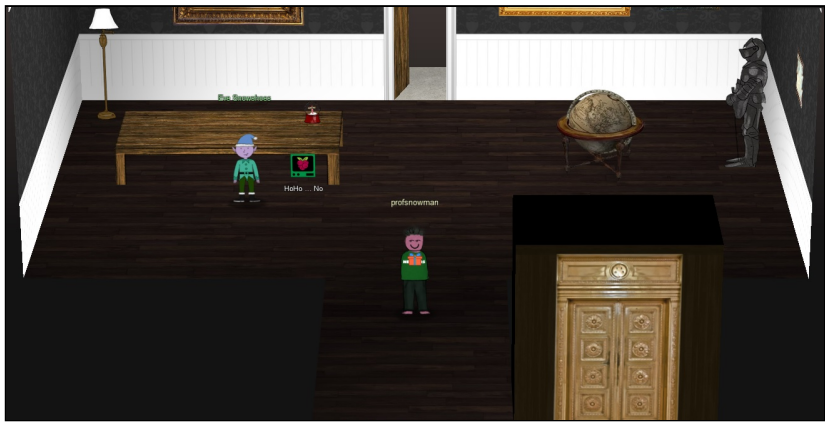
KringleCon 4: Calling Birds!

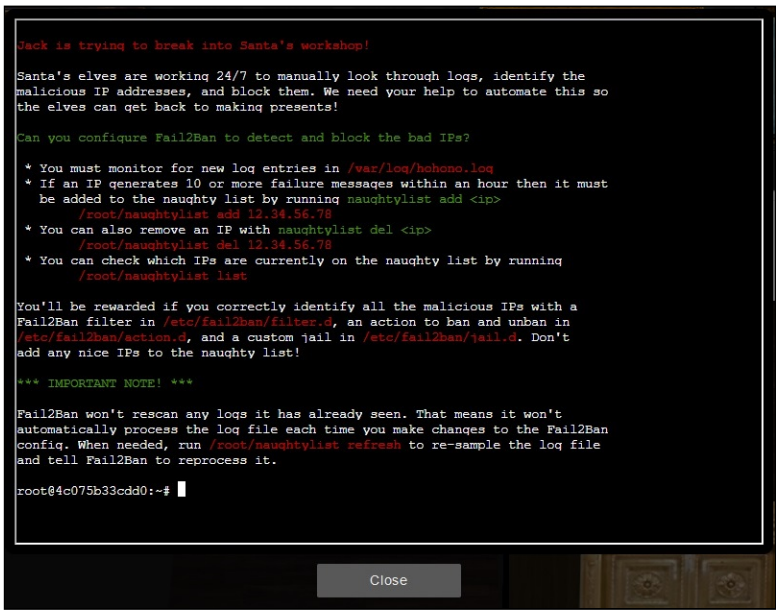
Santa's Office



1. Click to talk to Eve Snowshoes

```
Hey there, how's it going? I'm Eve Snowshoes.

Lately I've been spending a lot of cycles worrying about what's going on next door.

Before that, I was checking out Fail2Ban.

It's this slick log scanning tool for Apache web servers.

If you can complete this terminal challenge, I'd be happy to give you some things I've learned
about Kerberoasting and Active Directory permissions!

Why don't you do some work with Fail2Ban on this Cranberry Pi terminal first, then we'll talk
Kerberoasting and Active Directory. OK?
```

2. Click HoHo ... No Cranberry Pi terminal



3. Type `grep -i fail /var/log/hohono.log | tail -n 1`

```
2022-01-03 00:12:16 Failed login from 90.210.141.188 for morcel
```

4. Type `grep -v Failed /var/log/hohono.log | tail -n 1`

```
2022-01-03 00:12:34 Valid heartbeat from 44.239.132.43
```

5. Type `grep -Ev 'Failed|Valid' /var/log/hohono.log | tail -n 1`

```
2022-01-03 00:12:34 Login from 70.104.144.117 successful
```

6. Type `grep -Ei 'invalid|Invalid' /var/log/hohono.log | tail -n 1`

```
2022-01-03 00:10:45 Invalid heartbeat 'delta' from 170.181.65.180
```

7. Type `grep -Ev 'Failed|Valid|Invalid' /var/log/hohono.log | tail -n 1`

```
2022-01-03 00:12:34 Login from 70.104.144.117 successful
```

8. Type `grep -Ev 'Failed|Valid|Invalid|Login' /var/log/hohono.log | tail -n 1`

```
2022-01-03 00:12:32 69.44.10.44: Request completed successfully
```

9. Type `grep -Ev 'Failed|Valid|Invalid|Login|Request' /var/log/hohono.log | tail -n 1`

```
2022-01-03 00:12:14 90.210.141.188 sent a malformed request
```

