

## 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.

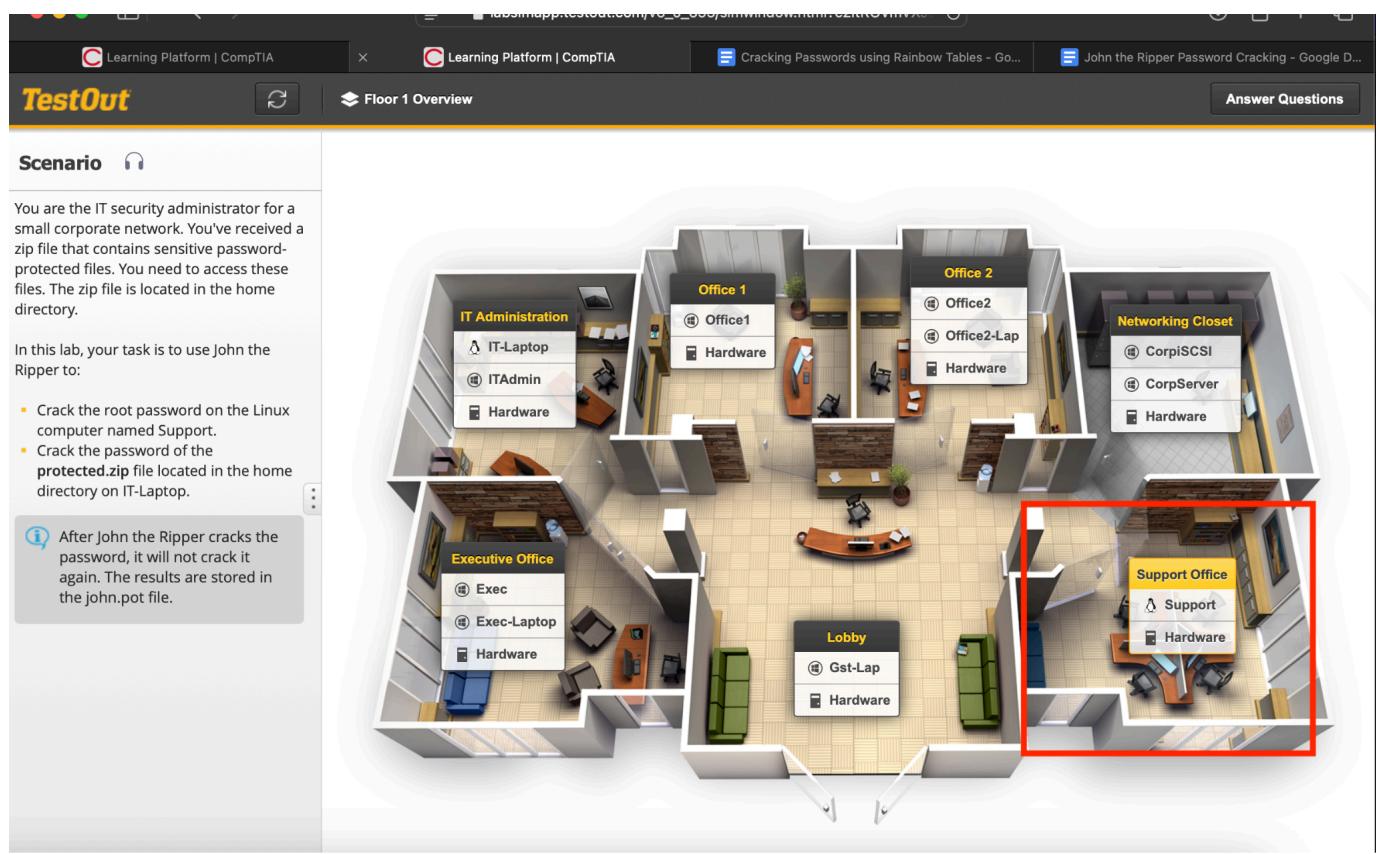
After John the Ripper cracks the password, it will not crack it again. The results are stored in the john.pot file.”

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](https://github.com/robertmcarpenter)  
Mon December 17th 2024



The screenshot shows a 3D floor plan of a corporate office. The layout includes several rooms: IT Administration, Office 1, Office 2, Networking Closet, Executive Office, Lobby, and Support Office. Each room contains icons representing hardware and software assets. A red box highlights the Support Office, which contains a computer named "Support".

**Scenario**

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.

