

himanshu sompura

by Himanshu Jigneshbhai Sompura

Submission date: 08-Jan-2026 10:36AM (UTC+0000)

Submission ID: 272506552

File name: 68163_Himanshu_Jigneshbhai_Sompura_himanshu_sompura_712353_338926656.docx (5.23M)

Word count: 5758

Character count: 34347



[DOCUMENT TITLE]

STUDENT NAME-



Table of Contents

Task 1	3
1. Introduction	3
2. Background of the Incident	3
3. Methodology and Analytical Approach.	4
4. Attack Reconstruction	6
4.1. First Compromise and Network Discovery.....	6
4.2. Implementation of Malicious Toolsets.	6
4.3. Sustaining Long-term Access.....	6
4.4. Escalation of Privileges.....	7
4.5. Internal Lateral Access and Internal Spread.....	7
4.6. Command and Control Operations.....	7
4.7. Data Theft and Creation of leverage.	7
4.8. Ransomware Activation and National Impact.....	8
5. MITRE ATT&CK Analysis	8
6. Root Cause Analysis.....	9
6.1. Gaps in Technology and Infrastructure	9
6.2. Organisational and Procedural Weaknesses.	10
6.3. Leadership, Oversight and Strategic Weaknesses.	10
7. Risk and Impact Assessment	10
8. Strategic Recommendations	13
9. Summary.....	14
Task 2	15
1. Introduction	15
2. Objective of the Engagement	15

3. Environment Overview.....	16
3.1. Hybrid Architecture Design	16
3.2. Network Segmentation and Access Control.....	17
4. Methodology.....	17
4.1. Planning and control measures in engagement.	17
4.2. Simulation of Adversary Behaviour.....	18
4.3. MITRE ATT&CK Framework Alignment	18
5. Execution Summary	19
5.1. Attacker System Placement.....	21
5.2. Safe Reconnaissance and Internal Mapping.....	21
5.3. Sensitive Asset Identification.....	22
5.4. Path Simulation of Data Exfiltration.....	22
6. Findings and Observations	22
6.1. Strengths on security identified.....	22
6.2. Limiting Factors of Visibility and Detection.....	23
REFERENCES	23

Task 1

1. Introduction

In May 2021, Ireland's Health Service Executive (HSE), the organization dealing with the provision of public healthcare and an extensive variety of clinical, administrative, and digital services, faced a historic cyber crisis. The IT infrastructure of the organisation was badly affected by a high level of ransomware attack, which was later determined to be carried out by the Conti cybercriminal group and has hampered the delivery of healthcare at a national level. Important clinical systems were put offline, regular and emergency services were held back, and hospitals and clinics were left to go back to manual operations, generating extensive operational pressure. The event was eventually pronounced the biggest emergency in the HSE history with all its vulnerability to cyber threats being of extreme nature to healthcare systems [1].

This threat analysis is a strategic threat analysis, which evaluates the incident in detail, how the attack occurred, methods and techniques of the threat actors, and weaknesses in the organisations and technology that facilitated the breach. It also evaluates long-term and short-term implications of the attack on the healthcare services and social trust of Ireland. The report will be concluded by viable recommendations that will be focused on enhancing cyber resilience, enhancing incident preparedness, and mitigating the occurrence and effects of such an attack in the future [1].

2. Background of the Incident

Ransomware attack against the HSE was not an isolated incident requiring a sudden attack but the culmination of a long-term and well-planned incursion. It was later found out that the attackers had into the HSE network several weeks prior to the deployment of the ransomware. The first breach took place in mid-March of 2021 with a phishing email being sent to an employee at the HSE with a malicious Microsoft excel attachment. After the file was opened on 18 March 2021, hidden malware operated on the work station of the user, which was later discovered to be the initial point of compromise or patient zero [2].

After this initial compromise, the threat actors outlined persistence in the environment and started systematic internal activities. During the next few weeks, they performed reconnaissance on the

network, stole user credentials, escalated privileges and laterally traversed systems. This incremental access enabled them to hit several hospitals and other important national healthcare websites that would have a great impact on the target of the attack [1].

As early as May 2021, the attackers had already gained high level administrative privileges, enabling them to access core servers in the National Healthcare Network without restriction. The malicious activity was to a large extent unnoticed or uncontrolled even though there were security alerts and warning indicators. The attackers launched the Conti ransomware on a massive scale on many systems in the early hours of 14 May 2021. Co-ordinated encryption of critical infrastructure compelled the HSE to close its national network as a containment policy which caused extensive disruption of clinical, diagnostic, administrative, and communication services throughout Ireland [2].

3. Methodology and Analytical Approach.

The current analysis of HSE ransomware case is based on the frameworks of cybersecurity investigation in order to provide the accuracy, structure, and objectivity of the research. Cyber Kill Chain model is employed as the main analytical prism that helps to reconstruct the path of the attacker, starting with first access and ending with eventual impact. The methodology assists in decomposing the incident into separate phases where each of the intrusion phases can be analyzed in a rational and chronological sequence [3].

The actions of the attackers to further reinforce the analysis are mapped to the MITRE ATT&CK framework. This will allow fundamental categorization of the tactics, techniques, and procedures (TTPs) used by the Conti ransomware group, which will give an overview of how the known adversarial techniques were implemented within the HSE environment. The paper only uses proven facts and official investigation reports and sources that have been verified publicly and no assumptions or speculative interpretations are made. It aims to give a fully developed, evidence-based strategic assessment that allows the true nature of the attack and its execution and implications to be reflected [3].

