IoT Penetration Testing Report

Prepared by:

<Team 2>

<5/4/2025>

CONFIDENTIAL

Table of Contents

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.

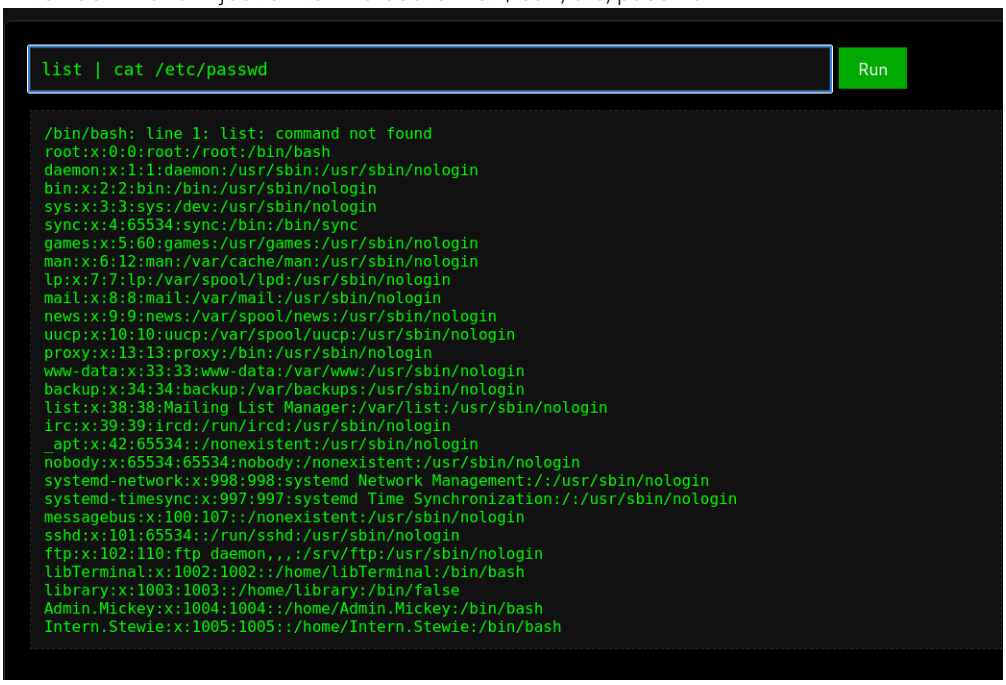
https://portswigger.net/web-security/os-command-injection

Steps for Reproduction

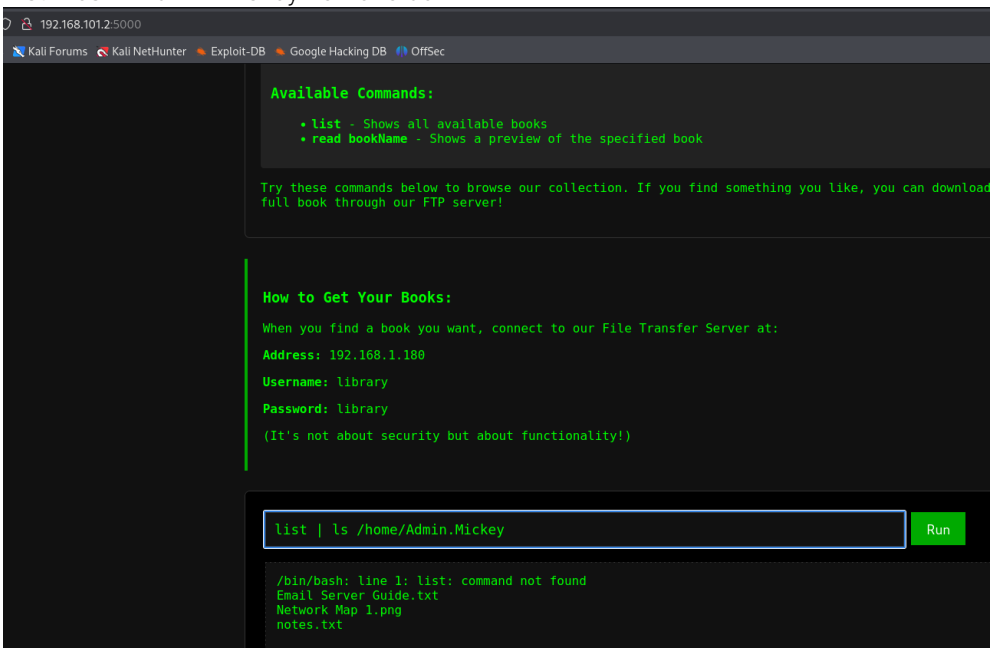
Write clear, step-by-step instructions that show how you found or tested this vulnerability. Include screenshots where possible

