forge the user into entering sensitive data on a commonly trusted screen [1]. As the years are passing these hacking tools are increasing in types and are getting more and more powerful with time. There has been an abundance in the variety and increase in the usage of these tools.

3. NETWORK ATTACK TYPES

Using MITRE ATT&CK and OWASP Top 10 Frameworks, the networks attacks are classified under group – attack - the network protocol-based attack, host-based attacks, and attacks on network application layer [3].

A. NETWORK PROTOCOL INTRUSIONS

The attacks which occur due to the flaws or problems in the networking protocols or weak or problematic software's that implements the networking protocols, these intrusions concentrate on the network and transport layer of the OSI layer [3].

1. Host & Port Scanning –

To identify hosts the hackers or attackers use these techniques, Denial of Service, ping broadcast and network scanning [3]. The attackers may send ICMP echo request and loop through the Ip addresses for systems to each address [3]. There are two specific uses of the broadcast ping – one is it denies the service by amplifying single, frequent ping request and the other is on the target subnet it identifies all hosts [3]. Thereby generating more ICMP echo responses which may cause temporary traffic congestion in the network [3]. This attack causes the network to slow down or make it inaccessible. After getting to know a valid host the attackers use port scanning to identify UDP and TCP services of the host. Some of the common port scanning includes, TCP Stealth Port scanning, TCP SYN port Scanning and UDP Port Scanning etc [3].

2. DNS Spoofing & Cache Poisoning –

These attacks occur when the attacker intercepts the traffic between the user and the gateway router through ARP (Address Resolution Protocol) cache poisoning attack [4]. In the DNS server the cache is a memory device with high speed, in this the response information is saved in the DNS server hierarchy in the DNS server [4].

3. Web Spoofing –

In this attack the attacker keeps a track of all the web traffic sent to the user's system, the attacker captures all the data which the user entered the web pages [3]. This attack is done using JavaScript segments and Web plug-ins [3]. Here the attacker sends the web link via malicious email or message, when the user visits the web page and responds then the attacker diverts the web traffic of the user to its own server.

4. Email Spoofing –

Like web spoofing, email spoofing attack is similar as it mimics the email address, this attack involves changing the email address to look like its email coming from a trusted source to help the attackers conceal their identity [3]. It's easier as SMTP servers requires no authentication.

5. Session Hijacking –

When the attacker controls an active TCP session between two systems, the TCP session hijacking occurs [3]. It can be carried out using source – routed IP packets [3].

6. Ping Of Death (Long ICMP) –

Its other name is 'Long ICMP; this comes under the category of Denial of Service (DoS) attack. This attack can be caused when the attacker sends IP packets larger than 65,536 bytes which isn't allowed according to the IP protocol, this is done intentionally as the attackers are aware that the packet can be broken down into smaller chunk adding more than 65,536 bytes [3].

B. HOST INTRUSION

Host intrusions in the operating system are discussed below:

1. *Password Sniffing* –

Password sniffer is a software which can help the attacker obtain passwords of the accounts on the other systems. Network protocols such as Telnet, FTP, POP, and others transmit passcodes as clear text. Software's such as Berkeley Packet Filter or Ethereal offers to sniff traffic on the network [3]. These sniffing programs eavesdrop to the bytes of each network connection [3]. The information heard is saved to a file and transferred to another host for the purpose of saving it [3].

2. *Remote Backdoor Access* –

This attack occurs when the hackers someone access a system and install a 'Backdoor' program which will allow the user to access the system from the remote location at his own convenience [3]. The hacker can also use this program to give access to other intruders [3].

3. *Disabling Security Options* –

Disabling the security options such as IDS, Firewall and etc to make the system vulnerable when the hacker access to a target terminal is Disabling Security Options [3]. Viruses and Trojans can also be used to carry out this attack.

4. *Mac Spoofing* –

The spoofing of the attacker MAC address to the user MAC address is MAC spoofing attack [3]. This can be carried out using Mac Makeup software and other MAC spoofing tools [3].

5. *IP Spoofing* –

This attack involves gaining unauthorized access to the system by sending packets to a system using Spoofed IP address to make it known that the message is from a trusted host [3]. To implement this attack the hacker captures packets to locate IP address of a trusted host [3]. This can be stopped using firewall filters and security enabled routers [3].

C. NETWORK APPLICATION LAYER INTRUSION

The following are the intrusions which target network application layer: -

Unauthorized use of NFS, Send mail debugging commands, Trivial File Transfer Protocol, RPC Portmapper Proxy, Use of login or rsh from untrusted hosts, insecure web server CGI programs, etc [3].