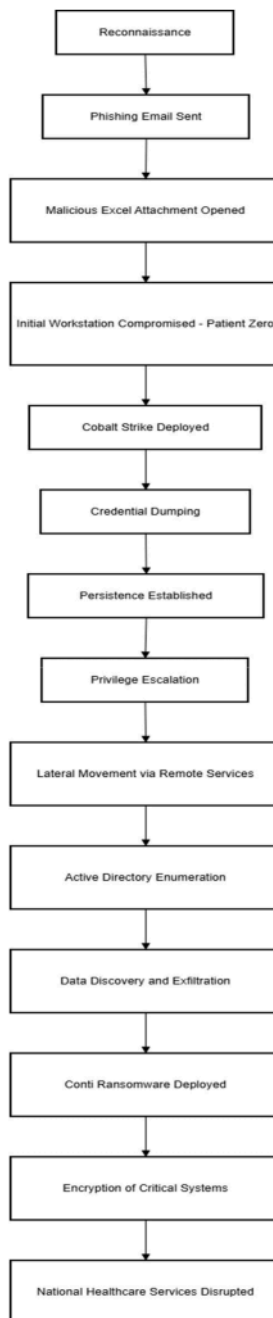


Figure 1-Attack Flow Diagram

The following flowchart shows the entire sequence of events during the Conti ransomware attack on the HSE, starting with reconnaissance and phishing, then internal exploitation and, and finally the mass encryption of systems that put healthcare services in Ireland in a frozen state [3].

4. Attack Reconstruction

4.1. First Compromise and Network Discovery.

The attack has started with a phishing attack on HSE employees, where a rogue spreadsheet has been provided to them through email. On 18 March 2021, an employee opened the attachment, and malware was embedded on the local machine, executed. This system was the first point of access by the attackers that provided them with a remote entry into the HSE environment. Based on this foothold, the attackers started to survey the internal network, probe system structures, determine high-valued assets, and map user privileges to identify possible paths to further access [4].

4.2. Implementation of Malicious Toolsets.

The attackers installed other malicious utilities once within the network to enhance their dominance. These incorporated the elements that are usually related to the Cobalt Strike framework, which allowed running the commands, monitoring the user activity, and harvesting the credentials. On 31 March 2021, security software reported alerts of suspicious behaviour which are similar to these tools. This, however, did not stop or escalate the activity, as they were on the passive monitoring mode of the endpoint protection system, and thus allowed the attackers to proceed with their activities without any hindrance [4].

4.3. Sustaining Long-term Access

In order to achieve persistence, the attackers applied persistent mechanisms on the compromised systems to achieve persistence. These methods were meant to persist in case of a system re-boot or user log-out so that the infected workstation would not be left out of control. On 23 March 2021, the attackers stopped relying on the initial phishing platform and were well established on a long-term basis within the HSE network [5].

4.4. Escalation of Privileges

In late March and all April, the attackers were working on elevating their access rights. Using system memory to retrieve credentials, including credentials stored in the LSASS process, they got accounts with high privileges in the form of usernames and passwords. This allowed them to gain access to important infrastructure including domain controllers and hospital servers, which greatly elevated the capacities of the attackers to manipulate systems and have a broader reach throughout the organization [5].

4.5. Internal Lateral Access and Internal Spread

With privileged credentials, the attackers traversed the network of HSE in April and early May on a lateral basis. Its combination of a flat network architecture and little internal segmentation enabled them to move through systems with little or no resistance. They had hacked into various hospital settings between 7 and 12 May 2021 using regular administrative procedures and remote access services like SMB, PsExec and RDP. In the process, the attackers were able to access extensive administrative and clinical systems and review sensitive data which was stored in the network [6].

4.6. Command and Control Operations.

The attackers had connections with the external command and control infrastructure during the intrusion. Instructions were relayed using encrypted Cobalt Strike beacons, stolen data was relayed and further actions were coordinated. Obfuscated and encrypted traffic was used to make it hard to detect them and to enable the attackers to remotely control compromised systems without being noticed instantly [6].

4.7. Data Theft and Creation of leverage.

During the days preceding the ransomware activation attackers stole HSE systems of massive amounts of sensitive information. Although the real numbers were not reported, during forensic analysis, it was proved that confidential information was stolen and eventually leaked into the internet. This stealing was a secondary pressure strategy, as it allowed the attackers to intimidate the disclosure of patient and organisational information publicly even in the event that the system recovery process was successful [7].

4.8. Ransomware Activation and National Impact.

Later in the evening of 14 May 2021, the final phase of the operation was initiated when the attackers deployed Conti ransomware on the many servers at once. Electronic health records, diagnostic platform, radiology services, and administrative databases were promptly encrypted, which are all critical healthcare systems. The synchronized deployment meant that it was planned and staged heavily beforehand. The HSE decided to disconnect the national network to stop the further spread as soon as it became evident that the scale of the compromise is tremendous. This move caused widespread disruption to the service, as hospitals and health care providers throughout Ireland were forced to go back to manual processes and this headlined one of the most serious operational disasters the entire national health care system has ever faced [8].

5. MITRE ATT&CK Analysis

The operations that can be seen in the case of the HSE ransomware are highly linked to various tactics and techniques that can be outlined within the MITRE ATT&CK framework, which can be used to show that the attack can be characterized as organized and well-defined. The first tradeoff is in agreement with the spear-phishing attachment method, in which a malicious document was deployed to get a first payload and create a foothold in the environment [8].

After the first access, the execution of malware and other supporting scripts indicates command-line execution and PowerShell abuse, which allowed the attackers to execute tools, load further executables, and communicate with the affected systems. Persistence mechanism was introduced to keep a continuous access whereby scheduled tasks were applied so that even after system restart or user logout the attackers could still have access [9].

