Internal Penetration Testing Report

Simulated Corporate Network Assessment – NewBizz Ltd

Prepared by: Yash Bhootra

Table of Contents

1. Executive Summary

This internal penetration test was conducted against a simulated corporate network comprising five virtual machines, each designed to replicate real-world configurations found in enterprise environments. The objective of this engagement was to assess the security posture of the systems, uncover vulnerabilities that could be exploited by an attacker, and provide actionable recommendations for remediation. The assessment targeted five virtual machines simulating a corporate network environment, covering web servers, Windows workstations, domain controllers, and database-backed systems.

The testing was authorised by NewBizz Ltd, and carried out under controlled conditions, using a combination of manual testing techniques and automated tools. The assessment followed industry-standard frameworks, including OWASP, NIST SP 800-115, and PTES, to ensure a comprehensive and ethically sound approach.

Across the five machines, the assessment revealed a total of 24 vulnerabilities, with 4 categorised as critical, 7 as high, 8 as medium, and 5 as low severity. The most impactful findings included unauthenticated remote code execution, SQL injection leading to administrative access, local privilege escalation to root, and NTLMv2 credential theft through LLMNR poisoning.

A summary of the key findings is provided below:

Severity	Count	Examples
Critical	4	Dirty COW (root escalation), SQLi to RCE, SMB relay
High	7	LLMNR spoofing, NTLMv2 relay, outdated WordPress, Apache CVEs
Medium	8	TLS 1.0/1.1 enabled, directory listing, shortname disclosure
Low	5	Version banners, missing headers, ICMP timestamps

Figure: Key Findings

These vulnerabilities demonstrate how an attacker could move from initial reconnaissance to full system compromise with relatively low effort. In several scenarios, the attacker was able to escalate from a web-based interface to full operating system control, or intercept credentials using legacy protocols and misconfigurations.

If these vulnerabilities existed in a production environment, the consequences could include unauthorised access to confidential data, system downtime, reputational damage, and potential non-compliance with regulations such as GDPR.

To mitigate these risks, a number of recommendations are provided throughout the report. At a strategic level, it is recommended that NewBizz Ltd:

- Enforces strict update and patching policies.
- Disables legacy services such as LLMNR and SMBv1.
- Implements multi-factor authentication (MFA) wherever feasible.
- Conducts regular vulnerability assessments.
- Establishes monitoring for unusual activity, such as credential relays or privilege escalations.

This report provides a comprehensive breakdown of each vulnerability, how it was discovered, the exploitation path, and specific guidance for remediation. It serves as a foundation for improving the organisation's security posture and reducing its exposure to both internal and external threats.

2. Introduction

This report documents the findings of a comprehensive internal penetration testing exercise carried out within a simulated lab environment designed to mirror the IT infrastructure of NewBizz Ltd. The engagement involved the testing of five virtual machines, each representing different components of a typical enterprise network, including a web server, database-backed application, domain controller, Windows workstation, and a standalone file and service host.

The purpose of this penetration test was to proactively assess the security resilience of these systems by emulating the tactics, techniques, and procedures (TTPs) of a malicious adversary. Through this simulation, the test aimed to uncover technical vulnerabilities, misconfigurations, and systemic weaknesses that could be exploited to compromise the confidentiality, integrity, or availability of the organisation’s digital assets.

The assessment was conducted over a defined period, under strict ethical and legal boundaries. All actions were performed with explicit authorisation, and no actual harm was caused to any services, data, or infrastructure during the test. The focus was on identifying exploitable conditions, demonstrating their potential impact, and providing meaningful remediation guidance to support risk reduction.

Background of the Engagement

As part of its cybersecurity assurance programme, NewBizz Ltd commissioned this internal penetration test to evaluate its exposure to internal threats and assess the strength of its security controls. The test was aligned with widely recognised frameworks such as the OWASP Testing Guide, NIST SP 800-115, and the Penetration Testing Execution Standard (PTES) to ensure that results would be relevant, reproducible, and actionable.

The simulated environment provided by the client was carefully configured to replicate real-world technologies and services in use across their production network. This included outdated content management systems (CMS), exposed Windows services, weak cryptographic configurations, and common authentication protocols - each selected to reflect actual business risk scenarios.

Purpose of the Test

The primary objectives of this penetration test are as follows:

- To identify exploitable vulnerabilities across internal systems.
- To simulate real-world attacks and demonstrate potential impact.
- To assess the organisation’s detection and mitigation readiness.
- To provide a clear set of recommendations to improve overall security posture.

By adopting an adversary-driven approach, this assessment intended not only to highlight technical flaws but also to demonstrate how these weaknesses could be chained together to compromise business-critical systems.

3. Scope and Methodology

3.1 Scope of Engagement

This penetration testing engagement was conducted with the objective of identifying vulnerabilities, assessing real-world exploitability, and evaluating the impact of security misconfigurations across five internally hosted

virtual machines. Each VM simulated key infrastructure or web application components typical of a corporate IT environment.

The scope was carefully defined to ensure a focused and ethical assessment, respecting operational constraints and legal boundaries.

Scope Definition Table:

Category	Details
In Scope	- Internal network services (e.g., SMB, FTP, RDP, SSH) - Internal web applications - Exploitation and post-exploitation - Privilege escalation - Lateral movement - Data exfiltration simulation
Out of Scope	- End-user interaction (e.g., phishing or vishing) - Social engineering attacks - Physical security controls - Denial-of-Service (DoS) attacks - Internet-facing systems (external penetration)
Constraints	- Testing was performed strictly out-of-hours - Activity was limited to virtual lab only

This scope ensured the test remained controlled and realistic while avoiding disruption to simulated business operations.

3.2 Methodology

The engagement followed a structured, multi-phase methodology based on established frameworks:

- NIST SP 800-115 - Technical guide to security testing and assessment
- OWASP Testing Guide v4 - Focused guidance for web application assessment
- PTES - For comprehensive penetration testing process and ethics

Penetration Testing Phases:

Phase	Description	Purpose
1. Reconnaissance	Passive and active information gathering on all machines	Identify open ports, services, versions, hostnames
2. Enumeration	In-depth probing of discovered services	User listing, SMB/FTP share discovery, web directory mapping
3. Vulnerability Assessment	Automated and manual vulnerability scanning	Identify software flaws, default credentials, outdated services
4. Exploitation	Leveraging discovered vulnerabilities to gain initial access	Execute payloads, bypass authentication, inject commands
5. Post-Exploitation	Privilege escalation, lateral movement, credential dumping, impact analysis	Simulate attacker behaviour post-access
6. Reporting	Documentation of vulnerabilities, risk analysis, evidence collection, and remediation advice	Provide actionable findings to technical and non-technical stakeholders

Each phase fed into the next, creating a robust and repeatable process of discovery, validation, and recommendation.

3.3 Tools Utilised During the Engagement

The table below outlines the tools used during each phase, along with their purpose, scope, and outcomes achieved:

Tool	Purpose	Scope of Use	Outcome
Nmap	Network mapping and port scanning	Initial reconnaissance of all five VMs	Identified open ports, running services, and OS fingerprints
Enum4linux-ng	SMB enumeration over NetBIOS/SMB	Enumeration of Windows services on machines with port 139/445 open	Extracted NetBIOS names, shares, users, and domain information
Nikto	Web server vulnerability scanning	Web application assessment on HTTP-enabled machines	Detected outdated server software and dangerous HTTP methods
Dirb	Web directory brute-forcing	Discovery of hidden files/directories in web applications	Revealed /admin, /uploads, and other misconfigured paths
Hydra	Brute-force login testing	Credential attacks on SSH, FTP, RDP, SMB	Recovered valid credentials for lateral access and privilege escalation
SQLmap	SQL injection automation	Automated testing for SQL injection vulnerabilities	Exploited login pages to extract databases and sensitive information
Metasploit	Exploitation framework	Payload generation, module exploitation, post-exploitation	Achieved shell access, privilege escalation, and credential harvesting
LinPEAS	Linux privilege escalation enumeration	Post-exploitation phase on compromised Linux systems	Identified SUID binaries, cron jobs, and kernel exploits
WinPEAS	Windows privilege escalation enumeration	Post-exploitation on Windows machines	Highlighted vulnerable services, weak permissions, and unquoted service paths
Impacket Suite	Protocol abuse, credential extraction	Tools like secretsdump.py, rpcdump.py, smbexec.py on SMB/RPC	Extracted password hashes, enumerated RPC interfaces, and executed commands
smbclient	Manual interaction with SMB shares	Validated accessible file shares and uploaded/downloaded files	Confirmed share permissions and accessed confidential files
OpenVAS	Vulnerability scanning and risk correlation	Cross-validation of discovered vulnerabilities	Identified misconfigurations, missing patches, and exploitable services
Nessus	Advanced vulnerability scanner	In-depth vulnerability scanning for CVEs and service flaws	Correlated with manual findings and discovered known high-impact CVEs
Searchsploit	Local exploit search from Exploit-DB	Manual correlation of CVEs with available exploits	Identified relevant public exploits for execution via Metasploit or standalone

Figure: Tools used during engagement

3.4 Legal and Ethical Considerations

This penetration test was authorised and conducted in accordance with UK cybersecurity laws and academic standards. The following considerations were upheld:

- Authorisation: Written permission was obtained from NewBizz Ltd before testing began.
- UK Legal Compliance: All activities conformed to the Computer Misuse Act 1990.
- Ethical Conduct: No unauthorised access or damage was caused outside the defined scope.
- Confidentiality: All sensitive data accessed was handled securely and not disclosed beyond this report.
- Auditability: Activities were logged, and all exploitation attempts were traceable for review.

This structured, lawful, and transparent approach ensured the test could deliver value while protecting client integrity and trust.

Machine 1: blog.mycompany.ex (192.168.241.151)

Technical Summary

The target host blog.mycompany.ex (IP: 192.168.241.151) is a web server running Apache 2.4.10 on Debian 8.0 (Jessie) with WordPress 3.8.1 as the primary web application. The system was identified to be end-of-life, lacking security patches, and exposed multiple high-risk services and interfaces. Several vulnerable components were identified, successfully exploited, and led to complete system compromise with root access.

Scanning and Enumeration

- **Nmap TCP Scan** revealed open ports:
    - 22 (OpenSSH 6.7p1)
    - 80 (Apache 2.4.10 on Debian)
    - 111 (RPCbind)
    - 50141 (status RPC)
- **OS Fingerprinting**: Debian 8.0 (Jessie) - End-of-Life (EOL)

```
┌──(root㉿kali)-[/home/kali/myhobby]
└─# nmap -sC -sV -p 22,80,111,50141 192.168.241.151 -oA targeted

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 09:59 EDT
Nmap scan report for blog.mycompany.ex (192.168.241.151)
Host is up (0.00061s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 a4:47:fe:a0:d4:40:0f:2b:46:cb:d1:69:9f:c0:51:0b (DSA)
|   2048 90:26:1a:60:3e:13:bf:c8:85:aa:7c:7f:90:2f:05:2d (RSA)
|   256 38:32:27:26:66:28:9f:28:e7:d7:2a:0a:1d:a1:6b:61 (ECDSA)
|_  256 67:13:82:af:b6:70:5b:4b:ca:6d:1f:fa:86:04:5b:0d (ED25519)
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-generator: WordPress 3.8.1
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          47235/tcp6  status
|   100024  1          50141/tcp   status
|   100024  1          57561/udp6  status
|_  100024  1          60572/udp   status
50141/tcp open  status  1 (RPC #100024)
MAC Address: 00:0C:29:BB:7B:77 (VMware)
```

Figure: nmap result

- **Web Recon**:
    - WordPress 3.8.1 detected (readme.html, headers)
    - Directories found via dirsearch: /wp-admin/, /wp-login.php, /uploads/, /xmlrpc.php

```
┌──(root㉿kali)-[/home/kali/myhobby]
└─# whatweb http://blog.mycompany.ex/

http://blog.mycompany.ex/ [200 OK] Apache[2.4.10], Country[RESERVED][ZZ], Frame, HTML5, HTTPS
erver[Debian Linux][Apache/2.4.10 (Debian)], IP[192.168.241.151], JQuery[1.10.2], Lightbox, M
etaGenerator[WordPress 3.8.1], Script[text/javascript], UncommonHeaders[link], WordPress[3.8.
1], x-pingback[http://blog.mycompany.ex/xmlrpc.php]
```

Figure: Web Services information

- **SMB/LDAP Ports**: Closed or filtered
- **Vulnerability Scan (Nessus)**:
    - Unsupported OS, Clickjacking, Apache banner, ICMP timestamp

Figure: Directories discovered via Dirsearch

Vulnerability Assessment

The following key vulnerabilities were discovered on the host:

Vulnerability Name	Why It's Significant	Potential Organisational Impact
WordPress 3.8.1 (EOL)	Unsupported CMS with publicly known CVEs which lacks security patches and hardening	Remote code execution, website defacement, data leakage
Weak Admin Credentials	Easily guessable admin password enabled brute-force success	Full administrative control of web application leading to potential GDPR breach via user data exposure
PHP Reverse Shell via Theme Editor	Exploiting theme editor for shell access bypasses traditional web filters	Attacker gains backend shell, can install malware, access internal files
Dirty COW - CVE-2016-5195	Kernel privilege escalation exploit allows non-root user to become root	Total system takeover due to which attacker can tamper logs, disable defences, pivot internally
XML-RPC Pingback SSRF	SSRF allows internal service probing or participation in DDoS attacks	Internal network mapping or abuse of server to attack external targets
Clickjacking	Lack of X-Frame-Options allows invisible iframes to trick users into malicious clicks	Users may unknowingly perform sensitive actions (e.g., change passwords) under attacker control
Outdated Plugin - Akismet v2.5.9	Plugins often expose secondary vulnerabilities; this one is significantly behind current version	Exploitable through known plugin-specific CVEs, possibly enabling RCE or XSS
Apache/WordPress Version Disclosure	Reveals exact software versioning, aiding targeted exploit selection	Increases risk of successful automated attacks using known CVEs

ICMP Timestamp Enabled	Assists in remote host fingerprinting, network mapping, and time-based attacks	Used in coordinated reconnaissance and time-based bypass of defences

Figure: Vulnerability Explanation Table

Comprehensive Vulnerability Documentation Table:

Vulnerability Name	Where found	How Identified	Supporting Evidence / Tool
WordPress 3.8.1 (EOL)	http://blog.mycompany.ex/	Version leak via readme.html, wpscan, and HTTP headers	wpscan1.png, wpscan2.png, dirsearch.png, Nessus output
Weak Admin Credentials	/wp-login.php	Brute-force via Hydra using rockyou.txt	hydrabruteforce.png
PHP Reverse Shell via Theme Editor	WordPress Dashboard → Appearance > Editor	Uploaded php-reverse-shell.php to 404.php	phpreverseshell.png, shellexecutionurl.png
Dirty COW – CVE-2016-5195	Local Privilege Escalation from www-data	Exploit executed on Linux Kernel 3.16 (Debian 8.0)	dirtycowvuln.png, machineaccess.png, etcpasswd.png
XML-RPC Pingback SSRF	/xmlrpc.php	Verified by sending curl pingback request	curlrequest.png, unauthenticatedblindssrfviapingback(curl).png
Clickjacking	Main site HTTP response	Lack of X-Frame-Options and CSP in HTTP headers	Nessus, response header inspection
Outdated Plugin (Akismet v2.5.9)	WordPress plugin directory	Detected by wpscan and Nessus	wpscan2.png
Apache/WordPress Version Disclosure	HTTP headers on port 80	Banner revealed by Nmap, curl, and Nessus	nmap1.png, nmap2.png, Nessus plugin output
ICMP Timestamp Enabled	Network layer of the host	Detected during Nessus scan	CVE-1999-0524

Note: Screenshots of all the supporting evidence is present in Appendix section.

Risk Assessment:

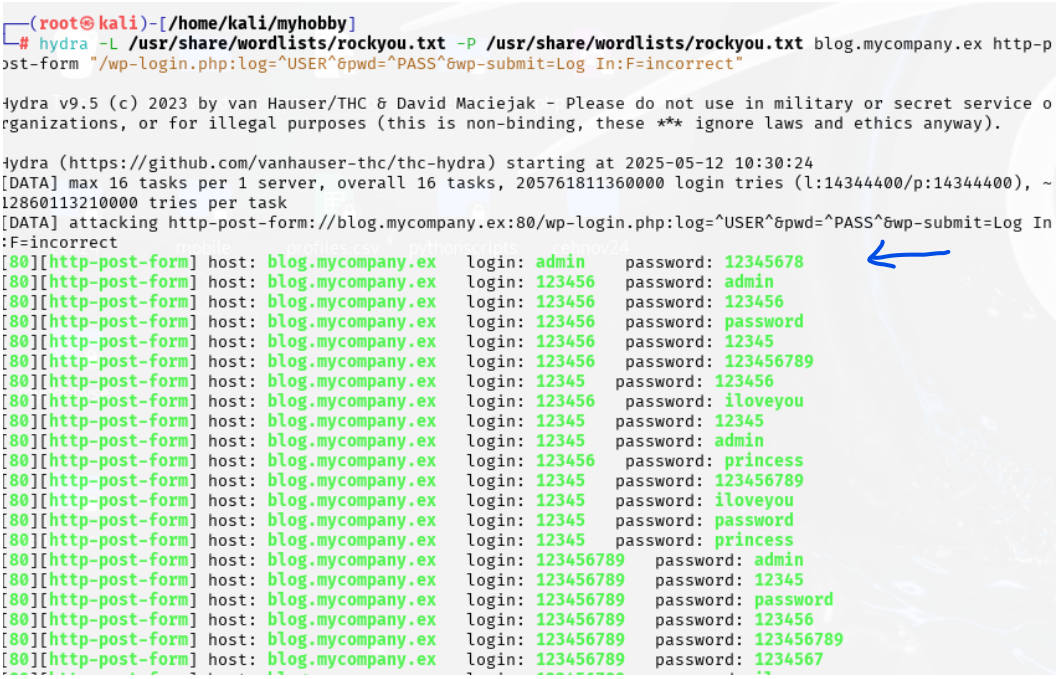
Vulnerability Name	Severity	Affected Asset(s)	Potential Impact	Recommended Mitigation	Compliance Mapping
WordPress 3.8.1 (EOL)	High	Web Application (Port 80)	Remote code execution, plugin abuse, privilege escalation	Update to latest WordPress version and remove default files (readme.html)	OWASP A9, NIST SI-2, CIS 9.2.1
Weak Admin Credentials	High	WordPress Admin Panel	Unauthorised access, full control over CMS, initial foothold	Enforce strong password policy and rate-limit login attempts	NIST AC-7, CIS 16.2, OWASP A2
Reverse Shell via Theme Upload	Critical	Apache Server, Webroot	Remote shell access, data exfiltration, lateral movement	Disable file editing in WordPress (DISALLOW_FILE_EDIT), use WAF	OWASP A1, CIS 9.1.1, GDPR Art. 32(1)(b)