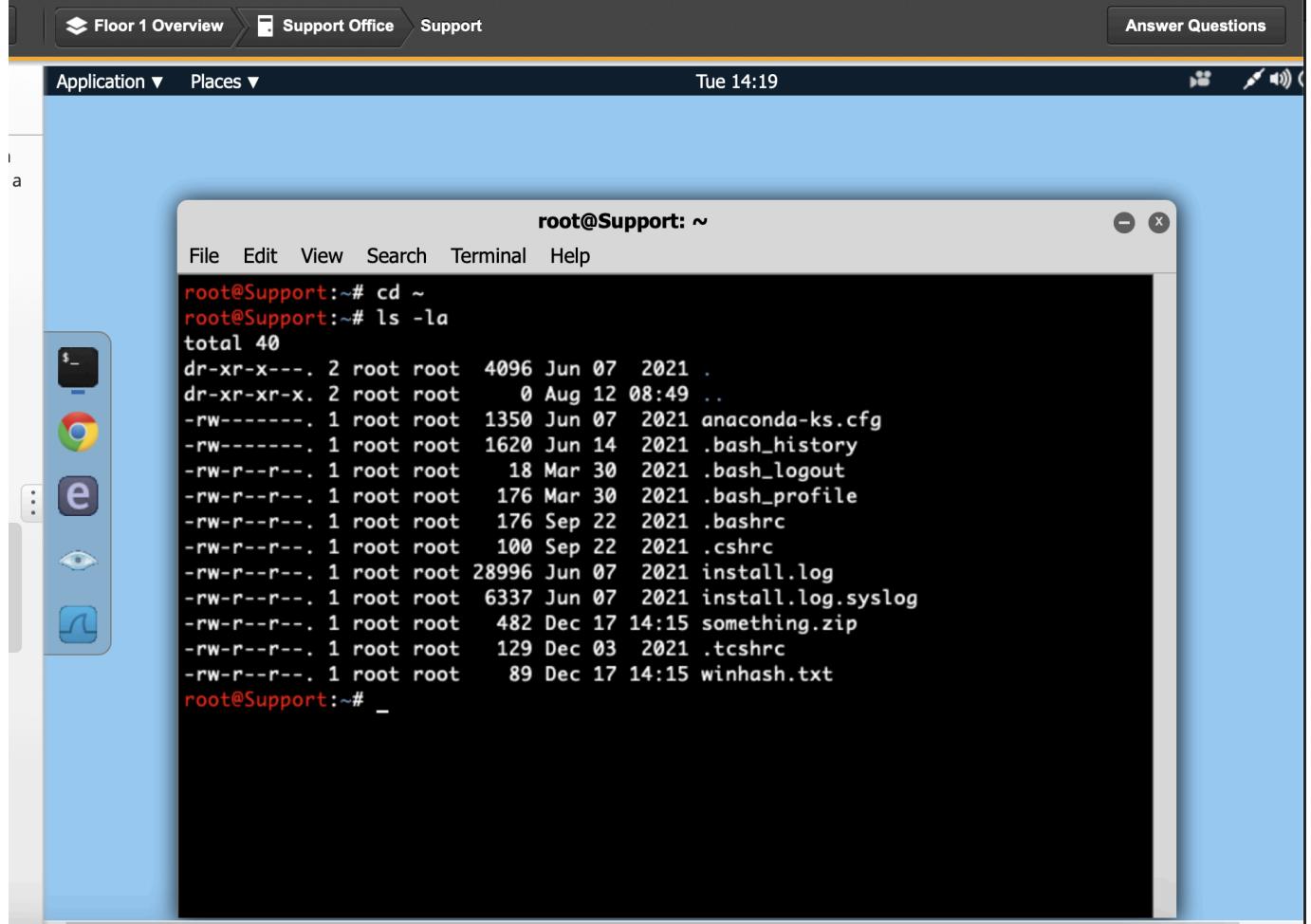
In this lab, your task is to use John the Ripper to:

- 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.

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

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.