Network Penetration Testing Report – Healios Pharmaceutical Company

Prepared By
Red Team – Cybersecurity Department of Healios Pharmaceutical Company

Redteam@hpc.ac.uk

TABLE OF CONTENT

1.1	Introduction	10
1.2	List of figures and tables	11
1.3	List of acronyms	12
1.4	Contingency Policy	13
1.5	Penetration Testing Framework	14
1.6	Penetration Testing Tools	15
1.7	Types of Attacks simulated	19
I.	List of vulnerabilities	19
II.	Attack tools used	20
III.	Protocols involved in the attack	21
IV.	How the attack was launched	22
V.	Result	23
1.8	Recommended Solutions	24
1.9	Cost of the solution	26
1.10	Timetable for execution	27

INTRODUCTION

Red Team employed by Healios Pharmaceutical Company (HPC) conducted a comprehensive security assessment on HPC on order to determine existing vulnerabilities and establish the current level of security risk associated with an environment and the technologies in use.

The purpose of the analysis was to gauge the security posture of the in-depth assets and recognise any diverging vulnerabilities by measuring them against system adapted controls.

The test scope for this assessment included three hosts on the association's internal network, an association – evaluating web application, and mobile application which is developed internally. Moreover, to discover any unsecured networks, insecure wireless protocols, or related security issues a wireless audit will be performed requested by HPC against their WIFI infrastructure.

Industry-standard based penetration testing framework and tools, testing was performed using Sniper, Nmap, Fierce, The Metasploit Framework, Open VAS, Wireshark, WPSScan, BurpSuite, Aircrack-ng, Tcpdump, Reaver, Arpspoof, and Asleep.

LIST OF FIGURES AND TABLE

TOPIC	PAGE NO.
CONTINGENCY POLICY	16
VULNERABILITIES SEVERITY	19
REFLECTED CROSS SITE SCRIPTING	19
MEDIUM SEVERITY VULNERABILITY ISSUES	20
SMTP SERVER WITHOUT AUTHENTICATION	20
FIXATION OF SESSION	21
UPDATE FUNCTIONALITY OF WEAK ACCOUNT	21
INSECURE SOFTWARE VERSION	21
USER AND E-MAIL ENUMERATION	22
RECOMMENDED SOLUTIONS FOR THE THREATS DISCOVERED	24
TIMELINE	27

LIST OF ACRONYMS

ASIC	Application Specific Integrated Circuit
DDOS	Distributed Denial of Service Attack
DFA	Deterministic Finite Automaton
DNS	Domain Name System
DoS	Denial of Service
NFA	Non-Deterministic Finite Automaton
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
OSHBIDS	Open-Source Host-based intrusion detection system
SPADE	Statistical Packet Anomaly Detection Engine
TCAM	Ternary Content Addressable Memories
TCP	Transmission Control Protocol

CONTINGENCY POLICY

Upon testing the security of the companies network the Redteam security propose the following contingency policy:

There are 7 integrated steps designed to progress into each stage of the development of the system life cycle [5](18): -

Sno.	Policy	Description
1	Developing the planning policy contingency statement.	A dedicated policy of formal department provides guidance and authority to the company which is necessary for an effective contingency plan.
2	Conducting the analysis of business impact (BIA)	To help and identify IT system the conduction of BIA is necessary. BIA template is provided to assist the user.
3	Identification of preventive controls	To increase system availability and reduce life cycle contingency costs measures are taken to reduce the effects of the systems disruption.
4	Developing a contingency IT plan	For restoring a damaged system, a detailed guidance and procedure plan should be given.
5	Developing recovery strategies	Ensuring the system is recovered quickly and effectively, thorough recovery strategies are given.
6	Planning to test, train, and exercise	To improve the plan effectiveness and overall secured analysis, its essential to test the plan to identify any gaps, and train to prepare for the recovery for plan activation.
7	Maintenance plan	To remain updated with the current system enhancement it is important that the plan is updated regularly.

PENETRATION TESTING FRAMEWORK

Methodology

1. Gathering Information

This phase of gathering information consists of searching reconnaissance, fingerprinting server, enumeration of application etc. This phase requires efforts to gather as much data about the company as possible and results in forming a list compiled of metadata and output which is raw. It also includes metafile leakage review, initial domain foot printing, application fingerprinting and service enumeration.

2. Threat Modelling

After collecting data from the last step, with the help of data collected, the vulnerabilities are identified in the application with security testing transitions. The following are involved in this step: Trade secrets, Sensitive documents, financial information, etc.

3. Vulnerability Analysis

Analysing the vulnerabilities and documenting them are a part of the vulnerability analysis. With the help of manual testing techniques and various security tools, this step is successfully carried out.

4. Exploitation

To determine the real environment risk, there is bypassing of security controls by establishing access to applications. Since the scanners are unable to perform, manual tests are carried out throughout this stage. Making it the most time-intensive phase. It includes SQL injection, buffer overflow, OS commanding, Cross-site script etc.

5. Reporting

This stage is supposed to help rank, deliver, and prioritize finding. And help in creating a clean and actionable report with attached evidence to the report stakeholders. With the help of Webex or in-person.