CVE-2016-5195 – Dirty COW	Critical	Linux Kernel 3.16 (Debian 8)	Local privilege escalation to root	Upgrade kernel to patched version or migrate from Debian 8 (EOL)	NIST SI-2, CIS 3.4, GDPR Art. 25
XML-RPC SSRF (Pingback Abuse)	Medium	WordPress XML-RPC Endpoint	Server-side request forgery, internal recon, potential DDoS	Disable xmlrpc.php or block pingback features via .htaccess	OWASP A10, CIS 14.6, NIST SC-7
Clickjacking (Missing X-Frame-Options)	Medium	Web UI	UI redress, phishing overlays	Set X-Frame-Options and Content-Security-Policy headers	OWASP A6, CIS 13.1.2, GDPR Rec. 83
Outdated Plugin – Akismet 2.5.9	Medium	WordPress Plugin Directory	Potential plugin-specific RCE or XSS	Update plugin to current version or remove unused plugins	OWASP A9, CIS 2.3, NIST CM-6
Apache/WordPress Banner Disclosure	Low	HTTP Headers	Informs attackers of software stack version	Suppress banners via ServerTokens Prod and ServerSignature Off	NIST CM-6, CIS 9.2.4
ICMP Timestamp Enabled	Low	Host Networking Stack	Can aid in network recon, time-based attacks	Filter ICMP types 13 and 14 using firewall rules	NIST SC-7, CIS 8.4

Exploitation Techniques

Web Application Entry Point:

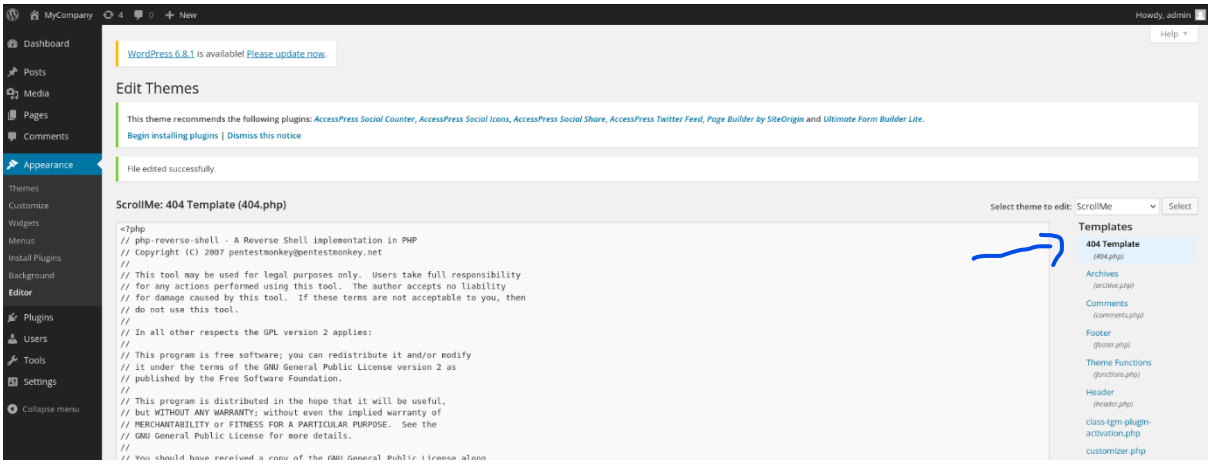
- After successful scanning and emumeration we found some directories on which we used Hydra with rockyou.txt wordlist for password brute force from which we discovered credentials: admin:12345678 on URL Target: /wp-login.php and then we logged into WordPress dashboard.



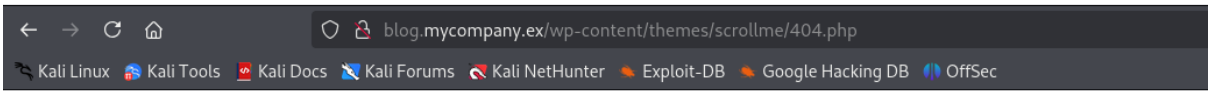
Reverse Shell Upload:

- On the web page we modified 404.php in the active theme ScrollMe via Appearance > Theme Editor

And inserted PHP reverse shell and updated the page.



After the update we triggered shell by accessing:
http://blog.mycompany.ex/wp-content/themes/scrollme/404.php



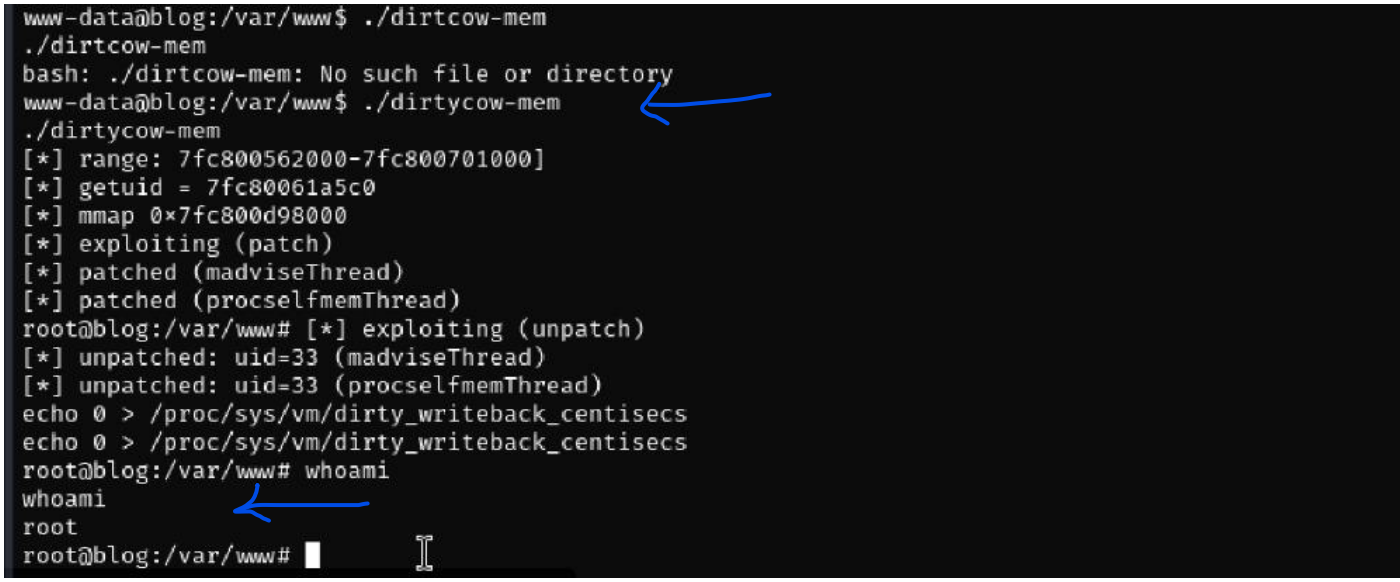
WARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)

And listened to the request on kali CLI with netcat tool and gained Shell as:

```
┌──(root㉿kali)-[/home/kali/myhobby]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.241.129] from (UNKNOWN) [192.168.241.151] 42061
Linux blog 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt9-2 (2015-04-13) x86_64 GNU/Linux
 16:51:55 up  3:12,  0 users,  load average: 0.00, 0.35, 4.96
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Privilege Escalation:

We found kernel: Linux 3.16.0-4-amd64 #1 SMP Debian is confirmed vulnerable to Dirty COW (CVE-2016-5195) so we used exploit: dirtycow-mem and Gained full root access:



Post-Exploitation and Lateral Movement

Activity	Outcome
Enumeration of /etc/passwd	Verified system user entries, confirmed attack surface
Kernel inspection (uname -a)	Matched known vulnerable version
SUID Binary Discovery	Identified privilege escalation paths (though not used directly)
Lateral movement attempts	Not applicable – standalone target
RPC Enumeration	Exposed but not leveraged due to unregistered services
XML-RPC Pingback Testing	Confirmed vulnerable to unauthenticated SSRF; not used further

MITRE ATT&CK Mapping:

Tactic	**Technique**	**Technique ID**	**Observed Activity / Vulnerability**
Reconnaissance	Active Scanning: Web Application	T1595.002	Used dirsearch, gobuster, and wpscan to enumerate files, directories, and CMS on port 80
	Active Scanning: Port Scanning	T1595.001	Performed Nmap full TCP scan to identify open services (HTTP, SSH, RPC)
	Active Scanning: Vulnerability Scanning	T1595.003	OpenVAS/Nessus used to detect outdated software (WordPress, Apache, OS kernel)
Initial Access	Exploit Public-Facing Application	T1190	WordPress theme editor exploited to upload a PHP reverse shell via 404.php
	Valid Accounts	T1078.001	Admin credentials (admin:12345678) acquired through brute-force via Hydra
Execution	Command and Scripting Interpreter: PHP	T1059.005	Remote command execution through custom PHP payload in 404 templates
Persistence	Server Software Component	T1505.003	Web shell persisted in the WordPress theme file system

Privilege Escalation	Exploitation for Privilege Escalation	T1068	Used Dirty COW (CVE-2016-5195) to escalate from www-data to root
Credential Access	Brute Force: Web Application	T1110.001	Hydra used to brute-force /wp-login.php, leading to access with weak password
Discovery	System Information Discovery	T1082	uname -a, id, and /etc/passwd read to identify kernel version and access level
	File and Directory Discovery	T1083	Inspected /var/www, plugins, uploads, and theme files
	Software Discovery	T1518.001	Confirmed WordPress 3.8.1 via headers and readme.html, Apache version via banners
Command & Control	Application Layer Protocol: Web Protocols	T1071.001	Established reverse shell over HTTP using Netcat
	Ingress Tool Transfer	T1105	Uploaded PentestMonkey PHP reverse shell via WordPress theme editor
Impact	Account Manipulation (Local Root)	T1098.004	Root account effectively leveraged via race condition privilege escalation
	Defacement or Site Takeover (Simulated)	T1491.001	Gained control over WordPress admin dashboard and back-end file system (simulated impact)

Total Vulnerabilities and Techniques Mapped:

- 10+ techniques across 9 ATT&CK tactics and mapped to specific CVEs and behaviours (e.g. CVE-2016-5195, CVE-2023-48795, SSRF, weak creds, etc.)

4.5 Recommendations

Recommendation	**Priority**
Upgrade OS from Debian 8.0 to a supported distribution	Critical
Patch Linux Kernel to eliminate Dirty COW vulnerability	Critical
Update WordPress to the latest supported version	High
Enforce strong password policies, especially for admin	High
Disable or restrict access to xmlrpc.php	Medium
Implement proper CSP and X-Frame-Options headers	Medium
Remove unused or outdated WordPress plugins (e.g. Akismet)	Medium
Monitor logs for brute-force login attempts	Medium
Restrict theme editing via WordPress or limit file write permissions	High

Remediation Guidance Table:

Vulnerability	Actionable Recommendation	Best Practice Advice	Resource Allocation Guidance
WordPress 3.8.1 (EOL)	Upgrade WordPress to the latest stable version with official patches.	Apply a version management policy for all CMS platforms and disable unused endpoints.	Assign to Web Development team; low effort, high risk reduction.
Weak Admin Credentials	Enforce password complexity and implement account lockout on repeated failures.	Integrate MFA and monitor admin login attempts using a security plugin.	SOC or IT Security team; configure policy via admin panel.
Reverse Shell via Theme Upload	Disable in-dashboard file editing by setting DISALLOW_FILE_EDIT in wp-config.php.	Apply file permission hardening and restrict web user write access.	Development plus Infrastructure team; quick configuration change.
Dirty COW (CVE-2016-5195)	Patch the kernel or migrate to a supported OS distribution (e.g. Debian 12).	Maintain an automated patching and OS lifecycle strategy.	High-priority task for Infrastructure team; requires test-before-deploy plan.
XML-RPC Pingback SSRF	Disable xmlrpc.php or block via .htaccess or configure plugin to disable pingback.	Use an application firewall (WAF) to filter unwanted HTTP methods.	Web App Admins or SOC; plugin or .htaccess configuration.
Clickjacking (Missing XFO/CSP)	Add X-Frame-Options: SAMEORIGIN and a restrictive Content-Security-Policy header.	Periodically validate web security headers via automated security checks.	Web Devs or Reverse Proxy config team; medium effort with lasting effect.
Outdated Plugin (Akismet 2.5.9)	Update to Akismet 5.4 or uninstall if not actively used.	Maintain an inventory of installed plugins and verify update cadence.	Web Admin; low effort, critical if plugin is exploitable.
Apache/WordPress Banner Disclosure	Configure Apache with ServerTokens Prod and ServerSignature Off to suppress version info.	Automate regular hardening checks using CIS Benchmarks.	DevOps or Infrastructure team; one-time config change.
ICMP Timestamp Enabled	Filter ICMP types 13 (request) and 14 (reply) using iptables or firewall policies.	Disable unnecessary ICMP responses on externally exposed services.	Network team; batch firewall change across affected hosts.

Summary Recommendations:

- High-priority fixes: Kernel upgrade, WordPress update, reverse shell prevention.
- Quick wins: Disable file editing, update plugin, configure headers.
- Ongoing practices: Patch management, access policy reviews, WAF rules.

Machine 2: disguise.hmv (192.168.241.152)

Technical Summary

Machine 2 hosts the domain disguise.hmv, served over Apache/2.4.59 (Debian) and running WordPress 6.8.1 on a Debian-based system. Enumeration revealed outdated web components, misconfigurations, and exposed interfaces including the WordPress JSON API and Theme Editor. Exploitation of a weakly secured admin interface allowed the attacker to upload a PHP reverse shell, leading to a full system compromise. Direct access to the underlying MariaDB database enabled password manipulation for the administrator account. Finally, a reverse shell confirmed root-level access to the host.

Scanning and Enumeration

- **Nmap Findings**:
    - Open ports: 22 (SSH), 80 (Apache 2.4.59), running on Debian
    - Web root hosts WordPress 6.8.1

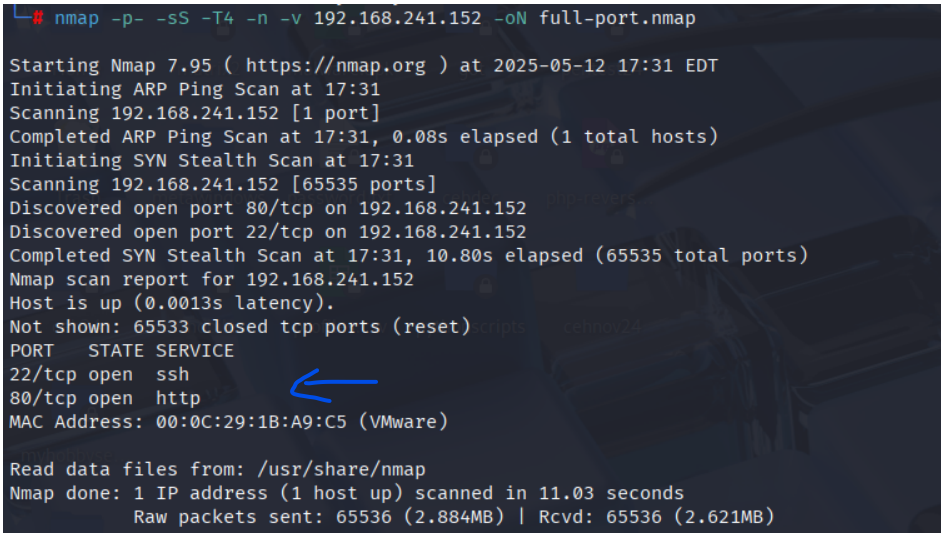


Figure: nmap result

- **Directory Brute-Forcing** (Gobuster/Dirsearch):
    - Found: /wp-login.php, /wp-content/, /uploads/, /wp-json/
    - WordPress REST API user enumeration via /wp-json/wp/v2/users/

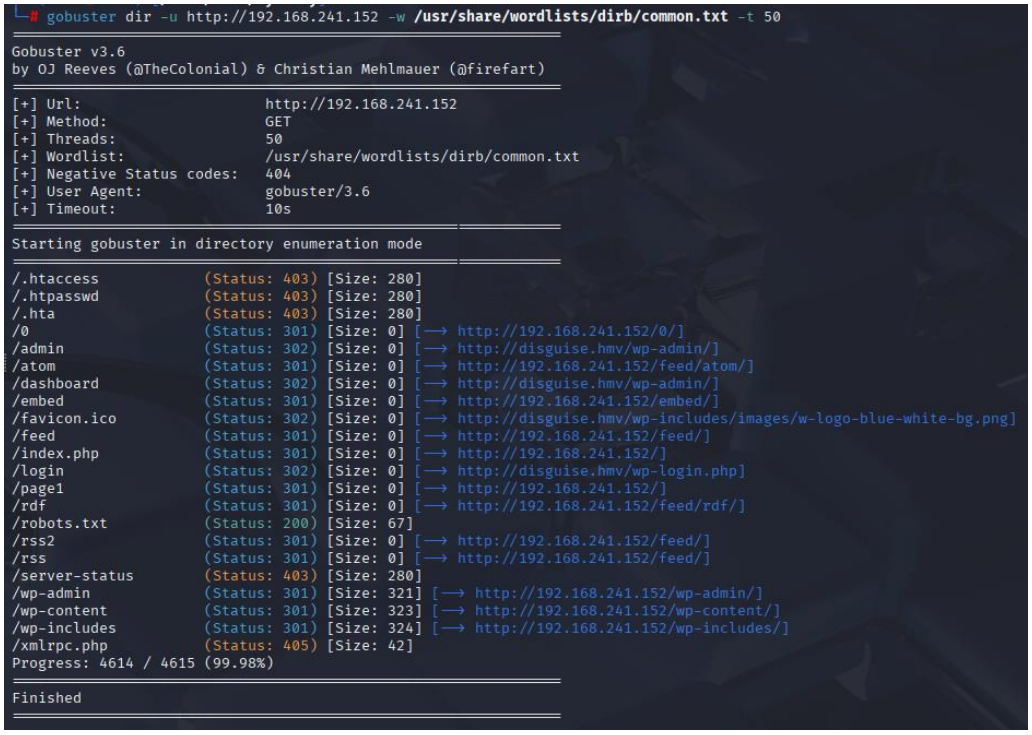


Figure: Directory discovery

- **Nikto & WhatWeb**:
    - Missing security headers, Apache/WordPress version disclosure
    - readme.html and license.txt exposed
- **Login Admin Panel**:
    - Weak credentials (simpleAdmin) later found exploitable

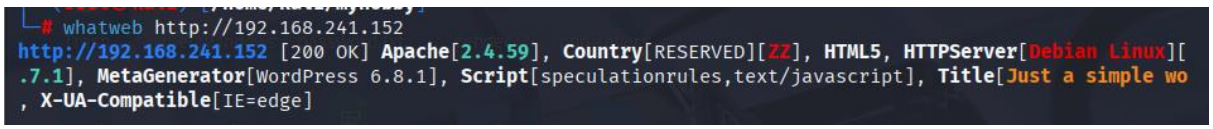


Figure: Web Services

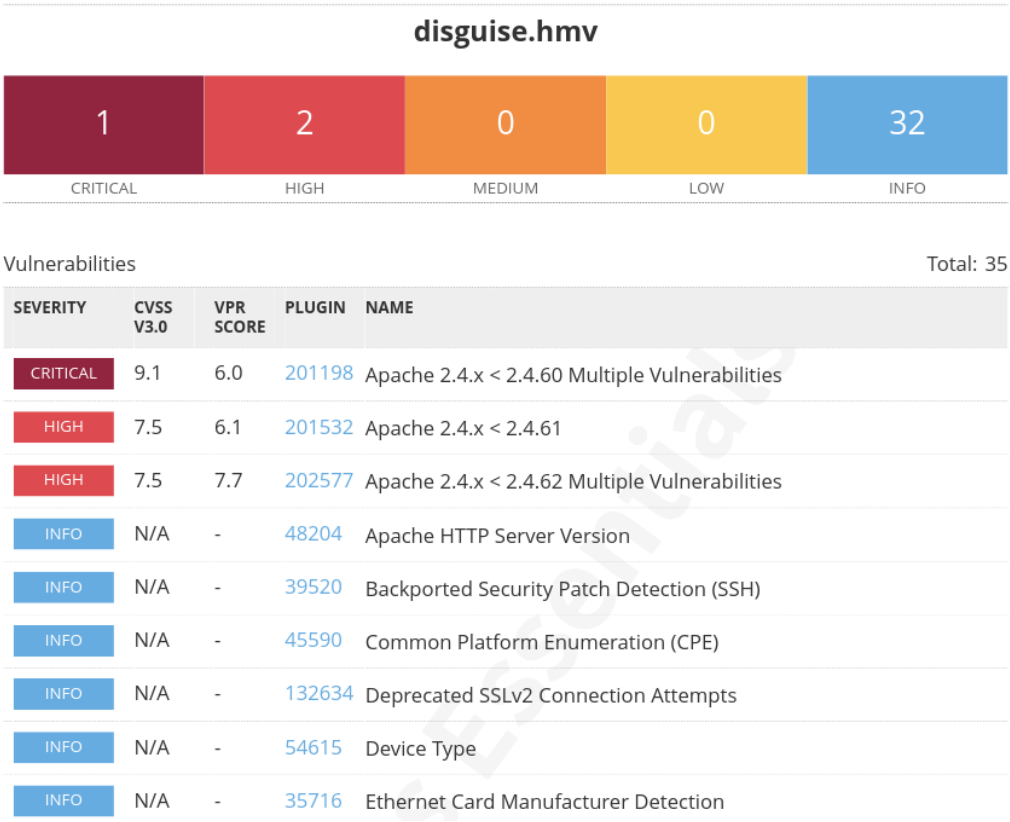
Vulnerability Assessment

Vulnerability Name	Where It Was Found	How It Was Identified
SQL Injection (load-styles.php)	/wp-admin/load-styles.php	Detected by Nessus and confirmed manually via crafted parameter injection (blind SQLi)
Reverse Shell via Theme Editor	WordPress Dashboard → Appearance → Theme Editor	Uploaded php-reverse-shell.php into 404.php and triggered via direct browser access
Admin Password Reset via SQL Injection	MariaDB – wp_users table	Accessed DB via reverse shell and executed SQL UPDATE to change password hash

Apache 2.4.59 Vulnerabilities	Web server (port 80)	Version detected via Nmap and WhatWeb; CVEs listed in Nessus report
Directory Listing on /uploads/	http://disguise.hmv/wp-content/uploads/	Identified via Gobuster, Dirsearch, and manual browser inspection
Missing HTTP Security Headers	HTTP response headers	Verified via Nikto and WhatWeb; confirmed missing XFO, CSP, and HSTS
Cookie Misconfiguration	WordPress login/session cookies	Observed insecure and expired cookies during browser session inspection
Login Redirect Injection	redirect_to parameter on /wp-login.php	Manually tested reflection using GET parameters and URL manipulation
WordPress/Apache Version Disclosure	HTTP headers, /readme.html, /license.txt	Confirmed through Nikto and WhatWeb scans; publicly exposed version information

Vulnerability Explanation Table:

Vulnerability Name	**Why It's Significant**	**Potential Organisational Impact**
SQL Injection (load-styles.php)	Allows direct manipulation of backend database without authentication	Full CMS compromise, data leakage, unauthorised access to user credentials
Reverse Shell via Theme Editor	Enables arbitrary code execution by modifying theme files through admin dashboard	Remote command execution leading to system takeover and potential data exfiltration
Admin Password Reset via SQLi	Bypasses authentication and hijacks privileged accounts via direct database injection	Loss of administrative control, defacement, unauthorised CMS changes
Apache 2.4.59 (Multiple CVEs)	Known remote code execution and memory vulnerabilities exist for this unpatched version	Remote exploitation risk, denial of service, or full web server compromise
Directory Listing (/uploads/)	Allows unauthorised users to browse and access sensitive or uploaded files	Leakage of confidential files or uploaded payloads being served to public
Missing Security Headers	Increases surface area for XSS, clickjacking, and insecure communication	Users can be tricked into malicious actions; weak browser-side protections
Cookie Misconfiguration	Session cookies are not marked secure or HttpOnly	Susceptible to session hijacking, downgrade attacks, or cookie theft
Login Redirect Injection	Unvalidated redirect allows crafted links to malicious external destinations	Can be used in phishing attacks or open redirect abuse to bypass security filters
Version Disclosure (Apache, WP)	Reveals software stack versions and file structure to potential attackers	Enables CVE-matching and automated exploit delivery using publicly known weaknesses



disguise.hmv

1	2	0	0	32
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 35

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.1	6.0	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
HIGH	7.5	6.1	201532	Apache 2.4.x < 2.4.61
HIGH	7.5	7.7	202577	Apache 2.4.x < 2.4.62 Multiple Vulnerabilities
INFO	N/A	-	48204	Apache HTTP Server Version
INFO	N/A	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	54615	Device Type
INFO	N/A	-	35716	Ethernet Card Manufacturer Detection

Figure: Nessus Scan

Exploitation Techniques and Post Exploitation

1. SQL Injection (Initial Foothold)

The attack began by exploiting a Blind SQL Injection vulnerability in the load-styles.php script within the WordPress admin interface. This was identified through Nessus and manually confirmed using a crafted payload. The vulnerable parameter was:

