Internship Completion Report

Muhammad Saad Sabir

Cyber Security Intern at YoungDev Interns

Introduction

This report documents the tasks completed during my 4-week internship as a Cyber Security Intern at YoungDev Interns. The internship provided hands-on experience in cybersecurity practices, including phishing awareness, two-factor authentication (2FA), firewall setup, and network analysis using NMAP.

Tasks Completed

2FA Task

Implemented and tested Two-Factor Authentication (2FA) for added security.

Two-factor authentication

...

Two-factor authentication adds an additional layer of security to your account by requiring more than just a password to sign in. [Learn more about two-factor authentication](#).

Preferred 2FA method

Set your preferred method to use for two-factor authentication when signing into GitHub.

GitHub Mobile ⇕

Two-factor authentication

GitHub Mobile

We sent you a sign-in request on your GitHub Mobile app. Approve the request to verify your identity.

Unable to verify with GitHub Mobile?

- Use your authenticator app
- Use a recovery code or begin 2FA account recovery

Firewall Task

Configured a firewall to protect the system from unauthorized access.

Configure passwordless authentication

Add a passkey

Your device supports passkeys, a password replacement that validates your identity using touch, facial recognition, a device password, or a PIN.
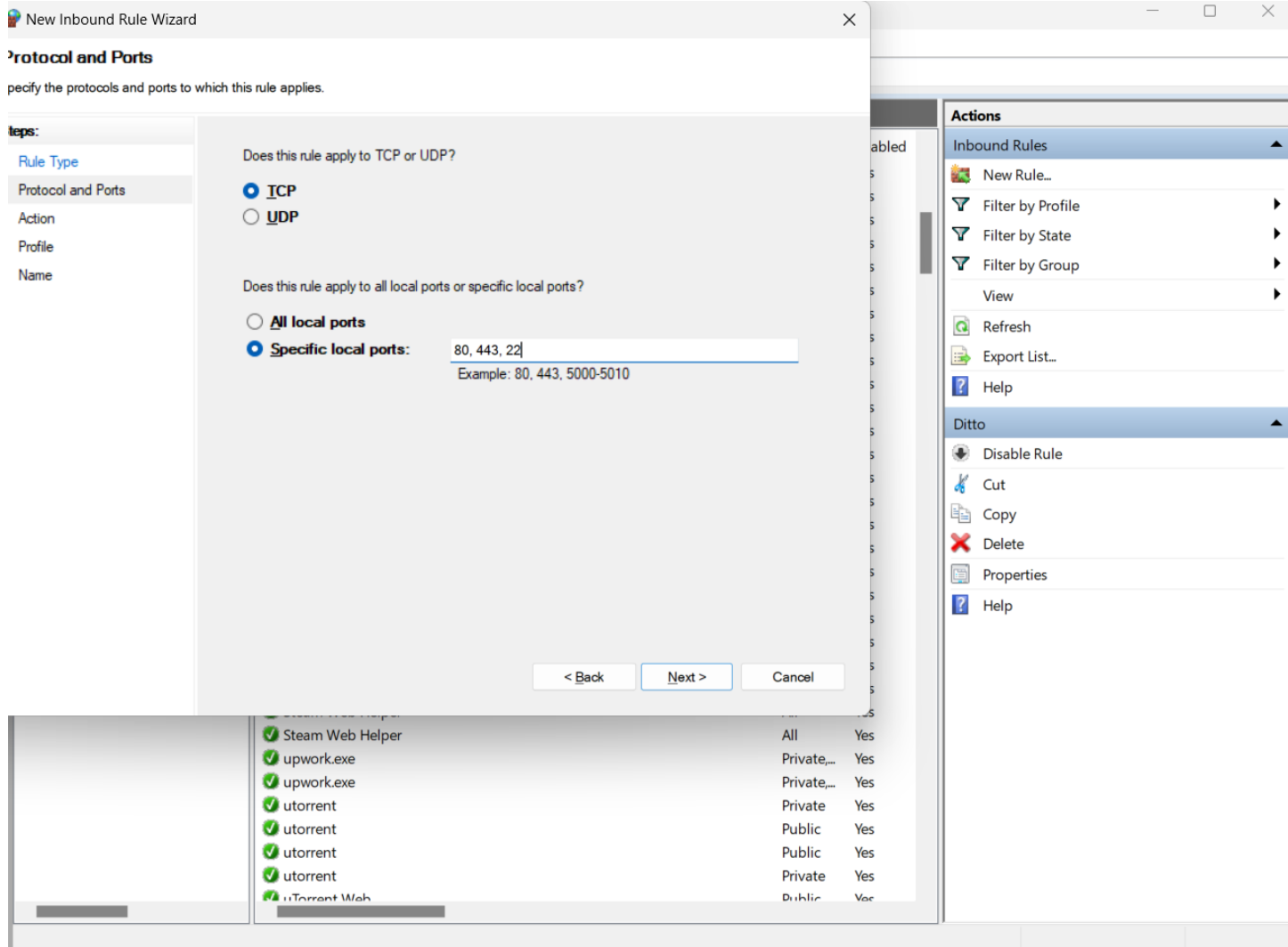
Passkeys can be used for sign-in as a simple and secure alternative to your password and two-factor credentials.

