



Module: Ethical Hacking

Module Code: ACCA7033

Submitted To:

Dr. Carlene Campbell

Associate Professor

University of Wales Trinity Saint David

Submitted By:

MD. Eyamin Molla

Student ID: 2425028

University Of Wales Trinity Saint David

Submission date: 14-01-2026

Abstract

This report presents the strategic-level analysis of a real-life cybersecurity breach and a realistic red team exercise in a regulated virtual laboratory setup. The first part presents a critical analysis of a recent high-tech cyber attack on a pharmaceutical or healthcare-related organisation, visualising the adversary's behaviour in relation to the MITRE ATT&CK Enterprise model, deconstructing the reasons for the breach, and recommending strategic prevention and detection strategies.

The second section describes a red team exercise, dubbed Operation IP Shield, that targeted an artificial hybrid infrastructure based on the Cureton Pharmaceutical Company (CPC). The engagement is similar to that of an Advanced Persistent Threat (APT) actor who is attempting to steal sensitive pharmaceutical research information. The operation will comprise rules of engagement, threat emulation planning, environmental design, reconnaissance and exploitation execution, data exfiltration, and detection gap analysis.

The report contains strategy recommendations and cost/benefit analysis, which involves the translation of technical findings into risk consideration on the business level. The overall idea is to demonstrate the level of offensive security proficiency, critical thinking, and professional writing in accordance with Level 7 postgraduate standards.

Table of Contents

Abstract.....	1
Tables of Figures.....	4
Table of Tables	5
1. Introduction.....	6
2. Task 1: Strategic Threat Analysis of a Real-World Cyber Attack	7
2.1 Attack Overview	7
2.2 MITRE ATT&CK Mapping.....	8
Reconnaissance and Discovery.	8
Initial Access	8
Execution and Persistence	9
Credential Access and Lateral Movement.....	9
Impact and Command and Control.	10
2.3 Root Cause Analysis	13
2.4 Strategic Prevention and Detection Recommendations.....	14
3. Task 2: Red Team Engagement – Operation IP Shield	15
3.1 Scenario Overview	15
3.2 Rules of Engagement.....	16
1. Purpose and Objectives	16
2. In-Scope / Out-of-Scope.....	16
3. Authorized Techniques and Constraints.	17

4. Assumptions	17
5. Stealth and Safety.....	17
6. Escalation and Communication.....	17
7. Legal and Ethical Conformity.	17
3.3 Threat Emulation Plan	18
3.4 Lab Environment Design & Architecture	19
Environment setup.....	21
3.5 Attack Narrative – Phase by Phase	26
Phase 1: Reconnaissance and Host Discovery	26
Phase 2: Service Discovery and Target Profiling	28
Phase 3: Web Enumeration and Data Discovery	29
Phase 4: Authenticated Access	29
Phase 5: Exfiltration.....	30
3.6 Technical Report – Blue Team View	31
3.7 Detection Gap Analysis	32
3.8 Strategic Recommendations	33
3.9 Cost–Benefit Analysis	34
3.10 Executive Brief – Board Level	34
4. Conclusion	35
References:.....	36

Tables of Figures

Figure 1: Network Architecture Diagram	20
Figure 2: Set up Windows 10 Pro	21
Figure 3: Set up Ubuntu	22
Figure 4: Set up Kali Linux	23
Figure 5: Set up the Windows Server 2022.....	24
Figure 6: Create the Domain Name	25
Figure 7: Reconnaissance and Host Discovery	27
Figure 8: Service Discovery and Target Profiling.....	28
Figure 9: Web Enumeration and Data Discovery.....	29
Figure 10: Authenticated Access.....	30
Figure 11: Confirm access and identity	30
Figure 12: Exfiltration.....	31
Figure 13: Detection Gap Analysis	33

Table of Tables

Table 1: MITRE ATT&CK Mapping.....	10
Table 2: Threat Emulation Plan	18

1. Introduction

Offensive security has evolved to be more than the traditional vulnerability scanning and penetration testing to sophisticated red teamwork, which simulates tactics, techniques, and procedures of the actual-world threat actors (Kovacevic and Gros, 2020). The current cyber attackers, and particularly the Advanced Persistent Threats (APT), are strategic, dwell longer and are concerned with stealth, persistence, and stealing valuable information. Commercial, scientific, and strategic value of proprietary research data, clinical trial results, and intellectual property is a very attractive target to pharma and healthcare organisations.

This report has two complementary purposes that are being addressed. It first gives a strategic analysis of a recent sophisticated cyber-attack of a pharmaceutical, healthcare, or research-based organisation. This paper examines the way the attack occurred, visualisation of enemy actions to the MITRE ATT&CK Enterprise framework, and identification of the technical, architectural, and organisational factors that contributed to a breach. Special focus is placed on the actualisation of why the existing security measures have failed to avert or react to the intrusion.

Second, these strategic insights are applied to the design and implementation of a red team exercise against a simulated pharmaceutical research setting in the report (Chang *et al.*, 2024). Operation IP Shield, as it is codenamed, is a simulation of activities of an APT that targets the theft of sensitive research information out of a hybrid enterprise system. All this is carried out under controlled academic lab conditions and is based on the principles and guidelines of engagement that are linked to ethical hacking.

It is not merely a piece focused on highlighting certain technical weaknesses but it is also focused on demonstrating how advanced attackers may operate, and how the organization may improve their position by making informed investment, become more visible, and it is also focused on the way to shift the architecture.

2. Task 1: Strategic Threat Analysis of a Real-World Cyber Attack

2.1 Attack Overview

The selected real-life case of cyber security incident is the 2020 ransomware attack of Universal Health Services (UHS), one of the largest healthcare providers in the United States. UHS owns hundreds of hospitals and medical facilities, and therefore, it is an important healthcare organisation, the services of which directly impact patient safety and clinical business. The assault is widely attributed to the Ryuk ransomware group, a profit-driven threat group that has been attacking medical and critical infrastructure organization's in multi-stage and complex assaults (Jimmy, 2023).

It is assumed that the attack was launched using a phishing email that assisted attackers in installing malware and establishing a foothold in the internal network. The attacker performed internal reconnaissance to target high-value systems on entry, escalated privileges and moved laterally through the network using compromised credentials. The attackers had installed ransomware payloads in servers and endpoints within a period of a few days to execute the final stage of encryption. This coordinated effort reached a limit of derailing the processes and reduced the possible response of the organisation.

The impact of the attack was short and sweet. Several facilities were put on unavailability due to the unavailability of clinical systems, electronic health records, laboratory services and internal communications. This pushed hospitals to revert to manual and paper systems that led to delayed treatment, cancelled surgeries and greater exposure to patient care (Kalantari *et al.*, 2025). In business terms, UHS registered colossal losses in system downtime, cost of recovery and loss in the operations. Regulatory and legal problems related to the incident were also the protection of data, patient safety, and legal issues of healthcare regulations.

This ransomware is evidence of the sophistication of the ransomware groups that operate as an APT, with stealth, lateral movement and timely precision. It provides a fine structure to examine adversary behaviour, map methodologies to the MITRE ATT&ACK framework, and identify which systemic security failures are relevant in the pharmaceutical and healthcare research setting.

2.2 MITRE ATT&CK Mapping

This section will trace the ransomware attack on the Universal Health Services (UHS) to the MITRE ATT&CK Enterprise 2021 and demonstrate that the attacker adhered to the attack lifecycle, and he did it in a logical and structured manner. The campaign may be viewed as a concerted effort to achieve the highest levels of access, persistence and operational effectiveness rather than individual attempts (Odongo, 2024).

Reconnaissance and Discovery.

- **T1046 – Network Service Discovery**

Once the attacker was granted first access, he performed internal scanning in order to identify active hosts and open services. This enabled the identification of the high-value systems, such as the clinical servers and file repositories, that would then be attacked to produce the best disruptive capacity.

- **T1016 System Network Discovery of configuration.**

The attacker gathered information on network configuration, routing, and this was utilised to construct internal segmentation and connectivity (Bugshan *et al.*, 2022). This knowledge helped to initiate the lateral flow in good time and reduce the unnecessary contact with the low-value systems.

Initial Access

- **T1566.001 – Spearphishing Attachment**

Phishing attachments are the most widespread and the most common first access technique within a healthcare facility. One of the most commonly reported parts of the incident in UHS is phishing, since it is the reported entry point and enables attackers to exploit human trust and defeat perimeter defences.

- **T1133 – External Remote Services**

The attackers can use weak or unprotected access to remote services, which are being used as an alternative access point or as a strong entry point. This kind of service is typical of healthcare organisations and can enable one to get it constantly without the recurrence of malware being present (Adebukola *et al.*, 2022).

Execution and Persistence

- **T1059.001 – PowerShell**

PowerShell was used to run the commands and control the payloads and was incorporated into the routine administration. The living off the land approach reduces the application of mistrustful binaries and complicates the detection of the endpoint.

- **T1053.005 – Scheduled Task**

The integration of the systems was made possible through scheduling. This approach adheres to a delay or synchronised deployment that is necessary in the operation of ransomware at scale.

- **T1543.003 – Windows Service**

The evolution/modification of Windows services allowed the attacker to leave a trace as well as execute the payloads at a higher privilege. The services are elements of trust, and hence, this method is effective, particularly in a business environment.

Credential Access and Lateral Movement.

- **T1003 – OS Credential Dumping**

Credential dumping was employed to provide privilege escalation and access to user reusable credentials (Sendelj and Ognjanovic, 2022). This significantly contributed to the horizontal movement of the attacker and the installation of the ransomware in a large number of systems.

- **T1078 – Valid Accounts**

The fact that the attacker had valid credentials enabled him to work in the background since the activities were on par with the normal behaviour of an administrator. This contributed to the inability to identify at an early stage.