Credential dumping was used to obtain privilege elevation with the help of pulling out sensitive authentication information out of the LSASS process. This was a backdoor to high-privilege accounts and control over critical servers and domain infrastructure. With these stolen credentials, the attackers conducted subsequent lateral movement through the network through trusted remote services including RDP, PsExec and SMB enabling them to gain access to as many hospital systems as they could with little resistance [9].

The Cobalt Strike was used to carry out command-and-control operations and served as an encrypted channel of communication to issue commands and sustain remote access as well as coordinate the activities of the attacks. This action matches ATT&CK strategies of remote executing commands and beaconing which aim to avoid detection and keep attacker control [10].

In the last phase, the Conti ransomware deployment and further encryption of the critical systems are related directly to the data encryption of impact technique. Before this, data leakage was performed via the same command-and-control systems which further strengthened the position of the attackers based on the threat of publicity of the data [11].

In general, mapping of this incident to the MITRE ATT&CK framework depicts a vertically oriented enterprise-wide intrusion. The attack followed a well-defined sequence of steps, including initial access, execution, persistence, privilege escalation, lateral movement, command-and-control, data exfiltration, and impact, which proved that the Conti operators had high technical capabilities as well as the degree of operational maturity of a typical human-operated ransomware teams [11].

6. Root Cause Analysis

6.1. Gaps in Technology and Infrastructure

The magnitude of the HSE breach was greatly contributed by the weaknesses in the technical environment under it. There was also the lack of effective internal network segmentation, which was one of the most important problems. Major portions of the national healthcare network were interconnected in a manner that was largely very broad which allowed attackers to wander freely as soon as they gained access. Isolation between systems was not as efficient and this minimized the containment controls [12].

Moreover, numerous endpoints and servers were operating incompatible and old operating systems, the most frequent being the legacy versions of Windows. They were systems that were not up to date on security and could easily be exploited. The fact that modern endpoint detection and response (EDR)-capabilities were not fully deployed also minimised visibility of the malicious activity and early stages of attacker behaviour could go undetected [12].

6.2. Organisational and Procedural Weaknesses.

In addition to technical complications, internal operational activities led to the intensity of the incident. The endpoint protection tools did not issue security alerts that were responded to decisively and in time. The antivirus software was configured to be used in a passive, alert-only mode, this was so that suspicious activity was recorded but not automatically blocked or escalated.

The company also did not have a centralised security monitoring and incident response capability. In the absence of a specific Security Operations Centre or similar facility, no system-wide correlation of individual alerts was in place and it took longer to identify a coordinated attack. Additionally, the procedures of incident response were not defined properly, or not practiced regularly, so the teams were not ready to respond to a nationwide cyber incident within a short time [13].

6.3. Leadership, Oversight and Strategic Weaknesses.

At the strategic level, the HSE had an intermittent cybersecurity governance. An overall executive authority that was clearly in charge of information security, or one that had a Chief Information Security Officer, was lacking to offer leadership and responsibility. There was no coordinated behavior and unified control over the distribution of cybersecurity responsibilities across various departments.

There was also a disparity in security standards and controls between hospitals and other related healthcare organizations, which introduced disproportional protection levels in the entire ecosystem. This discrepancy made the network more exposed to the attacker and made the network susceptible to the weakest areas. Moreover, the business continuity planning and disaster recovery were not developed. Lack of a current system documentation and an extensive asset inventory complicated the process of recovery and slowed down prioritisation efforts in the response stage.