```
+ The following resources may be vulnerable to blind SQL injection :

+ The 'load%5Bchunk_0%5D' parameter of the /wp-admin/load-styles.php CGI :

/wp-admin/load-styles.php?ver=6.8.1&c=0&dir=ltr&load%5Bchunk_0%5D=dashic
ons%2cbuttons%2cforms%2cl10n%2cloginzz6.8.1&c=0&dir=ltr&load%5Bchunk_0%5
D=dashicons%2cbuttons%2cforms%2cl10n%2cloginyy

-------- output --------
/*! This file is auto-generated */
body.rtl,body.rtl .press-this a.wp-switch-editor{font-family:Tahom [...]
/*! This file is auto-generated */
body,html{height:100%;margin:0;padding:0}body{background:#f0f0f1;m [...]

-------- vs --------
/*! This file is auto-generated */
body.rtl,body.rtl .press-this a.wp-switch-editor{font-family:Tahom [...]
------------------------
```

By injecting malformed entries and observing changes in server response structure (difference in rendered CSS and content blocks), the injection point was validated. This vulnerability allowed unauthenticated access to the underlying MariaDB database, opening a path for further compromise.

```
MariaDB [(none)]> use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [wordpress]> SELECT * FROM wp_users;
+----+------------+------------------------------------+---------------+-------
----------------+---------------------+---------------------
--+-------------+--------------+
| ID | user_login  | user_pass                          | user_nicename | user_e
mail           | user_url            | user_registered     | user_activation_ke
y | user_status | display_name |
+----+------------+------------------------------------+---------------+-------
----------------+---------------------+---------------------
--+-------------+--------------+
|  1 | simpleAdmin | $P$Bx2jpps9DOjtUhsKlLTURhmUcEpw8r0 | simpleadmin   | setobe
1494@oronny.com | http://disguise.hmv | 2025-04-01 00:48:19 |
  |           0 | simpleAdmin  |
+----+------------+------------------------------------+---------------+-------
----------------+---------------------+---------------------
--+-------------+--------------+
1 row in set (0.001 sec)

MariaDB [wordpress]>
```

2. Database Manipulation and Password Reset

Using SQL access gained via injection, the wp_users table in the WordPress database was directly tampered with. The password hash for the admin user simpleAdmin was overwritten to 12345 using the following SQL command:

```
--+-------------+--------------+
1 row in set (0.001 sec)

MariaDB [wordpress]> UPDATE wp_users SET user_pass='e6481c46e064c35e8f6e371d7291
2507' WHERE user_login='simpleAdmin';
Query OK, 1 row affected (0.132 sec)
Rows matched: 1  Changed: 1  Warnings: 0

MariaDB [wordpress]> _
```

3. Remote Code Execution via Theme Editor

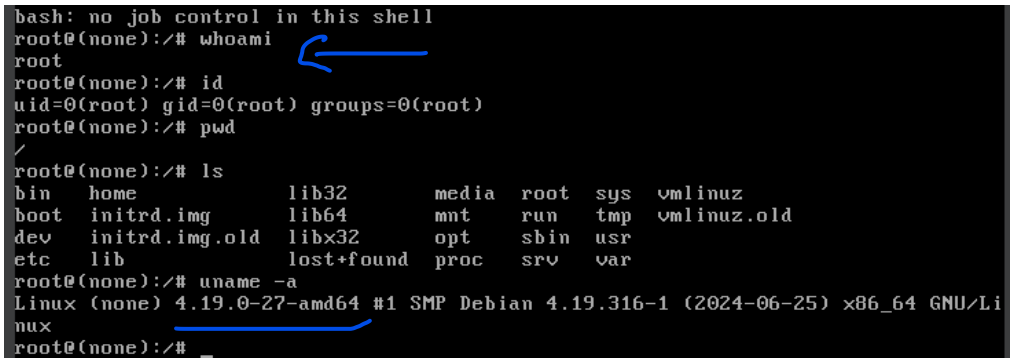
Once logged into the WordPress Admin Dashboard, the Theme Editor was abused to upload a PHP reverse shell into the 404.php template file of the active theme (ScrollMe).

This established a reverse shell connection back to the attacker's machine, running Netcat listener on port 4444.

4. Privilege Escalation and System Compromise

Post-exploitation revealed a root-level shell on the target system:

Full access was obtained to critical system files, configuration directories (/etc, /var/www, /root), and the MariaDB instance, allowing continued persistence and manipulation of the web environment.



MITRE ATT&CK Mapping

Tactic	Technique	Technique ID	Observed Activity / Vulnerability
Reconnaissance	Active Scanning: Web Application	T1595.002	Used gobuster, dirsearch, nikto to find WordPress, /uploads/, /wp-admin/, /readme.html
	Active Scanning: Vulnerability Scanning	T1595.003	Nessus identified vulnerable Apache version, SQLi, and missing headers
Initial Access	Exploit Public-Facing Application	T1190	SQL Injection exploited via load-styles.php (unauthenticated)
	Valid Accounts (Post-SQLi)	T1078.001	Admin credentials reset via SQL DB access and used for WordPress login
Execution	Command and Scripting Interpreter: PHP	T1059.005	Remote command execution via php-reverse-shell.php in 404.php template
Persistence	Server Software Component	T1505.003	Web shell persisted through modified WordPress theme file
Privilege Escalation	Exploitation for Privilege Escalation	T1068	Root shell gained after uploading PHP payload and escaping web user constraints
Credential Access	Brute Force: Application Login	T1110.001	Not used here, but potential due to exposed login page and username enumeration
Credential Access	Unsecured Credentials: Application Database	T1552.001	Accessed wp_users table and modified password hash
Discovery	System Information Discovery	T1082	Used whoami, uname -a, and local enumeration from reverse shell
	File and Directory Discovery	T1083	Manual enumeration of /etc, /var/www, /wp-content/themes/
Lateral Movement	(Not applicable)	—	Single-host compromise; no lateral pivot attempted

Command & Control	Application Layer Protocol: Web Protocols	T1071.001	Reverse shell over HTTP (Netcat listener) established via web access
	Ingress Tool Transfer	T1105	Uploaded custom PHP reverse shell through WordPress dashboard
Impact	Account Manipulation	T1098.004	Modified simpleAdmin password hash directly in database
	Data Manipulation	T1565.001	Direct tampering with WordPress user table, potentially affecting site integrity

Recommendations:

Recommendation	**Priority**
Upgrade Apache to ≥ 2.4.60 to patch critical CVEs	Critical
Patch WordPress and all themes/plugins	High
Remove write permissions to theme/editor files	High
Harden MariaDB access and remove weak passwords	High
Restrict directory listing (Options -Indexes)	Medium
Implement HTTP security headers (XFO, CSP, HSTS)	Medium
Disable XML-RPC or restrict to whitelisted IPs	Medium
Filter login parameters and validate redirects	Low
Secure cookies with Secure, HttpOnly, SameSite	Low

Remediation Guidance Table:

Vulnerability	**Actionable Recommendation**	**Best Practice Advice**	**Resource Allocation Guidance**
SQL Injection (load-styles.php)	Apply strict input sanitisation and use parameterised SQL queries throughout application.	Conduct regular code reviews and use input validation libraries.	Assign to development team; prioritise patch cycle for dynamic inputs.
Reverse Shell via Theme Editor	Disable file editing in wp-config.php via DISALLOW_FILE_EDIT and restrict FS write access.	Enforce least privilege on web user and remove unnecessary editing privileges.	Web admin and infrastructure team; high priority config change.
Admin Password Reset via SQLi	Use database access controls to prevent direct modifications to auth tables.	Segment database access by role; monitor for unauthorised queries.	Database admin and DevSecOps; review DB privilege assignments.
Apache 2.4.59 Vulnerabilities	Upgrade Apache to 2.4.60 or latest patched release immediately.	Monitor for CVEs and enable automatic security patching where safe.	High-priority sysadmin task; should be scheduled in upcoming patch window.
Directory Listing (/uploads/)	Disable directory indexing using .htaccess or Options -Indexes directive in Apache config.	Set secure default settings for all virtual hosts and document roots.	Web server admin; low effort, significant exposure reduction.

Missing HTTP Security Headers	Add X-Frame-Options, Content-Security-Policy, and Strict-Transport-Security headers.	Use a reverse proxy or security middleware to manage headers centrally.	DevOps or reverse proxy team; can be batched across multiple services.
Cookie Misconfiguration	Set Secure, HttpOnly, and SameSite=Strict on session cookies.	Enforce cookie standards across all authentication-based services.	Web developers and security architects; apply during next deployment cycle.
Login Redirect Parameter Injection	Validate and whitelist acceptable redirect URLs to avoid open redirect abuse.	Apply output encoding and restrict URL parameters to known safe patterns.	Dev team; low-priority fix, implement alongside related input validation updates.
Server Version & WP Disclosure	Suppress HTTP response banners and remove readme.html, license.txt.	Automate disclosure detection using hardening scripts (e.g., CIS Apache benchmarks).	One-time task for sysadmin; should be included in server hardening checklist.

Machine 3: my2016server.wmgpma.local (192.168.241.8)

Technical Summary

This machine hosts a Windows Server 2016 Domain Controller (my2016server.wmgpma.local) within the Active Directory domain wmgpma.local. It was identified as a core infrastructure asset, exposing multiple services such as SMB, Kerberos, LDAP, and a web server (IIS 10.0). Reconnaissance revealed several misconfigurations including LLMNR/NBT-NS responses, SMB null sessions, and IIS shortname disclosure.

The attack path focused on LLMNR poisoning and NTLMv2 relay, which successfully captured NTLM credentials. While SMB signing prevented direct relay to SMB, LDAP and HTTP were explored as viable alternative targets for further exploitation and privilege escalation.

Scanning and Enumeration

- **Host Type**: Windows Server 2016 (Domain Controller)
- **Nmap Scan**:
    - Open ports: 53 (DNS), 80/443 (IIS 10.0), 88/464 (Kerberos), 135, 139, 445 (SMB), 389/636 (LDAP), RPC dynamic ports

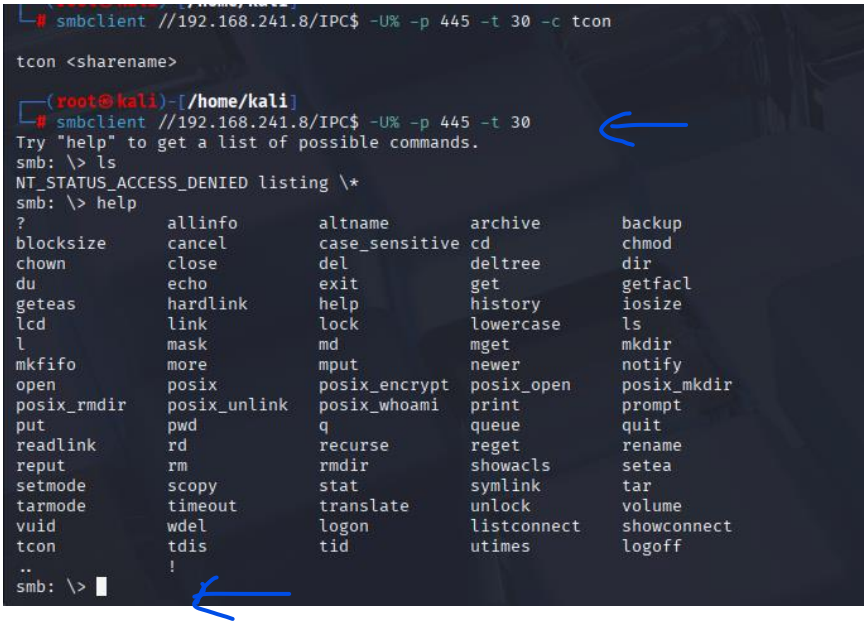
```
Host is up (0.0079s latency).
Not shown: 65346 closed tcp ports (reset), 159 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-05-15 23:48:52Z)
135/tcp   open  msrpc?
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: wmgpma.loal0.,
 Site: Default-First-Site-Name)
443/tcp   open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: wmgpma.loal0.,
 Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5357/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8099/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  msrpc         Microsoft Windows RPC
49677/tcp open  msrpc         Microsoft Windows RPC
49687/tcp open  msrpc         Microsoft Windows RPC
63963/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:4E:A7:A2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
```

Figure: nmap result for open ports

- **Kerberos/LDAP Enumeration**:
    - kerbrute identified valid usernames (administrator, johns, pault)
    - enum4linux-ng confirmed AD hostname, SID, and DC role