Mon December 17th 2024

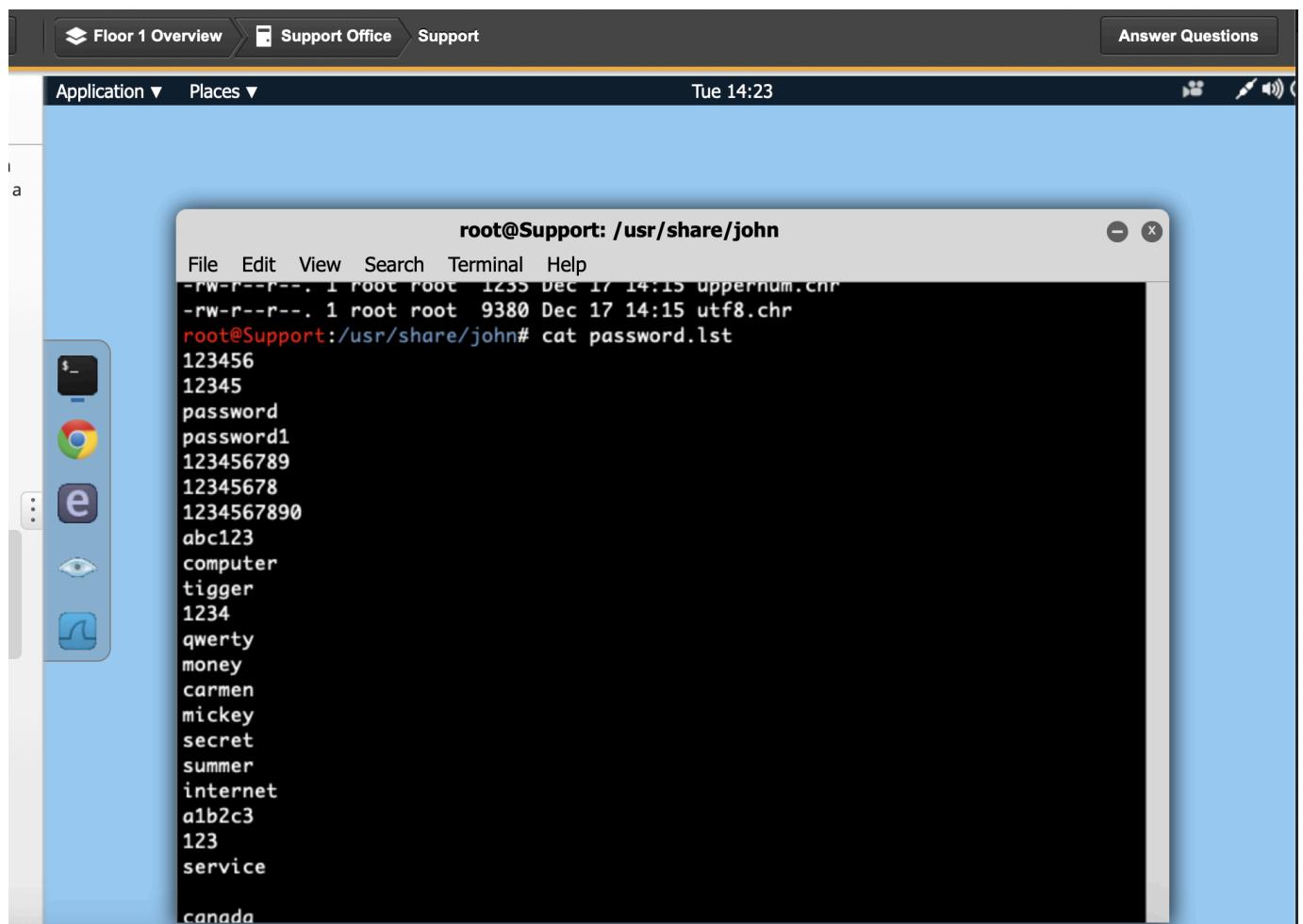


The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "root@Support: ~". The terminal content shows the user running the command "ls -la" which lists the contents of the current directory (~). The output includes files like ".bash\_history", ".bash\_logout", ".bash\_profile", ".bashrc", ".cshrc", "install.log", "install.log.syslog", "something.zip", ".tcshrc", and "winhash.txt". The desktop interface includes a dock with icons for a terminal, browser, email, and file manager, and a top bar with application and system status indicators.

```
root@Support:~# cd ~
root@Support:~# ls -la
total 40
dr-xr-x---. 2 root root 4096 Jun  7  2021 .
dr-xr-xr-x. 2 root root     0 Aug 12 08:49 ..
-rw-----. 1 root root 1350 Jun  7  2021 anaconda-ks.cfg
-rw-----. 1 root root 1620 Jun 14  2021 .bash_history
-rw-r--r--. 1 root root   18 Mar 30  2021 .bash_logout
-rw-r--r--. 1 root root  176 Mar 30  2021 .bash_profile
-rw-r--r--. 1 root root  176 Sep 22  2021 .bashrc
-rw-r--r--. 1 root root   100 Sep 22  2021 .cshrc
-rw-r--r--. 1 root root 28996 Jun  7  2021 install.log
-rw-r--r--. 1 root root  6337 Jun  7  2021 install.log.syslog
-rw-r--r--. 1 root root    482 Dec 17 14:15 something.zip
-rw-r--r--. 1 root root   129 Dec  3  2021 .tcshrc
-rw-r--r--. 1 root root    89 Dec 17 14:15 winhash.txt
root@Support:~# _
```

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](https://github.com/robertmcarpenter)  
Mon December 17th 2024



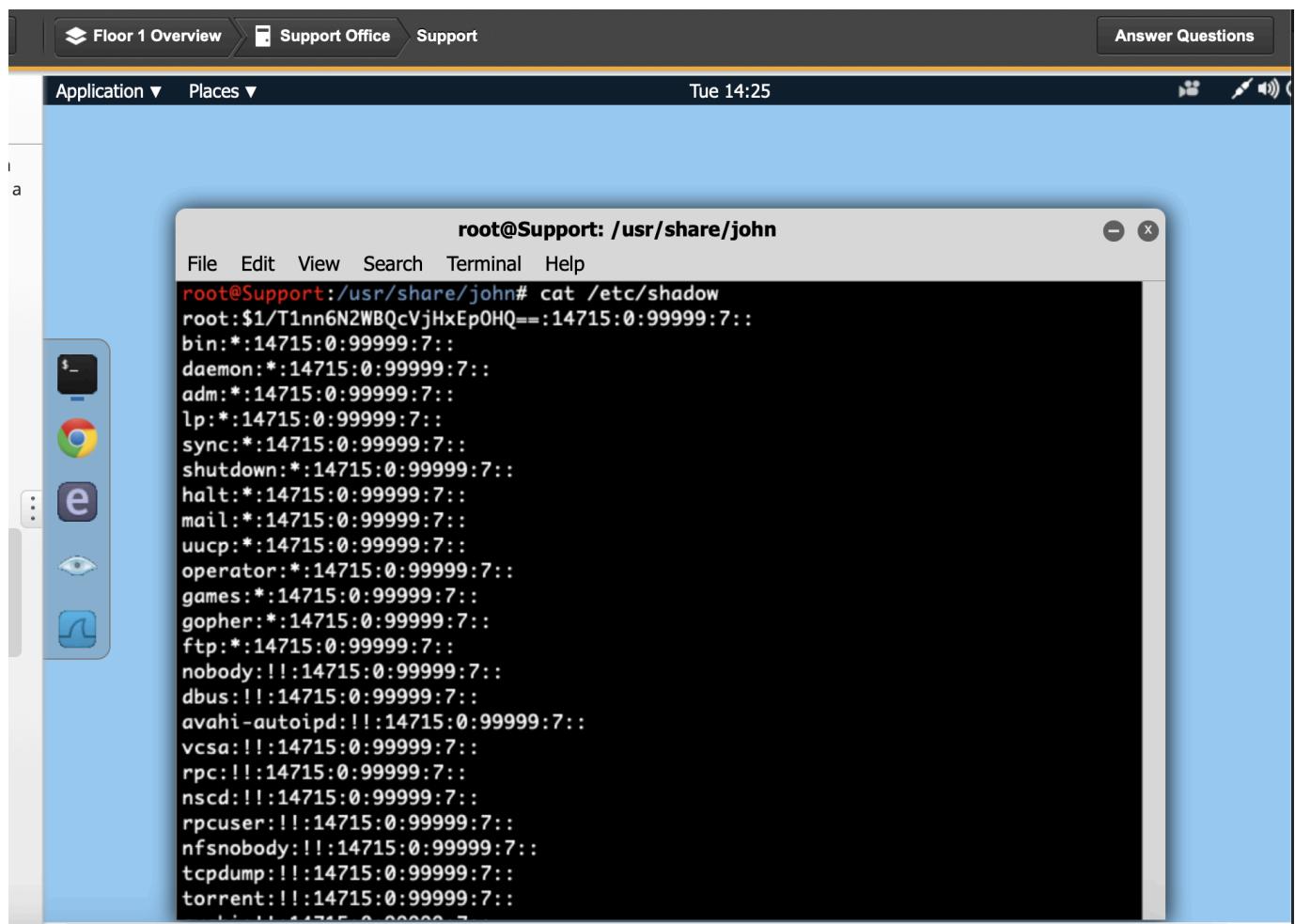
Awesome, we have a predefined Dictionary (also called a wordlist) we can use for the attack.