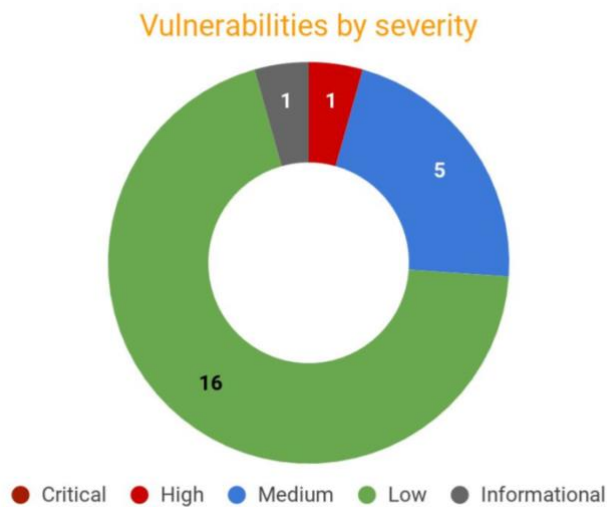
PENETRATION TESTING TOOLS USED

The following categories of pen testing tools are used in carrying out the assessment: -

1. Commercial Tools (i.e., AppScan, Burp Suite Pro, WebInspect)
2. Hacker Tools/ Open Source (i.e., BEeF, Metasploit, Kali Linux, OWASP Zap)
3. Tools developed by RedTeam (i.e., Metasploit modules, nmapcli, PlugBot, various scripts)

TYPES OF ATTACKS SIMULATED

A. LIST OF VULNERABILITIES



Severity	Critical	High	Medium	Low	Information
Sno.	0	1	5	16	1

High Severity Vulnerability Issues

1. Reflected Cross site Scripting

Proof Of Vulnerability:

Injection of JavaScript codes by the attacker into the URL to html code which is executed.



Medium Severity vulnerability Issues

1. Password Brute Force,

Proof Of Vulnerability:

After making 65 attempts at incorrect passwords, the user is still not locked and is successfully logged in after 66th attempt.

Request	Payload	Status	Error	Timeout	Length	Comment
56	tuckyout	200	☐	☐	70708	
57		200	☐	☐	70708	
58	princess	200	☐	☐	70708	
59	789456123	200	☐	☐	70708	
60	111111111	200	☐	☐	70708	
61	123654	200	☐	☐	70708	
62	princess1	200	☐	☐	70708	
63	888888	200	☐	☐	70708	
64	linkedin	200	☐	☐	70708	
65	michael	200	☐	☐	70708	
66		302	☐	☐	17649	

Request

Response

Raw

Headers

Hex

```

HTTP/1.1 302 Moved Temporarily
Content-Type: text/html; charset=UTF-8
Connection: close
Server: nginx
Date: Tue, 30 Oct 2018 16:52:46 GMT
Access-Control-Allow-Origin: *
Set-Cookie: PHPSESSID=blat6e0ohdg3acskgrf6bjCu7; expires=Wed, 31-Oct-2018 16:52:46 GMT; Max-Age=86400; path=/; domain=[REDACTED] secure; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: login=2737239f3a0f5b5346eb922e1970251cf05873c5c0; expires=Fri, 08-Jul-2050 18:39:25 GMT; Max-Age=999999999; path=/; domain=[REDACTED] secure
Set-Cookie: login=2737239f3a0f5b5346eb922e1970251cf05873c5c0; expires=Fri, 08-Jul-2050 18:39:25 GMT; Max-Age=999999999; path=/; domain=[REDACTED] secure
Set-Cookie: login=2737239f3a0f5b5346eb922e1970251cf05873c5c0; expires=Fri, 08-Jul-2050 18:39:25 GMT; Max-Age=999999999; path=/; domain=[REDACTED] secure
Content-Security-Policy-Report-Only: default-src 'self' [REDACTED] https://[REDACTED] frame-src 'self' 'unsafe-inline' https://[REDACTED]

```

2. SMTP server without authentication,
Proof Of Vulnerability:
Without authentication, the attacker has connected to the server and is successful in sending the email from the original to the attackers email.

```

root@kali:~# nc -nv [REDACTED]
(UNKNOWN) [REDACTED] 25 (smtp) open
220 [REDACTED] ESMTP Postfix (Debian/GNU)
HELO [REDACTED]
250 [REDACTED]
MAIL FROM:pentest1@[REDACTED].com
250 2.1.0 Ok
RCPT TO: pentest2@[REDACTED].com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
SUBJECT: Security Team

This email is from Manual Penetration Testing Team.

.
250 2.0.0 Ok: queued as DE524801BD
QUIT
221 2.0.0 Bye

