Lab Template – Ethan Roepke

1. **Describe what you did to** rockyou.txt.gz **that changed it to** rockyou.txt**.  If you ran a command, include the command and briefly explain why it worked.**

(5 points)

A command I ran was “gzip -d rockyou.txt.gz”

This command worked because gzip is the command for file compression/decompression and when we add ‘-d’, this tells us we want to decompress the file.

1. **Perform a dictionary password attack with this command. Take a screenshot once you’ve found the password.**

hydra -l santana -P /usr/share/wordlists/rockyou.txt ssh://x.x.x.123 -V

(10 points)

A screen shot of a computer

Description automatically generated

1. **Using SSH from your Kali VM, log into the user** santana **using the password you just found. Take a screenshot.**

(10 points)

A screenshot of a computer screen

Description automatically generated

1. **Execute the** net users **command on** X.X.X.108**.  Take a screenshot of successful execution.**

(10 points)

A screenshot of a computer

Description automatically generated

1. **With your reverse shell, run the following command and take a screenshot of the entire output for your lab report.**PS C:> **systeminfo**

(10 points)

A screenshot of a computer

Description automatically generated

1. **Show Shelly’s plaintext password(s) from the output of the John command.**

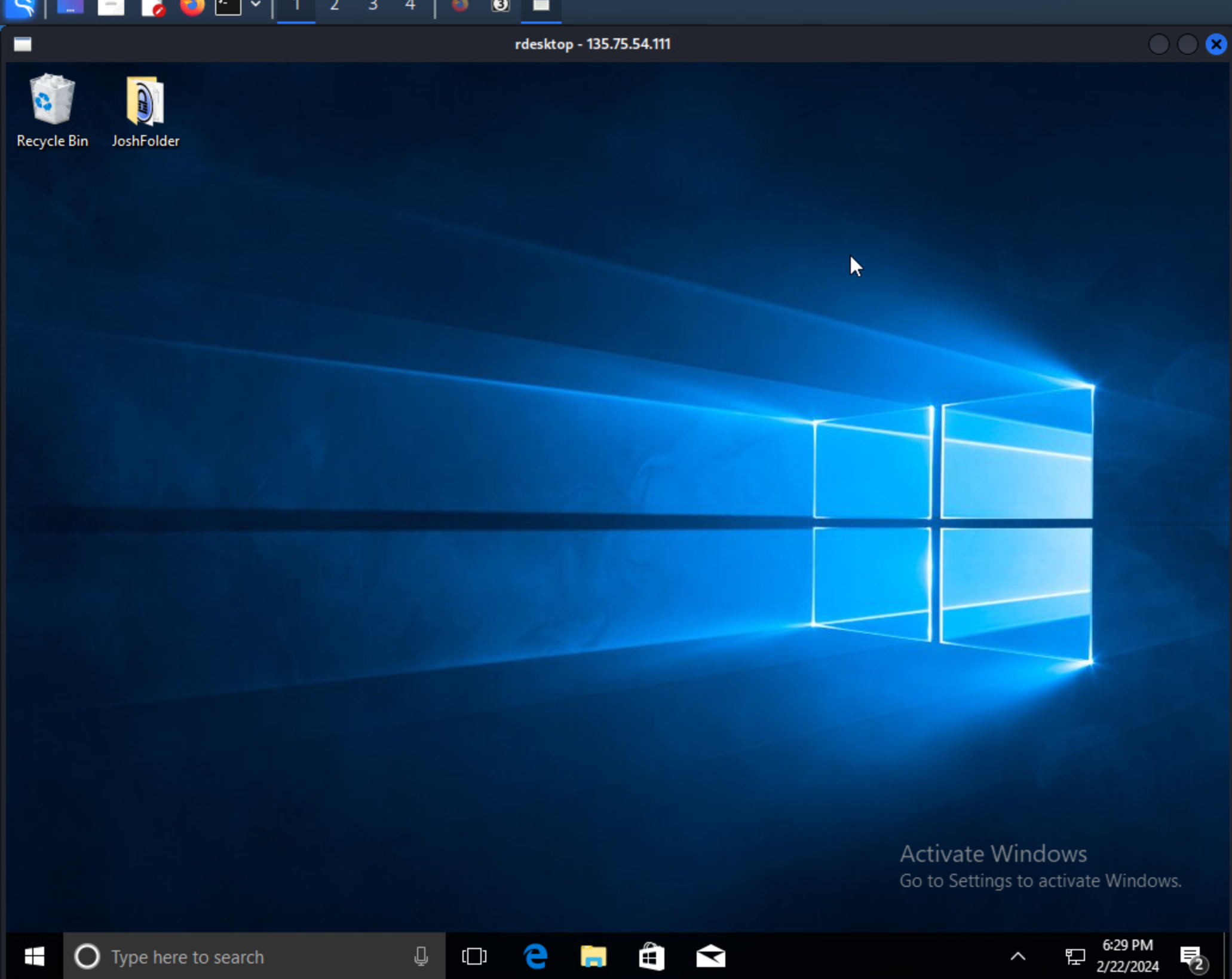
(10 points)

A screenshot of a computer

Description automatically generated

1. **Take a screenshot of the RDP session** *(include the* rdesktop - x.x.x.111 *heading)*

(10 points)



1. **Do some research on the internet. What happens if you RDP into this machine while the user Joshua is actively using the computer?**

(5 points)

I have found 2 possibilities that could happen when you RDP onto a machine while a user is active. The first is when you RDP onto the machine, the user of the machine will be interrupted with a message possibly letting them know someone is trying to have remote access and they can accept or deny it. Another possibility that could happen is a new session will be running while the users machine session will run in the background. This all depends on the configured setting for the users settings.

1. **When would we want to use smbmap w/ Pass the Hash over using RDP to connect to a machine?**

(10 points)

We would want to use smbmap w/Pass the Hash over using RDP to connect to a machine because RDP can be a strong bandwidth especially when the network bandwidth is limited, so using smbmap w/Pass the Hash will be beneficial and more efficient. Pass the Hash avoids sending plaintext passwords, which will prevent security measures installed.

1. **Take a screenshot of this command’s output after you’ve obtained your interactive shell on X.X.X.121:**

**echo “[netid]” && id && ip a**

(10 points)

Understood netid meant to be “eroepke” but inserted my ip address “135.75.54.121”

A computer screen shot of white text

Description automatically generated