Robert Carpenter
github.com/robertmcarpenter
Mon December 17th 2024

Lab 6.6.7 Password Cracking using John the Ripper on Kali Linux

From TestOut CompTIA Security+ Course

In this lab I will be cracking a password protected .zip archive using the popular Password Cracking tool John the Ripper.

The scenario for this lab is as follows:

"You are the IT security administrator for a small corporate network. You've received a zip file that contains sensitive password-protected files. You need to access these files. The zip file is located in the home directory.

In this lab, your task is to use John the Ripper to:

- **Crack the root password on the Linux computer named Support.**
- **Crack the password of the protected.zip file located in the home directory on IT-Laptop.**

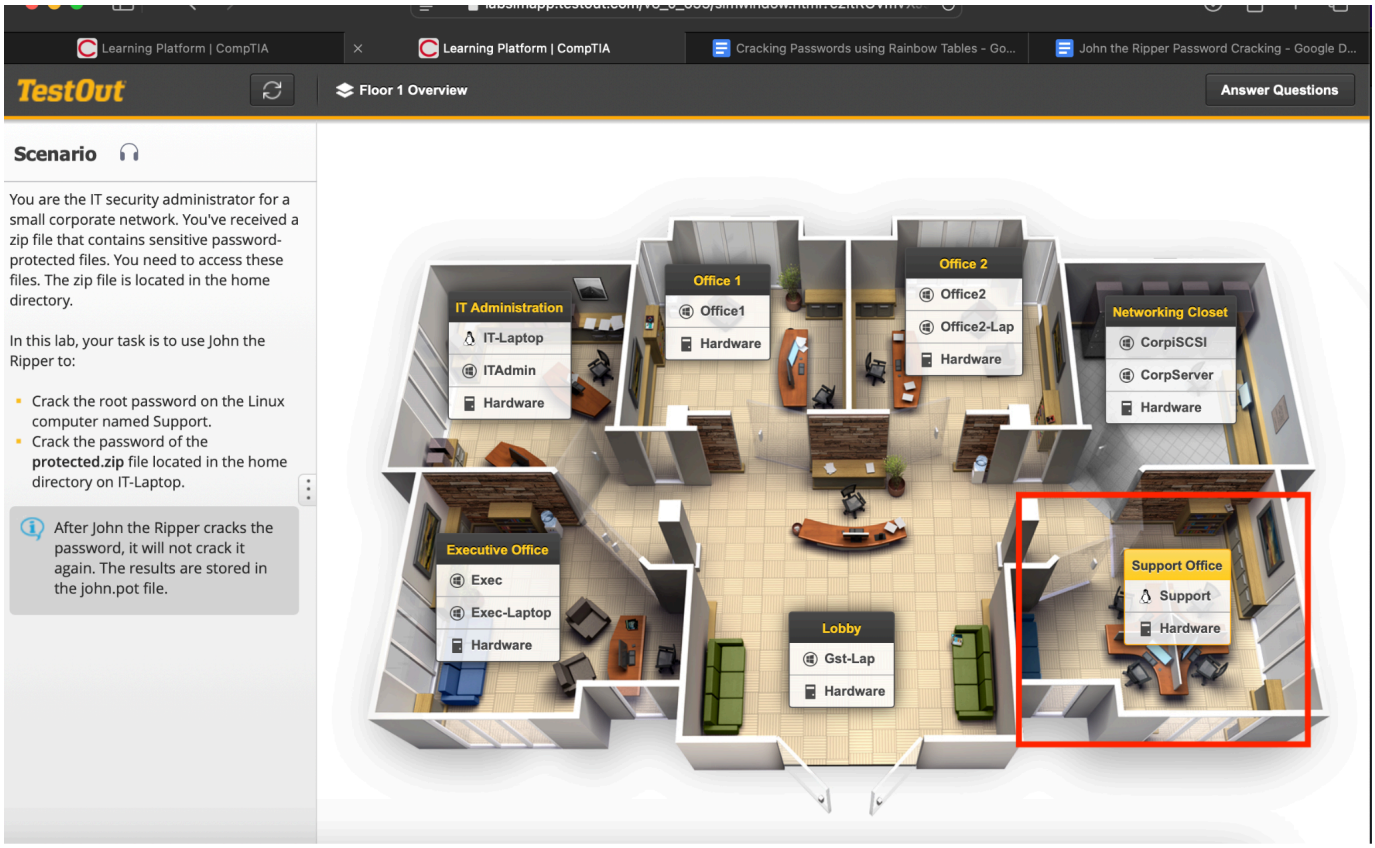
After John the Ripper cracks the password, it will not crack it again. The results are stored in the john.pot file."

My first task in this lab is to crack the root password of the Support Machine.

Note: This virtual lab environment assumes the environment of a typical corporate office.