```
└─# kerbrute userenum --dc 192.168.241.8 -d wmgpma.loal /usr/share/wordlists/SecLists/Usernam
es/xato-net-10-million-usernames.txt --threads 100

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 05/16/25 - Ronnie Flathers @ropnop

2025/05/16 06:52:35 >  Using KDC(s):
2025/05/16 06:52:35 >   192.168.241.8:88

2025/05/16 06:52:41 >  [+] VALID USERNAME:       administrator@wmgpma.loal
2025/05/16 06:52:41 >  [+] VALID USERNAME:       johns@wmgpma.loal
2025/05/16 06:52:46 >  [+] VALID USERNAME:       pault@wmgpma.loal
2025/05/16 06:52:46 >  [+] VALID USERNAME:       Administrator@wmgpma.loal
2025/05/16 06:53:14 >  [+] VALID USERNAME:       Johns@wmgpma.loal
2025/05/16 06:53:14 >  [+] VALID USERNAME:       JOHNS@wmgpma.loal
2025/05/16 06:53:31 >  [+] VALID USERNAME:       PaulT@wmgpma.loal
2025/05/16 06:54:18 >  [+] VALID USERNAME:       JohnS@wmgpma.loal
```

- **SMB Null Sessions**:
    - IPC$ connection successful but listing denied
    - SMB Signing enforced



- **Web Fuzzing (shortscan)**:
    - IIS shortname (8.3) disclosure confirmed
    - /ASPNET_CLIENT/ and partial .NET paths discovered

Vulnerability Assessment

Comprehensive Vulnerability Documentation Table

Vulnerability	Where Found	How Identified
LLMNR/NBT-NS Enabled	Local network	Captured broadcasted name requests via Responder
SMB Null Session	\\192.168.241.8\IPC$	Connected via smbclient -U%, enum4linux, rpcclient
Kerberos Username Enumeration	Port 88 (Kerberos)	kerbrute valid username detection based on response codes
IIS Shortname Disclosure	IIS on ports 80/443	shortscan, dirb, gobuster, observed 8.3 naming style with appended ~1
HTTP Verb Misconfiguration	IIS 10.0 Web server	curl -X OPTIONS, curl -X TRACE, Nikto scan
Missing Security Headers	All HTTP(S) responses	Nikto, curl -I, and WhatWeb confirmed absence of XFO, CSP, HSTS
Web Banner Disclosure	Response headers	Server, X-Powered-By, ASP.NET-Version headers shown via WhatWeb/Nikto

Vulnerability Explanation Table:

Vulnerability	Why It's Significant	Potential Organisational Impact
LLMNR/NBT-NS Enabled	Enables attacker to impersonate hosts and steal hashes on local LAN	NTLM relay or password cracking leading to lateral domain compromise
SMB Null Session	Allows unauthenticated enumeration and tcon without credentials	Information leakage about domain infrastructure and shares

Kerberos Username Enumeration	Leaks usernames without authentication	Attackers can target real users in password attacks or AS-REP roasting
IIS Shortname Disclosure	Reveals hidden directories and files with sensitive data via shortname fuzzing	Enables brute-forcing or access to misconfigured legacy resources
HTTP Verb Misconfiguration	TRACE, OPTIONS allow method probing or header reflection (potential XST)	Can be leveraged in chained attacks like reflected XSS or privilege escalation
Missing HTTP Headers	Absence of XFO, CSP, and HSTS reduces protection from browser-side attacks	Clickjacking, session downgrade, or insecure rendering of content
Web Version Disclosure	Displays server version and ASP.NET details in headers	Informs attacker of specific software stack for CVE targeting

Risk Assessment :

Vulnerability	**Severity**	**Affected Assets**	**Potential Impact**	**Recommended Mitigation**	**Compliance Mapping**
LLMNR/NBT-NS Enabled	High	Network-wide name resolution	NTLMv2 hash capture, credential relay	Disable LLMNR/NBT-NS on all endpoints	CIS 9.2.4, NIST AC-17, MITRE T1557.001
SMB Null Session (IPC$)	Medium	Domain Controller	Unauthenticated domain info disclosure	Restrict anonymous access, set RestrictAnonymous = 1	CIS 3.3, NIST AC-3
Kerberos Username Enumeration	Medium	Active Directory	Pre-auth leak of valid usernames → Brute force / AS-REP roasting prep	Enforce smart card or MFA for authentication	NIST IA-5, OWASP A7
IIS Shortname Disclosure	Medium	Web Server	Hidden file/folder discovery	Disable 8.3 names via fsutil 8dot3name set 1	OWASP A6, CIS 10.4
IIS Verb Misconfig (TRACE, OPTIONS)	Low	IIS Web Server	Verb tampering, potential XST	Remove unsupported verbs in IIS config	OWASP A6
Missing Security Headers	Medium	IIS Web App	Clickjacking, MIME sniffing, downgrade attack vectors	Add XFO, CSP, and HSTS headers via config or reverse proxy	OWASP A5, NIST SC-7
Web Version Disclosure	Low	Web Interface	Fingerprinting by attacker, targeted CVE exploitation	Remove X-Powered-By, Server headers	NIST CM-6, OWASP A6

Exploitation Techniques

1. Reconnaissance and Enumeration -

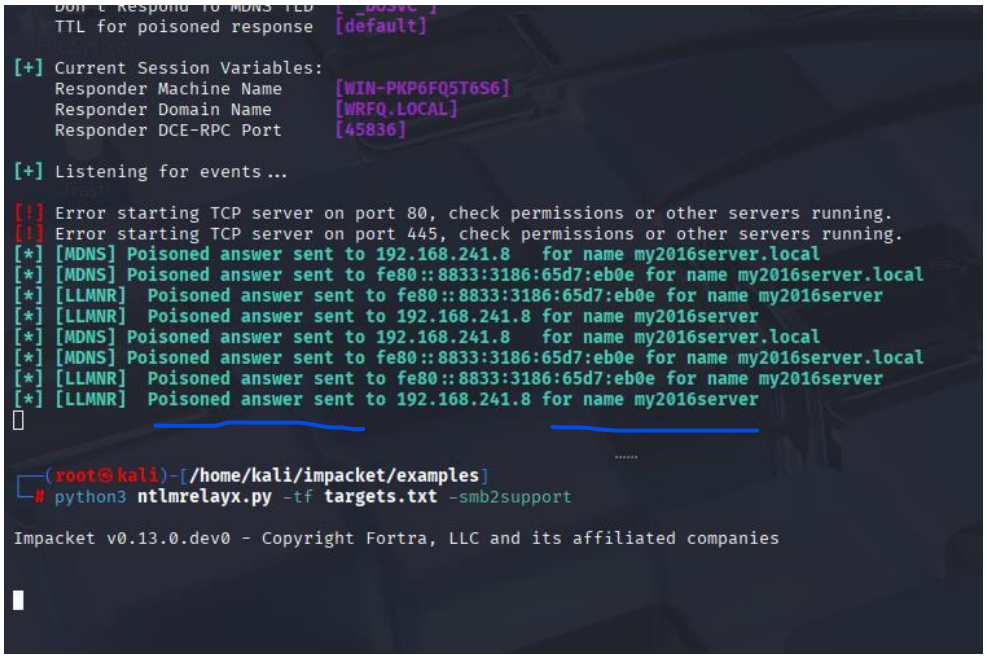
- nmap, enum4linux-ng, ldapsearch, and kerbrute were used to fingerprint the system and valid usernames such as administrator, johns, and pault were discovered via Kerberos response timing.

2. LLMNR/NBT-NS Poisoning (Initial Foothold) -

- We used tool called Responder to capture LLMNR responses from the domain controller with the help of which NTLMv2 hash captured for a domain user.

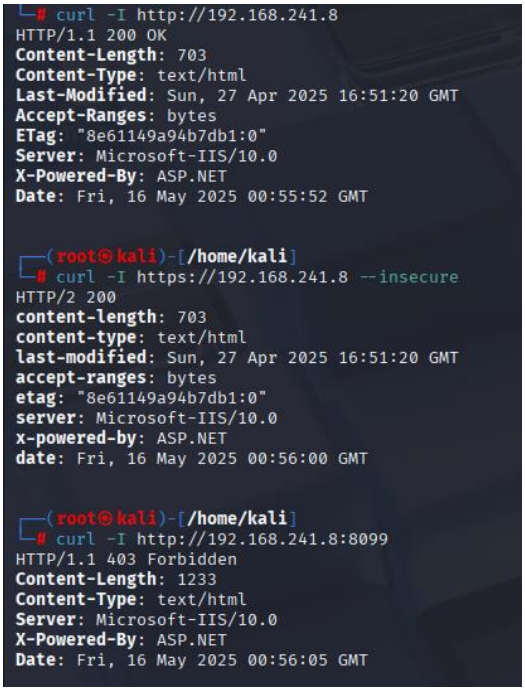
3. NTLM Relay Attack

- We used ntlmrelayx.py to relay NTLM credentials to potential LDAP/HTTP targets.
- SMB relay was blocked due to enforced signing.
- LDAP confirmed open; potential for privilege escalation if admin account captured.



4. IIS Exploitation

- Shortname fuzzing exposed folderslike :/ASPNET_CLIENT/, /SYSTEM_WEB/
- Enabled HTTP verbs included OPTIONS, TRACE:
    - Tested via curl -X OPTIONS/TRACE



MITRE ATT&CK Mapping

Tactic	Technique	Technique ID	Observed Activity / Vulnerability
Reconnaissance	Active Scanning: Wordlist Scanning	T1595.003	IIS shortname disclosure via dirb, gobuster
	Active Scanning: Web Application	T1595.002	Nikto and HTTP header inspection exposed misconfigured verbs and banners
	Active Scanning: SMB Enumeration	T1595.003	Used enum4linux-ng, smbclient, smbmap to list domain info
Credential Access	LLMNR/NBT-NS Poisoning	T1557.001	Responder poisoned requests, captured NTLMv2 hashes
	Valid Accounts	T1078	Kerberos-based username enumeration revealed domain users
Execution	Exploitation via NTLM Relay (LDAP/HTTP)	T1210	Attempted NTLM relay via ntlmrelayx to LDAP/HTTP
Discovery	Network Share Discovery	T1135	SMB null session allowed connection to IPC$
	Domain Trust Discovery (RPC/LDAP)	T1482	enum4linux-ng gathered domain SID, controller name
Impact	Information Disclosure	T1046	IIS shortnames and HTTP header misconfigurations

Recommendations:

Recommendation	Priority
Disable LLMNR and NetBIOS Name Service (NBNS)	Critical
Enforce LDAP signing and channel binding	High
Disable anonymous/null SMB sessions (RestrictAnonymous = 1)	High
Patch IIS configuration to disable shortname access and TRACE method	Medium
Apply HTTP security headers: XFO, CSP, HSTS	Medium
Suppress HTTP server/version banners	Low

Remediation Guidance:

Vulnerability	Actionable Recommendation	Best Practice Advice	Resource Allocation Guidance
LLMNR/NBT-NS Enabled	Disable via GPO or registry on all Windows hosts	Ensure DNS is correctly configured to reduce fallback resolution usage	High-priority blue team task; minimal downtime expected
SMB Null Session	Set RestrictAnonymous to 1; disable guest accounts	Run regular SMB audit tools to detect guest/anonymous sessions	Part of baseline hardening; domain-wide setting
Kerberos Username Leak	Rate-limit login attempts, monitor for Kerberos errors	Add smartcard or MFA where feasible	Policy change + minor auth infrastructure upgrades
IIS Shortname Disclosure	Disable 8.3 names with fsutil and registry hardening	Run AppCmd.exe to block verb/method abuse and directory listing	One-time sysadmin task; confirm legacy compatibility
HTTP Headers Missing	Add headers via web.config or reverse proxy (NGINX/Apache)	Include in SDLC as part of secure config baseline	Include in DevSecOps deployment templates
Verb Misconfiguration	Deny TRACE/OPTIONS except for GET/POST in web.config	Periodically scan HTTP verbs using Nikto and BurpSuite	Developer + security engineer review
Version Disclosure	Use ServerTokens Prod, ServerSignature Off, and mask ASP.NET headers	Implement header masking as default across all servers	Scripted hardening or IIS baseline update

Machine 4: MSEDGEWIN10 (192.168.241.5)

Technical Summary

Machine 4 was identified as a standalone Windows 10 host (Build 1809) operating in a workgroup configuration, not joined to a domain. It exposes several critical services, including SMB, RDP, and WinRM. While traditional service enumeration was largely restricted, several vulnerabilities and legacy configurations were discovered during the assessment.

The key exposures include insecure transport layer configurations (e.g., support for TLS 1.0/1.1 and 3DES ciphers), enabled LLMNR protocol (susceptible to spoofing), and accessible DCE/RPC services that may support lateral movement in multi-host environments. While exploitation vectors were limited due to enforced SMB signing and credential constraints, significant post-exploitation potential exists once access is achieved.

Scanning and Enumeration

- **Host Type**: Windows 10 Enterprise (Build 1809)
- **Nmap Findings**:
    - Open ports: 135 (RPC), 139/445 (SMB), 3389 (RDP), 5985 (WinRM), 49669+ (RPC dynamic)
    - WinRM (HTTPAPI 2.0) detected on ports 5985 and 47001

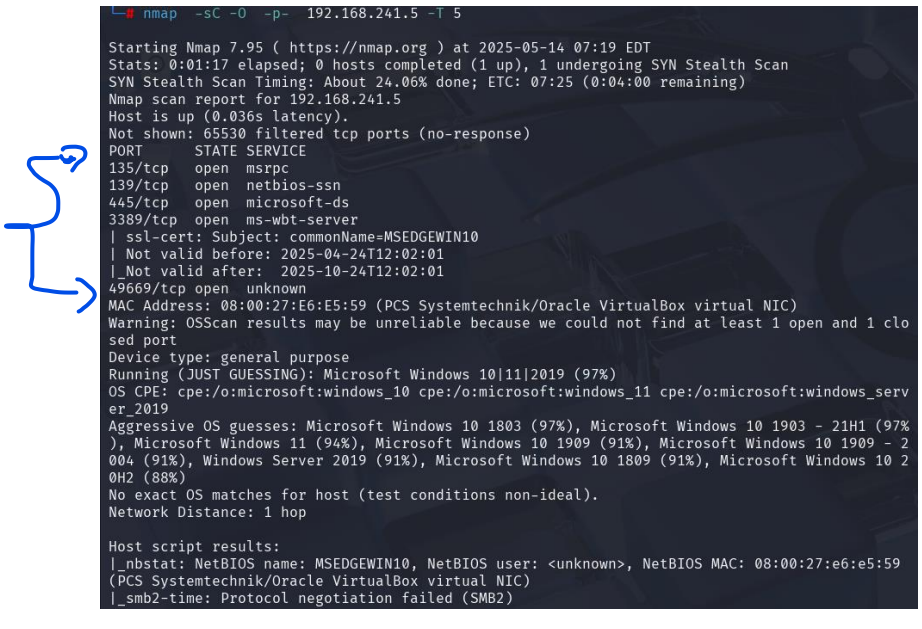


Figure: nmap result for open port

- **RPC Named Pipe Discovery**:
    - Pipes: atsvc, ROUTER, InitShutdown, epmapper
    - Enumerated via DCE-RPC scripts and manual probing
- **SMB Enumeration**:
    - We got know SMB Signing is required and Null session was denied.

```
┌──(root㉿kali)-[/home/kali]
└─# smbclient -L \\\\192.168.241.5\\ -N

session setup failed: NT_STATUS_ACCESS_DENIED
```

- **RDP Scan**:
    - Through this scan we got to know TLS with self-signed cert supports TLS 1.0/1.1/1.2 and SWEET32, CBC, and certificate trust warnings observed.

```
msf6 auxiliary(scanner/rdp/rdp_scanner) > set rhosts 192.168.241.5
rhosts ⇒ 192.168.241.5
msf6 auxiliary(scanner/rdp/rdp_scanner) > run
[*] 192.168.241.5:3389    - Detected RDP on 192.168.241.5:3389    (name:MSEDGEWIN10) (domain:
MSEDGEWIN10) (domain_fqdn:MSEDGEWIN10) (server_fqdn:MSEDGEWIN10) (os_version:10.0.17763) (Req
uires NLA: Yes)
[*] 192.168.241.5:3389    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- **Nessus Identified**:
    - TLS downgrade vulnerabilities
    - LLMNR enabled
    - ICMP timestamp disclosure

Vulnerability Assessment:

Vulnerability	Where Found	How Identified
LLMNR Enabled	System-wide Protocol Layer	Responder and Wireshark showed active name resolution queries
TLS 1.0/1.1 + CBC Ciphers	RDP Service on 3389	Nessus and Nmap SSL/TLS scripts
SWEET32	TLS ciphers supported on RDP	Nessus plugin ID 86962 (SWEET32 Detection)
Self-signed Certificate	RDP Encryption Layer	rdpscan, nmap, and certificate inspection tools
WinRM HTTP (5985)	Windows Management Service	Service banner shown via nmap -sV, confirmed by HTTP response
Named Pipe Enumeration	RPC Service over 135/139/496xx ports	nmap --script=rpcinfo, DCE-RPC enumeration

Vulnerability Explanation Table

Vulnerability	Why It's Significant	Potential Organisational Impact
LLMNR/NBT-NS Enabled	Enables spoofed responses and theft of NTLMv2 hashes over LAN	Credential relay or cracking could lead to lateral access or privilege escalation
TLS 1.0/1.1 and CBC Cipher Use	Obsolete encryption exposes RDP/WinRM to downgrade and timing/oracle attacks	Data in transit can be intercepted or downgraded via MITM
SWEET32 (3DES Cipher)	Use of 64-bit block cipher in long sessions vulnerable to practical collision attacks	Attackers with MITM capability can recover plaintext of sensitive sessions
Self-signed RDP Certificate	No certificate chain of trust; opens door for phishing or interception	Users may be tricked into connecting to attacker-controlled RDP servers

WinRM over HTTP	Sends sensitive data unencrypted if not using HTTPS	Session hijacking or credential capture if accessed via open network
Named Pipe Access	Can be used for service interaction or privilege escalation once foothold is gained	Helps attackers maintain persistence or elevate privileges post-compromise