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](https://github.com/robertmcarpenter)  
Mon December 17th 2024



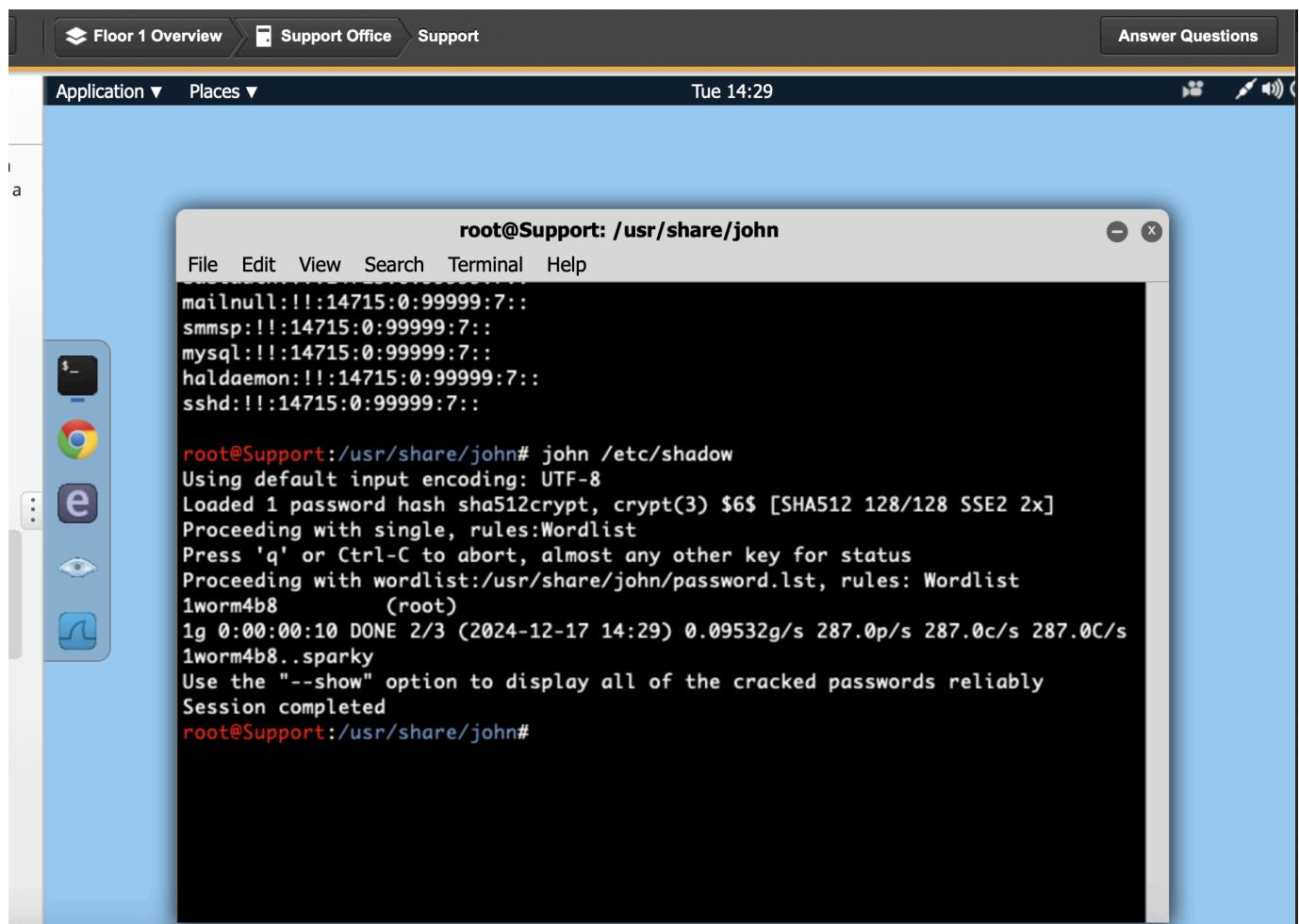
Note that I am currently logged in as the root user. If an attacker is able to use an exploit to escalate their privileges to root they still won't have the password to the root account. This means everytime the attacker wants to open a root shell, they will need to reattack the machine which creates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