Format example:

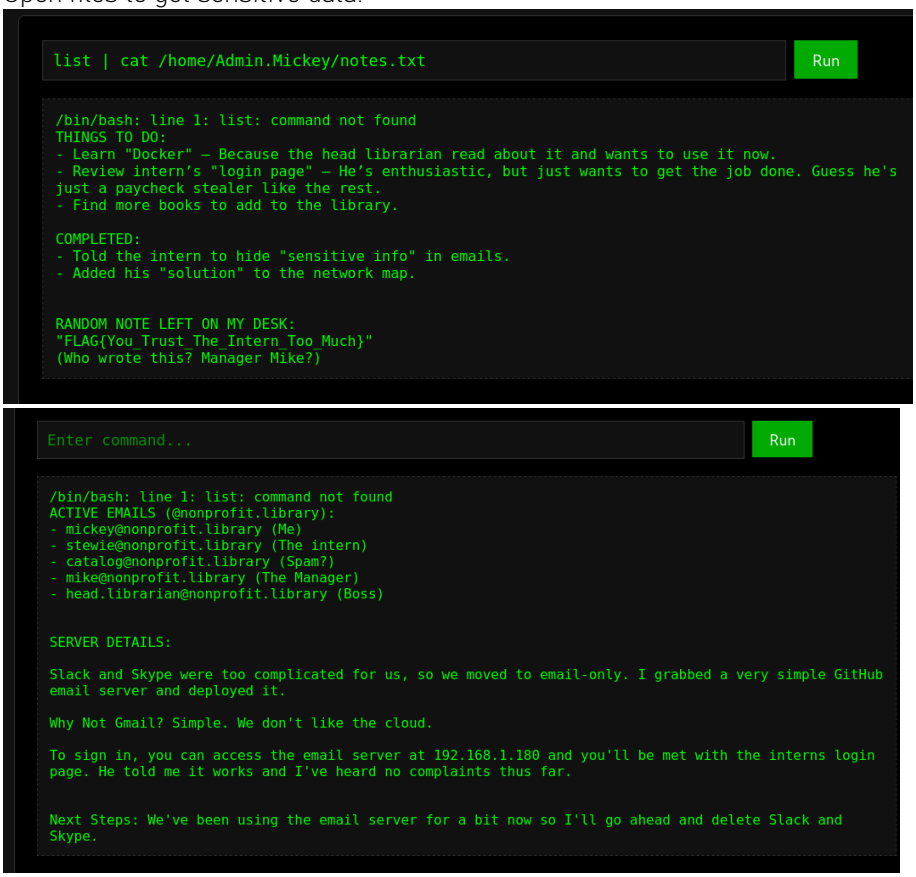
1. Navigate to http://192.168.101.2:5000
2. Enter Command Injection to find users: list | cat /etc/passwd