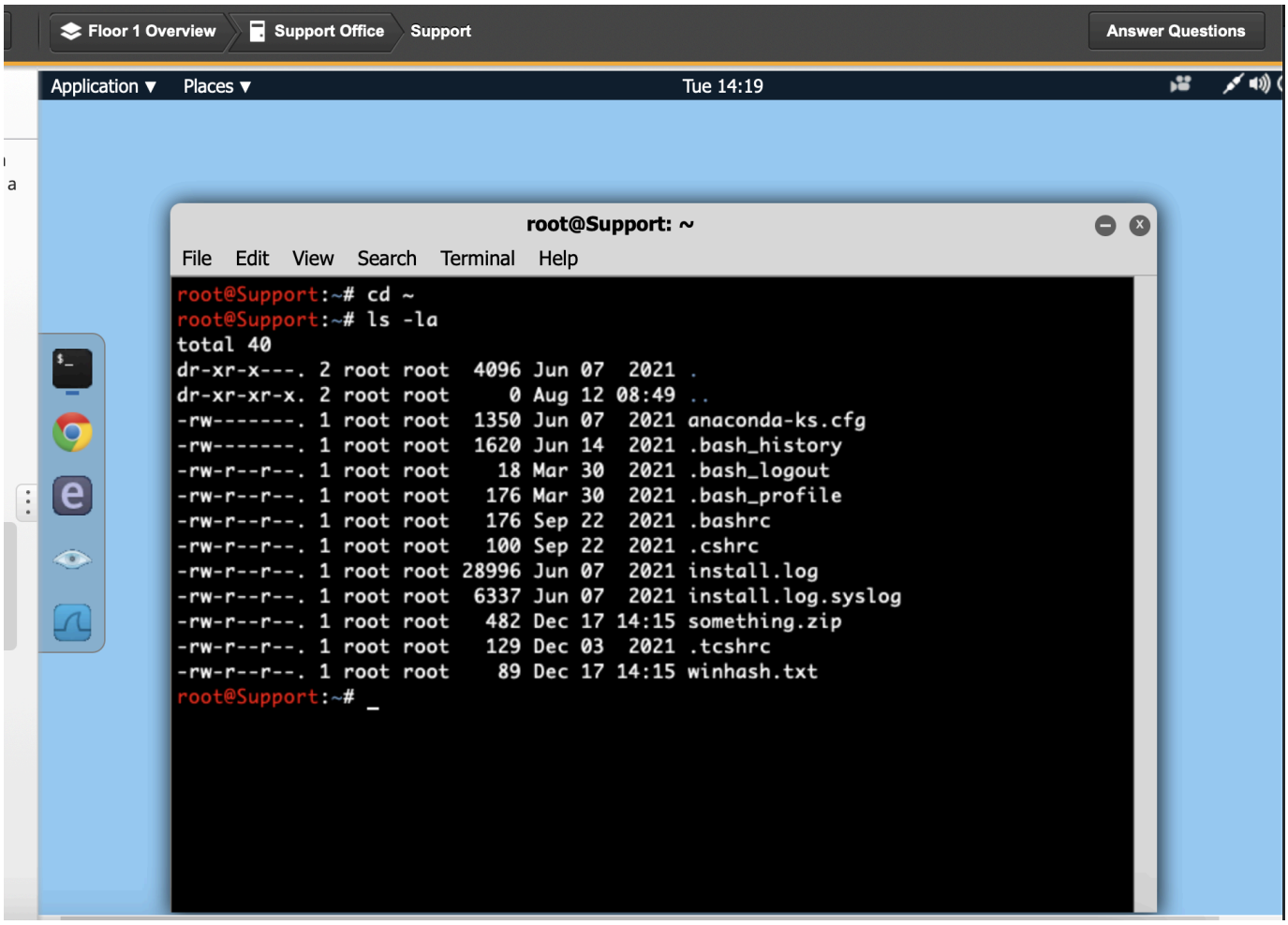
I will need to switch to that computer now.