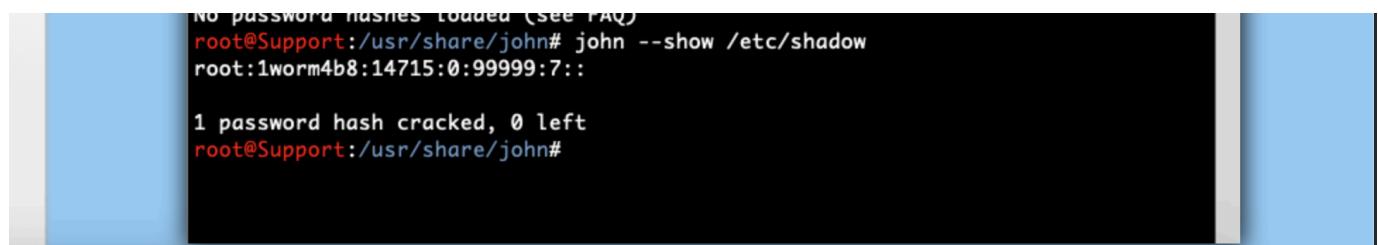
Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Mon December 17th 2024



The screenshot shows a terminal window titled "root@Support: /usr/share/john". The terminal output is as follows:

```
root@Support: /usr/share/john# john /etc/shadow
Using default input encoding: UTF-8
Loaded 1 password hash sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x]
Proceeding with single, rules:Wordlist
Press 'q' or Ctrl-C to abort, almost any other key for status
Proceeding with wordlist:/usr/share/john/password.lst, rules: Wordlist
1worm4b8      (root)
1g 0:00:00:10 DONE 2/3 (2024-12-17 14:29) 0.09532g/s 287.0p/s 287.0c/s 287.0C/s
1worm4b8..sparky
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@Support: /usr/share/john#
```

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.



```
No password hashes loaded (see FAQ)
root@Support: /usr/share/john# john --show /etc/shadow
root:1worm4b8:14715:0:99999:7::
```

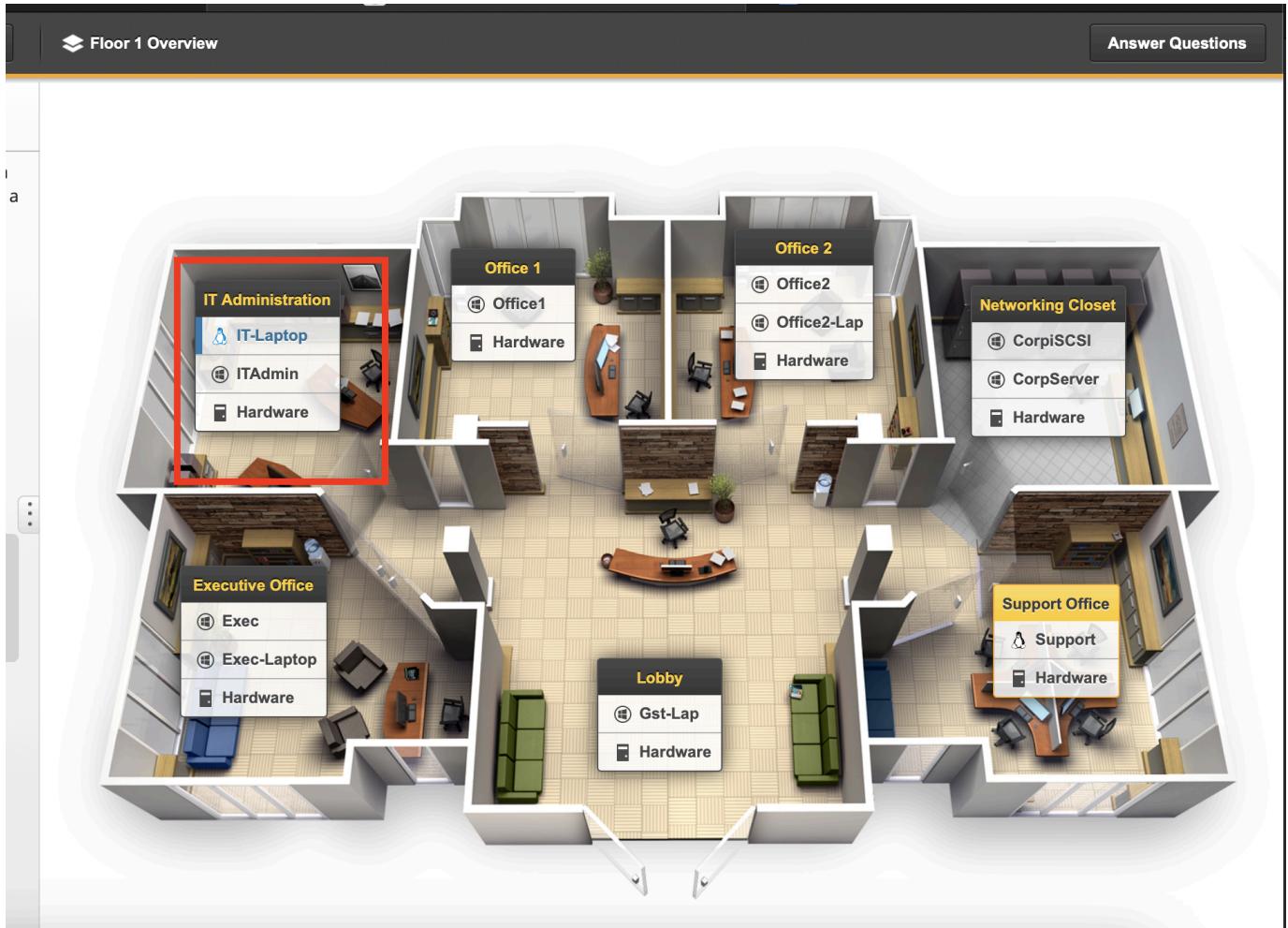
1 password hash cracked, 0 left

```
root@Support: /usr/share/john#
```