3. List files in Admin.Mickey home folder



4. Open files to get sensitive data.



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

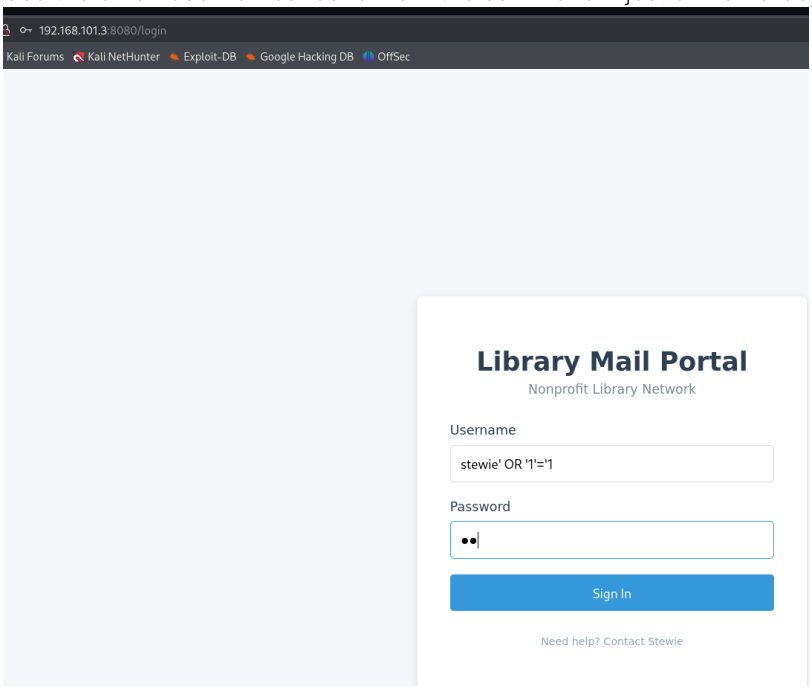
Input sanitization/validation to reject unexpected characters.

References

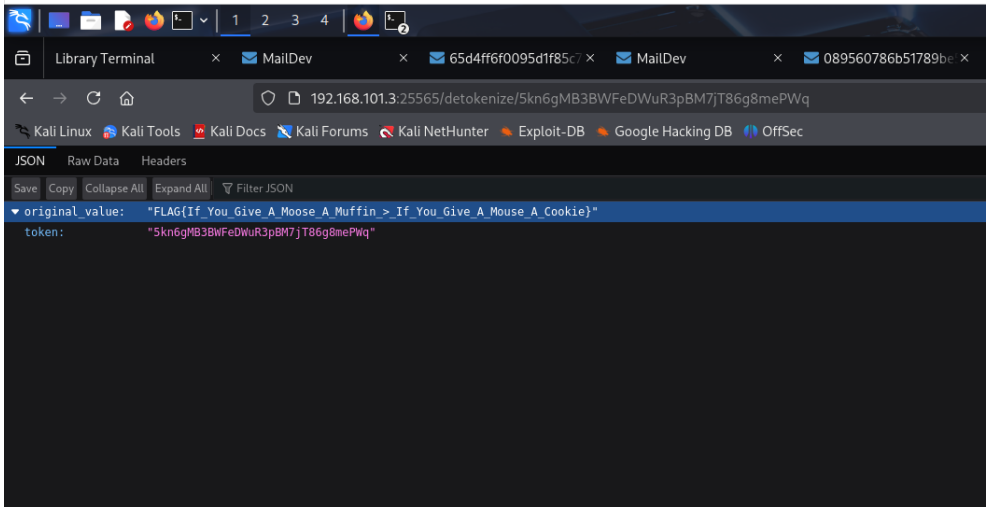
https://portswigger.net/support/using-sql-injection-to-bypass-authentication

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



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



Moderate Risk Findings

	EternalBlue Vulernablilty		
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