Robert Carpenter
github.com/robertmcarpenter
Mon December 17th 2024



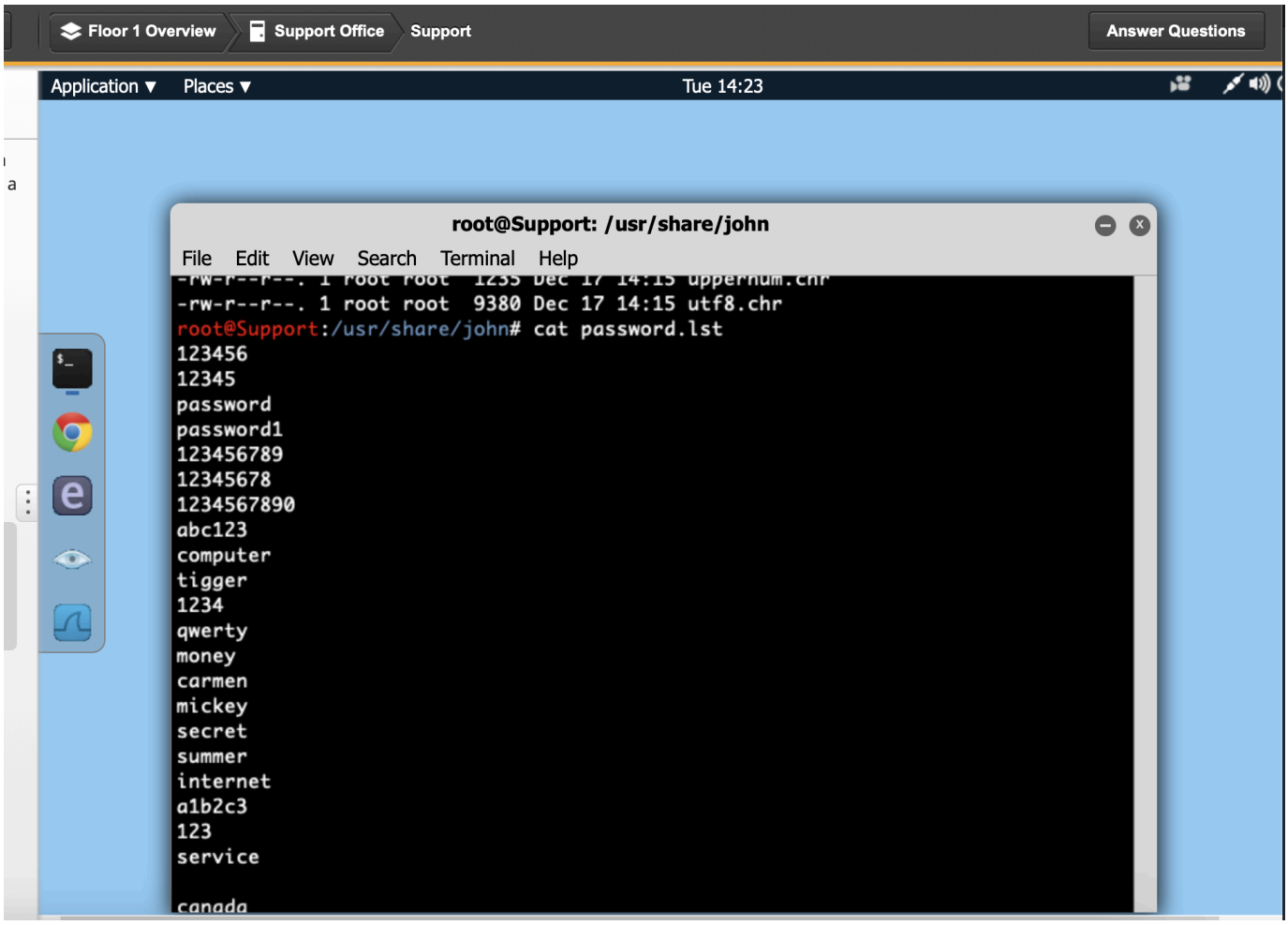
The Lab tells us that the .zip file we need to crack is on the home directory. I will **cd** to that directory and **ls -la** the directory to view the contents.

Robert Carpenter
github.com/robertmcarpenter
Mon December 17th 2024



As you can see **something.zip** is the target file in question. Let's go ahead and view the password list we are going to use with John the Ripper. This password list is located in **/usr/share/john.** I will change directories there, then **cat** out the password.lst file to verify we have a Dictionary to work with.