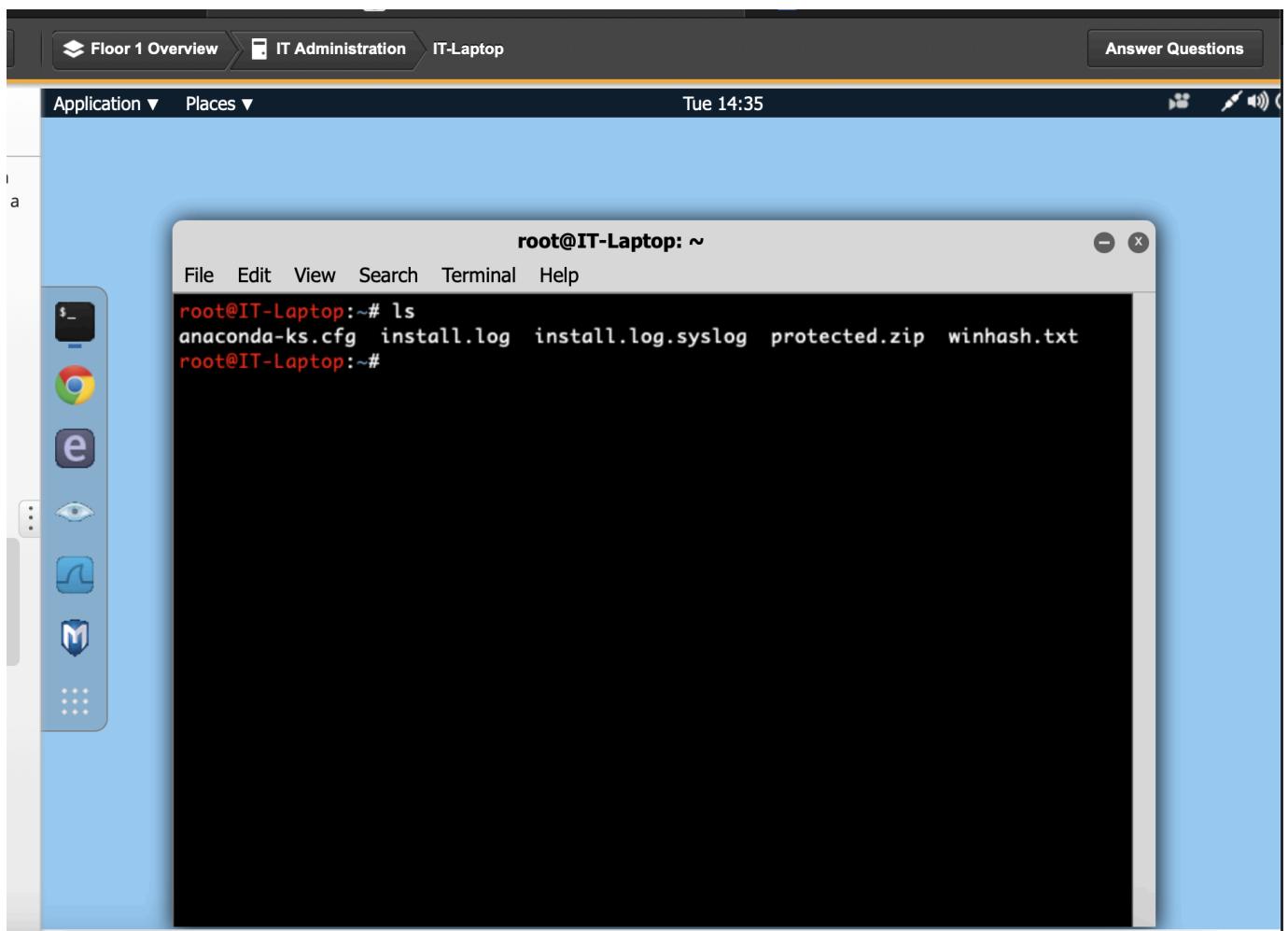
Success we've cracked the root password!