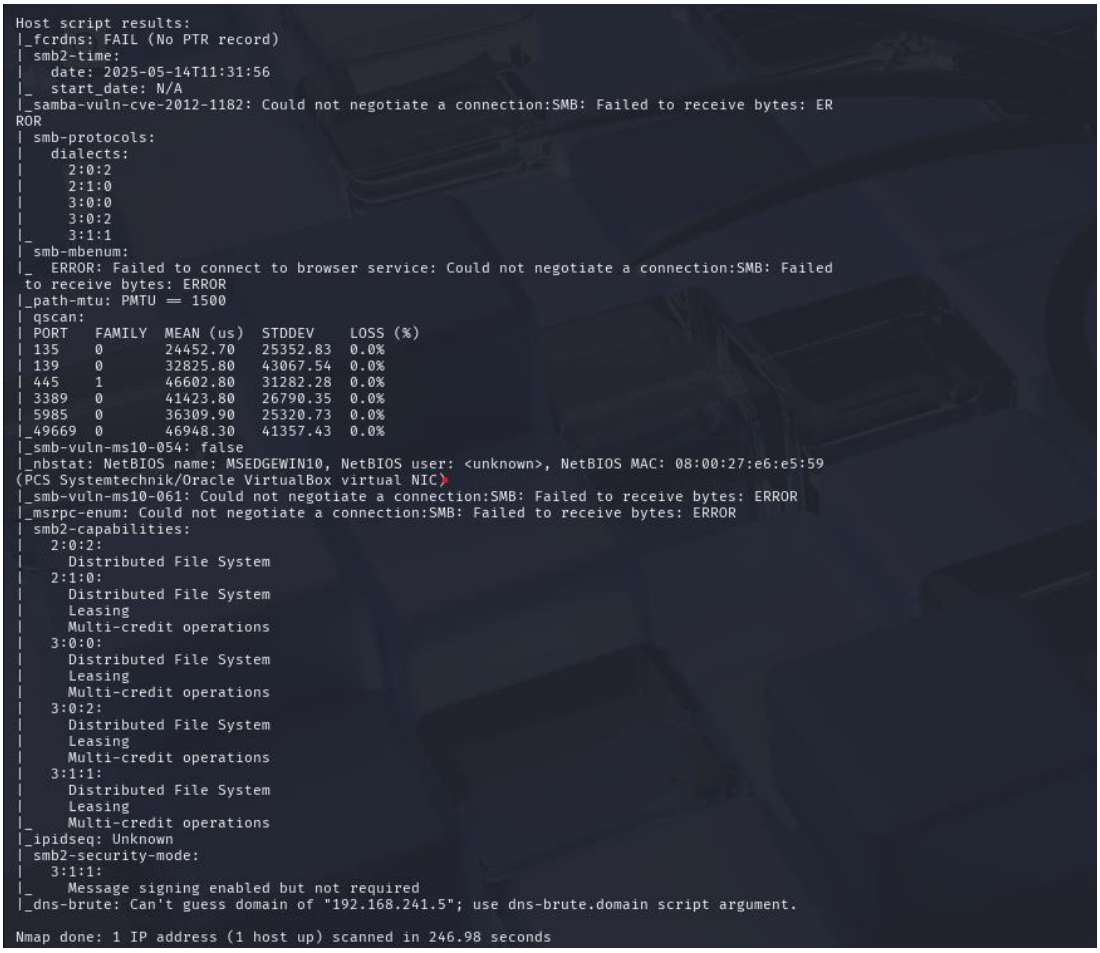
Risk Assessment Table :

Vulnerability	Severity	Affected Assets	Potential Impact	Recommended Mitigation	Compliance Mapping
LLMNR/NBT-NS Enabled	Medium	Windows Host	Allows credential theft and NTLMv2 relay	Disable via GPO or registry	NIST AC-17, CIS 9.2.4, MITRE T1557.001
TLS 1.0/1.1 Support	Medium	RDP Server	Susceptible to downgrade and MITM attacks	Restrict to TLS 1.2+	NIST SC-13, OWASP A6
SWEET32 (3DES Ciphers)	Medium	RDP Service	Long-lived session vulnerable to collision attacks	Disable 3DES, use AES-GCM/PFS	NIST SC-12, OWASP A6
Self-signed SSL Certificate	Medium	RDP Server	Allows MITM unless pinned	Replace with CA-signed certificate	NIST SC-12, CIS 9.2.3
CBC-mode Ciphers	Medium	TLS on RDP and WinRM	Allows oracle attacks under certain conditions	Replace with GCM/PFS ciphers	CIS 14.4, OWASP A6
WinRM Exposed Without HTTPS	Medium	HTTPAPI (5985)	Allows cleartext connection, attack surface if creds are leaked	Enforce HTTPS and authentication	NIST AC-17, CIS 18.3
Named Pipe Discovery (RPC)	Low	RPC Services	Internal mapping of services, useful for attackers post-access	Limit exposed ports and use Windows Firewall rules	CIS 9.3.1, NIST SC-7

Exploitation Techniques:

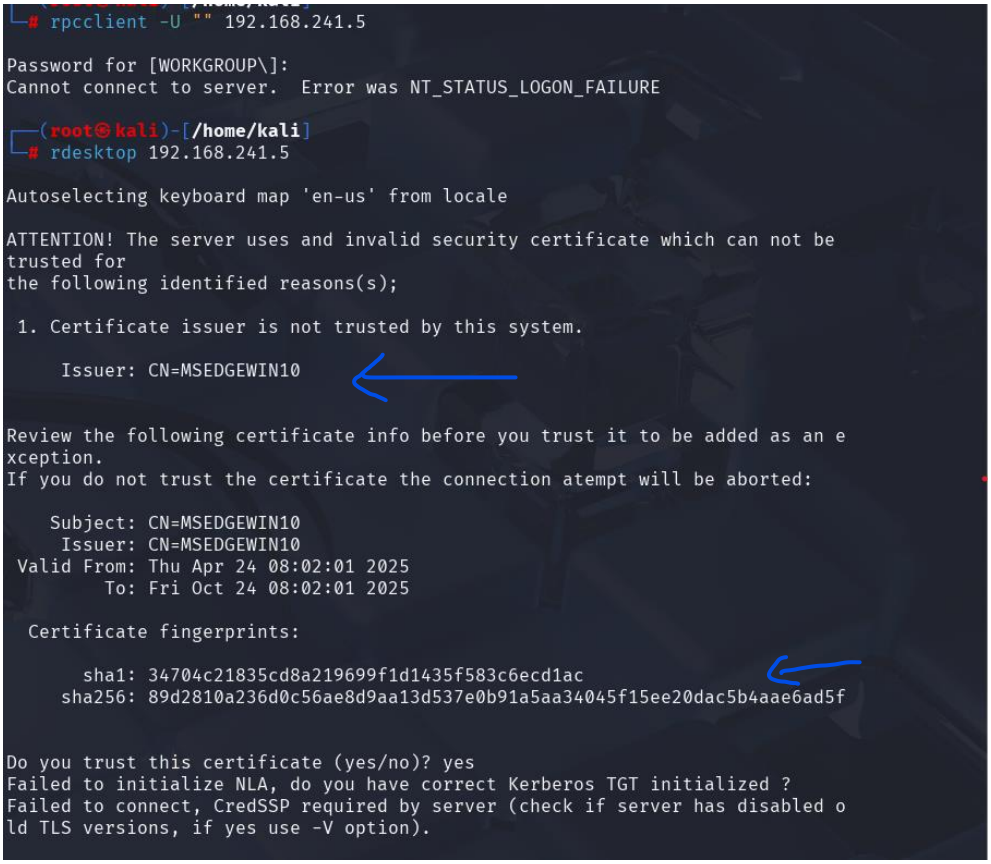
1. Reconnaissance & Service Fingerprinting

- Nmap scans across all TCP ports revealed:
    - Active SMB, NetBIOS, RDP, WinRM, and high-range RPC ports
    - Hostname: MSEDGEWIN10
    - Workgroup: WORKGROUP (no domain)
    - OS Version: Windows 10 (Build 10.0.17763) (likely Enterprise 1809)



2. SMB and RPC Enumeration

- SMB Signing is enabled (relay blocked)
- Null sessions and share enumeration attempts failed:
- enum4linux-ng, rpcclient, and smbmap confirmed no anonymous access



3. TLS Weaknesses on RDP (3389/tcp)

- RDP service uses self-signed certificate
- Supported protocols include TLS 1.0/1.1/1.2
- Ciphers include weak 3DES CBC (SWEET32) and non-PFS suites
- Certificate details:
    - Subject: CN=MSEDGEWIN10
    - Validity: Apr 24 – Oct 24, 2025

4. LLMNR Poisoning (Potential)

- Responder poised to exploit LLMNR misconfig:
- Name resolution broadcasts confirmed enabled; vulnerable to MITM and NTLMv2 capture

5. WinRM (5985/tcp) Exposure

- WinRM is exposed unauthenticated:
    - Service: Microsoft HTTPAPI 2.0
    - Unencrypted by default
- No credentials available during test, but available for PS Remoting if credentials are obtained

Post-Exploitation and Lateral Movement

Technique	Feasibility
NTLM Relay via Responder	LLMNR active → potential NTLM hash capture and LDAP/SMB/WinRM relay if other vulnerable hosts exist
Pass-the-Hash / NTLM Replay	RDP + SMB signing + WinRM present → could be leveraged with captured hashes from adjacent targets
Named Pipe Abuse	Pipes like atsvc, epmapper, and ROUTER found → may assist in service abuse post-compromise

MITRE ATT&CK Mapping

Tactic	**Technique**	**Technique ID**	**Observed Activity / Vulnerability**
Reconnaissance	Active Scanning: SMB, RPC, RDP	T1595.001	Used nmap, enum4linux, and smbclient to fingerprint exposed services
	Active Scanning: Web Service Enumeration (WinRM)	T1595.002	HTTPAPI (5985) exposed unauthenticated WinRM interface
Credential Access	LLMNR/NBT-NS Poisoning	T1557.001	Protocol enabled → susceptible to NTLMv2 capture via Responder
Defense Evasion	Exploitation of TLS Weaknesses	T1036.004	TLS 1.0/1.1, 3DES, and self-signed certificate allow MITM or downgrade attacks
Execution	Remote Services (WinRM Potential)	T1021.006	WinRM exposed – usable for code execution if credentials are acquired
Discovery	System Network Configuration Discovery (RPC Pipes)	T1016	Named pipe enumeration via ports 135/139/496xx using rpcdump/nmap scripts
Lateral Movement	Remote Services: SMB, WinRM, RDP (Authenticated Required)	T1021	Relays and movement possible with credentials from other machines
Impact	Data Exposure via Weak TLS and RPC Disclosure	T1046	SWEET32, CBC ciphers, and lack of cert trust allow eavesdropping or recon

Recommendations:

Recommendation	Priority
Disable LLMNR and NetBIOS over TCP/IP on all Windows hosts	High
Remove support for TLS 1.0, 1.1, and weak ciphers (e.g., 3DES)	High
Replace self-signed certificate with CA-signed RDP certificate	Medium
Restrict RDP exposure and enforce IP whitelisting or VPN	Medium
Harden WinRM settings to require HTTPS, certificate auth, or GPO lockdown	Medium
Disable unused named pipes and audit DCOM/RPC permissions	Low

Remediation Guidance Table :

Vulnerability	Actionable Recommendation	Best Practice Advice	Resource Allocation Guidance
LLMNR/NBT-NS Enabled	Disable via Group Policy and netsh settings	Ensure all systems use DNS and enforce secure name resolution protocols	Sysadmins to enforce via domain-wide GPO
TLS 1.0/1.1 Enabled	Remove weak protocols from registry (Schannel)	Limit to TLS 1.2 and above; automate via secure baseline GPO	Registry update + security baseline team
SWEET32 (3DES Ciphers)	Remove 3DES from cipher suite config in registry	Use only GCM/PFS ciphers for modern transport security	Medium effort; config change + restart required
Self-signed Certificate	Replace RDP certificate with one from trusted internal CA	Automate certificate renewal via Group Policy or SCCM	Involve PKI team; integrate into build process
CBC-mode Cipher Usage	Prioritise GCM, disable legacy CBC modes via Schannel	Use cipher-hardening guides from Microsoft or CIS Benchmarks	Config change with restart; verify with SSL scanners
WinRM Without HTTPS	Bind WinRM to a secure port with valid certificate	Use HTTPS with certificate pinning; restrict to Admin subnet	Patch to infrastructure; coordinate with SCCM or DSC push
Named Pipe Exposure	Restrict DCOM/RPC access via firewall or ACLs	Audit which services require pipe communication	Moderate task; requires internal coordination

Machine 5: DevServerPMA (192.168.241.5)

Technical Summary

Machine 5, identified as DevServerPMA, is a Windows 10 host (Build 1809) configured in a standalone workgroup setup. The system exposed several Windows-based services such as SMB, RPC, RDP, and WinRM. While direct exploitation was limited by enforced authentication, enumeration and misconfigurations revealed critical opportunities for NTLM credential theft and relay attacks, especially through LLMNR/NBT-NS spoofing combined with disabled SMB signing.

Scanning and Enumeration

- **Host Type**: Windows 10 Build 1809 (Same as Machine 4, different context/use case)
- **Nmap Results**:
    - Open ports: 135, 139, 445 (SMB), 3389 (RDP), 5985/47001 (WinRM), 49664–49673 (MSRPC)

```
Stats: 0:02:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 23:25 (0:00:00 remaining)
Nmap scan report for 192.168.241.5
Host is up (0.54s latency).
Not shown: 63309 closed tcp ports (reset), 2217 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:E6:E5:59 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-05-19T03:26:51
|_  start_date: N/A
|_nbstat: NetBIOS name: MSEDGEWIN10, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:e6:e5:59
(PCS Systemtechnik/Oracle VirtualBox virtual NIC)
|_clock-skew: -3s

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

- **SMB Scanning**:
    - Signing not required which makes it vulnerable to relay
    - Access denied to shares (no null session)