Add passkey

Ask me later

Not interested?

Don't ask again for this browser

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

- ◉ **TCP**
- ○ **UDP**

Does this rule apply to all local ports or specific local ports?

- ○ **All local ports**
- ◉ **Specific local ports:**   `80, 443, 22`

  Example: 80, 443, 5000-5010

[< Back]   [Next >]   [Cancel]

Actions

Inbound Rules

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...
- Help

Ditto

- Disable Rule
- Cut
- Copy
- Delete
- Properties
- Help

Steam Web Helper — All — Yes
upwork.exe — Private,... — Yes
upwork.exe — Private,... — Yes
utorrent — Private — Yes
utorrent — Public — Yes
utorrent — Public — Yes
utorrent — Private — Yes
uTorrent Web — Public — Yes

LastPass Task

New Inbound Rule Wizard   ✕

Set up and explored the functionality of LastPass for password management.
Name

Specify the name and description of this rule.

Steps:

- ● Rule Type
- ● Protocol and Ports
- ● Action
- ● Profile
- ● Name

Name:

PUBLIC PORTS

Description (optional):

Only ports 80,443,22 allow for public domains.

< Back   Finish   Cancel

LastPass •••I

All Items

Passwords

Notes

Applications

Addresses

Payment Cards

Bank Accounts

Welcome to LastPass!

There are no items in your vault.