- **T1021.002 – SMB/Windows Admin Shares**

The SMB allowed the host to move around laterally to carry out the tools and payloads efficiently. This trick is quite common in windows workplace, and so it becomes a normal network traffic.

Impact and Command and Control.

- **T1071.001 – Web Protocols**

The command-and-control communications use HTTP/HTTPS-enabled remote management without monitoring the network. They are documents that can scarcely be referred to as abnormal web traffic.

- **T1486 – Data Encrypted for Impact**

The final step was planned encryptions of systems, and it had an extensive impact on operations. The delay of this method till the greatest access was secured ensured significant clinical and business consequences.

Table 1: MITRE ATT&CK Mapping

Attack Phase	MITRE Tactic	Technique ID	Technique Name	Evidence from the Incident	Why This Technique Was Used
Reconnaissance	Reconnaissance	T1046	Network Service Discovery	Attackers scanned internal systems after initial access to identify reachable servers and services.	Enabled identification of high-value clinical and file servers for later encryption.
Discovery	Discovery	T1016	System Network Configuration Discovery	Network configuration details were gathered to understand	Helped attackers plan lateral movement and locate

				internal topology.	domain infrastructure.
Initial Access	Initial Access	T1566.001	Spearphishing Attachment	Reports indicate phishing emails were used to deliver malicious attachments.	Exploited human behaviour and bypassed perimeter controls at scale.
Initial Access	Initial Access	T1133	External Remote Services	Remote services were likely abused where access controls were weak or exposed.	Provided direct and persistent access to the environment.
Execution	Execution	T1059.001	PowerShell	PowerShell was used to execute commands and deploy tooling.	Allowed living-off-the-land execution, reducing detection risk.
Persistence	Persistence	T1053.005	Scheduled Task	Scheduled tasks were used	Ensured persistence and

				to automate execution.	coordinated ransomware deployment.
Persistence	Persistence	T1543.003	Windows Service	Malicious services were created or modified.	Enabled privileged and trusted execution across systems.
Credential Access	Credential Access	T1003	OS Credential Dumping	Credentials were harvested from compromised systems.	Enabled privilege escalation and lateral movement.
Defense Evasion	Defence Evasion / Persistence	T1078	Valid Accounts	Stolen credentials were reused for access.	Blended attacker activity with legitimate administrative actions.
Lateral Movement	Lateral Movement	T1021.002	SMB / Windows Admin Shares	SMB shares were used to move payloads.	Enabled efficient lateral movement across

					Windows hosts.
Command and Control	Command and Control	T1071.001	Web Protocols	HTTP/HTTPS traffic is used for communication.	Blended C2 traffic with normal web activity.
Impact	Impact	T1486	Data Encrypted for Impact	Ransomware encrypted systems across the network.	Maximised operational disruption and financial impact.

2.3 Root Cause Analysis

The effectiveness of the UHS ransomware attack was caused by a set of control vulnerabilities, architecture, inadequate monitoring and human factors instead of a technical failure (Shahzadi *et al.*, 2025). These systemic problems permitted the opponent to advance to various stages of the MITRE ATT&CK with little difficulty.

One of the main control failures was the absence of phishing-resistant multi-factor authentication (MFA) that was routinely implemented. This allowed Spearphishing Attachment (**T1566.001**) and External Remote Services (**T1133**) to offer a good initial access. After credentials were compromised, attackers were able to use Valid Accounts (**T1078**) without raising abnormal authentication notifications because of the lack of MFA. The endpoint security controls were also not appropriately adjusted, as they allowed running of PowerShell-based commands (**T1059.001**) and credential harvesting tasks without being detected early.

On the architectural side of the environment, the network was not segmented to a significant degree, and the attackers could conduct Network Service Discovery (**T1046**) and System Network Dynamic Discovery (**T1016**) to detect systems of interest. The isolation of privilege and segregated trust zones did not exist, and the lateral movement was therefore easily implemented through SMB and administrative shares (**T1021.002**) with a considerable magnitude of effect (Smiliotopoulos, Kambourakis and Kolias, 2023).

There were also monitoring and detection gaps, which also added to the breach. Despite the existence of logging mechanisms, suspicious behaviours were not sufficiently correlated, including abnormal execution of PowerShell and the creation of scheduled tasks (**T1053.005**) and modification of services (**T1543.003**). This led to late recognition of the last impact stage.

Lastly, human and process vulnerabilities, such as poor phishing knowledge and response time to an attack. This enabled adequate preparation of coordinated Data Encrypted for Impact (**T1486**) to achieve maximum disruption of operations.

2.4 Strategic Prevention and Detection Recommendations

The results of the strategic threat analysis suggest that an efficient defence against ransomware and APT-compliant campaigns needs a multilateral strategy focusing on prevention, early detection, and architectural resilience. The recommendations are intended to help address the identified weaknesses of the UHS attack, yet they apply to the pharmaceutical and healthcare research setting.

The implementation of phishing-resistant multi-factor authentication (MFA) for all user, administrative and remote access accounts is of the highest priority, as regarded to preventive control (Henricks and Kettani, 2019). This directly counters attacks like Spearphishing Attachment (**T1566.001**), External Remote Services (**T1133**) and abuse of Valid Accounts (**T1078**) since the attackers cannot gain access using stolen credentials. Parallel with that, privileged access management (PAM) ought to be presented with an aim of minimising the exposure of valuable administrative credentials and the efficiency of credential dumping approaches.

The capabilities in detection should be enhanced by means of better Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) tuning. To identify the suspicious use of living-off-the-land binaries, especially abnormal PowerShell execution (**T1059.001**), scheduled task creation (**T1053.005**), and unauthorised service modification (**T1543.003**), EDR policies should be set to monitor them. SIEM systems need to match endpoint and authentication with network telemetry to detect lateral movement through SMB and remote services (**T1021.002**) at the early phase of the attack cycle.

In architecture, zero-trust principles and robust network segmentation should replace flat network designs in organisations. Critical servers, research systems, and domain controllers should be separated into distinct security zones with strong access limitations (Ohri and Neogi, 2022). This restricts the effects of internal reconnaissance, like Network Service Discovery (**T1046**), and even restricts lateral movement once it has been compromised.

Prioritisation-wise, MFA implementation and EDR/SIEM initialisation are the most risk-reducing, with minimal cost of implementation in relation to the possible financial, regulatory, and reputational losses caused by operational outages caused by ransomware attacks. Although building modifications can be costlier, they offer them long term security against ransomware and threats posed by espionage. All these measures are aimed at making an organisation move toward being reactive in recovery and proactive in defence.

3. Task 2: Red Team Engagement – Operation IP Shield

3.1 Scenario Overview

Cureton Pharmaceutical Company (CPC) is a fictional pharmaceutical company that is about to achieve a big breakthrough in terms of R&D. The very high commercial and strategic value of the intellectual property of pharmaceuticals makes CPC fear that its research will be stolen by a high-tech competitor or an agent of the state ('Remote Systems: Building up a Distributed Architecture', 2023). In the provided case, the red team shall emulate an Advanced Persistent Threat (APT) to ascertain the extent to which the experimentally simulated CPC defences would have stood against a targeted intrusion to steal research.

The scenario includes a simulated business environment composed of a domain diagram of the Windows Active Directory setup that supports corporate identity and access, a domain-joined Windows 10 client that describes the endpoint of the staff, and an Ubuntu research data server that includes a dummy research file that can be retrieved through web services. The red team has a Kali Linux attacker computer, and is challenged to find, access and steal a predefined sample of falsified research data (formula.txt), without damaging the system.

3.2 Rules of Engagement

1. Purpose and Objectives

The operation IP shield is a red team exercise that is conducted in the case of Curetton Pharmaceutical Company (CPC). It is also designed to simulate an advanced persistent threat (APT) and steal intellectual property of pharmaceuticals without detection. This is to ensure that the defensive skills of CPC are tested under the conditions of the actual environment, and that the activity is approved, regulated, and not contrary to the demands of the ethical hacking or the academic evaluation (Kumar *et al.*, 2023).

2. In-Scope / Out-of-Scope

In-Scope:

- Windows server 2022 domain controller and Windows 10 domain-joined clients in an active directory environment.
- Applications Simulates sensitive intellectual property, opens HTTP and SSH servers with research data server (ubuntu based).
- Infrastructure Red a Red team infrastructure in a contained, virtualised laboratory environment on Kali Linux.

Out-of-Scope:

- Host operating systems, external or production networks.
- Denial-of-Service attacks or drainage attacks.

- Bad behaviors, including the deletion of data, the corruption of data, or the simulation of a ransom attack.
- There should be termination of any accidental penetration of out-of-scope systems.

3. Authorized Techniques and Constraints.

Legal techniques include reconnaissance, service discovery, exploitation of misconfigurations or weak authentication, Living-Off-the-Land, stealthy command-and-control communication and controlled exfiltration of fake research data. Permanent backdoors, unnecessary security configuration changes and zero-day vulnerabilities are prohibited.

4. Assumptions

Environment: The environment is a middle sized pharmaceutical organisation that is not that mature in security monitoring. SIEM and EDR solutions are in their minimal tuning form. The use of MFA is not always the case. Red team lacks an insider or past qualification.

5. Stealth and Safety

Participation gives greater weight to low noise, evasive techniques that seem part of routine administration (Cholyshkina *et al.*, 2024). System stability is checked periodically and all the activities that cause unintentional interference are terminated.

6. Escalation and Communication.

All the happenings and activities are recorded in the engagement. Any issue that would cripple the systems is overblown. Once the completion is done, a technical report containing detailed information is given to the stakeholders and an executive-level summary is given.

7. Legal and Ethical Conformity.

This interaction is used in a disciplined learning atmosphere of the laboratory only. Personal information and production machines are not involved. Institutional policy, the ethical hacking philosophy, and the principles of academic integrity are followed in any activity, and the findings are reported responsibly to improve the security position.