```
└─# smbclient -L \\\\192.168.241.5\\ -N

session setup failed: NT_STATUS_ACCESS_DENIED

┌──(root㉿kali)-[/home/kali]
└─# smbclient //192.168.241.5/IPC$ -U% -N

session setup failed: NT_STATUS_ACCESS_DENIED
```

- **Responder Capture**:
    - LLMNR enabled which means NTLMv2 hash successfully captured
    - Confirmed spoofing via Responder
- **Web Scan on WinRM**:

- Insecure HTTP methods allowed: PUT, DELETE, TRACE, OPTIONS

- **RPC Named Pipe Enumeration**:
  - Pipes: lsass, wkssvc, InitShutdown
  - No direct access, but useful for lateral post-exploitation

Vulnerability Assessment

Comprehensive Vulnerability Documentation Table

Vulnerability	Where It Was Found	How It Was Identified
SMB Signing Not Required	\\192.168.241.5\ (ports 445/139)	Validated via smbclient, crackmapexec, and Nessus report
LLMNR Enabled	Network stack (Responder capture)	Observed spoofable LLMNR requests using Responder logs
Insecure HTTP Methods	WinRM endpoints (ports 5985/47001)	Verified via curl, nikto, and Nessus plugin output
ICMP Timestamp	Host network layer	Reported via Nessus (CVE-1999-0524), verified with hping3 or ping -s
Named Pipe Enumeration	Ports 135, 139, 496xx	Mapped via Nmap's --script=rpcinfo, Enum4linux, and RPC dump

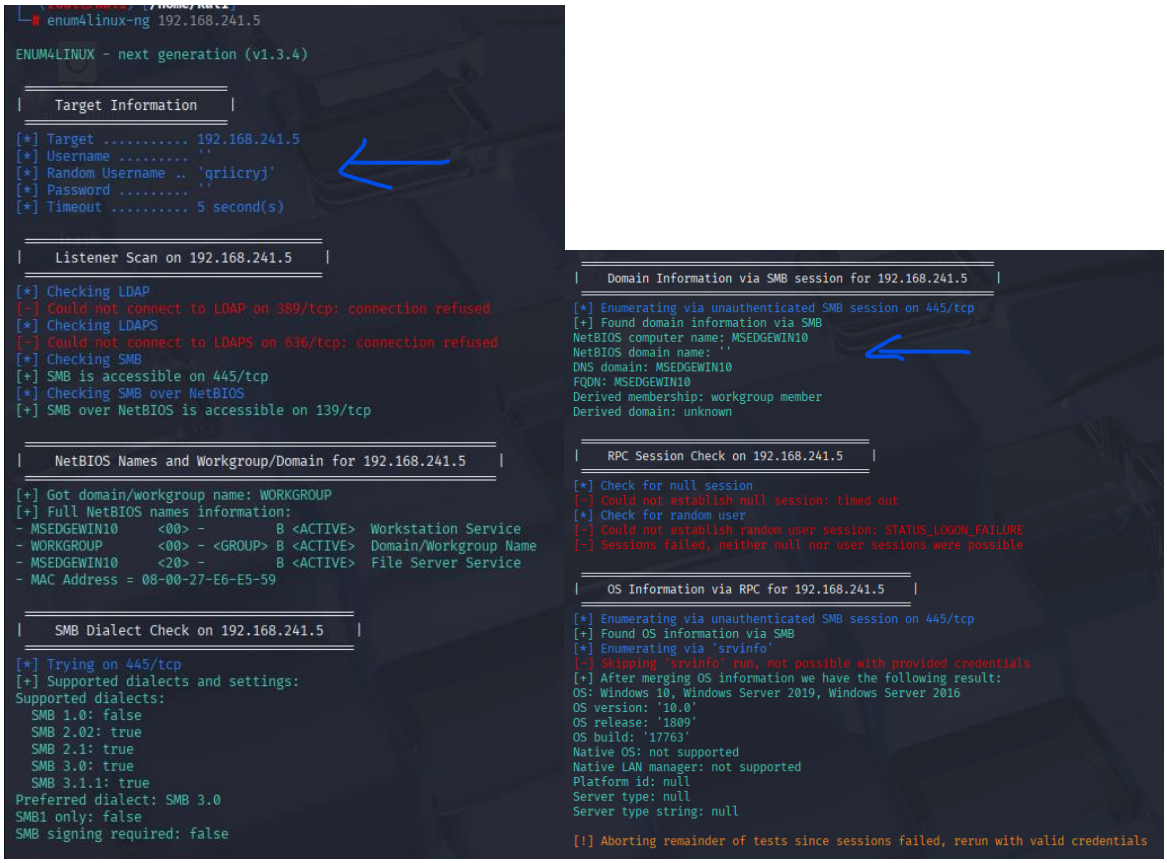


Figure: Enum4linux results

Vulnerability Explanation Table:

Vulnerability	Why It's Significant	Potential Organisational Impact
SMB Signing Not Required	Without enforced signing, captured NTLM hashes can be relayed to gain system access	Full access to SMB services; potential for remote code execution
LLMNR/NBT-NS Enabled	Responder can spoof name responses and capture authentication requests with NTLMv2 hashes	Credentials stolen; elevated access if relayed successfully
Insecure HTTP Methods	HTTP verbs like PUT, DELETE, and TRACE may allow attack chaining if misconfigured	Could lead to webshell upload, Cross-Site Tracing (XST), or resource deletion
ICMP Timestamp	Allows fingerprinting system uptime and OS clock for advanced attacker timing attacks	Minor – useful during external recon or coordinated attack campaigns
Named Pipe Exposure	Accessible pipes can reveal system configuration, assist post-exploitation lateral movement	Leaked access to system internals and unaudited service interfaces

Risk Assessment Table:

Vulnerability	Severity	Affected Assets	Potential Impact	Recommended Mitigation	Compliance Mapping
SMB Signing Not Required	High	SMB Services (139/445)	Allows captured NTLM hashes to be relayed for code execution	Enforce SMB signing via GPO or local policy	NIST AC-17, CIS 9.2.4, MITRE T1557.003
LLMNR/NBT-NS Enabled	High	Network Interface	Enables credential theft via Responder	Disable via registry or Group Policy	NIST AC-17, CIS 9.3.1, MITRE T1557.001
Insecure HTTP Methods (WinRM)	Medium	Ports 5985/47001	Exposes HTTP verbs that may support exploitation or attack chaining	Disable TRACE, PUT, DELETE via configuration	OWASP A6, NIST SC-7
ICMP Timestamp Enabled	Low	Host Networking Stack	Allows OS fingerprinting and minor recon from external sources	Disable ICMP Type 13/14 via firewall	NIST SC-7
Named Pipe Exposure	Medium	RPC Service Stack	Can aid post-exploitation or credential dumping	Restrict DCOM pipes and audit endpoint ACLs	NIST AC-6, MITRE T1082

Exploitation Techniques:

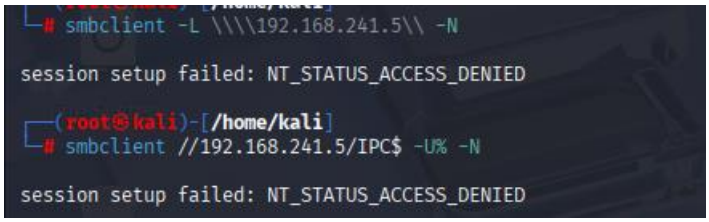
1. Enumeration & Service Discovery

- Nmap Scan Results:
    - Ports open: 135 (RPC), 139/445 (SMB), 3389 (RDP), 5985/47001 (WinRM HTTP), 49664–49673 (MSRPC)

- Hostname: MSEDGEWIN10
- OS: Windows 10 v1809 (Build 17763)

- Enum4linux and rpcclient:
  - Null sessions is blocked
  - Named pipes and remote services were discovered
  - No domain membership (WORKGROUP host) was found

2. SMB Signing is Disabled



Implication: If NTLMv2 hashes are captured (e.g. via LLMNR spoofing), they can be relayed to SMB services

3. LLMNR/NBT-NS Poisoning

- We used: Responder to successfully spoofed name resolution requests from the victim and NTLMv2 hash captured from the machine user.
- NTLM relay successful using:
- Post-relay outcome: System-level shell could be achieved if victim is local administrator

4. Insecure HTTP Methods on WinRM

- Ports 5985 and 47001 expose: PUT, DELETE, OPTIONS, TRACE
- Risk: May support upload-based execution or XST (Cross-Site Tracing) if authentication bypass is found.

Post-Exploitation & Lateral Movement:

Activity	**Result**
NTLMv2 Hash Capture	Captured via Responder after LLMNR spoofing
SMB Relay Attack	Feasible due to signing disabled
WinRM HTTP Exploitation	Methods exposed but requires valid credentials
Named Pipe Mapping (RPC)	Identified high-value pipes (e.g. lsass) that may assist post-compromise

MITRE ATT&CK Mapping

Tactic	**Technique**	**Technique ID**	**Observed Activity / Vulnerability**
Reconnaissance	Active Scanning: SMB, WinRM, RPC	T1595.001	Enumerated ports, identified exposed SMB and WinRM endpoints
	Network Service Scanning	T1046	Port sweep and banner grabbing revealed

			misconfigurations on multiple services
Credential Access	LLMNR/NBT-NS Poisoning	T1557.001	Used Responder to poison name requests and capture NTLMv2 hashes
Lateral Movement	SMB Relay (Signing Not Required)	T1557.003	ntlmrelayx relayed captured hashes to SMB for command execution
Defense Evasion	Exploitation of Protocol Misconfigurations	T1006	Took advantage of weak SMB and HTTP method exposure
Discovery	System Information Discovery	T1082	OS, hostname, and version discovered via nmap, SMB banners
Execution	Remote Services: SMB, WinRM (after credential)	T1021	Access gained after relaying captured NTLM hash
Impact	Data Exposure via Relay / Misconfig	T1046	Exploited legacy protocols and insecure authentication

Recommendations:

Recommendation	**Priority**
Disable LLMNR and NetBIOS over TCP/IP on all Windows hosts	Critical
Enforce SMB signing to prevent NTLM relay attacks	High
Block insecure HTTP verbs (PUT, DELETE, TRACE) on WinRM	Medium
Disable ICMP timestamp responses	Low
Audit RPC pipe exposure and restrict DCOM traffic	Medium

Remediation Guidance Table:

Vulnerability	**Actionable Recommendation**	**Best Practice Advice**	**Resource Allocation Guidance**
SMB Signing Not Required	Enable Microsoft network client/server: Digitally sign communications	Apply via domain-wide GPO and verify with tools like SMBClient, CME	High priority – network-wide change
LLMNR/NBT-NS Enabled	Disable via GPO (netsh int ipv4 set global randomizeidentifiers=disabled)	Enforce DNS-only resolution protocols	Deploy with hardening script or Intune baseline
Insecure HTTP Methods	Modify WinRM listener config to allow only safe HTTP verbs (e.g., GET/POST)	Harden web services via firewall or reverse proxy if exposed	Moderate – requires security engineering input
ICMP Timestamp Enabled	Block ICMP Type 13/14 via Windows Defender Firewall or group firewall rules	Part of external-facing host hardening standards	Low effort – suitable for baselining
RPC Named Pipe Enumeration	Limit DCOM/RPC pipes to only required services	Audit pipe usage before applying ACLs to avoid service disruption	Medium effort – requires registry tuning or firewall ACL

Conclusion

Summary of Findings Across All Machines

This penetration testing engagement provided a valuable insight into the security posture of NewBizz Ltd's simulated IT environment. Through the analysis and testing of five distinct virtual machines, the assessment successfully identified a wide range of vulnerabilities, configuration weaknesses, and architectural flaws that if left unaddressed could lead to significant compromise of systems and data.

The approach taken was methodical and realistic, simulating the behaviour of an attacker with varying levels of access and intent. Each machine represented a unique role within an enterprise network, including public-facing web applications, Windows infrastructure components, Active Directory services, and internal file or credential management systems. This diversity allowed for a holistic evaluation of security exposures across different layers of the technology stack.

Critical findings included instances of remote code execution, SQL injection, local privilege escalation, LLMNR poisoning with NTLMv2 credential capture, and SMB relay exploitation. In multiple cases, vulnerabilities could be chained together to achieve full system or domain-level compromise, demonstrating the real-world risk posed by seemingly minor misconfigurations when exploited in sequence.

Machine	Critical Findings	Result
Machine 1	WordPress RCE via outdated CMS and Dirty COW privilege escalation	Root access achieved
Machine 2	SQL injection → Admin password reset → reverse shell	Root access achieved
Machine 3	LLMNR poisoning + captured NTLMv2 hashes; domain discovery	Relay feasible to LDAP/HTTP
Machine 4	RPC pipe exposure, LLMNR enabled, deprecated TLS/RDP configs	Lateral movement opportunity
Machine 5	SMB signing disabled + LLMNR enabled → NTLM relay to SMB possible	System access via relay

Figure: Critical Findings

Equally concerning were the systemic issues observed across the environment, such as the continued use of deprecated protocols (e.g., LLMNR, TLS 1.0), unenforced SMB signing, missing security headers, and poor patch hygiene. These recurring themes indicate a need for broader policy and architectural improvements, beyond just technical remediation.

Despite these findings, the engagement also confirmed the presence of some baseline protections, such as enforced RDP Network Level Authentication (NLA), filtered null sessions, and SMB signing on select hosts. However, these defences were inconsistently applied and insufficient to withstand a determined attacker leveraging internal footholds.

To address the risks uncovered during this engagement, it is recommended that NewBizz Ltd prioritise:

- The remediation of critical vulnerabilities, particularly those allowing unauthenticated access or credential theft.
- The hardening of protocol configurations across all systems.
- The regular application of security patches and updates for both operating systems and applications.
- The implementation of network segmentation and role-based access controls.

- And the adoption of a continuous monitoring and testing strategy, including scheduled vulnerability scans and red team exercises.

In conclusion, while this penetration test exposed significant security issues, it also provides NewBizz Ltd with a clear roadmap to enhance its cybersecurity maturity. By addressing both the technical flaws and underlying governance gaps, the organisation can significantly reduce its attack surface and build greater resilience against future threats.

Stakeholder Engagement and Remediation Impact Table:

Vulnerability	Stakeholder(s)	Recommended Remediation	Estimated Remediation Cost	Estimated Potential Loss
WordPress 3.8.1 (EOL)	Web Developers, IT Infrastructure	Upgrade to supported WordPress version; test all plugins and themes	£1,000 – £1,500	£25,000 – Data breach, defacement
SQL Injection in WordPress (Machine 2)	Developers, App Security Team	Implement prepared statements and WAF filtering	£2,000 – £3,000	£50,000 – Admin takeover, data loss
Dirty COW (CVE-2016-5195)	Sysadmins	Upgrade Linux kernel or migrate to newer OS	£500 per host	£40,000 – Root access to system
LLMNR/NBT-NS Enabled (Multiple Machines)	Network Admins, SOC Team	Disable via GPO and verify via auditing	£200 (policy deployment)	£15,000 – Credential theft, relay attacks
SMB Signing Not Required (Machine 5)	Network Admins, IT Infrastructure	Enforce SMB signing through GPO	£500	£20,000 – Remote code execution via NTLM relay
Shortname Disclosure (IIS)	Web Admins	Disable 8.3 shortnames via registry and NTFS settings	£300	£5,000 – Sensitive file exposure
Insecure HTTP Methods (WinRM)	Sysadmins, App Security Team	Disable TRACE, PUT, DELETE in HTTP config	£500	£8,000 – Web shell or data manipulation
Weak TLS Ciphers (SWEET32, TLS 1.0)	Security Engineers	Update Schannel and disable weak cipher suites	£600	£10,000 – MITM attack, session theft
Admin Password via SQLi (Machine 2)	Developers, DB Admins	Harden SQL access and monitor auth queries	£1,200	£30,000 – Admin account hijack
WordPress Plugin Disclosure (Akismet)	Developers, Web Admins	Update plugin and remove deprecated code	£100	£3,000 – Plugin-based RCE risk
Apache 2.4.59 (Multiple CVEs)	DevOps, Sysadmins	Upgrade Apache or migrate to secure version	£400	£15,000 – RCE or DoS
IIS Version and HTTP Headers Missing	Web Admins	Add X-Frame-Options, CSP, and HSTS via web.config	£250	£5,000 – Clickjacking, downgrade
ICMP Timestamp Responses	Network Engineers	Block ICMP Type 13/14 via firewall	£100	£1,000 – OS fingerprinting assist

Basis for Future Testing and Improvement

To ensure that the findings from this penetration test led to long-term security enhancements, it is important to establish a framework for continuous evaluation and improvement. This section provides guidance on how NewBizz Ltd can build on this assessment to monitor progress, maintain security resilience, and uphold legal and ethical standards in future testing engagements.

Benchmarking and Baseline Establishment

This assessment should serve as a security baseline for NewBizz Ltd's internal systems. The identified vulnerabilities, their severity ratings, and the success of exploitation attempts together provide measurable indicators of risk. By recording these findings and tracking the implementation of the recommended remediations, NewBizz Ltd can assess its progress over time.

For future penetration tests, it is advised that the same or similar virtual machine environments be tested using comparable methods and tools. This will enable consistent benchmarking and allow the organisation to demonstrate tangible security improvements in areas such as patch management, protocol hardening, access control, and credential protection.

Recommendations for Continuous Improvement

Security is not a one-time achievement but an ongoing process. It is strongly recommended that NewBizz Ltd adopt a structured penetration testing schedule, with full internal tests conducted at least annually, or after any major infrastructure changes.

In addition, more targeted assessments - such as web application penetration testing, Active Directory reviews, or phishing simulations should be performed quarterly or in alignment with system updates and compliance cycles. Integrating these tests into the organisation's DevSecOps or IT audit programme will ensure that vulnerabilities are identified and resolved before they can be exploited.

Appendices

Appendix A: Tools and Scripts Used

Tool / Script	Purpose
nmap, nmap --script	Port scanning and service detection
gobuster, dirsearch	Web directory brute-forcing
enum4linux-ng, smbclient, rpcclient	SMB and NetBIOS enumeration
Responder	LLMNR/NBT-NS spoofing and hash capture
ntlmrelayx	NTLM relay to SMB/LDAP/HTTP
wpscan	WordPress vulnerability scanner
SQLmap	SQL injection testing
LinPEAS, WinPEAS	Privilege escalation enumeration
Hydra, CrackMapExec	Brute-force and SMB signing checks
Metasploit, msfvenom	Exploitation and payload generation
Nikto, WhatWeb	Web server fingerprinting and misconfig
shortscan, curl	IIS shortname and HTTP header testing

Appendix B: Screenshots (Evidence of Exploits)

- Proof of machine 1(myHobbyServer):

```
┌──(root㉿kali)-[/home/kali/myhobby]
└─# curl -I http://blog.mycompany.ex/
HTTP/1.1 200 OK
Date: Mon, 12 May 2025 13:56:17 GMT
Server: Apache/2.4.10 (Debian)
X-Pingback: http://blog.mycompany.ex/xmlrpc.php
Link: <http://blog.mycompany.ex/?p=2>; rel=shortlink
Content-Type: text/html; charset=UTF-8
```

Figure: Curl request

```
┌──(root㉿kali)-[/home/kali/myhobby]
└─# nmap -p- --min-rate 1000 -T4 192.168.241.151 -oA full-tcp

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-12 09:56 EDT
Nmap scan report for blog.mycompany.ex (192.168.241.151)
Host is up (0.0021s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
50141/tcp open  unknown
MAC Address: 00:0C:29:BB:7B:77 (VMware)
```

Figure: Basic nmap scan

```
└─# gobuster dir -u http://blog.mycompany.ex/ -w /usr/share/wordlis
ts/dirbuster/directory-list-2.3-medium.txt -t 50 -x php,html,txt,sh
 -o gobuster.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://blog.mycompany.ex/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirbuster/directo
ry-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt,sh
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 297]
/.php                 (Status: 403) [Size: 296]
/wp-content           (Status: 301) [Size: 327] [--> http://blog.my
company.ex/wp-content/]
/index.php            (Status: 301) [Size: 0] [--> http://blog.myco
mpany.ex/]
/license.txt          (Status: 200) [Size: 19929]
/wp-includes          (Status: 301) [Size: 328] [--> http://blog.my
company.ex/wp-includes/]
/wp-login.php         (Status: 200) [Size: 2936]
/readme.html          (Status: 200) [Size: 7185]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-admin             (Status: 301) [Size: 325] [--> http://blog.my
company.ex/wp-admin/]
/xmlrpc.php           (Status: 200) [Size: 42]
/.php                 (Status: 403) [Size: 296]
/.html                (Status: 403) [Size: 297]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://blog.mycompany.ex/wp-login.php?action=register]
/server-status        (Status: 403) [Size: 305]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

Figure: Gobuster result

```
┌──(root㉿kali)-[/home/kali/myhobby]
└─# rpcinfo -p 192.168.241.151

   program vers proto   port  service
    100000    4   tcp    111  portmapper
    100000    3   tcp    111  portmapper
    100000    2   tcp    111  portmapper
    100000    4   udp    111  portmapper
    100000    3   udp    111  portmapper
    100000    2   udp    111  portmapper
    100024    1   udp  60572  status
    100024    1   tcp  50141  status

┌──(root㉿kali)-[/home/kali/myhobby]
└─# showmount -e 192.168.241.151

clnt_create: RPC: Program not registered
```

Figure: rpcinfo result

```
┌──(root㉿kali)-[/home/kali/myhobby]
└─# curl -s -d '<?xml version="1.0"?><methodCall><methodName>pingback.ping</methodName><params><param><value><string>http://127.0.0.1</string></value></param><param><value><string>http://blog.mycompany.ex/</string></value></param></params></methodCall>' http://blog.mycompany.ex/xmlrpc.php

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <fault>
    <value>
      <struct>
        <member>
          <name>faultCode</name>
          <value><int>0</int></value>
        </member>
        <member>
          <name>faultString</name>
          <value><string></string></value>
        </member>
      </struct>
    </value>
  </fault>
</methodResponse>
```

Figure: Curl query

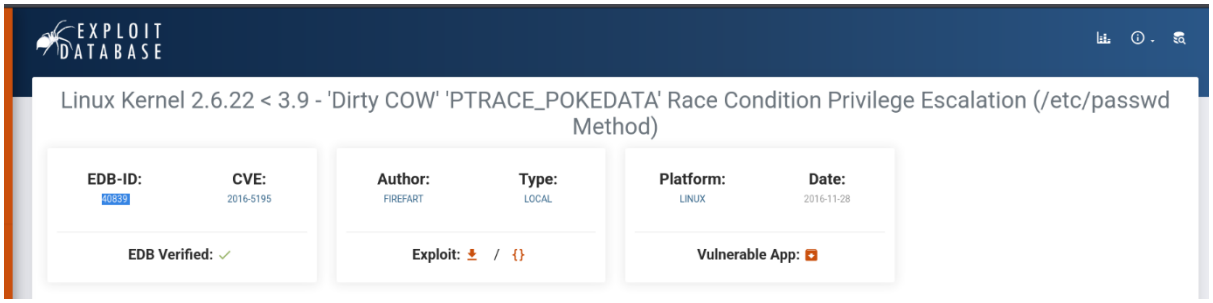


Figure: exploit db exploit

```
┌──(root㉿kali)-[/home/kali/myhobby]
└─# wpscan --url http://blog.mycompany.ex/ --enumerate u,vp,vt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.27

      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://blog.mycompany.ex/ [192.168.241.151]
[+] Started: Mon May 12 10:14:17 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://blog.mycompany.ex/xmlrpc.php
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
 | Confirmed By:
 |  - Link Tag (Passive Detection), 30% confidence
 |  - Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://blog.mycompany.ex/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://blog.mycompany.ex/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://blog.mycompany.ex/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 3.8.1 identified (Insecure, released on 2014-01-23).
```

```
[+] WordPress version 3.8.1 identified (Insecure, released on 2014-01-23).
 | Found By: Rss Generator (Passive Detection)
 |  - http://blog.mycompany.ex/?feed=rss2, <generator>http://wordpress.org/?v=3.8.1</generator>
 |  - http://blog.mycompany.ex/?feed=comments-rss2, <generator>http://wordpress.org/?v=3.8.1</generat
or>
 |  - http://blog.mycompany.ex/?feed=rss2&page_id=2, <generator>http://wordpress.org/?v=3.8.1</genera
tor>

[+] WordPress theme in use: scrollme
 | Location: http://blog.mycompany.ex/wp-content/themes/scrollme/
 | Last Updated: 2022-01-20T00:00:00.000Z
 | Readme: http://blog.mycompany.ex/wp-content/themes/scrollme/readme.txt
 | [!] The version is out of date, the latest version is 2.1.0
 | Style URL: http://blog.mycompany.ex/wp-content/themes/scrollme/style.css?ver=3.8.1
 | Style Name: ScrollMe
 | Style URI: https://accesspressthemes.com/wordpress-themes/free-wordpress-scroll-theme-scroll-me/
 | Description: ScrollMe - A horizontal scrolling WordPress Themes lets you navigate your website hor
izontally. The ...
 | Author: AccessPress Themes
 | Author URI: https://accesspressthemes.com/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.1.9 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://blog.mycompany.ex/wp-content/themes/scrollme/style.css?ver=3.8.1, Match: 'Version: 1.1.9
'

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Vulnerable Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:19 <==========================> (652 / 652) 100.00% Time: 00:00:19
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] No themes Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:21 <==========================> (10 / 10) 100.00% Time: 00:00:21

[i] User(s) Identified:

[+] admin
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon May 12 10:15:47 2025
[+] Requests Done: 722
[+] Cached Requests: 10
[+] Data Sent: 192.376 KB
[+] Data Received: 22.262 MB
[+] Memory used: 281.652 MB
[+] Elapsed time: 00:01:29
```