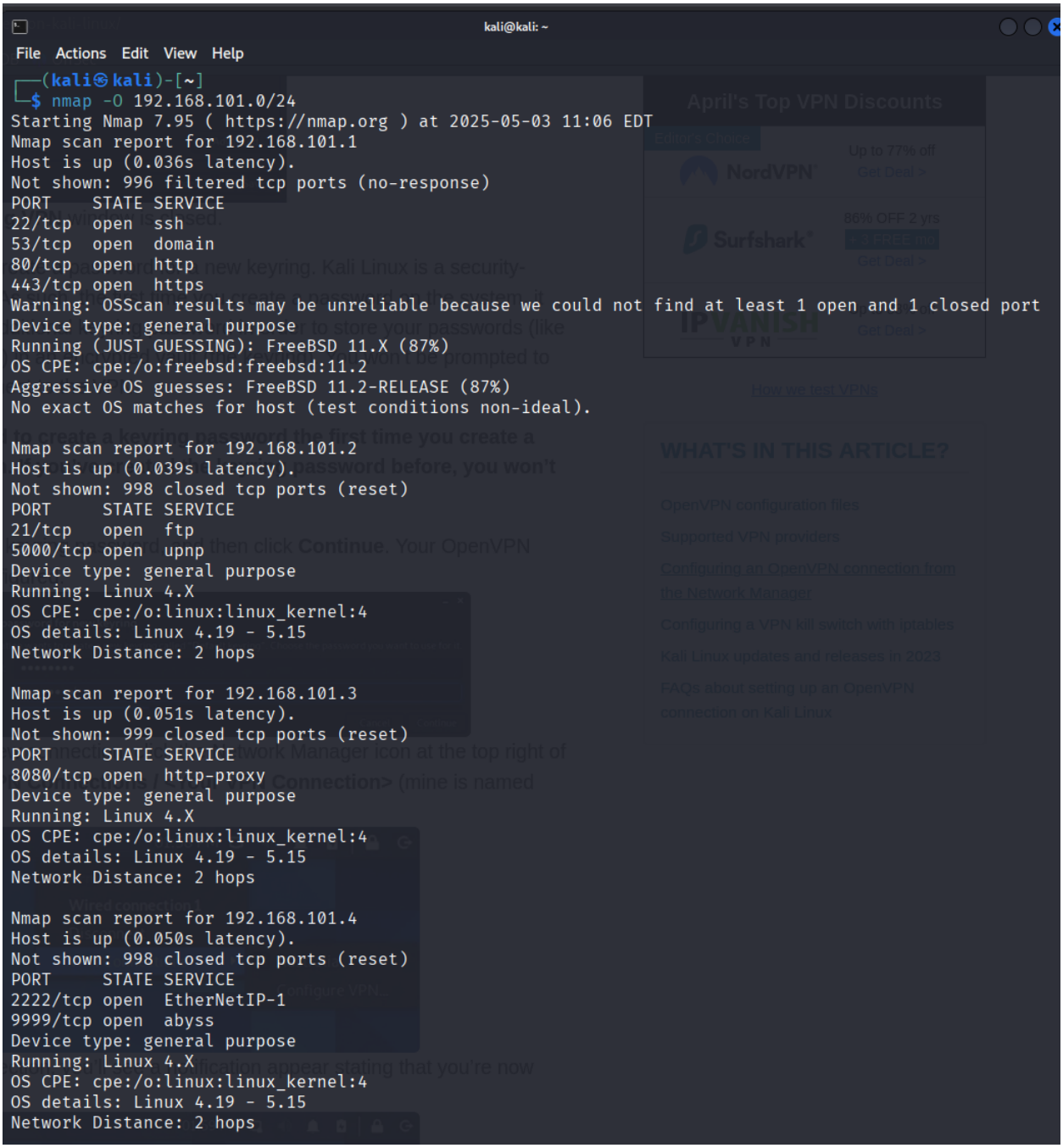
Use firewalls to block scans

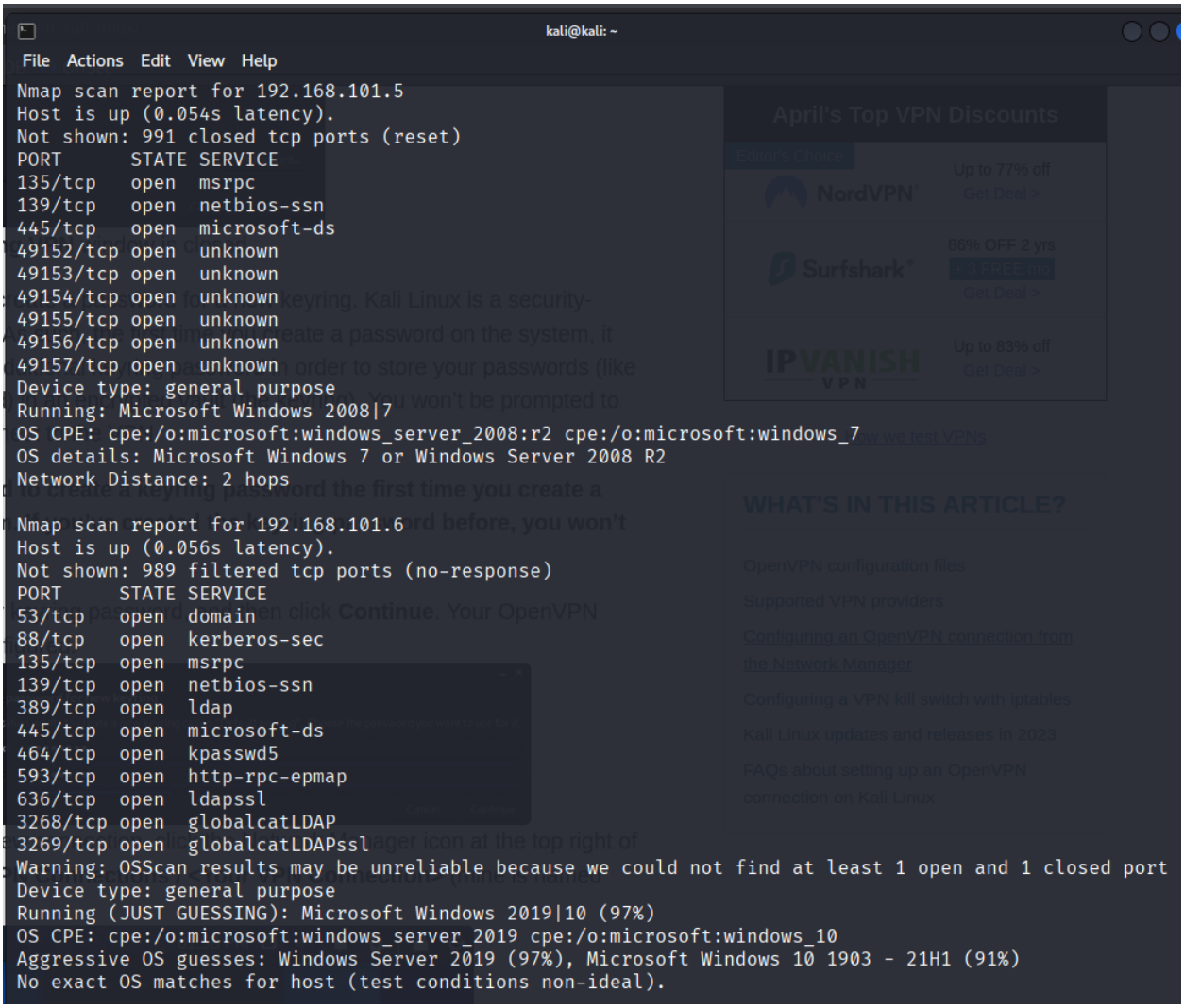