```

3. Insufficient expiration of session,
4. Fixation of session
Proof Of vulnerability
Same cookie value request made after logout.

```
curl -i -s -k -X '$GET' \

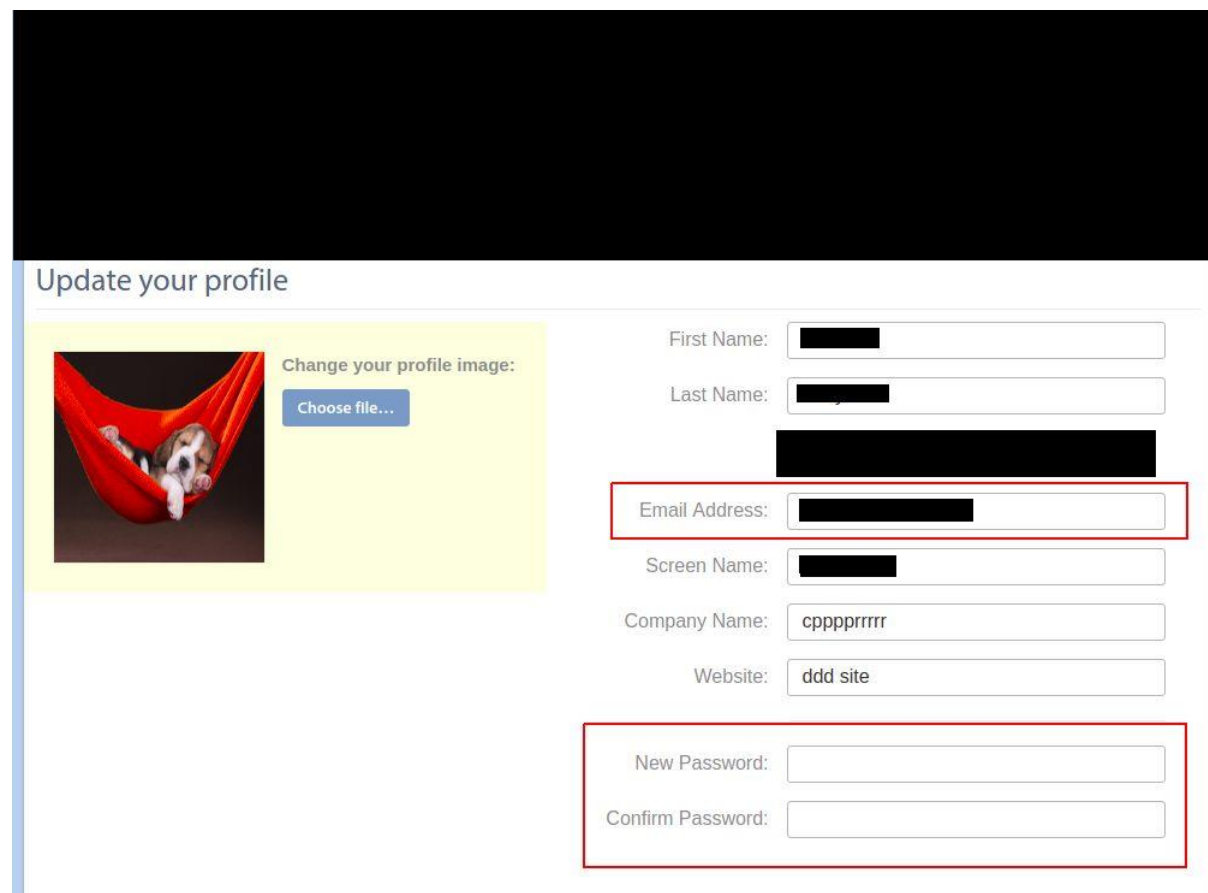
-H '$Host: www.client.com' login=2737239%3A0f5b53466b922e1970291cf05873c5c0; ' -H '$X-Forwarded-For:

spoofed.s6zuzg64yc4wqc6vs0nxrfqjmasci86x.burpcollaborator.net' \
-b '$login=2737239%3A0f5b53466b922e1970291cf05873c5c0' \
$'https://www.client.com/member/account-preferences'
```

5. Update functionality of weak account.

Proof Of vulnerability:

Email and password can be updated by the user without any authentication of the account, whether it belongs to the user or not.



Low Severity Vulnerabilities Issues

1. Insecure Software Version

Proof of Vulnerability:

Js lib vulnerable in the web server.

```
<!-- Scripts -->
<script type="text/javascript"
src="/js/lib/jquery-1.7.1.min.js"></script>
<script type="text/javascript"
src="/js/lib/jquery.easing.min.js"></script>
```

2. HSTS missing from HTTPS server
3. Cookie without Secure and HTTPOnly flags set
4. SSH Weak Algorithms Supported
5. Jira Sensitive Information Leakage
6. SSH Server CBC Mode Ciphers Enabled
7. SSH Weak MAC Algorithms Enabled
8. OpenSSH 6.0p1 multiple vulnerabilities
9. User and E-mail Enumeration

Proof of Vulnerability:

Enumeration of the user at login page.

Login to your account

Username or e-mail

Unrecognized username or E-mail: 123123123@gmail.com

Password

Forgot Password?