3.3 Threat Emulation Plan

The threat emulation plan will be operation IP Shield that will mimic a low-noise data theft campaign of the kind of APT (Zhu *et al.*, 2023). This will be the objective of this campaign, which will be to locate a simulated research datastore and steal one sensitive file and leave behind minimum traces that would otherwise increase defensive surveillance. The approach concentrates on finding comprehensive service enumeration and exploitation of lightly secured services but not on the disruptive exploitation practices.

The attacker will gain controlled access using valid credentials when there is an authenticated access via SSH. This stage proceeds to the data discovery, validation of file sensitivity and exfiltration on the common protocols (HTTP retrieval), to match the normal traffic patterns.

The rationale behind this map is to map every stage to MITRE ATT&CK techniques to have the operation described using common defensive terminology. This helps in the transformation of the activities of red team to a form that could be accessed by a blue team to carry out the works of detective engineering and enhance the response (Al-Saraireh and Masarweh, 2022). The plan also helps in reporting after engagement by matching against the ATT&CK technique identities the observed evidence (commands, logs, and artefacts).

Table 2: Threat Emulation Plan

Phase	Objective	MITRE Tactic	Technique ID	Technique Name	Evidence from Your Lab
Recon	Identify live hosts	TA0043	T1595	Active Scanning	nmap -sn 10.0.1.0/24
Recon	Identify services on	TA0043	T1046	Network Service Scanning	nmap -sS -p 22,80 ubuntu-ip

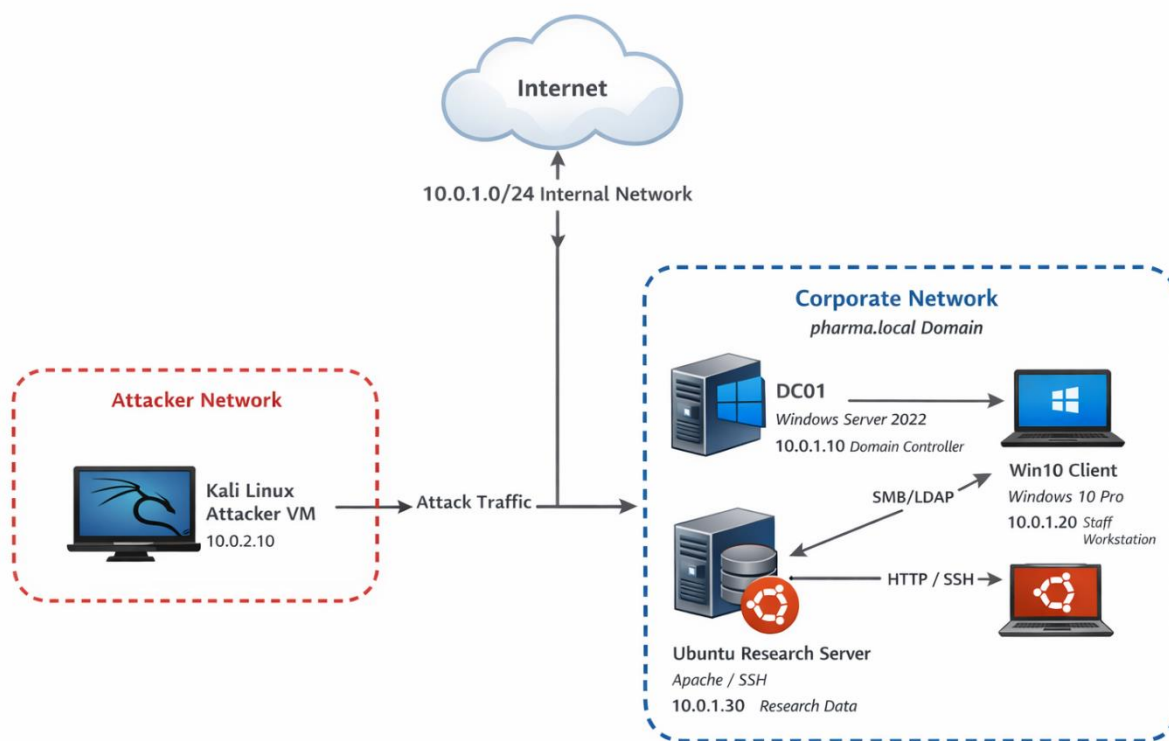
	research server				
Discovery	Identify accessible web content	TA0043	T1592	Gather Victim Host Information	curl http://<ubuntu-ip>/research/
Initial Access	Authenticate to server	TA0001	T1078	Valid Accounts	ssh <user>@<ubuntu-ip>
Collection	Locate target research data	TA0009	T1005	Data from Local System	/var/www/html/research/formula.txt
Exfiltration	Exfiltrate research file	TA0010	T1041	Exfiltration Over Web Service	curl ... -o formula_exfiltrated.txt

3.4 Lab Environment Design & Architecture

It is a managed virtual laboratory which was created to simulate a pharma research feel and may accommodate the plausible identity management, endpoint behaviour, and research data objective. The infrastructure has four Windows Server 2022 VM as the Domain Controller (DC01) of the domain pharma.local, a Windows 10 Pro client, which is a domain member, an Ubuntu server where the fake research data is stored with the assistance of the Apache web services, and a Kali Linux machine, which helps in reconnaissance and the execution of the attack.

Domain Controller was configured by configuring the Active Directory Domain Services as well as elevating the server to form the pharma.local forest (Iyer, Kabbur and Wali, 2020). The creation of Organisational Units and users was done based on a realistic enterprise hierarchy, including the regular users (e.g., “John Doe) and an administrative account (IT Admin). Windows 10 client was then configured and set up DNS to point towards Domain Controller, and then joined the domain, which confirmed that it was integrated as such commands as whoami, hostname, and nltest bore out.

The Ubuntu server was configured as a research data hosting server by starting apache2 and a directory /research was created on the under web root, where feasible research file (formula.txt) was generated. The local and Windows 10 machine and the Kali machine were tested to be accessible to browser and curl test.