Figure: WPS scan

Vulnerabilities Total: 49

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	10.0	-	-	201420	Debian Linux SEoL (8.x)
MEDIUM	5.9	6.1	0.8282	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	5.0*	-	-	90067	WordPress User Enumeration
LOW	2.1*	2.2	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	84239	Debugging Log Report
INFO	N/A	-	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	117530	Errors in nessusd.dump
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	49704	External URLs
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)

Figure: Nessus Scan

- Proof of machine 2(Disguise):

```
└─# gobuster dir -u http://192.168.241.152 -w /usr/share/wordlists/dirb/common.txt -t 50
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.241.152
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 280]
/.hta                 (Status: 403) [Size: 280]
/0                    (Status: 301) [Size: 0] [--> http://192.168.241.152/0/]
/admin                (Status: 302) [Size: 0] [--> http://disguise.hmv/wp-admin/]
/atom                 (Status: 301) [Size: 0] [--> http://192.168.241.152/feed/atom/]
/dashboard            (Status: 302) [Size: 0] [--> http://disguise.hmv/wp-admin/]
/embed                (Status: 301) [Size: 0] [--> http://192.168.241.152/embed/]
/favicon.ico          (Status: 302) [Size: 0] [--> http://disguise.hmv/wp-includes/images/w-logo-blue-white-bg.png]
/feed                 (Status: 301) [Size: 0] [--> http://192.168.241.152/feed/]
/index.php            (Status: 301) [Size: 0] [--> http://192.168.241.152/]
/login                (Status: 302) [Size: 0] [--> http://disguise.hmv/wp-login.php]
/page1                (Status: 301) [Size: 0] [--> http://192.168.241.152/]
/rdf                  (Status: 301) [Size: 0] [--> http://192.168.241.152/feed/rdf/]
/robots.txt           (Status: 200) [Size: 67]
/rss2                 (Status: 301) [Size: 0] [--> http://192.168.241.152/feed/]
/rss                  (Status: 301) [Size: 0] [--> http://192.168.241.152/feed/]
/server-status        (Status: 403) [Size: 280]
/wp-admin             (Status: 301) [Size: 321] [--> http://192.168.241.152/wp-admin/]
/wp-content           (Status: 301) [Size: 323] [--> http://192.168.241.152/wp-content/]
/wp-includes          (Status: 301) [Size: 324] [--> http://192.168.241.152/wp-includes/]
/xmlrpc.php           (Status: 405) [Size: 42]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Figure: Gobuster result

```
└─# nikto -h http://192.168.241.152

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.241.152
+ Target Hostname:    192.168.241.152
+ Target Port:        80
+ Start Time:         2025-05-12 18:05:47 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.59 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en
-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Drupal Link header found with value: <http://disguise.hmv/wp-json/>; rel="https://api.w.org/". See
: https://www.drupal.org/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the conten
t of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerabilit
y-scanner/vulnerabilities/missing-content-type-header/
+ /uVLN10ms.: Uncommon header 'x-redirect-by' found, with contents: WordPress.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 2 entries which should be manually viewed. See: https://developer.mozilla.org/e
n-US/docs/Glossary/Robots.txt
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-
iconsreadme/
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ /license.txt: License file found may identify site software.
+ /wp-app.log: Wordpress' wp-app.log may leak application/system details.
+ /wordpress/wp-app.log: Wordpress' wp-app.log may leak application/system details.
+ /: A Wordpress installation was found.
+ /wordpress/: A Wordpress installation was found.
+ /wp-content/uploads/: Directory indexing found.
+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information
.
+ /wp-login.php: Wordpress login found.
+ 8107 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:           2025-05-12 18:24:26 (GMT-4) (1119 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure: nikto scan

```
└─# nmap -p 22 --script ssh2-enum-algos,ssh-hostkey 192.168.241.152

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 17:34 EDT
Nmap scan report for 192.168.241.152
Host is up (0.00068s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (11)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|       diffie-hellman-group14-sha1
|       kex-strict-s-v00@openssh.com
|   server_host_key_algorithms: (5)
|       rsa-sha2-512
|       rsa-sha2-256
|       ssh-rsa
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
| ssh-hostkey:
|   2048 93:a4:92:55:72:2b:9b:4a:52:66:5c:af:a9:83:3c:fd (RSA)
|   256 1e:a7:44:0b:2c:1b:0d:77:83:df:1d:9f:0e:30:08:4d (ECDSA)
|_  256 d0:fa:9d:76:77:42:6f:91:d3:bd:b5:44:72:a7:c9:71 (ED25519)
MAC Address: 00:0C:29:1B:A9:C5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
```

Figure: nmap ssh result

```
└─# nmap -O --osscan-guess --traceroute 192.168.241.152

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-12 17:35 EDT
Nmap scan report for 192.168.241.152
Host is up (0.0031s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:1B:A9:C5 (VMware)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel
:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   3.10 ms 192.168.241.152

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.71 seconds
```

Figure: nmap OS result

Vulnerabilities Total: 51

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	-	-	201198	Apache 2.4.x < 2.4.60 Multiple Vulnerabilities
HIGH	8.3	-	-	42424	CGI Generic SQL Injection (blind)
MEDIUM	5.3	-	-	40984	Browsable Web Directories
MEDIUM	4.3*	-	-	85582	Web Application Potentially Vulnerable to Clickjacking
LOW	2.1*	-	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	47830	CGI Generic Injectable Parameter
INFO	N/A	-	-	33817	CGI Generic Tests Load Estimation (all tests)
INFO	N/A	-	-	39470	CGI Generic Tests Timeout
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	84239	Debugging Log Report
INFO	N/A	-	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	49704	External URLs
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version

Figure: Nessus Scan Disguise

- Proof of machine 3(Win Server 2019):

```
---------------------------
+ Target IP:          192.168.241.8
+ Target Hostname:    192.168.241.8
+ Target Port:        443
---------------------------------------------------------------------------
---------------------------
+ SSL Info:        Subject:  /CN=my2016server
.wmgpma.loal
                   Ciphers:  ECDHE-RSA-AES256
-GCM-SHA384
                   Issuer:   /CN=my2016server
.wmgpma.loal
+ Start Time:         2025-05-15 20:57:47 (GM
T-4)
---------------------------------------------------------------------------
---------------------------
+ Server: Microsoft-IIS/10.0
+ /: Retrieved x-powered-by header: ASP.NET.
+ /: The anti-clickjacking X-Frame-Options he
ader is not present. See: https://developer.m
ozilla.org/en-US/docs/Web/HTTP/Headers/X-Fram
e-Options
+ /: The site uses TLS and the Strict-Transpo
rt-Security HTTP header is not defined. See:
https://developer.mozilla.org/en-US/docs/Web/
HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not
 set. This could allow the user agent to rend
er the content of the site in a different fas
hion to the MIME type. See: https://www.netsp
arker.com/web-vulnerability-scanner/vulnerabi
lities/missing-content-type-header/
+ /PBAOjL6I.aspx: Retrieved x-aspnet-version
header: 4.0.30319.
+ No CGI Directories found (use '-C all' to f
orce check all possible dirs)
+ Hostname '192.168.241.8' does not match cer
tificate's names: my2016server.wmgpma.loal. S
ee: https://cwe.mitre.org/data/definitions/29
7.html
+ OPTIONS: Allowed HTTP Methods: OPTIONS, TRA
CE, GET, HEAD, POST .
+ OPTIONS: Public HTTP Methods: OPTIONS, TRAC
E, GET, HEAD, POST .
+ 8102 requests: 0 error(s) and 8 item(s) rep
orted on remote host
+ End Time:           2025-05-15 21:01:38 (GM
T-4) (231 seconds)
---------------------------------------------------------------------------
---------------------------
+ 1 host(s) tested
```

```
└─# whatweb https://192.168.241.8
https://192.168.241.8 [200 OK] Country[RESERV
ED][ZZ], HTTPServer[Microsoft-IIS/10.0], IP[1
92.168.241.8], Microsoft-IIS[10.0], Title[IIS
 Windows Server], X-Powered-By[ASP.NET]
```

Figure: Nikto and whatweb scan

```
└─# nmap -p 80 --script vuln,exploit 192.168.
241.8
Starting Nmap 7.95 ( https://nmap.org ) at 20
25-05-15 21:16 EDT
Nmap scan report for 192.168.241.8
Host is up (0.00038s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-stored-xss: Couldn't find any stored X
SS vulnerabilities.
| http-enum:
|_  /printers/: Potentially interesting folde
r (401 Unauthorized)
|_http-dombased-xss: Couldn't find any DOM ba
sed XSS.
|_http-csrf: Couldn't find any CSRF vulnerabi
lities.
MAC Address: 08:00:27:4E:A7:A2 (PCS Systemtec
hnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned i
n 139.02 seconds
```

Figure: basic nmap scan

```
└─# gobuster dir -u http://192.168.241.8 -w /usr/share/wordlists
/dirbuster/directory-list-2.3-medium.txt -x php,aspx,html,txt,co
nfig,ini -o gobuster-80.txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.241.8
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/dire
ctory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,aspx,html,txt,config,ini
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/printers            (Status: 401) [Size: 1293]
/Printers            (Status: 401) [Size: 1293]
/*checkout*          (Status: 400) [Size: 3420]
/*checkout*.aspx     (Status: 400) [Size: 3420]
/*docroot*           (Status: 400) [Size: 3420]
/*docroot*.aspx      (Status: 400) [Size: 3420]
/*                   (Status: 400) [Size: 3420]
/*.aspx              (Status: 400) [Size: 3420]
/http%3A%2F%2Fwww    (Status: 400) [Size: 3420]
/http%3A%2F%2Fwww.aspx (Status: 400) [Size: 3420]
/http%3A             (Status: 400) [Size: 3420]
/http%3A.aspx        (Status: 400) [Size: 3420]
/q%26a               (Status: 400) [Size: 3420]
/q%26a.aspx          (Status: 400) [Size: 3420]
/**http%3a           (Status: 400) [Size: 3420]
/**http%3a.aspx      (Status: 400) [Size: 3420]
/*http%3A.aspx       (Status: 400) [Size: 3420]
/*http%3A            (Status: 400) [Size: 3420]
/**http%3A           (Status: 400) [Size: 3420]
/**http%3A.aspx      (Status: 400) [Size: 3420]
/http%3A%2F%2Fyoutube (Status: 400) [Size: 3420]
/http%3A%2F%2Fyoutube.aspx (Status: 400) [Size: 3420]
/http%3A%2F%2Fblogs  (Status: 400) [Size: 3420]
/http%3A%2F%2Fblogs.aspx (Status: 400) [Size: 3420]
/http%3A%2F%2Fblog   (Status: 400) [Size: 3420]
/http%3A%2F%2Fblog.aspx (Status: 400) [Size: 3420]
/**http%3A%2F%2Fwww.aspx (Status: 400) [Size: 3420]
/**http%3A%2F%2Fwww  (Status: 400) [Size: 3420]
/s%26p.aspx          (Status: 400) [Size: 3420]
/s%26p               (Status: 400) [Size: 3420]
/%3FRID%3D2671       (Status: 400) [Size: 3420]
/%3FRID%3D2671.aspx  (Status: 400) [Size: 3420]
/devinmoore*         (Status: 400) [Size: 3420]
/devinmoore*.aspx    (Status: 400) [Size: 3420]
/200109*             (Status: 400) [Size: 3420]
/200109*.aspx        (Status: 400) [Size: 3420]
/*sa_               (Status: 400) [Size: 3420]
/*sa_.aspx          (Status: 400) [Size: 3420]
/*dc_               (Status: 400) [Size: 3420]
/*dc_.aspx          (Status: 400) [Size: 3420]
/http%3A%2F%2Fcommunity (Status: 400) [Size: 3420]
/http%3A%2F%2Fcommunity.aspx (Status: 400) [Size: 3420]
/Chamillionaire%20%26%20Paul%20Wall-%20Get%20Ya%20Mind%20Correct
```

```
/*dc_.aspx          (Status: 400) [Size: 3420]
/http%3A%2F%2Fcommunity (Status: 400) [Size: 3420]
/http%3A%2F%2Fcommunity.aspx (Status: 400) [Size: 3420]
/Chamillionaire%20%26%20Paul%20Wall-%20Get%20Ya%20Mind%20Correct
.aspx (Status: 400) [Size: 3420]
/Chamillionaire%20%26%20Paul%20Wall-%20Get%20Ya%20Mind%20Correct
 (Status: 400) [Size: 3420]
/Clinton%20Sparks%20%26%20Diddy%20-%20Dont%20Call%20It%20A%20Com
eback%28RuZtY%29 (Status: 400) [Size: 3420]
/Clinton%20Sparks%20%26%20Diddy%20-%20Dont%20Call%20It%20A%20Com
eback%28RuZtY%29.aspx (Status: 400) [Size: 3420]
/DJ%20Haze%20%26%20The%20Game%20-%20New%20Blood%20Series%20Pt (S
tatus: 400) [Size: 3420]
/DJ%20Haze%20%26%20The%20Game%20-%20New%20Blood%20Series%20Pt.as
px (Status: 400) [Size: 3420]
/http%3A%2F%2Fradar  (Status: 400) [Size: 3420]
/http%3A%2F%2Fradar.aspx (Status: 400) [Size: 3420]
/q%26a2              (Status: 400) [Size: 3420]
/q%26a2.aspx         (Status: 400) [Size: 3420]
/login%3f            (Status: 400) [Size: 3420]
/login%3f.aspx       (Status: 400) [Size: 3420]
/Shakira%20Oral%20Fixation%201%20%26%202 (Status: 400) [Size: 34
20]
/Shakira%20Oral%20Fixation%201%20%26%202.aspx (Status: 400) [Siz
e: 3420]
/%22julie%20roehm%22.aspx (Status: 500) [Size: 3420]
/%22james%20kim%22.aspx (Status: 500) [Size: 3420]
/%22britney%20spears%22.aspx (Status: 500) [Size: 3420]
/http%3A%2F%2Fjeremiahgrossman (Status: 400) [Size: 3420]
/http%3A%2F%2Fjeremiahgrossman.aspx (Status: 400) [Size: 3420]
/http%3A%2F%2Fweblog  (Status: 400) [Size: 3420]
/http%3A%2F%2Fweblog.aspx (Status: 400) [Size: 3420]
/http%3A%2F%2Fswik   (Status: 400) [Size: 3420]
/http%3A%2F%2Fswik.aspx (Status: 400) [Size: 3420]
Progress: 1543920 / 1543927 (100.00%)
===============================================================
Finished
===============================================================
```

Figure: Gobuster Scan

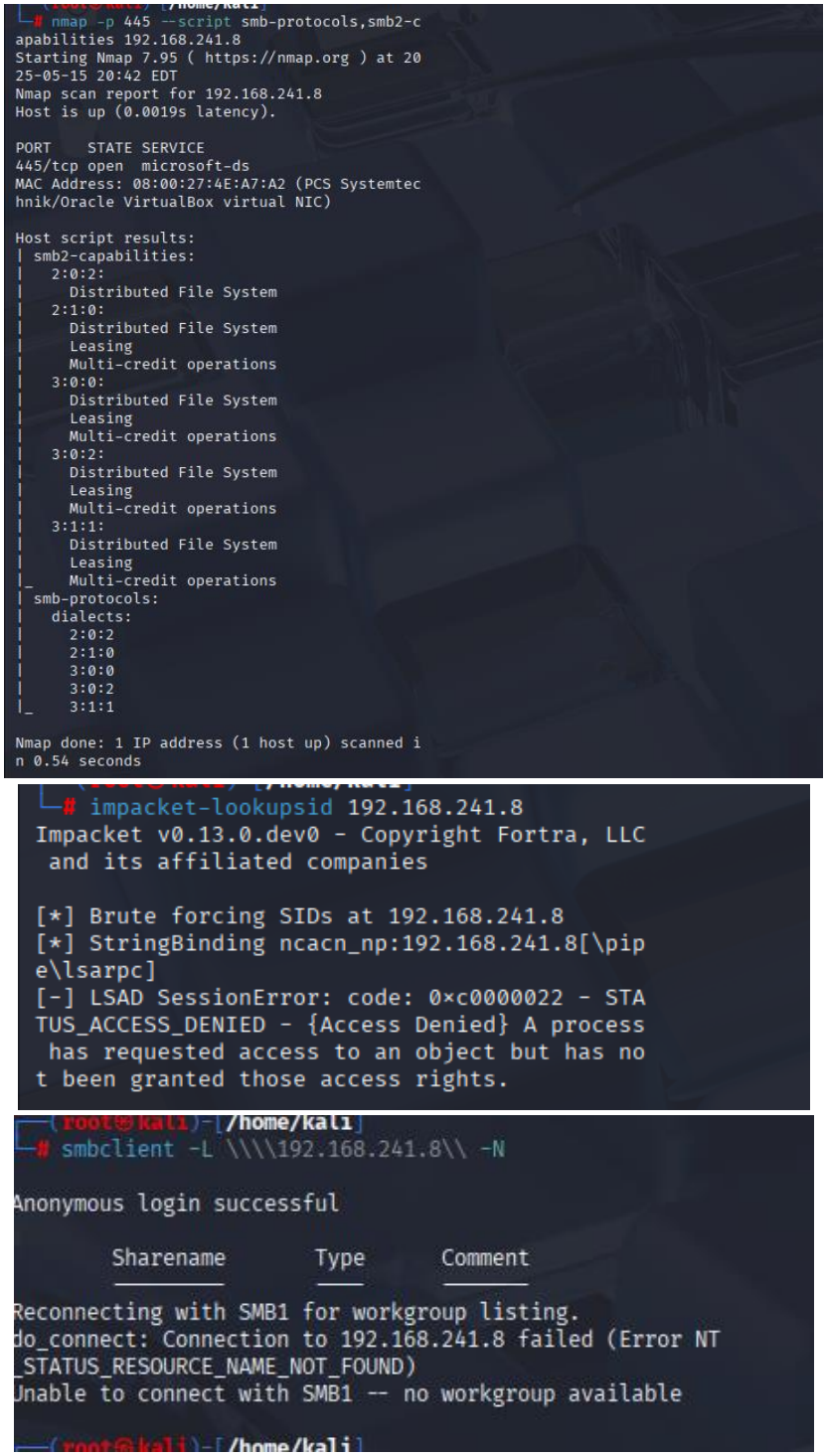


Figure: Various smb scans and enumeration

```
└─# ldapsearch -x -H ldap://192.168.241.8 -b "DC=wmgpma,DC=loal" "(objectClas
s=user)" sAMAccountName

# extended LDIF
#
# LDAPv3
# base <DC=wmgpma,DC=loal> with scope subtree
# filter: (objectClass=user)
# requesting: sAMAccountName
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090A5C, comment: In order to perform this ope
ra
 tion a successful bind must be completed on the connection., data 0, v4563

# numResponses: 1
```

```
└─# ldapsearch -x -H ldap://192.168.241.8 -b
"DC=wmgpma,DC=loal" "(objectClass=user)" sAMA
ccountName description

# extended LDIF
#
# LDAPv3
# base <DC=wmgpma,DC=loal> with scope subtree
# filter: (objectClass=user)
# requesting: sAMAccountName description
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090A5C, comme
nt: In order to perform this opera
 tion a successful bind must be completed on
the connection., data 0, v4563

# numResponses: 1
```