LOGIN

10. Apache Tomcat/8.5.6 multiple vulnerabilities
11. User and E-mail Enumeration
12. Possible BREACH vulnerability
13. Possible Secure Client-Initiated Renegotiation
14. Possible RC4 vulnerability
15. Possible LUCKY13 vulnerability
16. Possible Beast Vulnerability
17. Possible SWEET32 vulnerability

B. ATTACK TOOLS: -

1. Nmap
2. Burp Suite Pro
3. TestSSL
4. Nikto
5. Dirbuster
6. GoBuster
7. Arachni
8. Nessus
9. Hydra
10. Harvester

11. Sublister

C. PROTOCOLS INVOLVED IN THE ATTACK

1. Injection
2. Sensitive Data Exposure
3. Broken Authentication
4. XML External Entities (XXE)
5. Security Configuration
6. Broken Access Control
7. Cross – site Scripting (XSS)
8. Using Components with Known Vulnerabilities
9. Insecure Deserialization
10. Insufficient Logging and Monitoring

D. LAUNCH OF THE ATTACK

The penetration testing assessment includes the following steps: -

1. Understanding the network analysis
2. Flaw hypothesis
3. Hypothesis testing to reject or confirm
4. To yield other hypothesis, extension of successful tests.

Penetration testing should be structured according to perceived risk and component unit, at feature and system level. During the test phase of the methodology, these could be considered [6].

E. RESULTS

This stage is the results of the testers, the results, and the target entity [6]. For the target entity its essential to be aware of the typical attacker's data on its vulnerabilities by operations, techniques, and tools the attacker rely on [6]. To address the problems, the steps to be taken should be corrective and reactive [6]. The remediations strategies for BOG and TuneStore could be before placing the user's input data to sanitize them [6]. And the SQL injection attacks can be protected by passing username and passwords which do not contain any bad character.

RECOMMENDED SOLUTIONS FOR THE THREATS DISCOVERED.

Threats	Recommendations	Software/hardware and Defence Strategy required
Reflected Cross Site Scripting (XSS)	To prevent reflected cross site scripting its required that the untrusted data is separated from the active browser content.	• Use of frameworks designs which escape XSS. • Use of Ruby on Rails, React JS • Using XSS prevention Cheat Sheet, helps in filtering out user input sufficiently.
SMTP server without authentication	Implementing access and authentication control.	Making sure only few people in the organization have access to the server.
Password Brute Force	A couple of recommendations can be used to prevent password brute force.	• Account lockout Policy • Prevention of automated submissions of the login page by adopting a challenge-response test. • Progressive delays • IP address lock-out.
Session Fixation	Prompt visibility of the login function to the user by disallowing reuse of the session token and invalidating a user's session.	After logging out, the user browser should be provided with a new session id by the server.
Insufficient session expiration	After a predefined idle time has passed or rather after a timeout, the web application should invalid the session and the user should be able to logout when needed. This keeps the session ID lifespan small.	
Weak account preferences update functionality	Sensitive action check like password change and. Email address update of users should be implemented.	• Email confirmation • Two – factor authentication • SMS confirmation
Possible SWEET32 vulnerability	When used in CBC mode the 64 bits legacy block ciphers are vulnerable to	

	practical collisions attack.	
Possible LUCKY13 vulnerability	To using AEAD algorithms avoid using TLS in to switch and CBC-mode.	
Possible Beast vulnerability	Use protocols which are immune to the BEAST attack for users connect, such as TLS 1.1 or TLS 1.2 protocols and disable TLS 1.0.	
Possible RC4 Vulnerability	To avoid use of RC4 ciphers, reconfigure the affected applications.	For browser and webserver support, consider using TLS 1.2 with AES-GCM suites.
Possible BREACH vulnerability	The effectiveness is measured by mitigations.	• Separating secrets from user input • Disabling HTTP compression • Randomizing secrets per request • Protecting vulnerable pages with CSRF • Masking secrets • Length hiding • Rate-limiting the requests
Possible secure client-initiated renegotiation	On the server, disabling the SSL renegotiation support.	Instead of HTTP, using port 443 as TCP for passing the requests to the server.
User and email enumeration	In the functionality provide less verbose responses.	

COST

Cost Factor 1: Time and Scale of the engagement

Primary factor of the cost factor is based on the time taken to carry out the assessment. There are several stages in the assessment which require various amount of time and effort. It includes several stages such as: - Reconnaissance, Exploitation, and Command & control.

Cost Factor 2: Resources and Availability

To fulfil the obligations of the assessment the red team require minimal resources such as hardware and software depending on the requirement. Critical areas include: - Installation, Payload and delivery and Actions on the objectives.

Cost Factor 3: Remediation and retesting

It's a critical stage of the assessment and these considerations impact the organisation and the scope of the red team assessment.

Price of the Red Team engineer per week: - 312 £

Duration of the assessment is 32 weeks

TOTAL – 10,000 £

TIMELINE

Red Team has been engaged by the HPC to undertake security testing against the company server infrastructure. The testing took place over the period from Jan '20 to Aug '20. During this period the company's server was assessed and analysed using several attack tools under the supervision of the experienced technical team.