Robert Carpenter
github.com/robertmcarpenter
Mon December 17th 2024



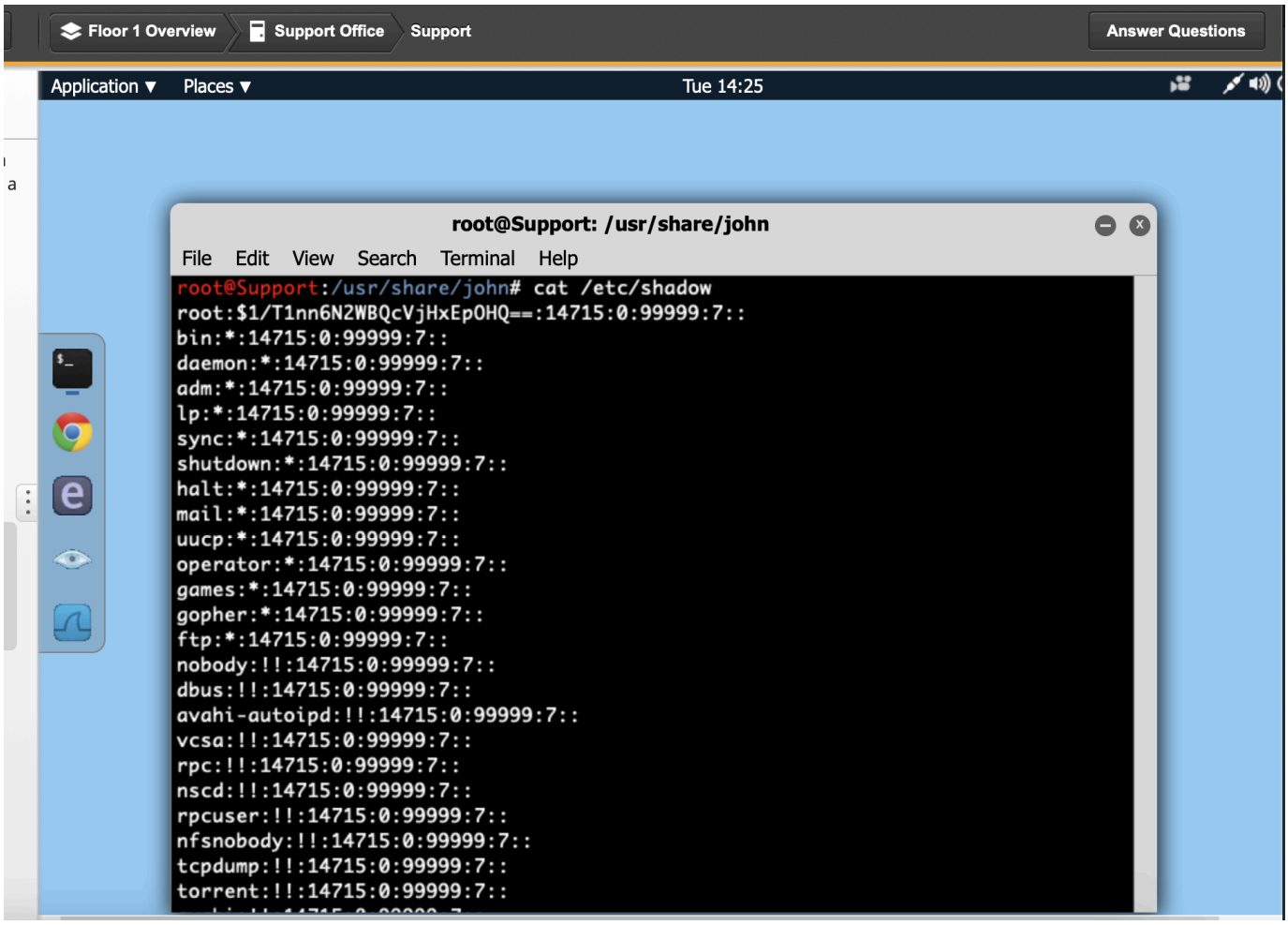
Awesome, we have a predefined Dictionary (also called a wordlist) we can use for the attack.

All Linux passwords are located in the **/etc/shadow** file , and should be unreadable because they are most often (if configured correctly) just hash representations of the actual password. This is no problem for John the Ripper to handle.

Let's verify that the password for the root account is not in cleartext. If it is, then our job is much easier and we don't have to use this cracking tool.