+
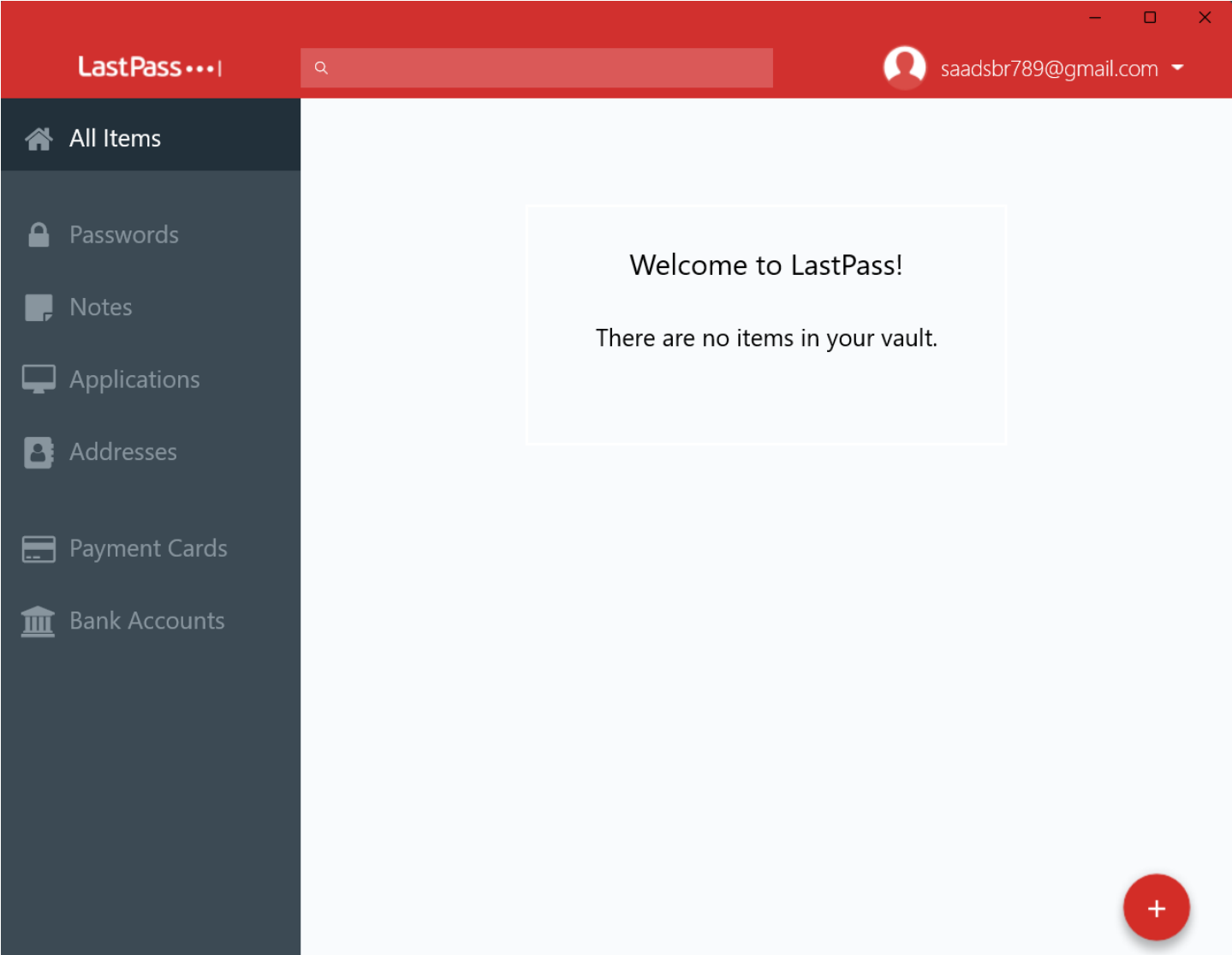
NMAP Task

Used NMAP for network analysis and vulnerability scanning.

```
┌──(kali⊕Saad-DT)-[~]
└─$ nmap -sV 172.██████/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-24 22:28 PKT
Nmap scan report for 172.██████.11
Host is up (0.00018s latency).
All 1000 scanned ports on 172.██████.11 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (1 host up) scanned in 12.62 seconds
```

```
┌──(kali㉿Saad-DT)-[~]
└─$ ping tesla.com
PING tesla.com (2.18.51.207) 56(84) bytes of data.
64 bytes from a2-18-51-207.deploy.static.akamaitechnologies.com (2.18.51.207): icmp_seq=1
ttl=39 time=241 ms
^C
--- tesla.com ping statistics ---
2 packets transmitted, 1 received, 50% packet loss, time 1001ms
rtt min/avg/max/mdev = 241.424/241.424/241.424/0.000 ms


┌──(kali㉿Saad-DT)-[~]
└─$ nmap -sn 2.18.51.00/24 -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-24 22:31 PKT
Initiating Ping Scan at 22:31
Scanning 256 hosts [2 ports/host]
Completed Ping Scan at 22:31, 3.70s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 227 hosts. at 22:31
Completed Parallel DNS resolution of 227 hosts. at 22:31, 1.18s elapsed
Nmap scan report for 2.18.51.0 [host down]
Nmap scan report for 2.18.51.1 [host down]
Nmap scan report for a2-18-51-2.deploy.static.akamaitechnologies.com (2.18.51.2)
Host is up (0.28s latency).
Nmap scan report for a2-18-51-3.deploy.static.akamaitechnologies.com (2.18.51.3)
Host is up (0.28s latency).
Nmap scan report for a2-18-51-4.deploy.static.akamaitechnologies.com (2.18.51.4)
Host is up (0.28s latency).
Nmap scan report for a2-18-51-5.deploy.static.akamaitechnologies.com (2.18.51.5)
Host is up (0.28s latency).
Nmap scan report for a2-18-51-6.deploy.static.akamaitechnologies.com (2.18.51.6)
Host is up (0.28s latency).
Nmap scan report for a2-18-51-7.deploy.static.akamaitechnologies.com (2.18.51.7)
Host is up (0.28s latency).
Nmap scan report for a2-18-51-8.deploy.static.akamaitechnologies.com (2.18.51.8)
Host is up (0.28s latency).
Nmap scan report for a2-18-51-9.deploy.static.akamaitechnologies.com (2.18.51.9)
Host is up (0.28s latency).
Nmap scan report for a2-18-51-10.deploy.static.akamaitechnologies.com (2.18.51.10)
Host is up (0.28s latency).
Nmap scan report for a2-18-51-11.deploy.static.akamaitechnologies.com (2.18.51.11)
Host is up (0.25s latency).
```

Phishing Task

Analyzed phishing tactics including:

- Non-professional email formats.

- Poor grammar and irrelevant attachments.

- Unusual links and attempts to extract personal information.

Protect yourself from phishing

Phishing (pronounced: fishing) is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information -- such as credit card numbers, bank information, or passwords -- on websites that pretend to be legitimate. Cybercriminals typically pretend to be reputable companies, friends, or acquaintances in a fake message, which contains a link to a phishing website.

What is phishing?

URGENT! Your account has been Compromi

URGENT! Your account has been Co

Well-known Company <no
7/14/2020 4:33 PM

To: nestorwilke@outlook.com

VM - 7/14/2020 - Cellphone - Missed
497 bytes

Thank you for your feedback!