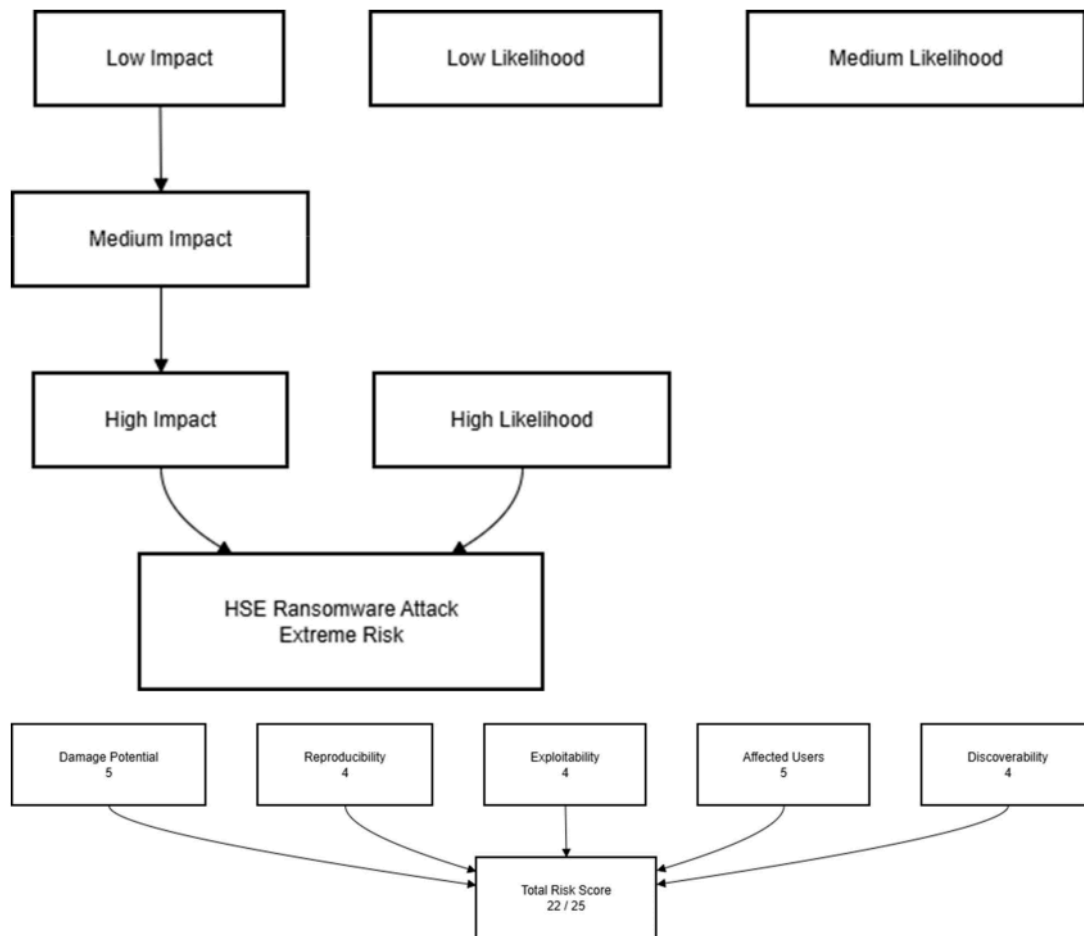
7. Risk and Impact Assessment

The impact of the ransomware attack on the national healthcare of Ireland had both short-term and long-term effects. Critical information technology systems that assist in patient care were made inaccessible and hospitals and clinics had to use manual and paper-based procedures. This abrupt withdrawal greatly affected the normal functioning and emergency services as outpatient

appointments were delayed, there were backlogs in diagnosing patients, and there was a long queue in the emergency departments. Services with high dependency levels like radiology and oncology were affected especially as some patients have had to wait longer to get services that are time sensitive.

In addition to disruption of operations, the incident came with severe legal, regulatory and privacy risks. The illegal access and release of confidential patient and organisational information put the HSE under the risk of compliance breaches and reputational harm. Criminal proceedings had to be taken in order to contain further spread of compromised information. The recovery was not quick and not that easy; systems and services could be restored only after a great amount of coordination and it took several months, and the complete operational recovery lasted until the summer of 2021.

Strategically, the incident highlighted how the healthcare industry is appealing to ransomware groups. The sensitivity of the data, dependence on IT systems to operate its operations, and the high level of downtime intolerance, contributed greatly to the probability of attack and its potential consequences. The magnitude of the disruption, which includes thousands of systems and millions of patients in the country, classifies this incident as a strong example of extreme organisational risk. Not only did it cause a loss of money, but also had direct effects on patient safety, service disruption, and national trust in healthcare infrastructure.



Interpretation

The HSE incident is rated the highest in the risk matrix of likelihood and impact, as it is a systemic risk of healthcare infrastructure being vulnerable to ransomware. This classification is also supported by the DREAD assessment with almost maximum scores in all dimensions. The presence of high damage potential, the prevalent impact on users, and the relatively easy exploitability all present arguments as to why this incident is a critical and long-lasting threat to the functioning of the healthcare of the nation.

8. Strategic Recommendations

The HSE ransomware incident illustrates the necessity of the thorough and longlasting change of the cybersecurity approach on a national healthcare scale. To combat the threats in the future, leadership, technology, operations, and organisational culture must be improved in coordination and technical solutions alone will not work.

Cybersecurity needs to be put on the strategy list at the governance level with the executive ownership. A specialised cybersecurity team should be supported by creating a specific information security leadership role to ensure accountability, consistency, and control of all healthcare organisations. Such a structure must provide a consistent level of security and allow to make decisions in line during an incident.

Infrastructure wise, there is a need to be modernized. The decommissioning of legacy and unsupported systems must be carried out in a systematic manner and the systems substituted with secure, proactive supported platforms. The network architecture must also be redesigned to impose high levels of segmentation and zero-trust, so that attackers cannot move laterally once they have initially compromised it. These controls would greatly minimize the area of blast of future intrusion.

There should also be an improvement in detection and response capabilities. By developing a national Security Operations Centre, the country would be capable of monitoring continuously, centralised alert correlations and fast escalations of incidents. Combining better endpoint detection and responses with improved logging and threat intelligence would allow seeing into bad behavior earlier and intervene sooner.

Other protection strategies must involve implementation of multi-factor authentication on all privileged and remote-access accounts, strict vulnerability and patches management systems, and regular staff security awareness training. Phishing is also one of the main attack vectors and therefore continuous education is of the essence in minimizing the risk associated with human beings.

Lastly, organisational resilience should be enhanced with a sound incident response and disaster recovery planning. Procedures to follow when responding are clearly documented, tabletop and

live exercises are conducted on a regular basis, and backup and restoration capabilities are well tested so that disruption of services in case of a future incident is reduced. With preparedness integrated into routine, the HSE will be able to minimize the time of recovery, save the lives of patients, and build more trust in the capacity of the national healthcare system to resist cyber threats.

9. Summary

The HSE ransomware attack is an example of how a single, low-high-complexity attack-vector can grow into a national crisis when used in combination with systemic technical vulnerabilities, operational failures, and uncoordinated cybersecurity management. A phishing email started to develop into a sophisticated intrusion, which lasted a long time and was executed with professional-level equipment, by which the hackers used the known vulnerabilities, installed the tooling, and managed to stay unnoticed to organize and conduct a coordinated ransomware attack.

The consequences of the event spread far beyond the digital infrastructure. The impact caused a direct disruption on critical clinical systems that impact directly on healthcare delivery in the whole of Ireland and added pressure on staff besides affecting timely patient care. The given case highlights the fact that any cybersecurity failure in the healthcare setting is not a technical matter but might also be translated into a risk to the safety and confidence of the population.

All in all, such analysis supports the criticality of the enhanced cybersecurity policy, modernised infrastructure, and exerciseable operational preparedness among healthcare organizations. Through taking a proactive and tactically aligned stance with cyber resilience, national healthcare systems will be able to play a bigger role in preventing, detecting and responding to more advanced cyber threats of the future.