Simulated Corporate Lab Network Architecture

Figure 1: Network Architecture Diagram

Environment setup

Setup of the VM's

1. Set up Windows 10 Pro

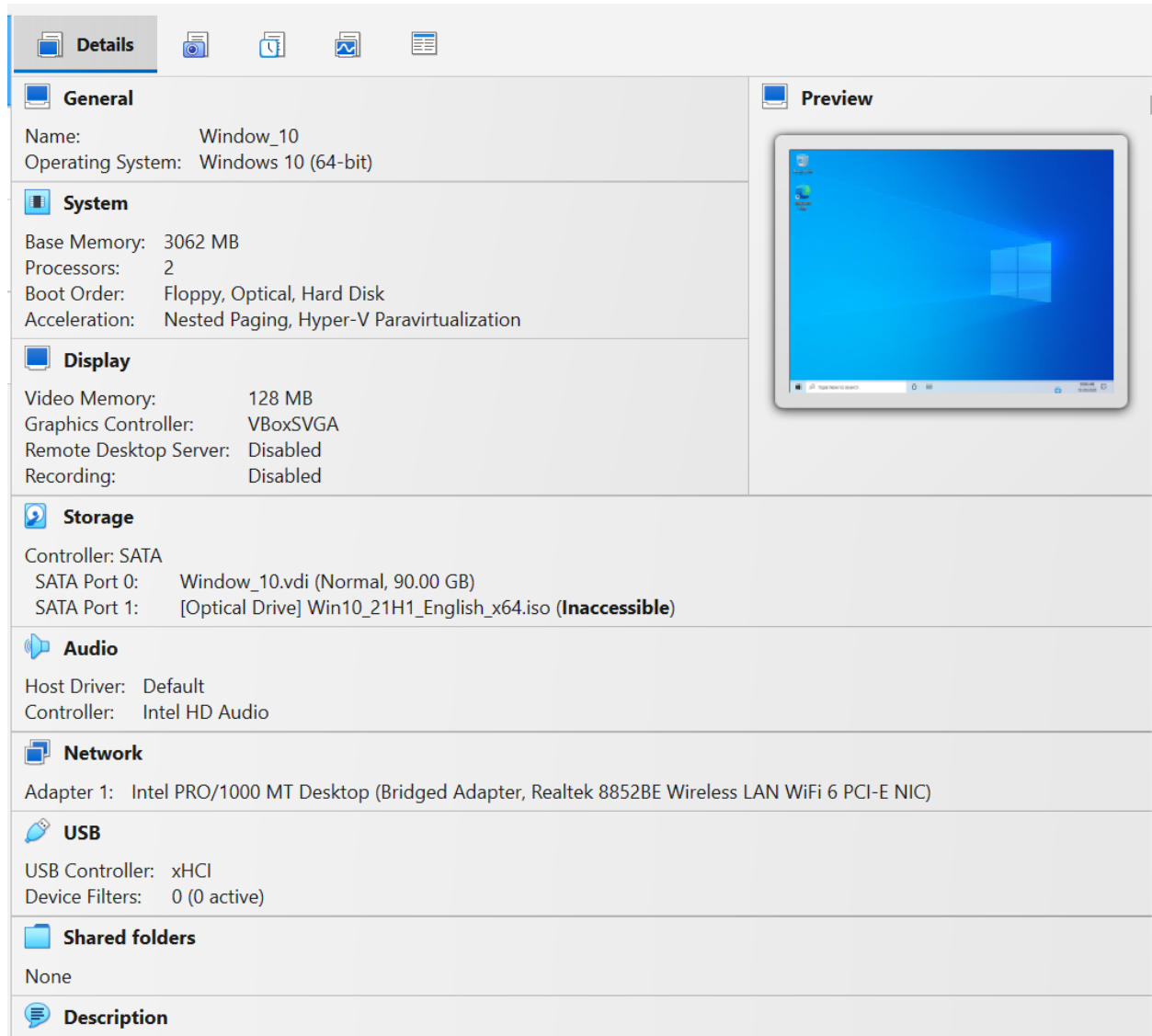


Figure 2: Set up Windows 10 Pro

2. Set up Ubuntu

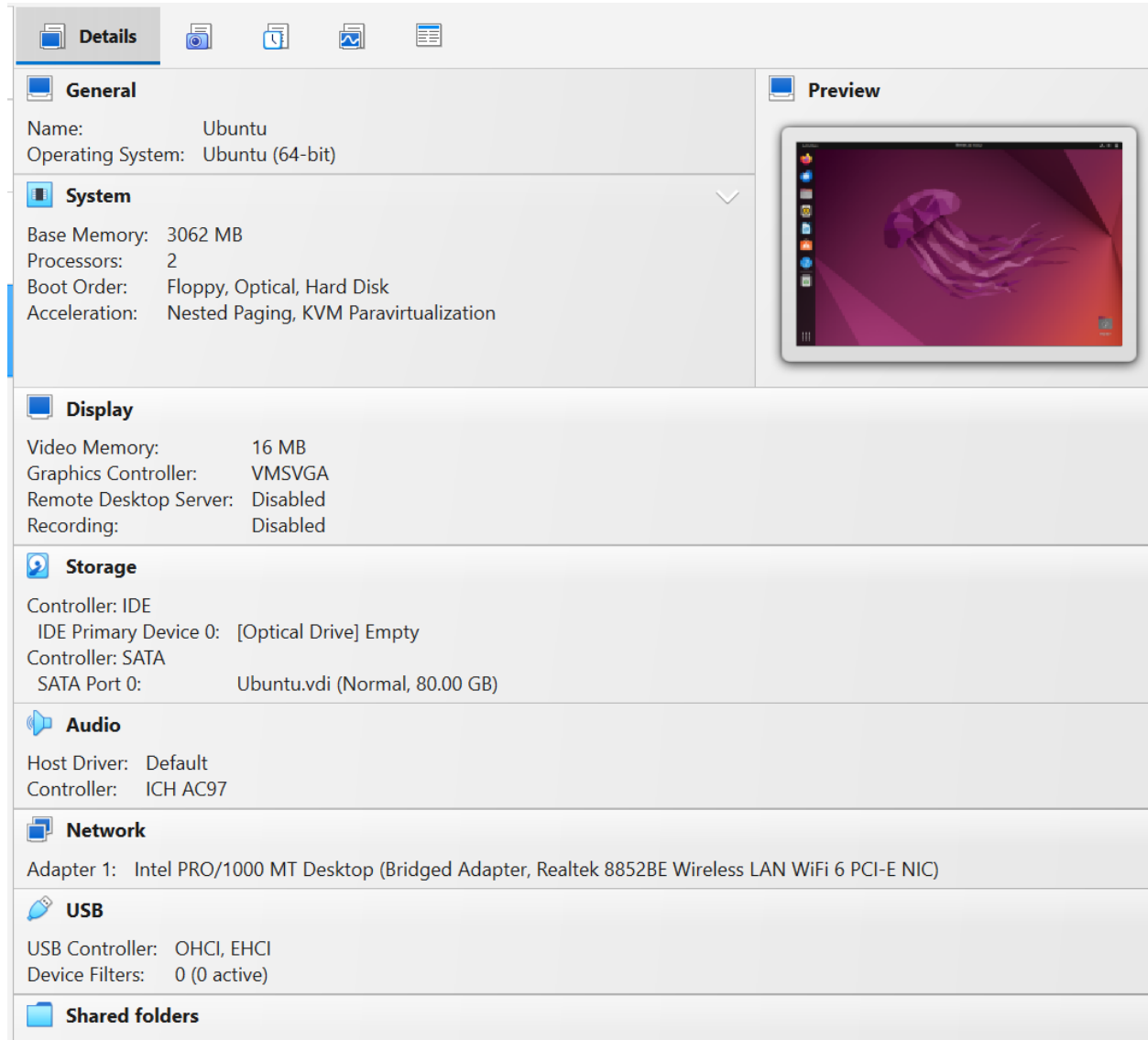


Figure 3: Set up Ubuntu

3. Set up Kali Linux

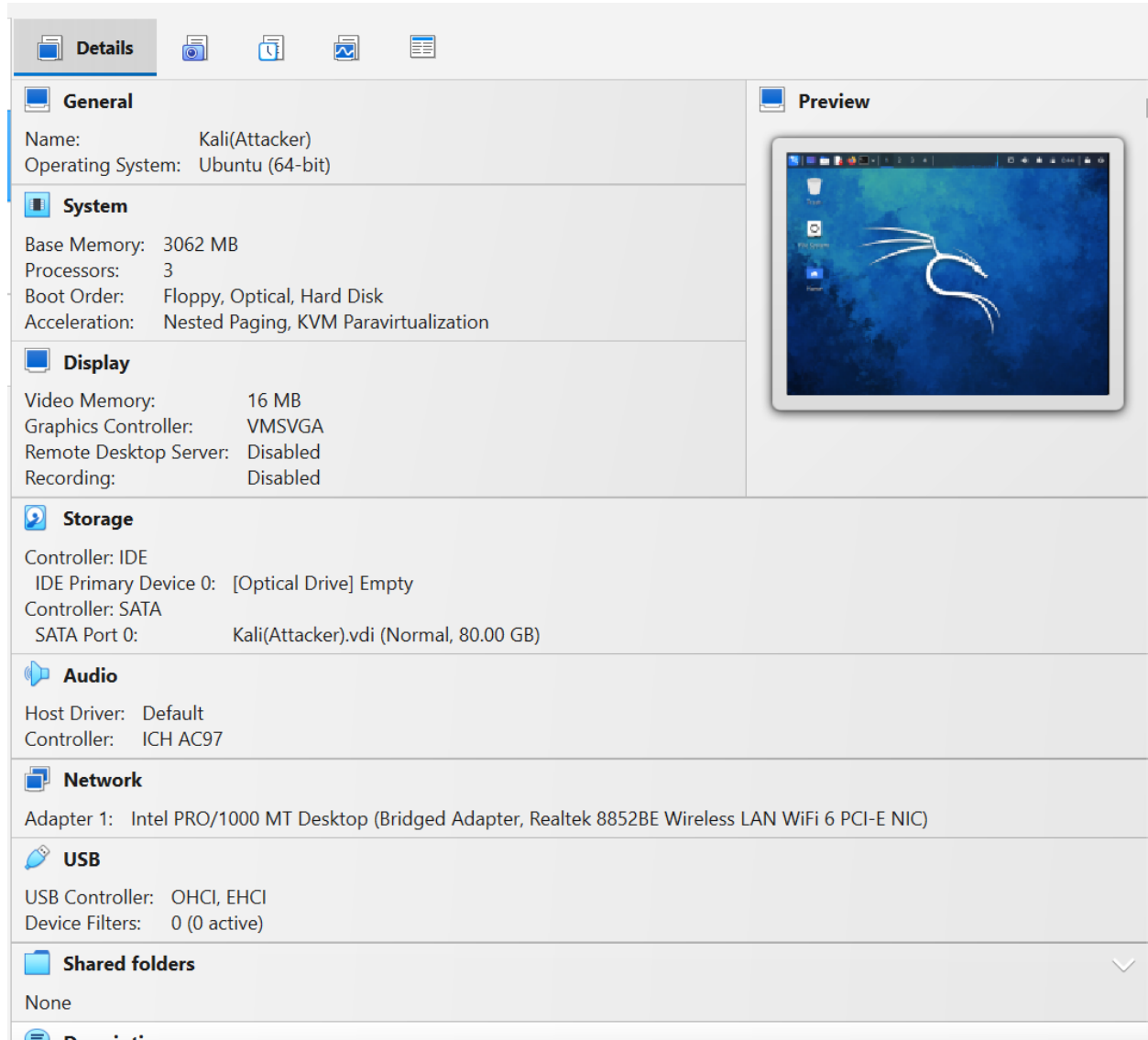


Figure 4: Set up Kali Linux

4. Set up the Windows Server 2022

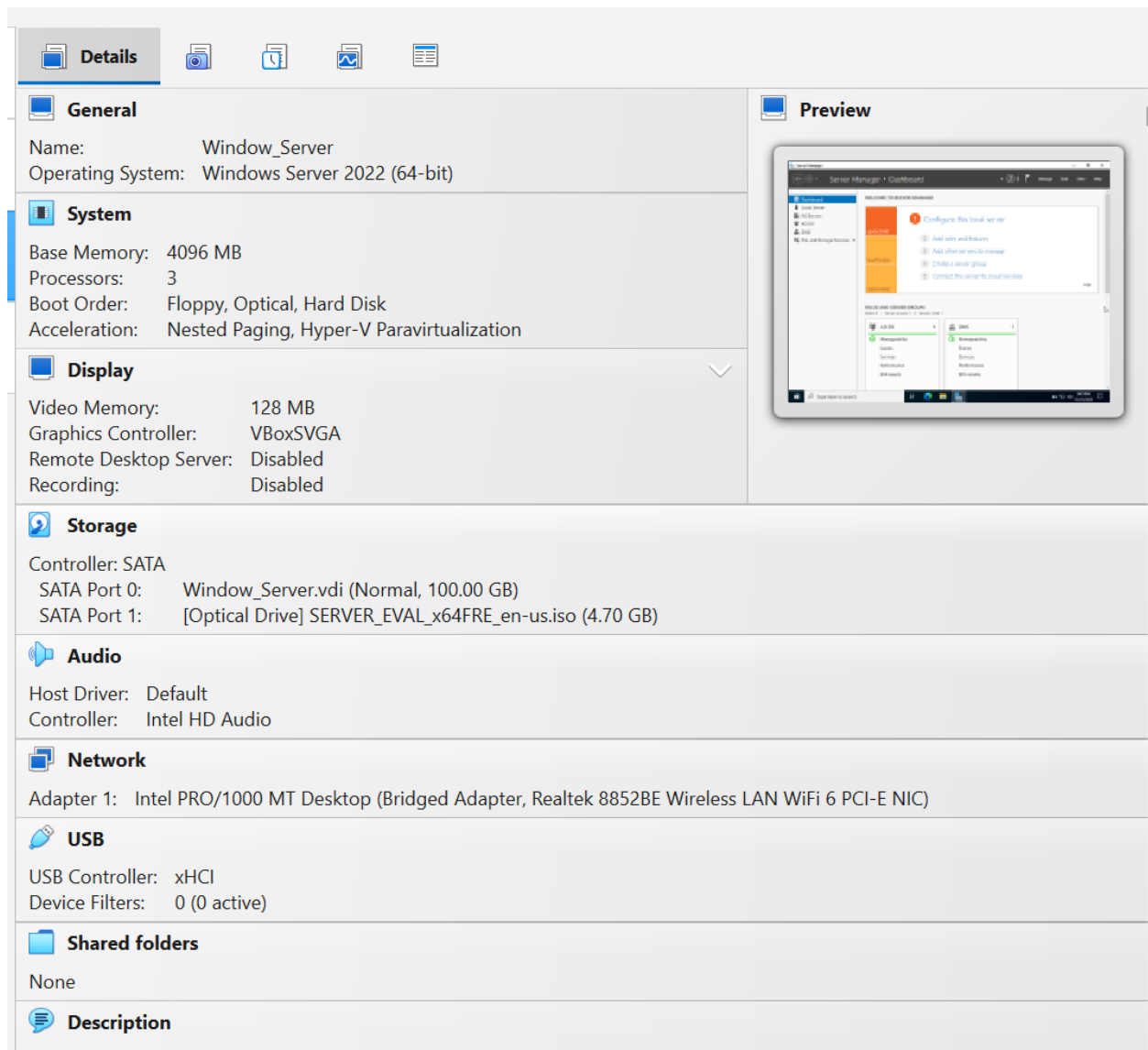


Figure 5: Set up the Windows Server 2022

Create the Domain Name (pharma.local)

1. Open server manager
 - a. Click Manage
 - b. Click Add Roles and Features
2. Add AD DS Role
 - a. Server: Select DC01