I will issue **cat /etc/shadow:**

Robert Carpenter
github.com/robertmcarpenter
Mon December 17th 2024



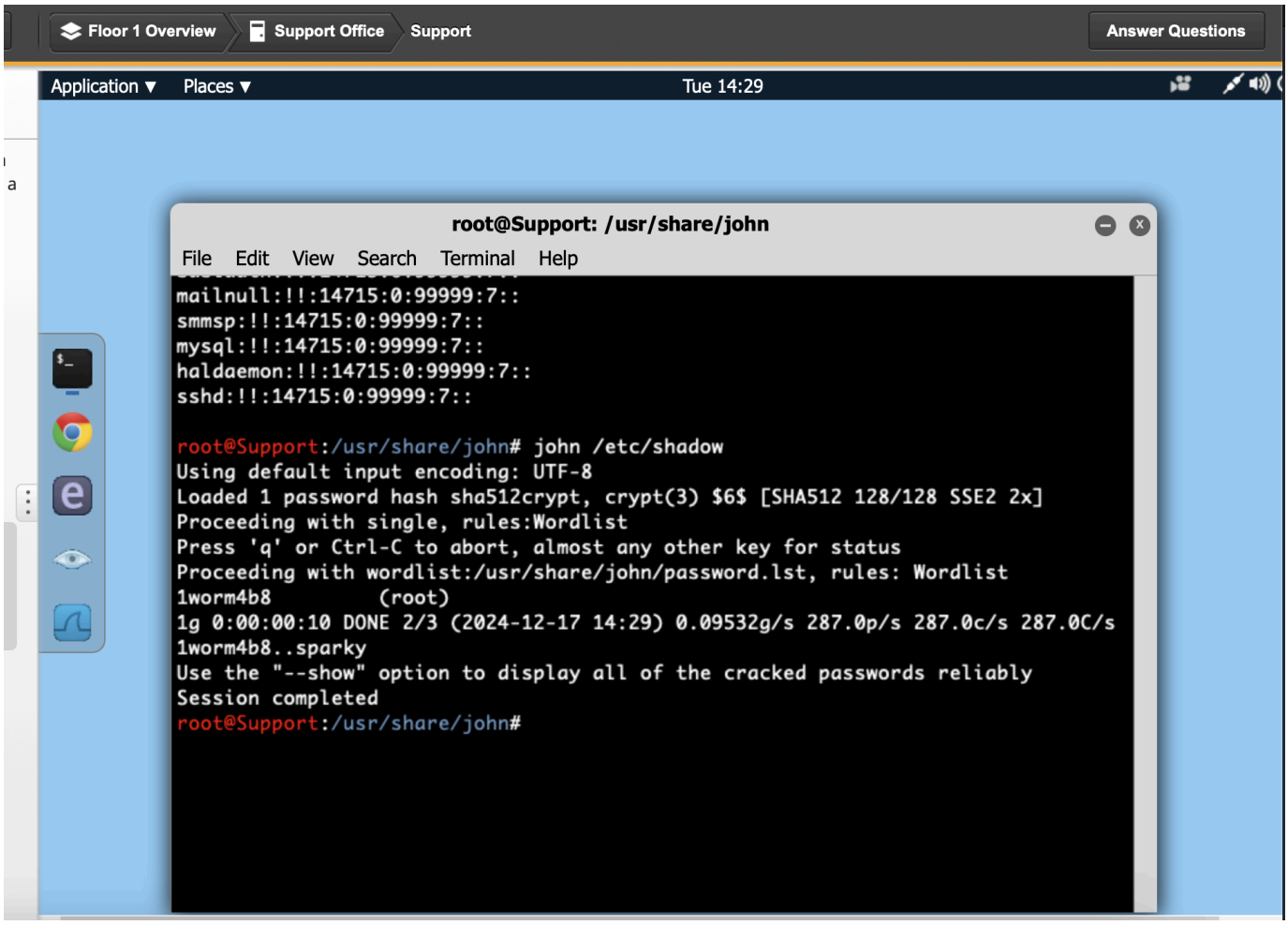
Note that I am currently logged in as the root user. If an attacker is able to use an exploit to escalate their privileges to root they still won't have the password to the root account. This means everytime the attacker wants to open a root shell, they will need to reattack the machine which creates a "digital footprint."

Anytime an attacker can log in to a system the "normal" way is better for them to stay under the radar due to the intrusiveness of some exploits. This is why the root password is so valuable.

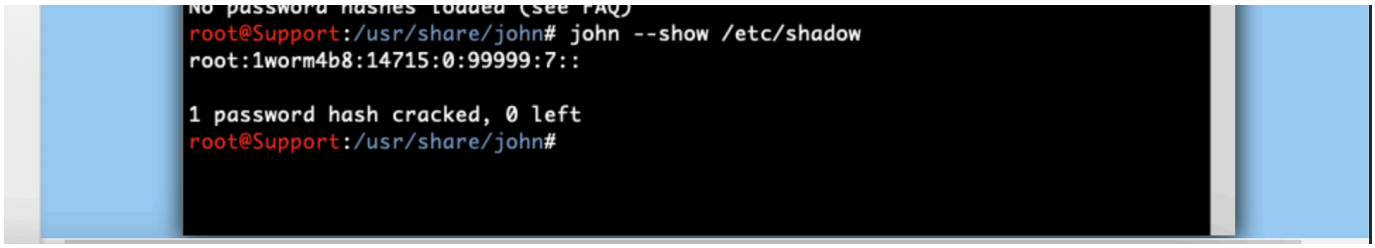
I will now crack the root password using the command:

John /etc/shadow

Robert Carpenter
github.com/robertmcarpenter
Mon December 17th 2024



I can see that the password is **1worm4b8..sparky** . The password is surrounded by the other telemetry provided to us by John the Ripper, so the command tells us we can simply use **john –show** command to print out the passwords more reliably.