Task 2

1. Introduction

This report is a simulation on Red Team exercise on Cureton Pharmaceutical Company (CPC) under Operation IP Shield. CPC is in the pharmaceutical research industry, and proprietary research data and clinical information is one of the most valuable resources and is vulnerable to advanced cyber attackers. The main aim of this exercise was to test the capability of CPC to survive, identify and counter the advanced threat conditions such as high-caliber criminal organizations or professionally sponsored agents, which are normally interested in interfering with intellectual property [11].

The test was conducted in a controlled hybrid test environment that replicated the operational environment of CPC. This consisted of simulated on-premises research network together with an AWS hosted cloud-based portal infrastructure. The simulation purely depended on the tools of graphical user interface (GUI), configuration analysis, and observational methods provided through the AWS Management Console. There was no active vulnerability scanning, active malware deployment or intrusive exploitation of the exercise.

This engagement was to procedurally simulate adversarial behaviour, paths, and lateral manoeuvres typical of an advanced threat actor, and operate within ethical limits and evaluation limitations entirely. The purpose of the exercise was to gain useful information on the defensive posture of CPC, threat detection capabilities, and overall resiliency to cyber threats made with using intellectual property because it did not disrupt the exercise.

2. Objective of the Engagement

The main purpose of this engagement was to assess how a persistent attacker can use his way into the hybrid technology environment of Cureton Pharmaceutical Company and advance into the high-value assets, in particular, research ownership and confidential clinical information. Instead of conducting live exploitation or extracting actual information, this exercise was aimed at determining possible attack paths and finding architectural and procedural vulnerabilities that can be exploited by a sophisticated threat agent [12].

Besides the modeling of the adversarial access and movement, the assessment aimed to determine the efficiency of the current defensive controls such the existence of visibility, monitoring, and detection capabilities. Special focus was also put on the identification of the gaps that may slow down or eliminate the detection of malicious activity and the areas where the existing controls proved resilient.

The interaction was also going to result in actionable risk-informed suggestions that would enhance the security posture of CPC. Finally, the exercise would increase the organisational preparedness, raise awareness within the organisation about cyber risk, and gain further insight into the threats of running a hybrid environment, which incorporates on-premises infrastructure with cloud-based services [13].

3. Environment Overview

3.1. Hybrid Architecture Design

The test environment simulated was meant to replicate a hybrid enterprise infrastructure that is reflective of the operations infrastructure of Cureton Pharmaceutical Company. It consisted of two major logical environments, one being a research-oriented internal network and the other being a cloud-based open platform. The simulated internal environment mirrored CPC in terms of its research and development system and featured a central management system, a research data warehouse, and a user workstation that was filled with representative (non-production) research data [14].

The external environment was the clinical trial portal of CPC and they were held in a different virtual cloud based network. Such an environment came equipped with a privately hosted application server, which was used to support a publicly accessible service, which enabled realistic modelling of interaction of attackers with internet-facing assets. The AWS graphical management interface was used to create and manage all the networking components of the network such as virtual networks, subnets, routing settings, gateways and access control mechanisms. The general design was typical of enterprise hybrid architectures because of built in security controls overlayed, regulated interconnectivity and logical isolation of internal and external resources.

3.2. Network Segmentation and Access Control.

The principles of strong segmentation were used across the environment so that they could resemble the way security is practiced in an enterprise. The user workstations, administrative systems and research data servers were put in separate user network segments within the research network. The subnet that was hosting sensitive research data was secluded to form a high-value asset that needed higher security.

The application server was deployed in a private subnet and components that needed to communicate externally were put in a special public one in the cloud-hosted portal environment. Controlled virtual network peering between the internal research environment and the cloud portal was also facilitated, by allowing the setup of such a peering only using AWS graphical interface. The flow of access between systems was controlled by the security group rules that had a narrow range and allowed only necessary lines of communication [15].

This design segregation guaranteed that inter environmental traffic was intentional and limited, and appropriately representative of best-practice enterprise network designs and gave a realistic foundation to evaluate how adversary movement may be in a hybrid infrastructure.

4. Methodology

4.1. Planning and control measures in engagement.

Before the actual exercise started a detailed Rules of Engagement (RoE) framework was put in place to control every activity during the assessment. This plan identified the extent of the involvement, accepted systems and environments and provided rigorous boundaries on the operation. Misuse like live exploitation, unauthorised privilege escalation, data modification and installing offensive security tools were specifically forbidden.

It was only allowed to use low-risk operations such as passive visibility of cloud formations, audit the access controls via the AWS graphical interface, and non-intrusive connectivity tests. These restrictions made sure that the exercise was safe, controlled and non-disruptive and still gave a realistic insight into adversarial behaviour. The method was meant to conform to the organisational security policies and the academic standards of assessment.

4.2. Simulation of Adversary Behaviour

Instead of actual attacks, the methodology was aimed at the reconstruction of the decision-making process and movement patterns of a highly competent threat actor. An initial foothold was created by setting up a notional presence of an attacker within the public-facing section of the cloud portal environment. It was based on this position that the assessment focused on the analysis of observable network relationships, available resources, and metadata that is disclosed by the configuration settings.