 - b. Roles: Active Directory Domain Services
 - c. Add Features
 - d. Next -> Install

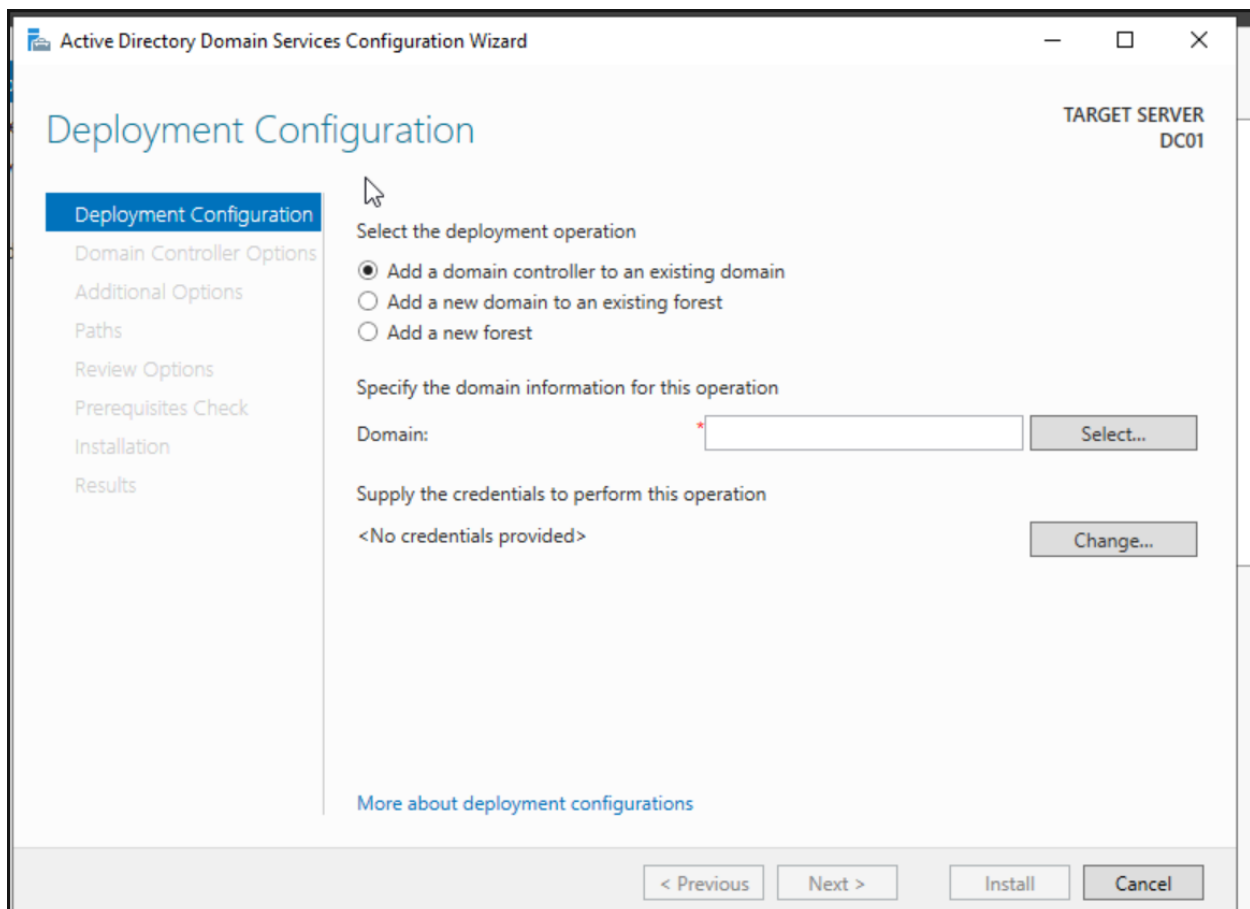
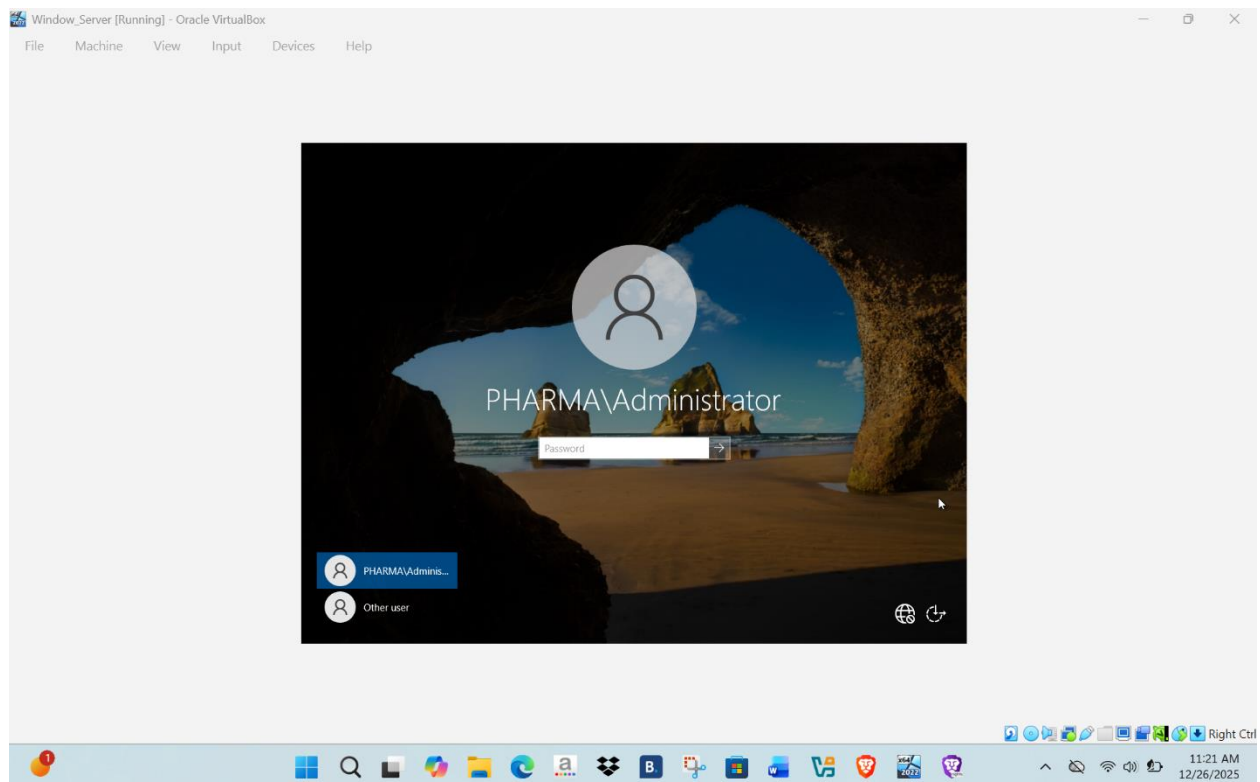


Figure 6: Create the Domain Name

Click on the Add New Forest: Type “pharma.local” and click on Change.

Promote this server to a domain controller

After this, log in as Pharma \ Administrator.



3.5 Attack Narrative – Phase by Phase

Phase 1: Reconnaissance and Host Discovery

The attack commenced at the Kali attacker machine, where the network configuration was verified and access to the target systems confirmed. The red team then conducted a host discovery on the subnet using an ICMP sweep, which identified the live hosts.