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

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](https://github.com/robertmcarpenter)  
Mon December 17th 2024



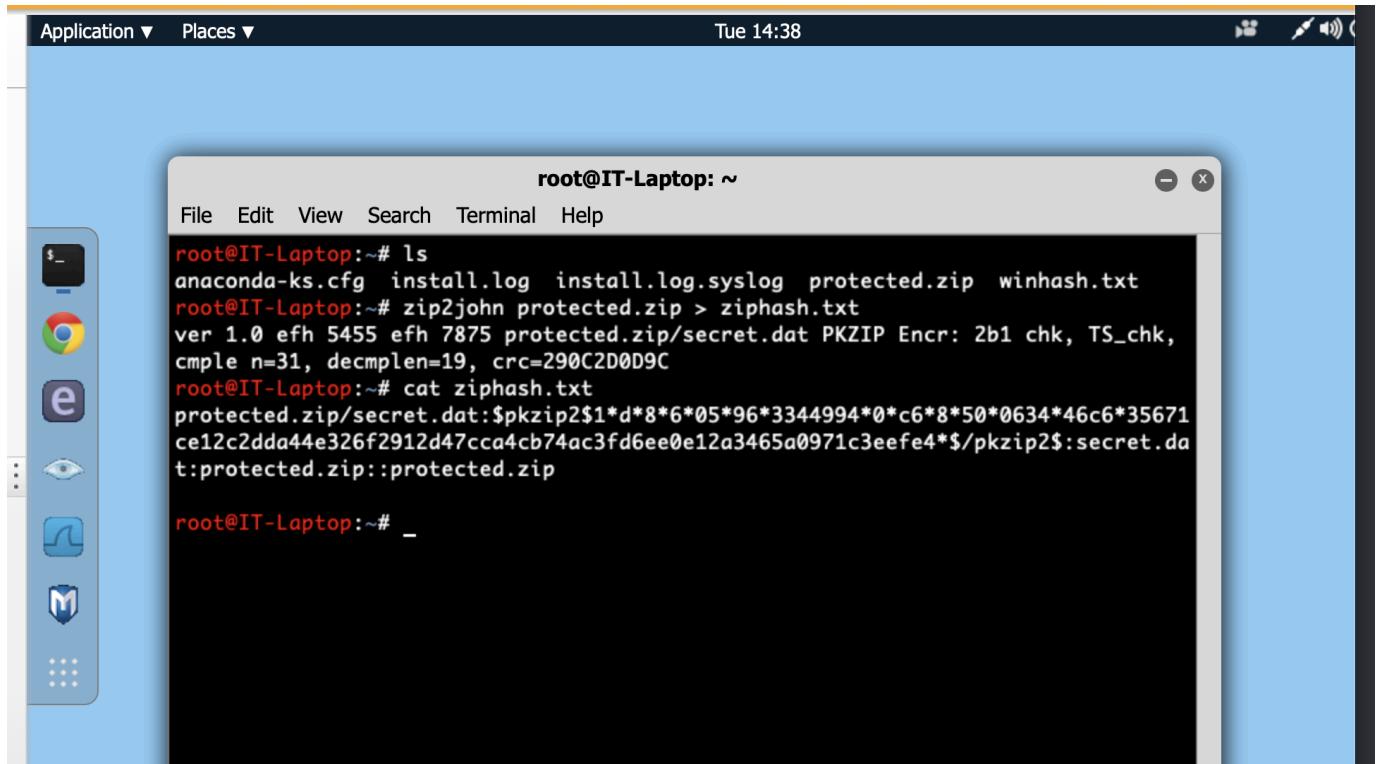
Now that I'm here I issued an **ls** command to view the contents of this home directory.

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](https://github.com/robertmcarpenter)  
Mon December 17th 2024



```
root@IT-Laptop:~# ls
anaconda-ks.cfg  install.log  install.log.syslog  protected.zip  winhash.txt
root@IT-Laptop:~# zip2john protected.zip > ziphash.txt
ver 1.0 efh 5455 efh 7875 protected.zip/secret.dat PKZIP Encr: 2b1 chk, TS_chk,
cmple n=31, decmplen=19, crc=290C2D0D9C
root@IT-Laptop:~# cat ziphash.txt
protected.zip/secret.dat:$pkzip2$1*d*8*6*05*96*3344994*0*c6*8*50*0634*46c6*35671
ce12c2dda44e326f2912d47cca4cb74ac3fd6ee0e12a3465a0971c3eefe4*$/:pkzip2$::secret.da
t:protected.zip::protected.zip

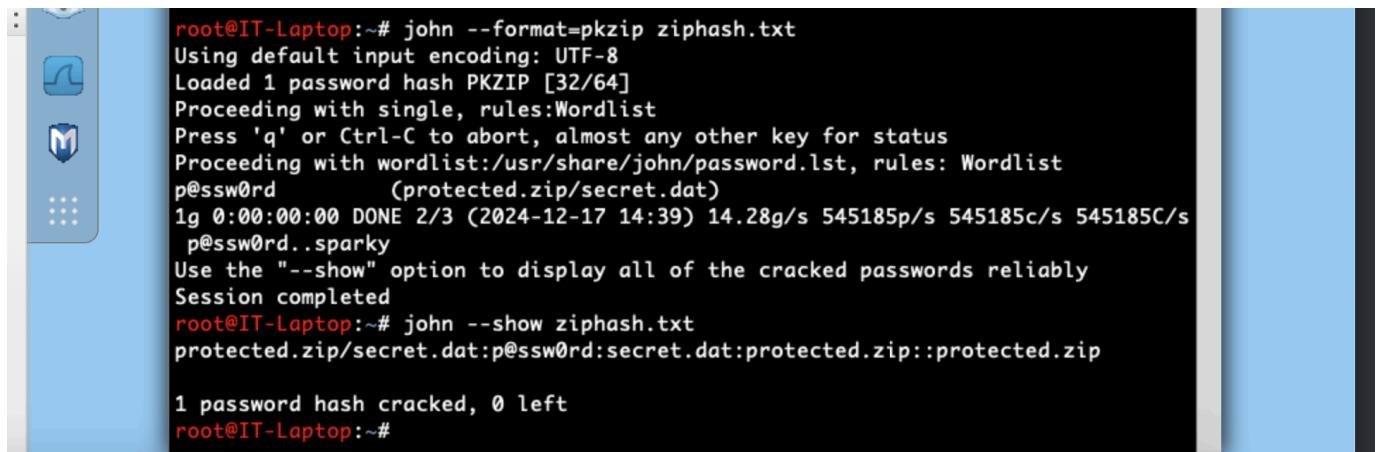
root@IT-Laptop:~# _
```