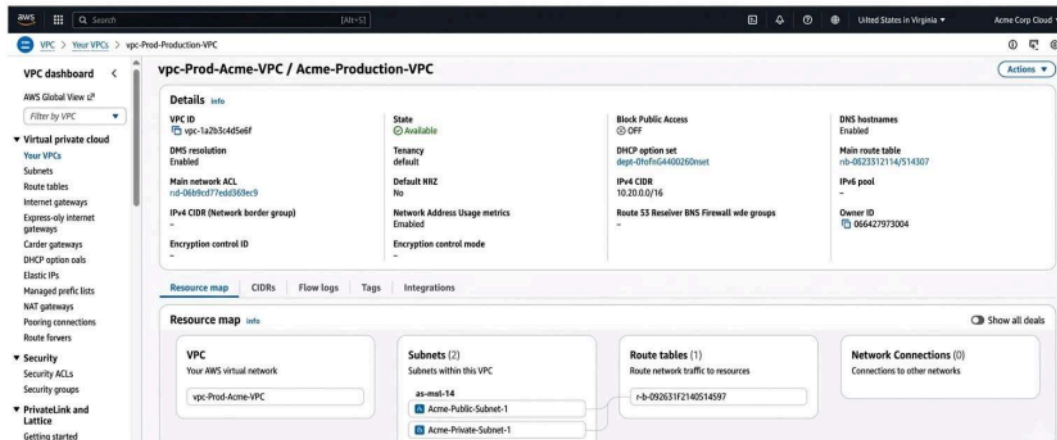
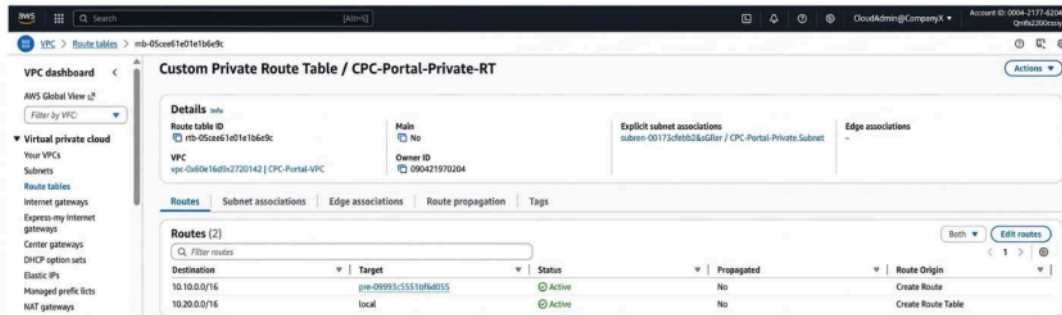
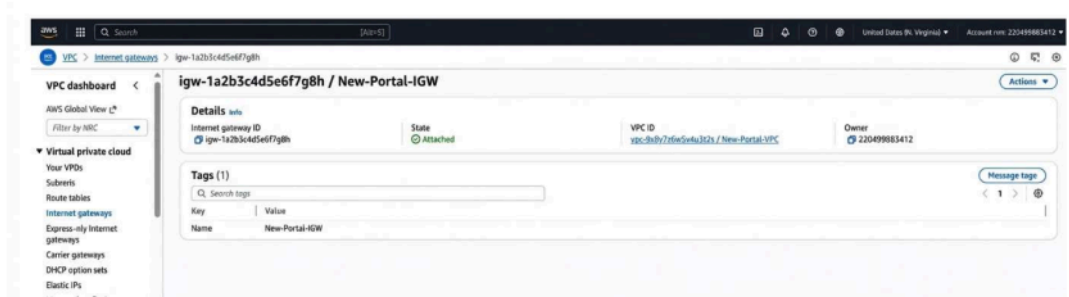
The activity consisted of analyzing the way forward of an adversary that could rationally navigate the environment based on routing paths, trust relations and access controls. Basic operating system level connectivity tests had been employed to confirm theoretical access without passing harmful commands or automated scans. This method offered a realistic representation of reconnaissance and situational awareness operations that are done by attackers, but in a non-invasive position.

4.3. MITRE ATT&CK Framework Alignment

To provide consistency and analytical integrity, the simulation was mapped to pertinent tactics and techniques in the MITRE ATT&CK framework. Reconnaissance efforts were paralleled with methods related to network and system intelligence gathering, which is a reflection of how enemies map the target environments with the goal of determining where they can enter and their exit routes. Creation of the simulated attacker system was aligned to ideas of infrastructure development, which is the way threat actors prepare tools of operation.

The discovery activities were modeled on the controlled observation of the visibility of the accounts, network connections, and available services, the reflection of the typical adversarial discovery approaches without the implementation of malicious behavior. The concepts of data collection and exfiltration were expressed in form of the artificially created research data in the environment bearing in mind that no real or sensitive information was accessed. This methodical mapping gave the exercise technical richness and offered a clear academic basis of assessing adversarial behaviour in hybrid clouds.

5. Execution Summary



Project Neptune VPC

Details

VPC ID: vpc-0a23a073a7730142

State: Available

Block Public Access: Disabled

ENI resources: 1

Subnets: 3

Route tables: 1

Network connections: 1

Resource map

VPC: Your AWS VPC network

Subnets (3):

- Project Neptune DB Subnet
- Project Neptune RT Subnet
- Project Neptune Private Subnet

Route tables (1):

- Project Neptune RT
- Project Neptune Private RT
- Project Neptune Public RT
- Project Neptune Private RT

Network connections (1):