Task	Jan '20	Feb '20	Mar '20	Apr '20	May '20	Jun '20	Jul '20	Aug '20
Planning								
Research								
Design and development								
Implementation								
Follow-up and action								

PART B

FORENSICS REPORT

OVERVIEW / CASE SUMMARY

On November 11, 2022, Healios Pharmaceutical Company (HPC) filed an amended complaint to Ceac Cybersecurity and Forensics Ltd (CCFL) seeking to appoint a Computer Forensics Investigator to investigate an incident and recover deleted files containing sensitive data. HPC IT department has claimed that an ex-employee, a research scientist named, Nera Star who was working on a human vaccine for Monkeypox treatment left the company a week ago and during a regular backup cycle it was noticed that her machine hasn't been backed up which means deletion of files containing the chemical formulae and mathematical codes.

OBJECTIVES

This report is a summary of Computer Forensics Investigator's findings regarding the investigation of the incident and recovery of the deleted files based on the analysis of the data produced by the company HPC and their ex-employee, Nera Star, pursuant to data received as part of expedited discover.

EVIDENCE ANALYSED

Pursuant to the HPC IT team's order, Computer Forensics Investigator collected data made available by the company. He inspected the data on the following data for analysis according to the terms of the company's protocol:

Research documents need to be stored in MS Word or Rich Text Format.
Critical documents were stored as PDF to prevent tampering.
Nera's files have 270 pages of sensitive formulae.

To reconstruct the deleted files in the file system [7]. This research is divided into four primary stages:

1. Disk Imaging
2. File type identification
3. Accessing MFT
4. Corruption Check

Whereas file reconstruction consists of the following

1. Undelete
2. Analysis
3. Verification

INVESTIGATION STEPS

The investigation steps are described in the following points below [7]:

1. To obtain duplicates of storage media that is similar to the actual storage media, duplication of storage media contents is essential.

2. To search records from the existing directories and files it's important to access and read MFT records.
3. Using parsing on MFT record extraction of metadata.

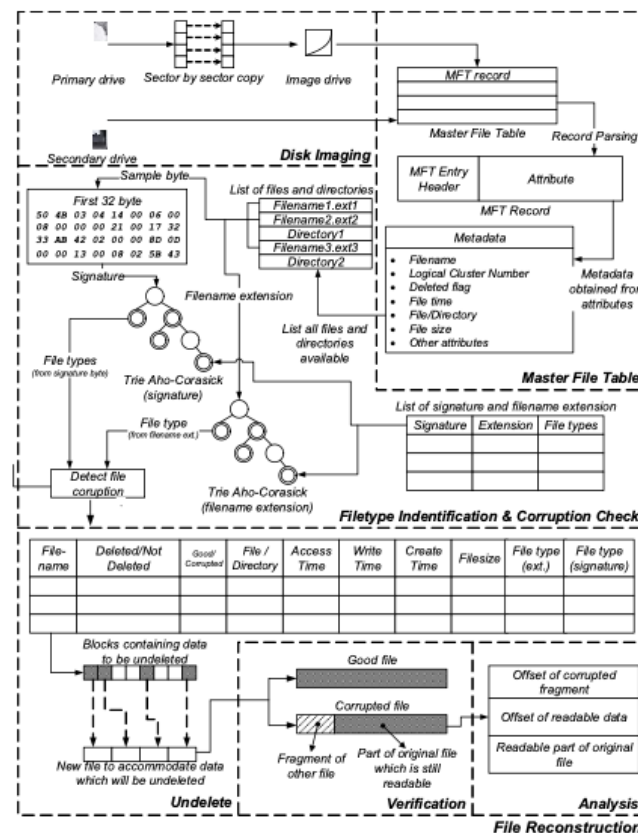


Figure 1. Proposed method-general architecture

4. To obtain filename extension, performing parsing on file name.
5. Cluster occupied file as sample and taking 32 bytes of it.
6. Based on actual file extensions and signature, building trie using AHO-Corasick.
7. Based on filename extension and signature and identifying file type.
8. Results of signature-based identification to check if the file was damaged, by comparing the results if the file type identification based on the extension of the filename.
9. Registration of the file along with its details, such as timestamp, file type, file condition and other types of data.
10. Reconstruction of the file based on the metadata received from MFT, reconstructed files verification by file opening and checking for signature to identify if the recovery file is experiencing any damage, to analyse the files which are damaged and read the information readable in the files.
11. After all the steps are performed the file recovery can be performed on the file system deleted files.

DISK IMAGING

Disk Imaging is a step which involves duplicating the data of the stored media in the level sector, to acquire duplicate data which is like the original data including the MFT and boot sector [7] . To read and to access the MFT record, this acquired duplicate data is used.

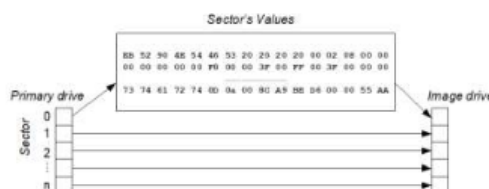


Figure 2. Disk Imaging Scheme

MASTER FILE TABLE (MFT)

To break up each record based on the MFT entry header, every record fore through the parsing process [7]. With the help of the MFT the condition and type of the records can be known. The condition can be known by comparing the result of the file based on the extension of the filename and the signature.