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...**

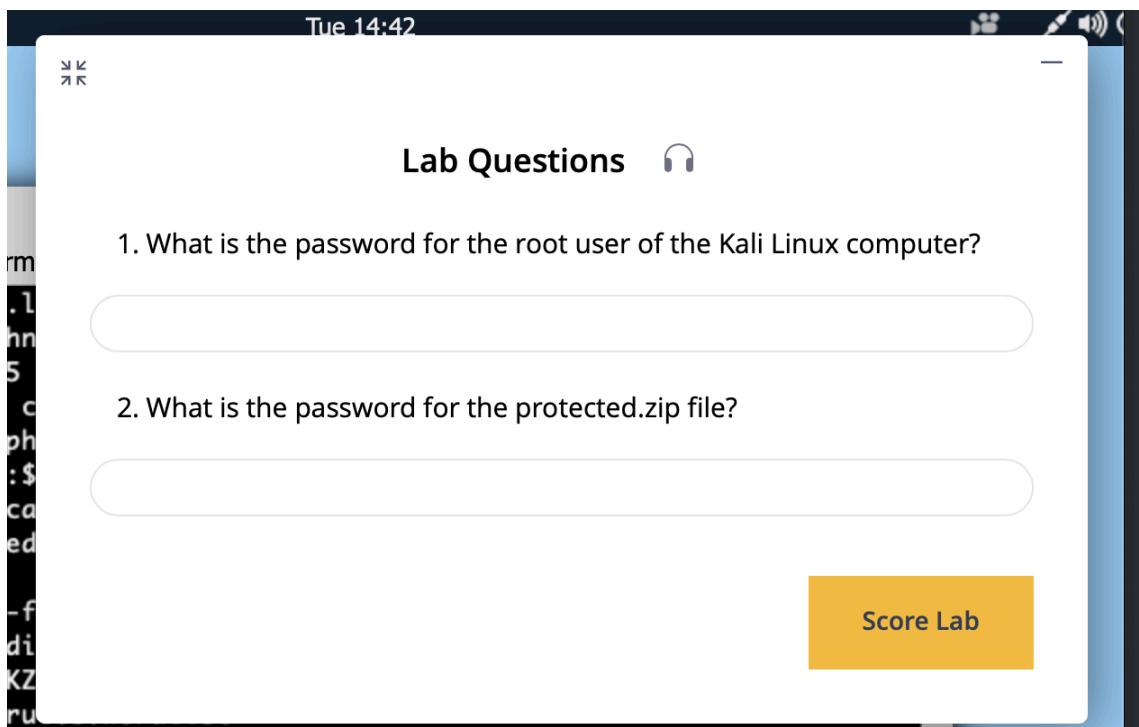
**John --show ziphash.txt**



```
root@IT-Laptop:~# john --format=pkzip ziphash.txt
Using default input encoding: UTF-8
Loaded 1 password hash PKZIP [32/64]
Proceeding with single, rules:Wordlist
Press 'q' or Ctrl-C to abort, almost any other key for status
Proceeding with wordlist:/usr/share/john/password.lst, rules: Wordlist
p@ssw0rd      (protected.zip/secret.dat)
1g 0:00:00:00 DONE 2/3 (2024-12-17 14:39) 14.28g/s 545185p/s 545185c/s 545185C/s
p@ssw0rd..sparky
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@IT-Laptop:~# john --show ziphash.txt
protected.zip/secret.dat:p@ssw0rd:secret.dat::protected.zip

1 password hash cracked, 0 left
root@IT-Laptop:~#
```

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!



Tue 14:42

## Lab Questions

1. What is the password for the root user of the Kali Linux computer?

2. What is the password for the protected.zip file?

Score Lab

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

Robert Carpenter  
[github.com/robertmcarpenter](https://github.com/robertmcarpenter)  
Mon December 17th 2024