- Project Neptune DB

sg-1a2b3c4d5e6f7g8h9 - Production-Web-App-SG

Details

Security group name: Production-Web-App-SG

Security group ID: sg-1a2b3c4d5e6f7g8h9

Description: Security group for main production web application and database

VPC ID: vpc-abcdef01234567890

Owner: 123456789012

Inbound rules count: 3

Outbound rules count: 1

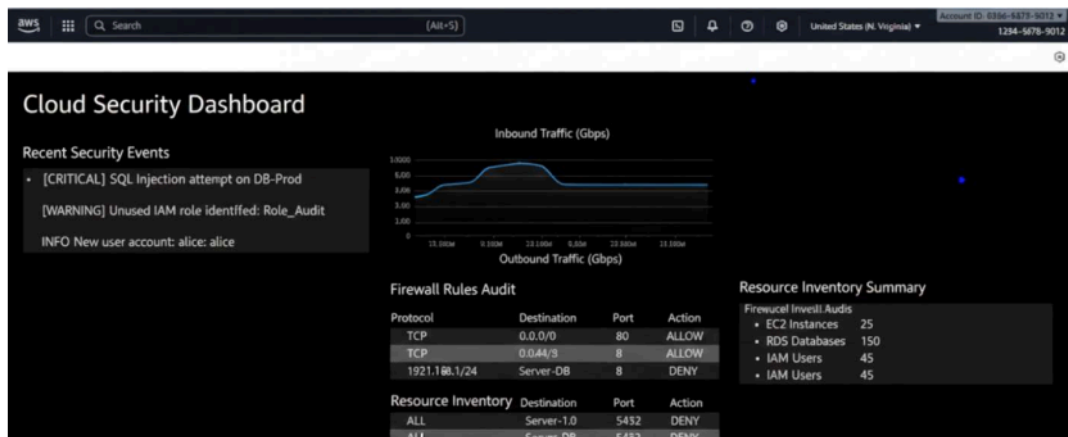
Inbound rules (3)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Port range
-	sg-a1b2c3d4e5f6g7h8	IPv4	HTTPS	TCP	443	0.0.0.0/0
-	sg-i9j0k1l2m3n4o5p6	IPv4	SSH	TCP	22	192.168.10.0/24
-	sg-n7r8e9f0a1b2c3d4	IPv4	MySQL/Aurora	TCP	3306	0.0.0.0/0

Cloud Resources

Instances (5)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
Web-Server-Prod	i-0abcde1234567890	Running	t3.large	2/3 checks passes	54.215.100.000	us-west-2a	-
Database-Dev	i-0fghi9876543210	Running	t3.micro	2/3 checks passes	Frommesterbb	us-west-2a	-
Worker-Serve	i-0jklm9999999999	Running	Stopped	2/3 checks passes	[Owner: JohnD]	35.160.XXX.X	-
LoadBalancer-Ext	elb-abcd1234567890	us.micro	3/3 checks passes	[Public: True]	[Public: True]	-	
SS-Bucket-Logs	extensio1234567890	us.micro	3/3 checks passes	Compliance: Yes	Compliance: Yes	-	



```

Scanning subnet: 192.168.1.0/24
Device: 192.168.1.1, Router
Device: 192.168.1.10, Type: PC, Router, Vendor: Vendor : Cisco
Device: 192.168.1.15, Type: User: Alice
Device: 192.168.1.15, Type: Server: Server : Printer
Device: 192.168.1.10, 20

Traceroute to 8.8.8.8
1. Traceroute: 8.8.8.8
Composite destination: 202 routed fwb batt ploupa global dynamic snad
2. Host: 192.168.1.10, 10.10.10.10, 10.10.10.10
Traceroute: 202 10.10.10.10, 10.10.10.10
3. Host: 192.168.1.10, 10.10.10.10, 10.10.10.10
4. Host: 192.168.1.10, 10.10.10.10, 10.10.10.10

```

5.1. Attacker System Placement

In the Portal VPC, a special instance of a hypothetical attacker was placed in the public subnet to simulate the first stage of an external attacker. This virtualized environment enabled the team to test internal connectivity safely, learn about possible attack vectors and see how an attacker would hypothetically locate himself in the environment. The case was not offensive at all, and no active exploitation and security-changing tools were present.

5.2. Safe Reconnaissance and Internal Mapping.

Resource mapping and network visibility was achieved by using purely passive, risk-free techniques. The spelling of routing tables, subnets and security was reviewed at the AWS console. In-built system commands and GUI-based instance metadata inspection were used to give a clue about network relationships, connectivity of a host, and available services. Simple connectivity

tests were conducted as a check that theoretical communication routes existed between the simulated attacker system and internal assets. There were no active scanning or enumeration tools involved and the engagement was conducted in accordance to the predetermined Rules of Engagement.

5.3. Sensitive Asset Identification.

In order to simulate the possible targeting of proprietary research information, a dummy file of high value information was put in the file server of the research network. This enabled the exercise to show how an enemy would find areas of significant value without having real sensitive information. By determining the location and the availability of these resources, CPC would have known the possible risk points and how attackers would conceptualize how to get these assets in the real world scenario.

5.4. Path Simulation of Data Exfiltration.

Although there was no exfiltration done, there was a theoretical route recorded to demonstrate how the information could be carried out of the internal file server to an attacker controlled system in the event security controls were not implemented or configured. This theoretical framework emphasized the need to have proper network segmentation, monitoring and access control policies. The simulation of this pathway provided CPC with an understanding of possible vulnerabilities and defensive steps that would ensure that real-world data is not compromised.

6. Findings and Observations

6.1. Strengths on security identified

The emulated environment had a well-founded security design. Natural separation of workloads was always applied and network segmentation was efficient to make sure unwarranted exposure between systems is not done. The access control mechanisms were also scoped accordingly and the routing configuration only permitted intended communication paths without interfering with clear delimitations between the internal and external environment. In general, the hybrid architecture was the reflection of a considerate security-first attitude and a good foundation to secure valuable pharmaceutical research resources.

6.2. Limiting Factors of Visibility and Detection

Although the structural controls are strong, it was possible to identify the opportunities of improvement in the field of monitoring and detection. There was poor visibility of internal assets especially in relation to host identification and name resolution which may slow down prompt threat identification. There was little endpoint level monitoring which minimised the potential to detect the presence of anomalous behaviour or lateral movement in the environment.