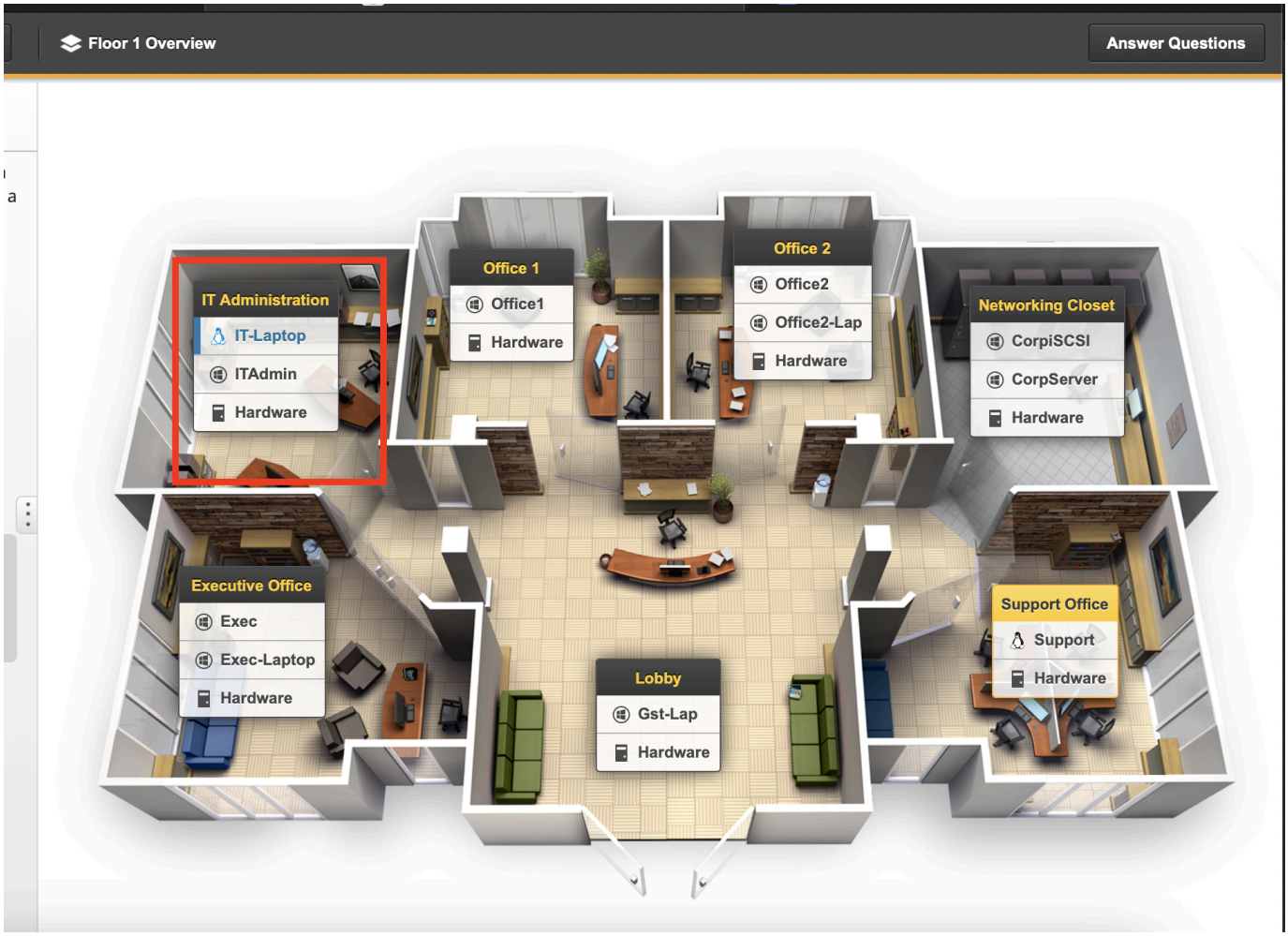


Success we've cracked the root password!