References

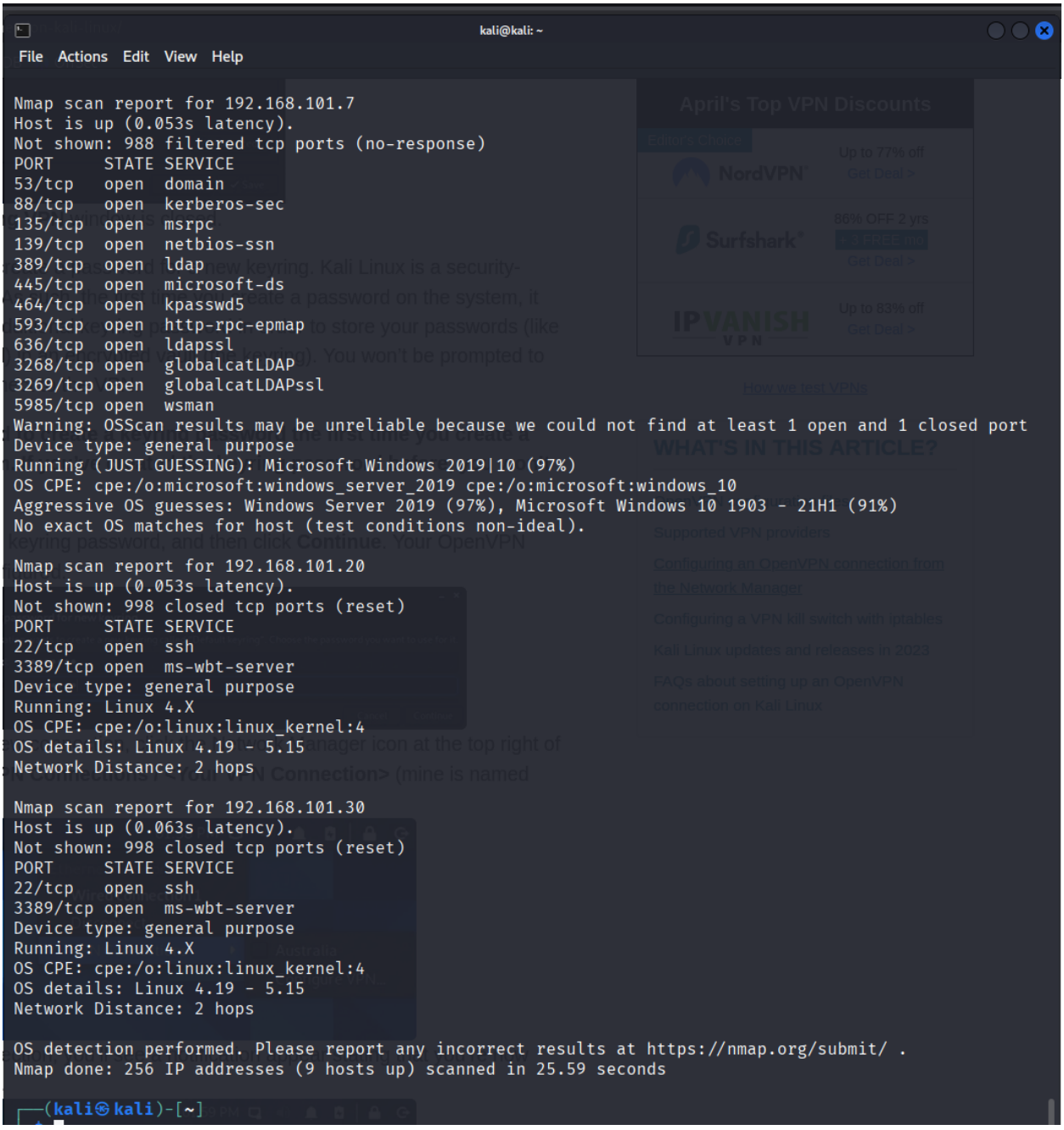
https://www.redhat.com/en/blog/quick-nmap-inventory

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







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