There were also no deployed network traffic inspection and centralised alerting mechanisms that were fully deployed on all segments. This prevented the efficiency of the threat detection at the early stages and minimised the organisations capability to detect suspicious activity in a fast manner. Situational awareness and response preparedness would greatly be enhanced by improving telemetry gathering and implementation of the detection systems.

REFERENCES

- [1] Yaacoub, Jean-Paul A., Hassan N. Noura, Ola Salman, and Ali Chehab. "A survey on ethical hacking: issues and challenges." arXiv preprint arXiv:2103.15072 (2021).
<https://arxiv.org/abs/2103.15072>
- [2] Yaacoub, Jean-Paul A., Hassan N. Noura, Ola Salman, and Ali Chehab. "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations." Internet of Things and Cyber-Physical Systems 3 (2023): 280-308.
<https://www.sciencedirect.com/science/article/pii/S2667345223000238>
- [3] Raman, R., Calyam, P., & Achuthan, K. (2024). ChatGPT or bard: who is a better certified ethical hacker?. Computers & Security, 140, 103804.
<https://www.sciencedirect.com/science/article/pii/S0167404824001056>

- [4] Maulana, Furqan, Hanif Fajri, Muhammad Fakhrol Safitra, and Muharman Lubis. "Unmasking log4j's vulnerability: protecting systems against exploitation through ethical hacking and cyberlaw perspectives." In 2023 9th international conference on computer and communication engineering (ICCCE), pp. 311-316. IEEE, 2023. <https://ieeexplore.ieee.org/abstract/document/10246082/>
- [5] Nasir, M. Shahzar, Hamayun Khan, Ahmad Qureshi, Arslan Rafiq, and Taha Rasheed. "Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review." *Spectrum of engineering sciences* 2, no. 3 (2024): 420-454. <https://sesjournal.com/index.php/1/article/view/56>
- [6] Filinovych, Valeriia, and Assel Mukasheva. "Can hacking be ethical: A legal review." (2025). <https://ceur-ws.org/Vol-4024/short04.pdf>
- [7] Erdődi, L., & Zennaro, F. M. (2022). The Agent Web Model: modeling web hacking for reinforcement learning. *International Journal of Information Security*, 21(2), 293-309. <https://link.springer.com/article/10.1007/s10207-021-00554-7>
- [8] Dhirani, Lubna Luxmi, Noorain Mukhtiar, Bhawani Shankar Chowdhry, and Thomas Newe. "Ethical dilemmas and privacy issues in emerging technologies: A review." *Sensors* 23, no. 3 (2023): 1151. <https://www.mdpi.com/1424-8220/23/3/1151>
- [9] Formosa, Paul, Michael Wilson, and Deborah Richards. "A principlist framework for cybersecurity ethics." *Computers & Security* 109 (2021): 102382. <https://www.sciencedirect.com/science/article/pii/S0167404821002066>
- [10] Aibekova, Altynai, and Vinesha Selvarajah. "Offensive security: Study on penetration testing attacks, methods, and their types." In 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pp. 1-9. IEEE, 2022. <https://ieeexplore.ieee.org/abstract/document/9792772/>
- [11] González, Ariel López, Mailyn Moreno-Espino, Ariadna Claudia Moreno Román, Yahima Hadfeg Fernández, and Nayma Cepero Pérez. "Ethics in artificial intelligence: An approach to cybersecurity." *INTELETICA* 1, no. 1 (2024): 38-54. <http://inteletica.iberamia.org/index.php/journal/article/view/7>

- [12] Vadisetty, R., 2024, March. AI-Based Smart Governance. In International Ethical Hacking Conference (pp. 481-496). Singapore: Springer Nature Singapore. https://link.springer.com/chapter/10.1007/978-981-97-8457-8_30
- [13] Heiding, Fredrik, Sotirios Katsikeas, and Robert Lagerström. "Research communities in cyber security vulnerability assessments: A comprehensive literature review." Computer Science Review 48 (2023): 100551. <https://www.sciencedirect.com/science/article/pii/S1574013723000187>
- [14] George, A. Shaji, and S. Sagayarajan. "Securing cloud application infrastructure: understanding the penetration testing challenges of IaaS, PaaS, and SaaS environments." Partners Universal International Research Journal 2, no. 1 (2023): 24-34. <https://www.puirj.com/index.php/research/article/view/84>
- [15] Kuforiji, John. "The importance of integrating security education into university curricula and professional certifications." International Journal of Technology, Management and Humanities 11, no. 03 (2025): 1-10. <https://www.ijtmh.com/index.php/ijtmh/article/download/147/146>

FINAL GRADE

GENERAL COMMENTS

76/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

GRADING FORM: L7 - (ETHICAL HACKING)

HIMANSHU JIGNESHBHAI SOMPURA

76

ENGAGEMENT WITH LIT (15)

Engagement with Literature Skills



Engagement with academic literature. Sources are relevant. IEEE referencing used.

13

KNOWLEDGE & UNDERSTANDING (10)

Knowledge and Understanding Skills

-  Demonstrates understanding of ransomware operations, MITRE ATT&CK and healthcare targeting at postgraduate level. **9**

COGNITIVE & INTELLECTUAL (40)

Cognitive and Intellectual Skills

-  Critical analysis of the HSE incident with clear reasoning and strategic insight. Task 2 shows good conceptual adversary thinking. Both tasks met the criteria. **32**

PRACTICAL APPLICATION (30)

Practical Application Skills

-  The executives summary provides a number of screenshots that needs to be numbered, named and discussed. No lab build diagram, ATT&CK mapping, etc. **18**

TRANSFERABLE SKILLS (5)

Transferable Skills for Life and Professional Practice

-  Professional structure flow and cover page present. Paragraphs fully formatted and justified. **4**