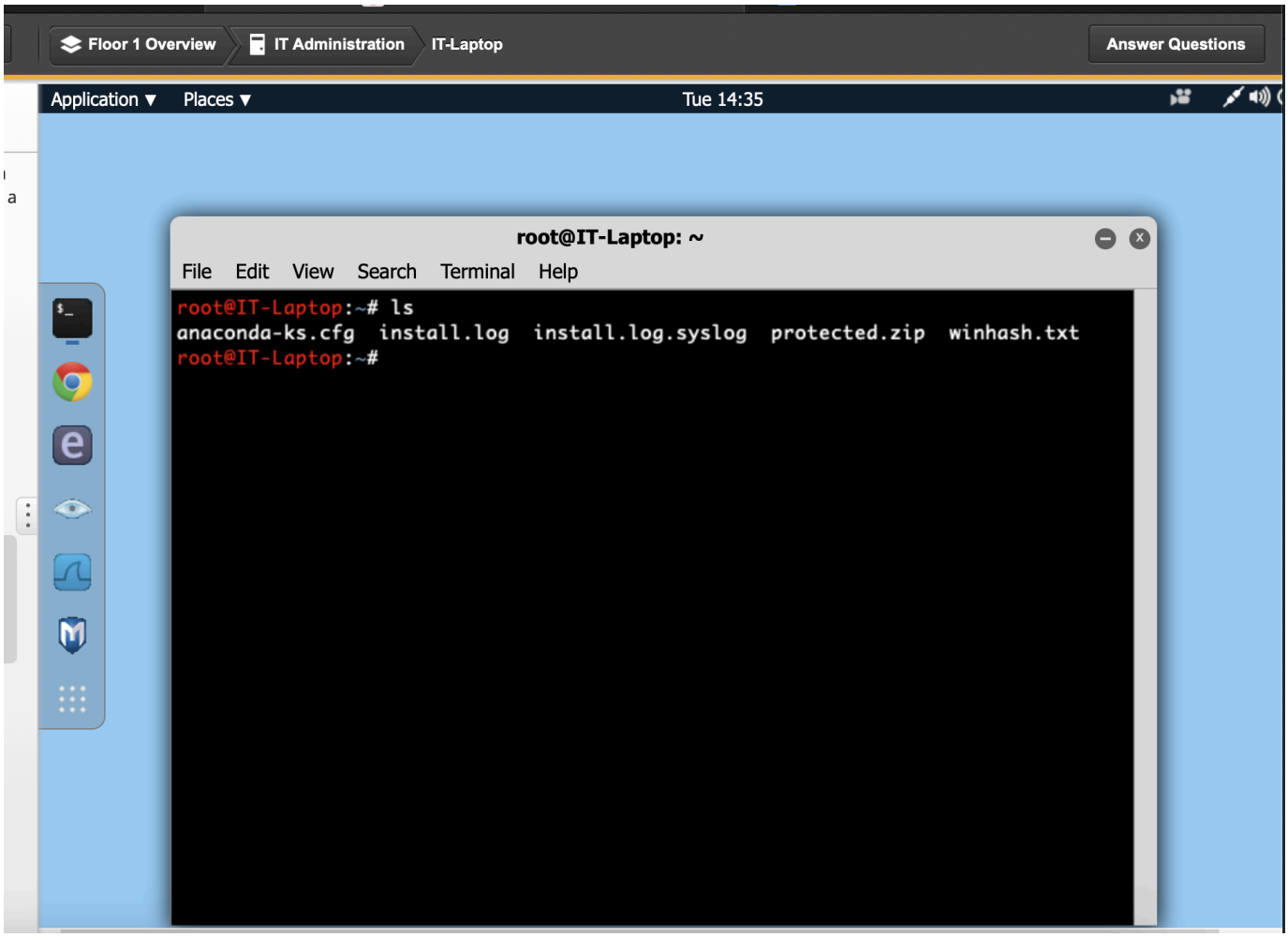
Now I will move on to the next part of this lab which is for me to crack the password to the .zip archive thats protected in the root home directory.

Robert Carpenter
github.com/robertmcarpenter
Mon December 17th 2024

The Lab wants us to crack the .zip on the IT-Laptop machine. I will now need to exit this Support machine and head over to that one.



Robert Carpenter
github.com/robertmcarpenter
Mon December 17th 2024



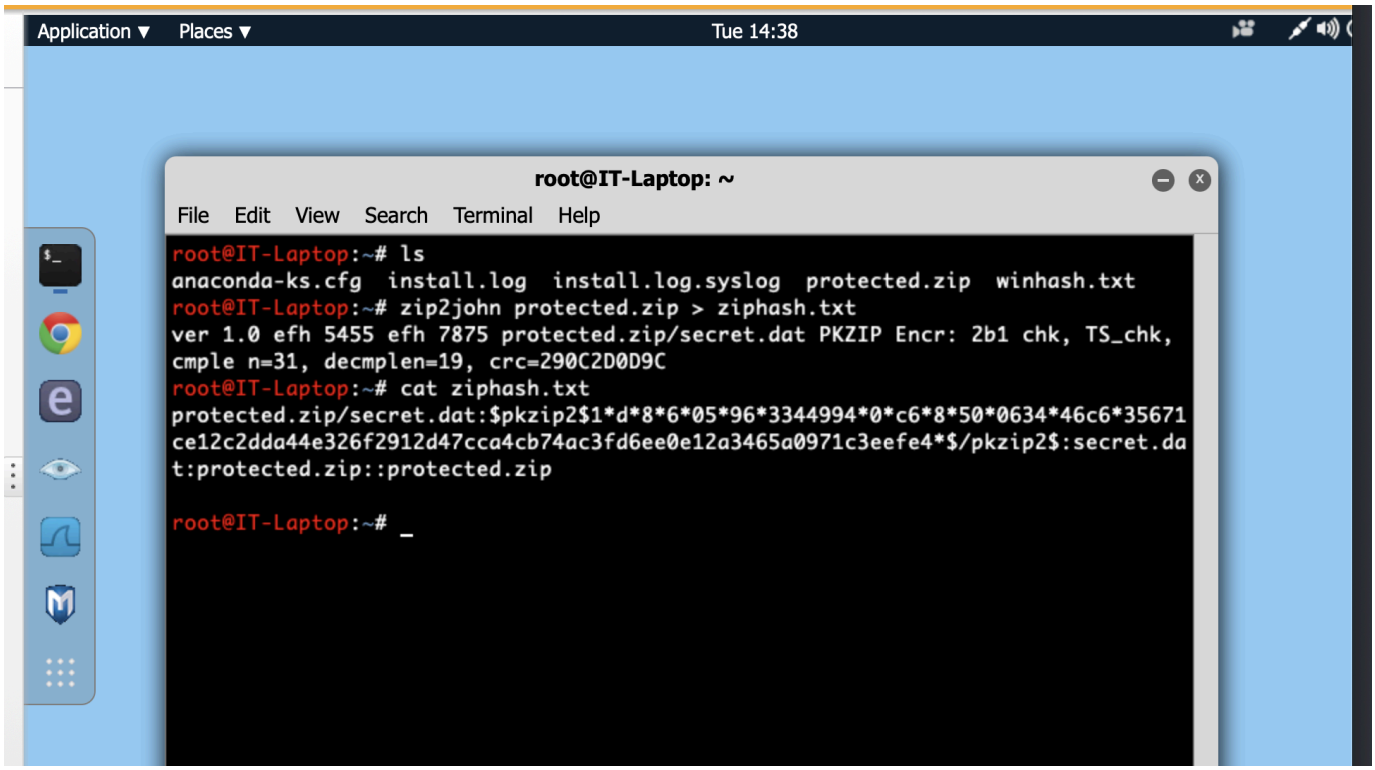
Now that I'm here I issued an **ls** command to view the contents of this home directory.