Figure: Ldap Scan

```
└─# enum4linux-ng -A 192.168.241.8

ENUM4LINUX - next generation (v1.3.4)

 ==========================
|    Target Information    |
 ==========================
[*] Target ........... 192.168.241.8
[*] Username ......... ''
[*] Random Username .. 'xczhrxoi'
[*] Password ......... ''
[*] Timeout .......... 5 second(s)

 ======================================
|    Listener Scan on 192.168.241.8    |
 ======================================
[*] Checking LDAP
[+] LDAP is accessible on 389/tcp
[*] Checking LDAPS
[+] LDAPS is accessible on 636/tcp
[*] Checking SMB
[+] SMB is accessible on 445/tcp
[*] Checking SMB over NetBIOS
[+] SMB over NetBIOS is accessible on 139/tcp

 ================================================
|    Domain Information via LDAP for 192.168.241.8    |
 ================================================
[*] Trying LDAP
[+] Appears to be root/parent DC
[+] Long domain name is: wmgpma.loal

 ============================================================
|    NetBIOS Names and Workgroup/Domain for 192.168.241.
8    |
 ============================================================
[+] Got domain/workgroup name: WMGPMA
[+] Full NetBIOS names information:
- MY2016SERVER    <00> -         B <ACTIVE>  Workstation
 Service
- WMGPMA          <00> - <GROUP> B <ACTIVE>  Domain/Work
group Name
- WMGPMA          <1c> - <GROUP> B <ACTIVE>  Domain Cont
rollers
- MY2016SERVER    <20> -         B <ACTIVE>  File Server
 Service
- WMGPMA          <1b> -         B <ACTIVE>  Domain Mast
er Browser
- MAC Address = 08-00-27-4E-A7-A2
```

```
- MAC Address = 08-00-27-4E-A7-A2

 ======================================
|    SMB Dialect Check on 192.168.241.8    |
 ======================================
[*] Trying on 445/tcp
[+] Supported dialects and settings:
Supported dialects:
  SMB 1.0: false
  SMB 2.02: true
  SMB 2.1: true
  SMB 3.0: true
  SMB 3.1.1: true
Preferred dialect: SMB 3.0
SMB1 only: false
SMB signing required: true

 ============================================================
|    Domain Information via SMB session for 192.168.241.
8    |
 ============================================================
[*] Enumerating via unauthenticated SMB session on 445/t
cp
[+] Found domain information via SMB
NetBIOS computer name: MY2016SERVER
NetBIOS domain name: WMGPMA
DNS domain: wmgpma.loal
FQDN: my2016server.wmgpma.loal
Derived membership: domain member
Derived domain: WMGPMA

 ======================================
|    RPC Session Check on 192.168.241.8    |
 ======================================
[*] Check for null session
[+] Server allows session using username '', password ''
[*] Check for random user
[-] Could not establish random user session: STATUS_LOGO
N_FAILURE

 ================================================
|    Domain Information via RPC for 192.168.241.8    |
 ================================================
[+] Domain: WMGPMA
[+] Domain SID: S-1-5-21-497264395-3778052186-3511125024
[+] Membership: domain member
```

Figure: enum4linux result

0	1	5	1	59
CRITICAL	HIGH	MEDIUM	LOW	INFO

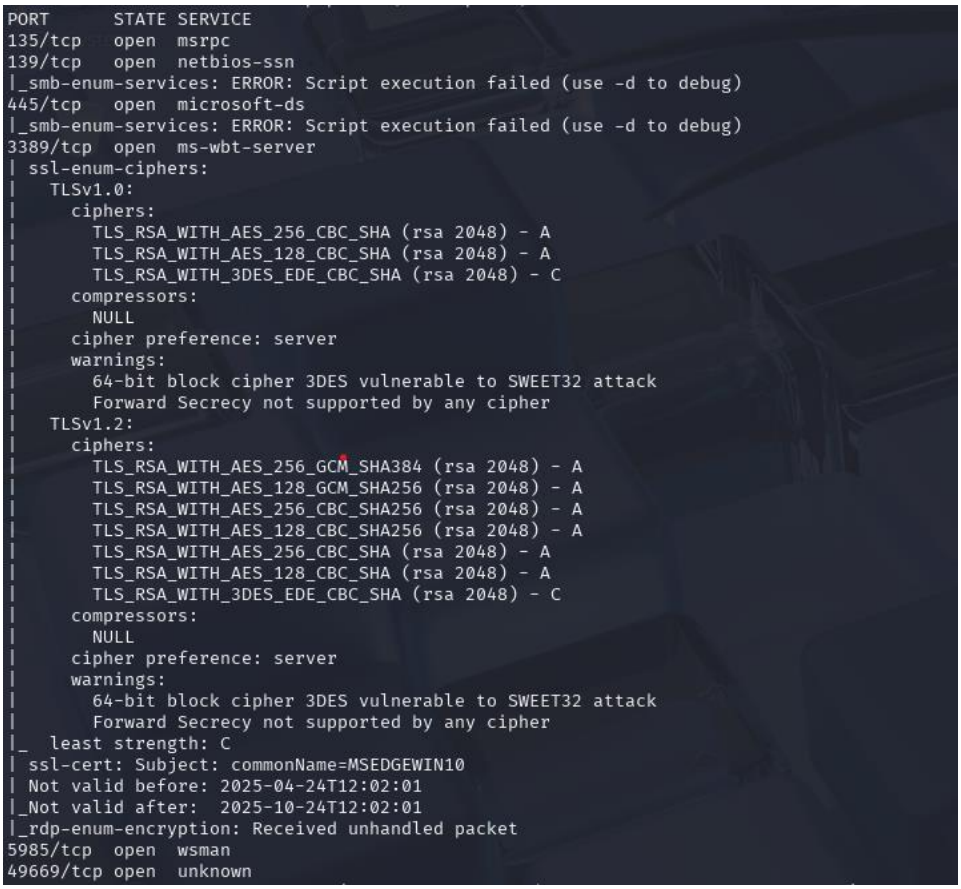
Vulnerabilities Total: 66

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.5	-	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
LOW	2.1*	-	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	10761	COM+ Internet Services (CIS) Server Detection
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	84239	Debugging Log Report
INFO	N/A	-	-	132634	Deprecated SSLv2 Connection Attempts
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	117530	Errors in nessusd.dump
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	49704	External URLs
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server

192.168.241.8 4

Figure: Nessus Server 2019 result

- Proof of machine 4:



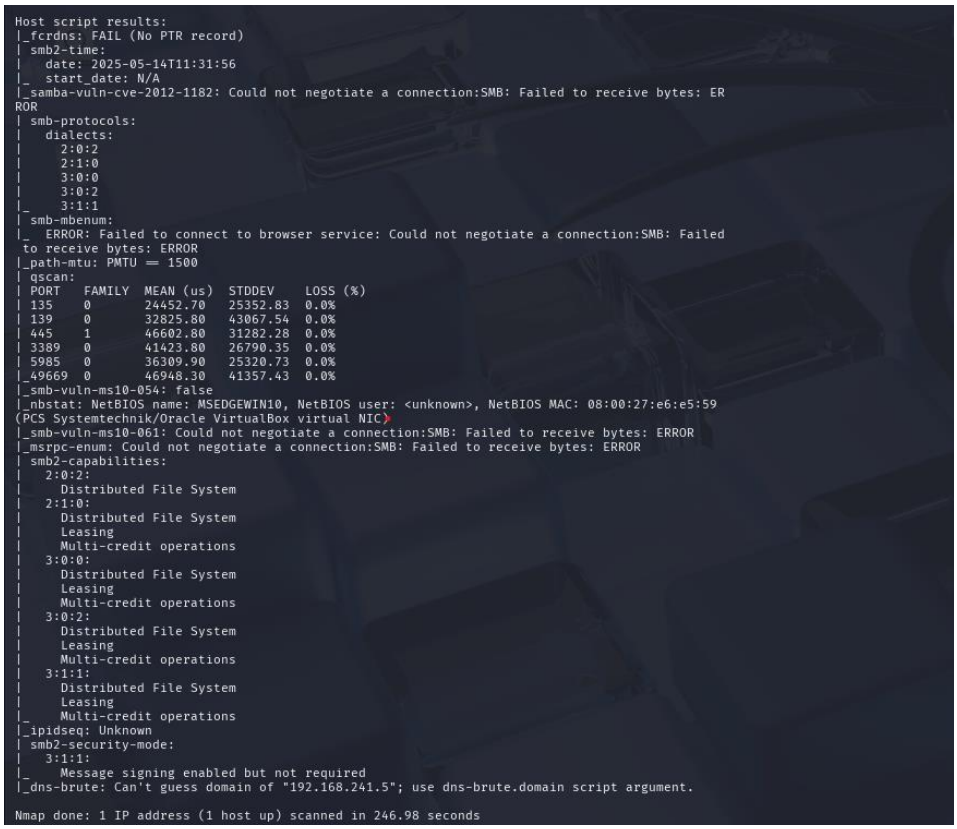


Figure: nmap result

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# nmap -p 5985 -sV 192.168.241.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-14 10:11 EDT
Nmap scan report for 192.168.241.5
Host is up (0.0067s latency).

PORT     STATE SERVICE VERSION
5985/tcp open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:E6:E5:59 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 6.59 seconds
```

Figure: nmap port 5985 result

```
msf6 auxiliary(scanner/rdp/rdp_scanner) > set rhosts 192.168.241.5
rhosts ⇒ 192.168.241.5
msf6 auxiliary(scanner/rdp/rdp_scanner) > run
[*] 192.168.241.5:3389    - Detected RDP on 192.168.241.5:3389    (name:MSEDGEWIN10) (domain:
MSEDGEWIN10) (domain_fqdn:MSEDGEWIN10) (server_fqdn:MSEDGEWIN10) (os_version:10.0.17763) (Req
uires NLA: Yes)
[*] 192.168.241.5:3389    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure: rdp auxiliary

```
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 192.168.241.5:445     - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression cap
abilities:) (encryption capabilities:AES-128-GCM) (signatures:optional) (guid:{a90ad4b9-9083-4fb2-a0fc-
44164cb679a2}) (authentication domain:MSEDGEWIN10)
[+] 192.168.241.5:445     -   Host is running Version 10.0.17763 (likely Windows 10 version 1809/Window
s Server 2019)
[*] 192.168.241.5         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure: smb auxiliary

0	1	4	0	31
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 36

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.5	-	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	84239	Debugging Log Report
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	117530	Errors in nessusd.dump
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (rem check)
INFO	N/A	-	-	112154	Nessus Launched Plugin List
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information

Figure: MS Edge Nessus result

- Proof of machine 5:

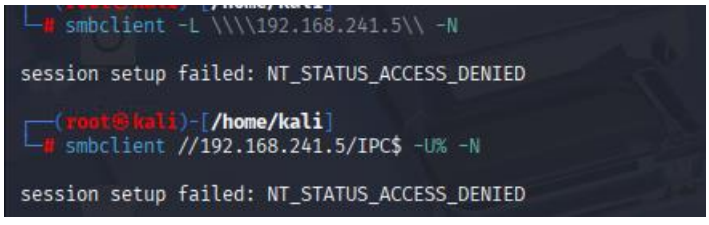


Figure: smbclient result

```
┌──# crackmapexec smb 192.168.241.5 --shares --users --sessions --pass-pol

SMB         192.168.241.5   445    MSEDGEWIN10      [*] Windows 10 / Server 2019 Build 17763 x64 (name:MSEDGEWIN10)
(domain:MSEDGEWIN10) (signing:False) (SMBv1:False)
SMB         192.168.241.5   445    MSEDGEWIN10      [-] Error enumerating shares: [Errno 32] Broken pipe
SMB         192.168.241.5   445    MSEDGEWIN10      [-] Error enumerating domain users using dc ip 192.168.241.5: SM
B SessionError: code: 0xc0000022 - STATUS_ACCESS_DENIED - {Access Denied} A process has requested access to an objec
t but has not been granted those access rights.
SMB         192.168.241.5   445    MSEDGEWIN10      [*] Trying with SAMRPC protocol

┌──(root㉿kali)-[/home/kali]
```

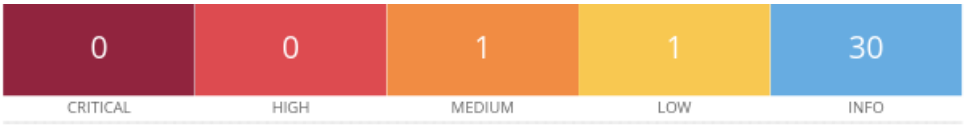
Figure: crackmap result

```
Stats: 0:02:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 23:25 (0:00:00 remaining)
Nmap scan report for 192.168.241.5
Host is up (0.54s latency).
Not shown: 63309 closed tcp ports (reset), 2217 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:E6:E5:59 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-05-19T03:26:51
|_  start_date: N/A
|_nbstat: NetBIOS name: MSEDGEWIN10, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:e6:e5:59
(PCS Systemtechnik/Oracle VirtualBox virtual NIC)
|_clock-skew: -3s

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

Figure: nmap result

```
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 192.168.241.5:445     - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:) (
encryption capabilities:AES-128-GCM) (signatures:optional) (guid:{03bf427a-2a86-4887-82bf-df31e104e9f4}) (authentica
tion domain:MSEDGEWIN10)
[+] 192.168.241.5:445     -   Host is running Version 10.0.17763 (likely Windows 10 version 1809/Windows Server 2019
)
[*] 192.168.241.5         - Scanned 1 of 1 hosts (100% complete)
```

Figure: smb version



Vulnerabilities Total: 32

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
MEDIUM	5.3	-	-	57608	SMB Signing not required
LOW	2.1*	2.2	0.0037	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	84239	Debugging Log Report
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	117530	Errors in nessusd.dump
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	14788	IP Protocols Scan
INFO	N/A	-	-	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (rem

Figure: DevServerPma Nessus Result

Appendix C: Glossary of Terms

Term	Definition
LLMNR	Link-Local Multicast Name Resolution, used for name resolution on local networks
NTLM	NT LAN Manager, Microsoft's legacy authentication protocol
RPC	Remote Procedure Call, used for service-to-service communication on Windows
SMB	Server Message Block, protocol used for file sharing and remote service access
AS-REP Roast	Attack on Kerberos accounts without pre-authentication
Web Shell	A script uploaded to a web server to provide remote shell access
GPO	Group Policy Object – used to apply settings across Windows domain environments
CWE	Common Weakness Enumeration – standard for software vulnerability classification

Appendix D: Compliance Mapping

Standard	Mapped Controls
OWASP Top 10	A1 (Injection), A2 (Broken Auth), A5 (Misconfig), A9 (Components w/ Known Vulns)
NIST 800-53	AC-17, SC-12, SI-2, IA-5, AC-6
CIS Controls	CIS 3 (Data Protection), CIS 9 (Limiting Network Ports), CIS 18 (Pen Testing)
GDPR	Article 32 – Security of Processing; Article 25 – Data Protection by Design

References

CIS (Centre for Internet Security), 2023. *CIS Controls v8 – Implementation Group 1*. [online] Available at: https://www.cisecurity.org/controls [Accessed 19 May 2025].

Microsoft, 2024. *Security Compliance Toolkit*. [online] Microsoft Docs. Available at: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10 [Accessed 19 May 2025].

MITRE ATT&CK, 2024. *MITRE ATT&CK Framework*. [online] Available at: https://attack.mitre.org/ [Accessed 19 May 2025].

National Institute of Standards and Technology (NIST), 2022. *Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations*. [online] Gaithersburg, MD: NIST. Available at: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final [Accessed 19 May 2025].

Nessus, 2025. *Tenable Plugin Library*. [online] Available at: https://www.tenable.com/plugins [Accessed 19 May 2025].

Open Web Application Security Project (OWASP), 2021. *OWASP Testing Guide v4*. [online] Available at: https://owasp.org/www-project-web-security-testing-guide/stable/ [Accessed 19 May 2025].

OWASP, 2023. *OWASP Top Ten Web Application Security Risks*. [online] Available at: https://owasp.org/www-project-top-ten/ [Accessed 19 May 2025].

Offensive Security, 2024. *Kali Linux Tools Documentation*. [online] Available at: https://tools.kali.org/ [Accessed 19 May 2025].

Tenable, 2025. *Nessus Vulnerability Scanner*. [software] Available at: https://www.tenable.com/products/nessus [Accessed 19 May 2025].

Wang, D. and Wang, P., 2020. *On the Security of the NTLM Protocol*. *IEEE Transactions on Dependable and Secure Computing*, 17(5), pp.958–971. doi:10.1109/TDSC.2019.2902043.