FILE SIZE

To obtain file metadata in order to process reconstruct like number of logical clusters occupied by the file, filename, flag to determine the deleted file and other information its mandatory to process parsing [7]. All files with deleted flag will be listed based on the metadata [7].

Table 1. MFT Record																
Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	46	49	4C	45	30	00	03	00	57	34	80	00	00	00	00	00
10	03	00	01	00	38	00	01	00	E0	01	00	00	00	04	00	00
20	00	00	00	00	00	00	00	00	06	00	00	00	00	03	00	00
30	03	00	00	00	00	00	00	00	10	00	00	00	48	00	00	00
40	00	00	18	00	00	00	00	00	30	00	00	00	18	00	00	00
50	24	CC	73	D0	62	D9	CF	01	24	CC	73	D0	62	D9	CF	01
60	24	CC	73	D0	62	D9	CF	01	24	CC	73	D0	62	D9	CF	01
70	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
80	30	00	00	00	68	00	00	00	00	00	18	00	00	00	01	00
90	50	00	00	00	18	00	01	00	05	00	00	00	00	00	05	00

FILE IDENTIFICATION AND CORRUPTION CHECKING

This stage is about, determining whether the files contained in the storage media are corrupted [7]. Performance of the identification of the file type is based on the file signature and filename extension [7]. Derivation of the filename extension is from the name of the file and the derivation of the file signature is from the header of the file by considering the sample of the first 32 bytes [7].

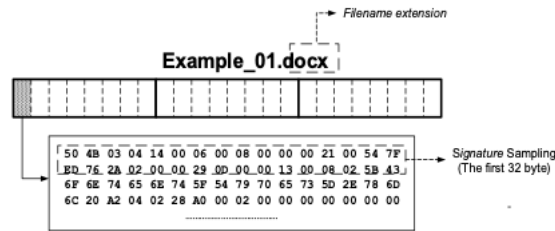


Figure 3. Filename extension and signature sample

Table 2. List of Filename Extension and Signature to be utilized

No	Filename Extension	Signature	Description
1.	DOC, DOCX, PPT, PPTX, MSI, VSD, XLS, XLSX	50 4B 03 04 14 00 06 00 - D0 CF 11 E0 A1 B1 1A E1 25 50 44 46	Document or Microsoft file
2.	PDF, FDF	25 50 44 46	Adobe Portable Document Format
3.	JPEG, JPG	- FF D8 FF E0 00 10 4A 46 49 46 00 01 01 - FF D8 FF E0 - FF D8 FF E1 - FF D8 FF E8 - FF D8 FF	JPEG file
4.	PNG	89 50 4E 47 0D 0A 1A 0A	PNG file
5.	GIF	47 49 46 38 39 61 4E 01 53 00 C4	GIF file
6.	MP3	49 44 33	MP3 file
7.	MKV	1A 45 DF A3 93 42 82 88 6D 61 74 72 6F 73 6B 61	Matroska file
8.	MP4, M4V	66 74 79 70 33 67 70 35 66 74 79 70 4D 53 4E 56 66 74 79 70 6D 70 34 32	MPEG-4 video file
9.	EXE	4D 5A	Executable file
10.	RAR	52 61 72 21 1A 07 00 52 61 72 21 1A 07 01 00	Compressed archive
11.	ZIP, JAR	57 69 6E 5A 69 70 50 4B 03 04 50 4B 05 06 50 4B 07 08	Zip archive

FILE RECONSTRUCTION

To perform the file reconstruction, the parsing process is used which helps us to get the metadata obtained from the MFT records [7]. File name, the size of the allocation and Logical Cluster Number (LCN) is required for the File reconstruction [7].

Table 4. Information Used in Undelete Process

No	Information	Details
1.	Filename	The filename corresponds to the entry on MFT.
2.	File/Directory	Entry type, whether an entry for a file or directory. Obtained from flags on MFT records
3.	Deleted	Condition whether the entry has been deleted or is still in use. Retrieved from the flag in the MFT record.
4.	Condition	Condition of the file damage obtained from the identification and comparison of file types.
5.	Write Time	The time a file is written.
6.	Create Time	The time a file was created.
7.	Access Time	The time a file is accessed.
8.	Signature Filetype	File type based on the identification of first 32 bytes of file.
9.	Filename Extension Filetype	File type based on the identification of filename extension.
10.	Allocation Size	The size of file allocation in storage media. This information will be used in file reconstruction.
11.	Logical Cluster Number	The number of clusters occupied by the file. This information will be used to read the data stored in the cluster in file reconstruction process.