1. Identify Live Hosts
 - a. From Kali, run:
 - i. `nmap -sn 10.0.1.0/24`

Kali(Attacker) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

1 2 3 4

```
(kali@kali)-[~]
$ nmap -sn 10.0.1.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-26 03:56 EST
Nmap scan report for 10.0.1.1
Host is up (0.017s latency).
Nmap scan report for 10.0.1.27
Host is up (0.71s latency).
Nmap scan report for 10.0.1.38
Host is up (2.4s latency).
Nmap scan report for 10.0.1.41
Host is up (1.1s latency).
Nmap scan report for 10.0.1.48
Host is up (0.39s latency).
Nmap scan report for 10.0.1.77
Host is up (1.3s latency).
Nmap scan report for 10.0.1.80
Host is up (0.080s latency).
Nmap scan report for 10.0.1.93
Host is up (0.77s latency).
Nmap scan report for 10.0.1.134
Host is up (3.4s latency).
Nmap scan report for 10.0.1.143
Host is up (0.031s latency).
Nmap scan report for 10.0.1.153
Host is up (1.6s latency).
Nmap scan report for 10.0.1.154
Host is up (0.20s latency).
Nmap scan report for 10.0.1.155
Host is up (0.53s latency).
Nmap scan report for 10.0.1.163
Host is up (0.13s latency).
Nmap scan report for 10.0.1.164
Host is up (0.13s latency).
Nmap scan report for 10.0.1.171
Host is up (0.14s latency).
Nmap scan report for 10.0.1.174
Host is up (0.0023s latency).
Nmap scan report for 10.0.1.177
Host is up (0.0020s latency).
Nmap scan report for 10.0.1.191
Host is up (0.10s latency).
Nmap scan report for 10.0.1.222
Host is up (3.1s latency).
Nmap scan report for 10.0.1.235
Host is up (3.1s latency).
Nmap scan report for 10.0.1.252
Host is up (1.0s latency).
Nmap done: 256 IP addresses (22 hosts up) scanned in 40.02 seconds

(kali@kali)-[~]
$
```

Figure 7: Reconnaissance and Host Discovery

Phase 2: Service Discovery and Target Profiling

After the red team spotted the Ubuntu research server, they were doing a targeted scan of the server with a service scan that targeted SSH (22) and HTTP (80). This made the server a known authenticated/unauthenticated data access point, developing the choice to attempt low-friction access techniques in the first place.

Identify Services in the Research Server (Ubuntu)

- b. From kali
 - i. `nmap -sS -p 22,80 ubuntu-ip`

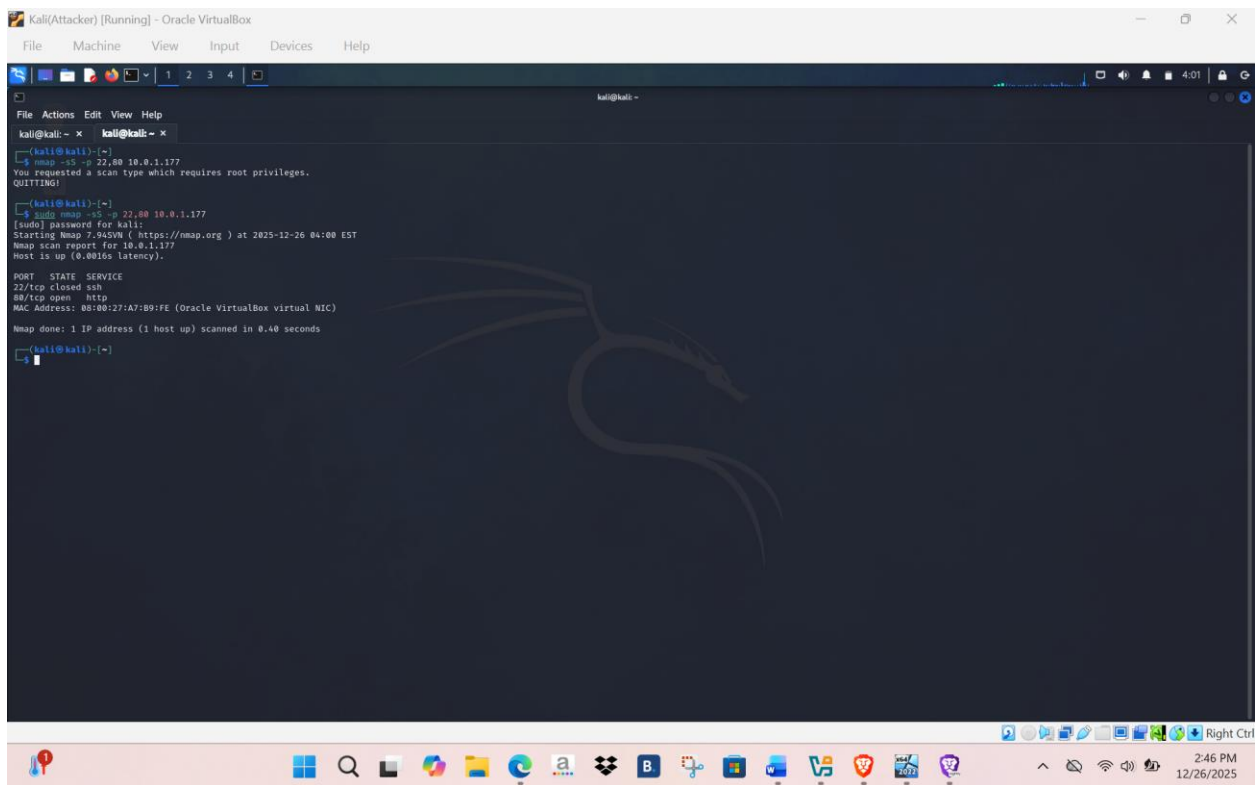
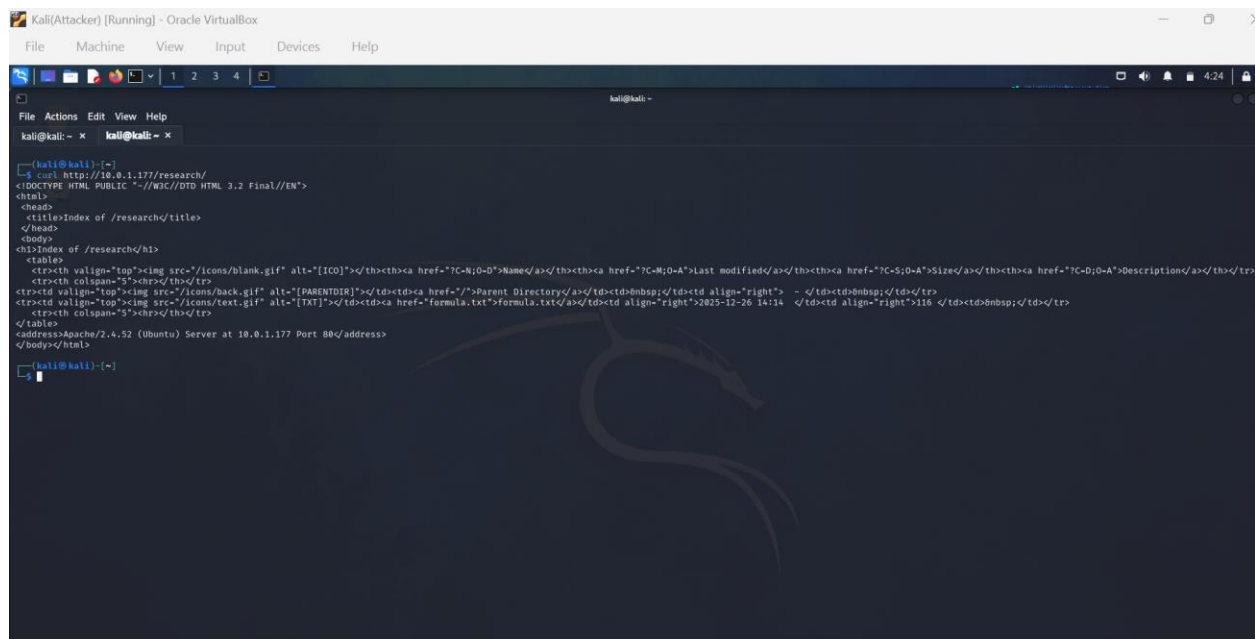


Figure 8: Service Discovery and Target Profiling

Phase 3: Web Enumeration and Data Discovery

Curl was used by the red group to list the content of the HTTP and ensure that sensitive files were not disclosed. The target file and /research directory were on the HTTP, meaning that there was an access control vulnerability, and a bad actor could access the file without exploitation.