I see that there is a **protected.zip** file here. This is the target .zip file I will be cracking with John the Ripper. Before I can do it, I need to use a supporting binary called **zip2john** so I can generate a hash that John the Ripper can use.

Zip2john will display the hash on **STDOUT** but I want it in a file. To do that I can issue:

Zip2john protected.zip > ziphash.txt

Robert Carpenter
github.com/robertmcarpenter
Mon December 17th 2024



We now have a hash that John the ripper can use! We can now issue the password cracking command:

John –format=pkzip ziphash.txt

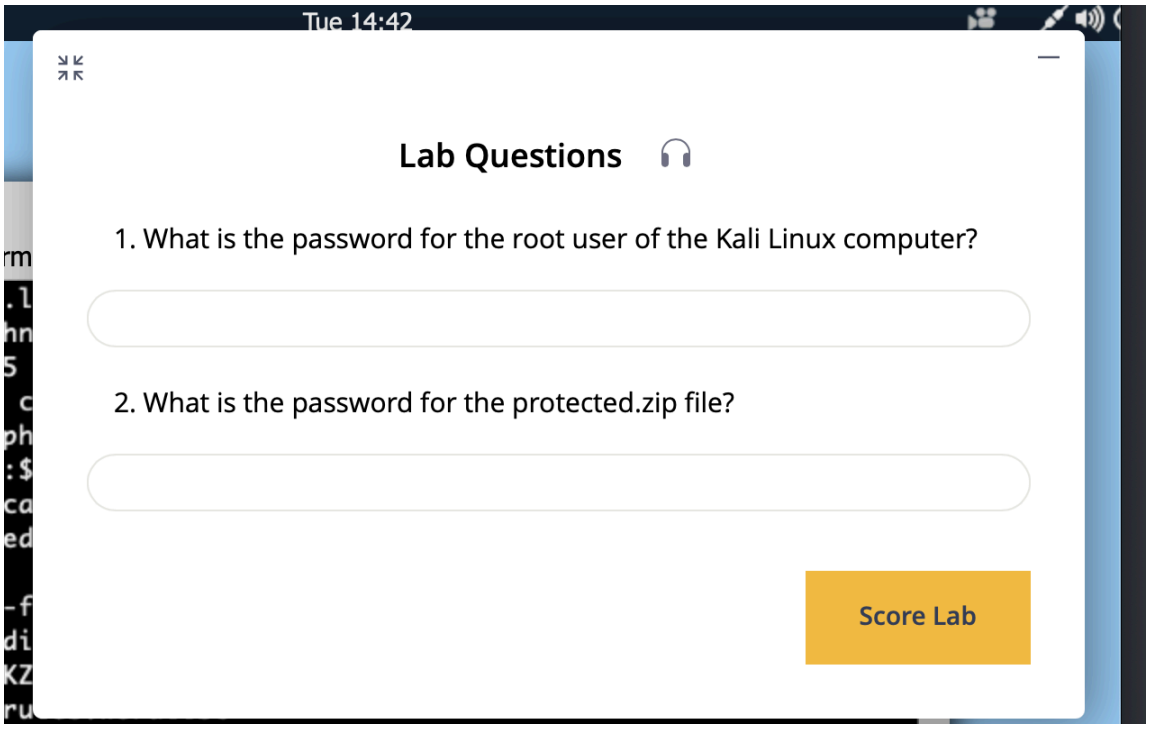
Then…

John –show ziphash.txt

As you can see the password to the zip file was cracked. The value is **p@ssw0rd.**

I will now answer the final questions of this lab and conclude!

Robert Carpenter
github.com/robertmcarpenter
Mon December 17th 2024



1. **Password of root account = 1worm4b8**
2. **Password of protected.zip = p@ssw0rd**

Robert Carpenter
github.com/robertmcarpenter
Mon December 17th 2024