UNDELETE PROCESS

It involves building a new file with similar name and size of the allocation as the original file to be restored. Reading the data of the cluster stored in the buffer of the recovered file and opening the LCN. The contents are transferred to the new file in hexadecimal ratios. Until the data of each cluster of the deleted files are transferred to the new file, this process is continued [7].

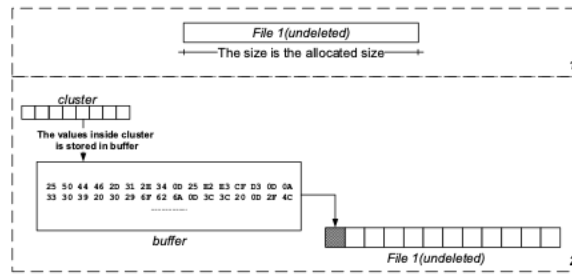


Figure 5. File reconstruction process at the time of recovery

VERIFICATION PROCESS

The verification process is to decide whether the file is damaged or not. By opening with its default application, the file is verified. If the hexadecimal value of the file is read, then that means the file is damaged [7].

ANALYSIS PROCESS

To determine whether the file is corrupted completely or partially the analysis of the damaged file is conducted [7]. If it's known that the file is overwritten partially then with the help of the remaining information, the data can be derived from the original file [7].

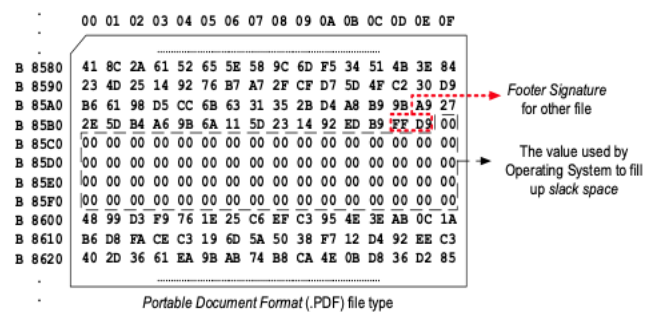


Figure 6. Analysis of damaged files

CONCLUSION

To investigate the incident and recover deleted files containing the chemical formulae and mathematical codes – the failure of the system backup – either its logical structure or the hardware presented problems significantly for the Computer Forensics Investigator [7]. To recover the files from the non-backed up system could have resulted in both the loss of the subject material and cause seizure of the equipment used by the Forensic investigator.

However, with the help of the resolved methodology followed by the forensic investigator, they were able to resolve the issue and recover the deleted files. Saving the company HPC from the loss of USD 3 million from various contracts with the suppliers.

COST

Fatema Namazi, Red Team Engineer
 321 Sycamore, Albany, NY 12208
 Phone (123) 456-7890 Fax (123) 456-7891



INVOICE NO. 1002

DATE 11/10/22

BILL TO

Healios Pharmaceutical
 Company (HPC),
 Cataldo Capon
 2345 5th Ave.
 Madison, WI 53705

SHIP TO

Same as Recipient

INSTRUCTIONS

Express Overnight Delivery

QUANTITY

DESCRIPTION

UNIT PRICE

TOTAL

£5,000+VAT

/year

12

Includes everything from both our
 Cyber Essentials and Cyber
 Essentials Plus plans at a discount
 over purchasing them separately

75.00

5000.00

SUBTOTAL

5000.00

SALES TAX

45.00

SHIPPING & HANDLING

24.99

TOTAL DUE BY DATE 12/30/22

5069.99

Thank you for your business!

REFERENCES

- [1] C. Thomas, Introductory Chapter: Computer Security Threats, .
- [2] Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition, 2nd Edition, .
- [3] Dr.Md.Yusuf Mulge, "Intrusion Detection For Known And Unknown Security Attacks ," International Journal of Engineering Sciences & Research Technology (Ijesrt), vol. Mulge, 1(10), (Mulge, 1(10)), pp. 586-591, 2012.
- [4] Mohammed Abdulridha Hussain et al, "DNS protection against spoofing and poisoning attacks," in 3rd International Conference on Information Science and Control Engineering, July, 2016, pp. 1308-1312.
- [5] Marianne Swanson et al, "Contingency Planning Guide for Information Technology Systems," 06/13/02. Available:
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34.pdf>. DOI:
<https://doi.org/10.6028/NIST.SP.800-34>.
- [6] Aileen G. Bacudio et al, "An Overview of Penetration Testing," International Journal of Network Security & its Applications (IJNSA), vol. Vol.3, (No.6), pp. 19-38, 2011. . DOI:
<http://dx.doi.org/10.5121/ijnsa.2011.3602>.
- [7] Opim Salim Sitompul, Andrew Handoko and Romi Fadillah Rahmat, "File Reconstruction in Digital Forensic ," TELKOMNIKA Indonesian Journal of Electrical Engineering 16(2), vol. Vol.16, (No.2), pp. 776-794, 2018. Available:
https://www.researchgate.net/publication/323153691_File_Reconstruction_in_Digital_Forensic. DOI: 10.12928/TELKOMNIKA.v16i2.8230.