- a. Direct access to research data
 - ii. `curl http://10.0.1.177/research`



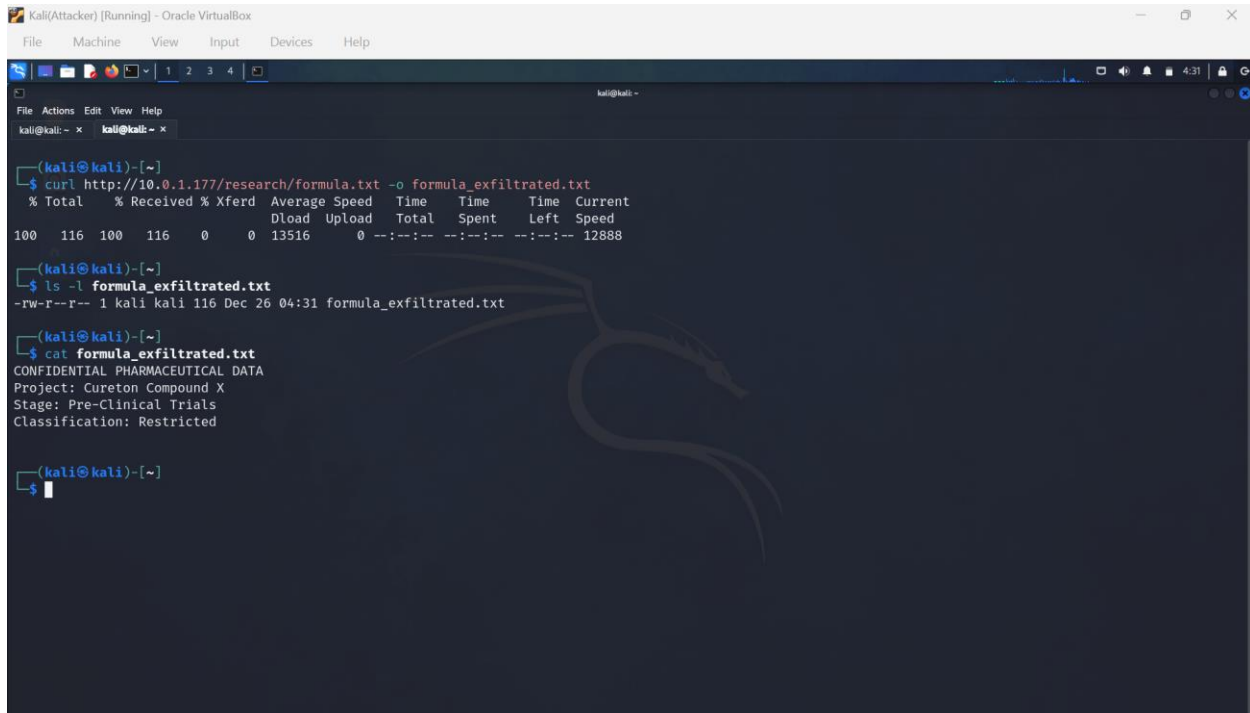
```
kali@kali:~$ curl http://10.0.1.177/research/
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<title>Index of /research/</title>
</head>
<body>
<h1>Index of /research/</h1>
<table>
<tr>
<th>valign="top"></th>
<th>colspan="5"><th>colspan="5"><th>colspan="5"><th>colspan="5"><th>colspan="5">
<tr>
<td>valign="top"></td>
<td><a href="/">Parent Directory</a></td>
<td align="right">-</td>
<td align="right"></td>
<td align="right"></td>
<tr>
<td>valign="top"></td>
<td><a href="formula.txt">formula.txt</a></td>
<td align="right">2025-12-26 14:14</td>
<td align="right">116</td>
<td align="right"></td>
<tr>
<td colspan="5"></td>
</tr>
</table>
<address>Apache/2.4.52 (Ubuntu) Server at 10.0.1.177 Port 80</address>
</body>
</html>
```

Figure 9: Web Enumeration and Data Discovery

Phase 4: Authenticated Access

The red team made sure that connection and access authentication were done using legitimate credentials in the places where SSH access was free (Ylonen, 2019). This assists in enforcing a realistic path of APT where valid accounts can be acquired with the help of weak passwords, reuse, or operational leakage.

1. Test SSH connectivity
Command: `sudo ssh username_ubuntu@ip_ubuntu`



```
(kali@kali)-[~]
$ curl http://10.0.1.177/research/formula.txt -o formula_exfiltrated.txt
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 116 100 116 0 0 13516 0 --:--:-- --:--:-- --:--:-- 12888

(kali@kali)-[~]
$ ls -l formula_exfiltrated.txt
-rw-r--r-- 1 kali kali 116 Dec 26 04:31 formula_exfiltrated.txt

(kali@kali)-[~]
$ cat formula_exfiltrated.txt
CONFIDENTIAL PHARMACEUTICAL DATA
Project: Cureton Compound X
Stage: Pre-Clinical Trials
Classification: Restricted

(kali@kali)-[~]
$
```

Figure 12: Exfiltration

3.6 Technical Report – Blue Team View

This operation demonstrates a series of assaults on a simulated reconnaissance to a data exfiltration research setting. Some reconnaissance was first carried out with the assistance of host discovery and service scanning, which assisted in locating the Ubuntu research server and services that are presented to the world (Kashyap and Selvarajah, 2021). The vulnerability of the research file was confirmed through the aid of HTTP enumeration, which would allow an attacker to receive a sensitive research file without authorisation and would be able to collect and exfiltrate it. Authorised access was also demonstrated in places where SSS existed, showing how legitimate credentials would increase the power of attackers to conduct additional reconnaissance and presence.

The tools were necessary to host and service discovery (nmap), HTTP enumeration and exfiltration (curl), and authenticated access (ssh). MITRE ATT&CK mapping is composed of Active Scanning and Network Service Scanning of recon, Valid Accounts of the authenticated access, and Exfiltration Over Web Service of file extraction.

The success parameters confirmed that formula.txt was retrieved from the server of research, and generation of formula exfiltrated.txt was generated in the attacker's system. Evidence should be provided as the command output, timestamps where possible and also a screenshot of the source file path on Ubuntu and the exfiltrated file on Kali.

3.7 Detection Gap Analysis

The interaction showed the weaknesses in the detection of the web access pathway and the authenticated access pathway (Anas, Elgamel and Youssef, 2024). The access to the research file was possible via the HTTP protocol, i.e., there was no proper access control and monitoring of the access to the sensitive content. As seen in the example of Apache logs, where the request was logged, the absence of alerting and correlation would make the defenders appreciate the activity retrospectively.

Authentication activities in the case of SSS can be recorded in the auth.log of /var. However, unless baseline profiles, alert thresholds, or centralised monitoring are used, suspicious patterns of access, such as suspicious source IPs, recursive log-in attempts or newly created users, can be ignored. In addition, when monitoring maturity is low, ordinary administrative processes (e.g. curl requests or SSH logins) do not separate malicious behaviour and normal behaviour.

To prove this, the following commands were used to tail Apache access logs and grep SSH authentication logs to support the engagement that was performed and analyse web and authentication logs (Sadat, Naseri and Salamzada, 2024). The fact that logging does not exist is not the gap to critically bridge, but that detection logic (SIEM rules, EDR telemetry correlation, and response processes) does not exist to detect and respond to a low-noise pattern of data theft.

1. Detection Gaps
 - a. `sudo grep "sshd" /var/log/auth.log | tail -n 30`
 - b. `sudo tail -n 30 /var/log/apache2/access.log`

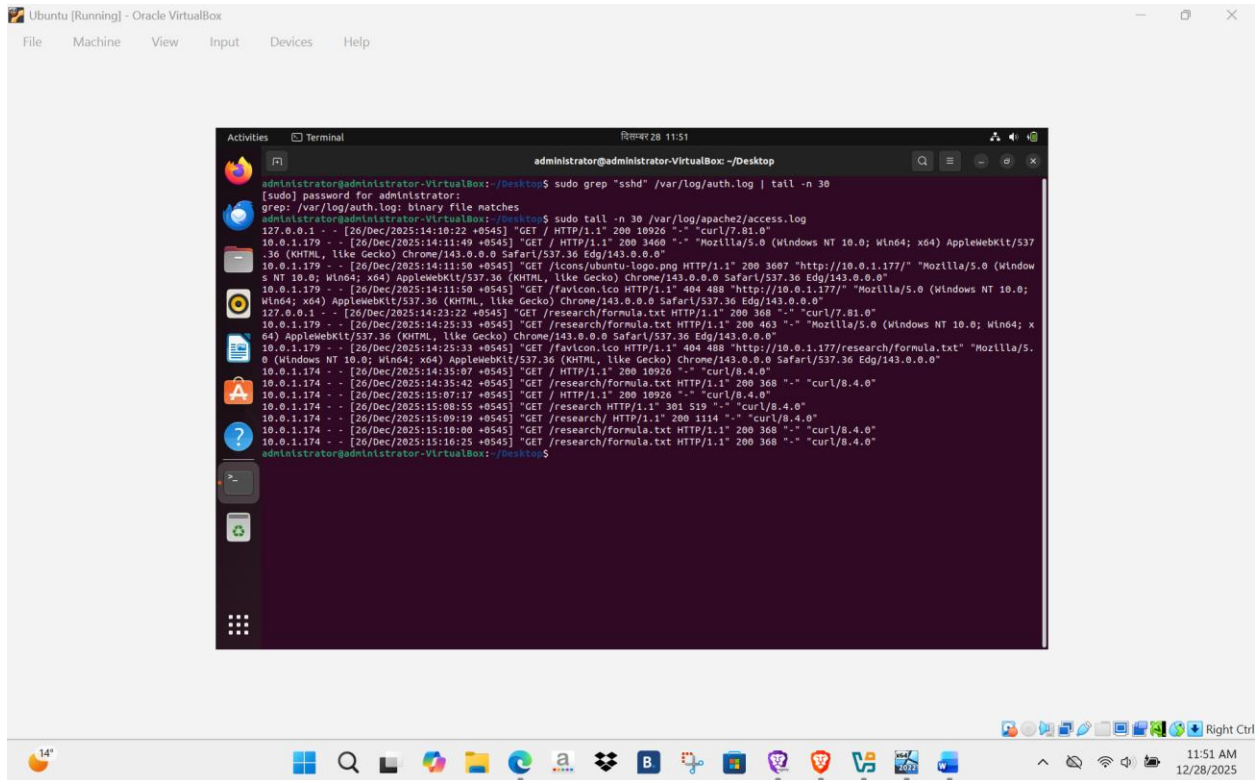


Figure 13: Detection Gap Analysis

3.8 Strategic Recommendations

CPC is urged to work on the controls that will be able to prevent and stop the credential abuses directly, reduce the chances of the possibility of lateral movement and increase the sensitivity of data access (Smiliotopoulos, Kambourakis and Kolias, 2024). To begin with, implement a strong identity control, i.e. phishing-resistant MFA, on remote-access accounts and administrative accounts. This reduces the degree of efficiency of attackers using the legitimate accounts and credential reuse designs.

Second, have the least privileged and safeguarded server access controls. The research data directory should not be made publicly available, i.e. over unauthenticated HTTP, unless it is necessary to do so, and sensitive data should be protected by access control, authentication and monitoring. Where needed, SSS, and force key-based authentication, block source networks, and monitor the abnormal pattern of authentication.

Third, improve detection engineering. Apache and SSH logs will be forwarded to a central SIEM, and correlation rules, i.e. notifications of access to sensitive paths (/research/), recurring requests to research files, access to SSS via odd sources, and odd administrative usage will be done (Rahdari *et al.*, 2025). The endpoint controls (EDR) must be set to identify suspicious patterns of discoveries and credential access attempts on Windows endpoints in case of an expansion of the scenario.

3.9 Cost–Benefit Analysis

The basic mechanisms, such as MFA, centralised log assembly, SIEM correlation regulations, and tighter access to delicate research data, are typically cheap to moderate to set up in comparison to the economic impacts of intellectual property theft. With a pharmaceutical organisation, loss of proprietary research may translate into a competitive drawback, a slowing in the development of products and direct loss of revenue as well as regulatory and reputational damage.

The implementations of quick wins with high returns include but are not limited to, the deployment of the MFA, restricting unauthenticated access to the research directories and supporting centralised monitoring not only of web but also SSS access (Williamson and Curran, 2021). These have a direct impact on reducing the risk of success of attackers through conventional means and increasing early warning.

3.10 Executive Brief – Board Level

The research information stored within CPC could be accessed and extracted without difficulty from the environment, as was the case in the Operation IP Shield. The attacker simulated and discovered the position of the research server in a short time, guaranteed that it had sensitive content that could be retrieved through the use of regular web services and was capable of stealing a file that had the potential to possess valuable intellectual property. More to the point, this can be performed without being immediately detected unless monitoring is established to inform every time unauthorised access to sensitive resources can occur (Muwardi *et al.*, 2021).

With CPC, the business risk is clear: the theft of the research information could annihilate the years of the investment and the position of the organisation as a competitor. The proposed capabilities, in particular, the increased control over identity verifications (MFA), the increased control over

access to research materials, and the improved monitoring and notification, can be characterised as a possible strategic investment that can reduce the likelihood and the severity of an actual breach.

4. Conclusion

This report has demonstrated the way current computer threats are carried out in a systematic, methodical manner and how red team exercises can provide an invaluable feedback on the organisational vulnerabilities to security that do not always manifest themselves through conventional responses. The report considered a realistic scenario of a cyber attack on a medical facility and traced the actions of the attacker to the MITRE ATT&CK framework to establish a clear understanding of the manner in which advanced threat operators proceed through the initial access and operational impact.

According to this analysis, the red team interaction that was dubbed as operation IP Shield was an application of these ideas on a managed pharmaceutical research. The assault demonstrated that a hacker with any desire might locate unsecured services, access to sensitive research data, and have the capability to steal intellectual property with the minimum resistance and notice possible. These findings show that technical vulnerabilities alone are rarely used to achieve success in an attack, but systemic vulnerabilities, such as poor identity control, underdeveloped monitoring, and flat architecture, render organisations susceptible.

The latter is supported by the strategic analysis, along with the practical analysis, such as the necessity to invest in the layered security control, which entails phishing-resistant authentication, detection engineering, and architectural separation of the key research systems. On the business side, the cost of these kinds of controls is much lower than the potential financial, regulatory, and reputational losses of intellectual property theft or even the interruption of operations. To sum up, it was demonstrated in this paper that red teaming is potentially valuable as a proactive tool, which may promote cyber resilience and informed and risk-based decision-making regarding security.

References:

- Adebukola, A.A. et al. (2022) 'Cyber Security as a Threat to Health Care', *Journal of Technology and Systems*, 4(1), pp. 32–64. Available at: <https://doi.org/10.47941/jts.1149>.
- Al-Saraireh, J. and Masarweh, A. (2022) 'A novel approach for detecting advanced persistent threats', *Egyptian Informatics Journal*, 23(4), pp. 45–55. Available at: <https://doi.org/10.1016/j.eij.2022.06.005>.
- Anas, A., Elgamal, S. and Youssef, B. (2024) 'Survey on detecting and preventing web application broken access control attacks', *International Journal of Electrical and Computer Engineering (IJECE)*, 14(1), p. 772. Available at: <https://doi.org/10.11591/ijece.v14i1.pp772-781>.
- Bugshan, W.M. et al. (2022) 'Role of Health Awareness Campaigns in Improving Public Health: A Systematic Review', *International Journal of Life Science and Pharma Research* [Preprint]. Available at: <https://doi.org/10.22376/ijpbs/lpr.2022.12.6.L29-35>.
- Chang, C.T. et al. (2024) 'Red Teaming Large Language Models in Medicine: Real-World Insights on Model Behavior'. Available at: <https://doi.org/10.1101/2024.04.05.24305411>.
- Cholyshkina, O. et al. (2024) 'Public participation and innovative technologies: the role of artificial intelligence in public administration and sustainable development', *Salud, Ciencia y Tecnología - Serie de Conferencias*, 3, p. 974. Available at: <https://doi.org/10.56294/sctconf2024974>.
- Henricks, A. and Kettani, H. (2019) 'On Data Protection Using Multi-Factor Authentication', in *Proceedings of the 2019 International Conference on Information System and System Management*. New York, NY, USA: ACM, pp. 1–4. Available at: <https://doi.org/10.1145/3394788.3394789>.
- Iyer, N.C., Kabbur, A.M. and Wali, H.G. (2020) 'Implementation of Active Directory for efficient management of networks', *Procedia Computer Science*, 172, pp. 112–114. Available at: <https://doi.org/10.1016/j.procs.2020.05.016>.

Jimmy, F. (2023) ‘Understanding Ransomware Attacks: Trends and Prevention Strategies’, Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(1), pp. 180–210. Available at: <https://doi.org/10.60087/jklst.vol2.n1.p214>.

Kalantari, R. et al. (2025) ‘Surgical interruptions and preventable delays in the operating rooms of academic teaching hospitals’, Patient Safety in Surgery, 19(1), p. 41. Available at: <https://doi.org/10.1186/s13037-025-00470-y>.

Kashyap, P. and Selvarajah, V. (2021) ‘Analysis of Different Methods of Reconnaissance’, in. Available at: <https://doi.org/10.2991/ahis.k.210913.064>.

Kovacevic, I. and Gros, S. (2020) ‘Red Teams - Pentesters, APTs, or Neither’, in 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO). IEEE, pp. 1242–1249. Available at: <https://doi.org/10.23919/MIPRO48935.2020.9245370>.

Kumar, J.R.R. et al. (2023) ‘Evaluation of the extent and demanding roles of ethical hacking in cybersecurity’, Journal of Autonomous Intelligence, 7(1). Available at: <https://doi.org/10.32629/jai.v7i1.1246>.

Muwardi, R. et al. (2021) ‘Network Security Monitoring System Via Notification Alert’, Journal of Integrated and Advanced Engineering (JIAE), 1(2), pp. 113–122. Available at: <https://doi.org/10.51662/jiae.v1i2.22>.

Odongo, M. (2024) ‘Health Communication Campaigns and Their Impact on Public Health Behaviors’, Journal of Communication, 5(2), pp. 55–69. Available at: <https://doi.org/10.47941/jcomm.1980>.

Ohri, P. and Neogi, S.G. (2022) ‘Software-Defined Networking Security Challenges and Solutions: A Comprehensive Survey’, International Journal of Computing and Digital Systems, 12(1), pp. 383–400. Available at: <https://doi.org/10.12785/ijcds/120131>.

Rahdari, A. et al. (2025) ‘A Survey on Privacy and Security in Distributed Cloud Computing: Exploring Federated Learning and Beyond’, IEEE Open Journal of the Communications Society, 6, pp. 3710–3744. Available at: <https://doi.org/10.1109/OJCOMS.2025.3560034>.

‘Remote Systems: Building up a Distributed Architecture’ (2023) Humanitarian and Natural Sciences Journal, 4(10). Available at: <https://doi.org/10.53796/hnsj41023>.

Sadat, S.E., Naseri, M.F. and Salamzada, K. (2024) ‘Identifying and Mitigating Web Application Vulnerabilities: A Comparative Study of Countermeasures and Tools’, International Journal Software Engineering and Computer Science (IJSECS), 4(3), pp. 1109–1127. Available at: <https://doi.org/10.35870/ijsecs.v4i3.3138>.

Sendelj, R. and Ognjanovic, I. (2022) ‘Cybersecurity Challenges in Healthcare’, in. Available at: <https://doi.org/10.3233/SHTI220951>.

Shahzadi, A. et al. (2025) ‘Safeguarding the healthcare sector from ransomware attacks: insights from a literature review’, PeerJ Computer Science, 11, p. e3073. Available at: <https://doi.org/10.7717/peerj-cs.3073>.

Smiliotopoulos, C., Kambourakis, G. and Kolias, C. (2023) ‘Detecting Lateral Movement: A Systematic Survey’. Available at: <https://doi.org/10.2139/ssrn.4606223>.

Smiliotopoulos, C., Kambourakis, G. and Kolias, C. (2024) ‘Detecting lateral movement: A systematic survey’, Heliyon, 10(4), p. e26317. Available at: <https://doi.org/10.1016/j.heliyon.2024.e26317>.

Williamson, J. and Curran, K. (2021) ‘The Role of Multi-factor Authentication for Modern Day Security’, Semiconductor Science and Information Devices, 3(1), pp. 16–23. Available at: <https://doi.org/10.30564/ssid.v3i1.3152>.

Ylonen, T. (2019) ‘SSH Key Management Challenges and Requirements’, in 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). IEEE, pp. 1–5. Available at: <https://doi.org/10.1109/NTMS.2019.8763773>.

Zhu, T. et al. (2023) ‘APTSHIELD: A Stable, Efficient and Real-Time APT Detection System for Linux Hosts’, IEEE Transactions on Dependable and Secure Computing, 20(6), pp. 5247–5264. Available at: <https://doi.org/10.1109/TDSC.2023.3243667>.