10. Type the following at the prompt

```
echo [customjail] > /etc/fail2ban/jail.d/customjail.conf
echo enabled = true >> /etc/fail2ban/jail.d/customjail.conf
echo logpath = /var/log/hohono.log >> /etc/fail2ban/jail.d/customjail.conf
echo maxretry = 10 >> /etc/fail2ban/jail.d/customjail.conf
echo findtime = 1h >> /etc/fail2ban/jail.d/customjail.conf
echo bantime = 2h >> /etc/fail2ban/jail.d/customjail.conf
echo filter = naughty >> /etc/fail2ban/jail.d/customjail.conf
echo action = ban_naughty >> /etc/fail2ban/jail.d/customjail.conf
echo [Definition] > /etc/fail2ban/filter.d/naughty.conf
echo 'failregex = ^ Login from <HOST> rejected due to unknown user name$' \
>> /etc/fail2ban/filter.d/naughty.conf
echo '            ^ Invalid heartbeat .+ from <HOST>$' >> /etc/fail2ban/filter.d/naughty.conf
echo '            ^ <HOST> sent a malformed request$' >> /etc/fail2ban/filter.d/naughty.conf
echo '            ^ Failed login from <HOST> for .+$' >> /etc/fail2ban/filter.d/naughty.conf
echo [Definition] > /etc/fail2ban/action.d/ban_naughty.conf
echo 'actionban   = /root/naughtylist add <ip>' >> /etc/fail2ban/action.d/ban_naughty.conf
echo 'actionunban = /root/naughtylist del <ip>' >> /etc/fail2ban/action.d/ban_naughty.conf
```

11. Type `service fail2ban restart`

```
 * Restarting Authentication failure monitor fail2ban                                [ OK ]
```

12. Type `/root/naughtylist refresh`

```
Refreshing the log file...
root@073a147ace98:~# Log file refreshed! It may take fail2ban a few moments to re-process.
68.61.202.91 has been added to the naughty list!
155.174.179.182 has been added to the naughty list!
191.242.85.38 has been added to the naughty list!
196.7.137.96 has been added to the naughty list!
194.55.176.35 has been added to the naughty list!
71.100.210.118 has been added to the naughty list!
191.43.15.47 has been added to the naughty list!
78.246.220.95 has been added to the naughty list!
100.162.31.112 has been added to the naughty list!
144.169.221.61 has been added to the naughty list!
139.252.250.104 has been added to the naughty list!
183.22.120.43 has been added to the naughty list!
159.141.238.84 has been added to the naughty list!
49.138.126.188 has been added to the naughty list!
47.22.64.250 has been added to the naughty list!
141.29.248.122 has been added to the naughty list!
You correctly identifed 16 IPs out of 16 bad IPs
You incorrectly added 0 benign IPs to the naughty list




**********************************************************************
* You stopped the attacking systems! You saved our systems!
*
* Thank you for all of your help. You are a talented defender!
**********************************************************************
```

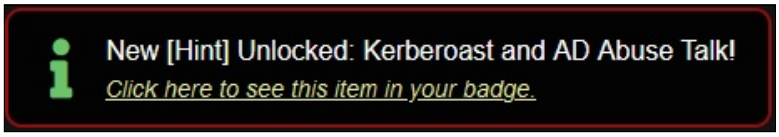
13. Click the `Close` button

14. Click to talk to `Eve Snowshoes`

```
Fantastic! Thanks for the help!

Hey, would you like to know more about Kerberoasting and Active Directory permissions abuse?
```

15. Click to talk to Eve Snowshoes

```
There's a great talk by Chris Davis on this exact subject!
```



16. Click to talk to Eve Snowshoes

```
There are also plenty of resources available to learn more about Kerberoasting specifically.
```

17. Click to talk to Eve Snowshoes

```
If you have any trouble finding the domain controller on the 10.X.X.X network, remember that,
when not running as root, nmap default probing relies on connecting to TCP 80 and 443.
```

18. Click to talk to Eve Snowshoes

```
Got a hash that won't crack with your wordlist? OneRuleToRuleThemAll.rule is a great way to grow
your keyspace.
```

19. Click to talk to Eve Snowshoes

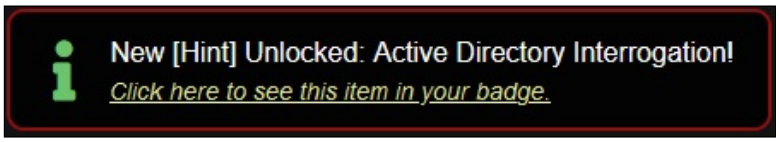
> Where'd you get your wordlist? CeWL might generate a great wordlist from the ElfU website, but it will ignore digits in terms by default.

20. Click to talk to Eve Snowshoes

> So, apropos of nothing, have you ever known system administrators who store credentials in scripts? I know, I know, you understand the folly and would never do it!

21. Click to talk to Eve Snowshoes

> The easy way to investigate Active Directory misconfigurations (for Blue and Red alike!) is with Bloodhound, but there are native methods as well.

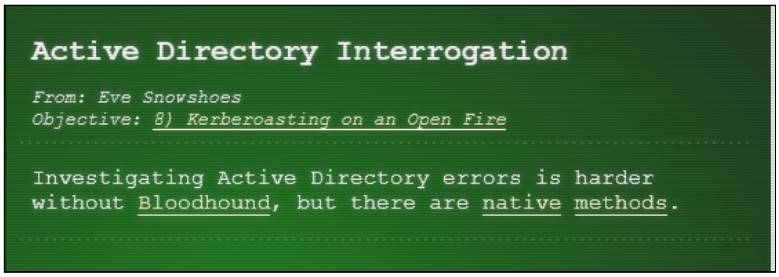


22. Click to talk to Eve Snowshoes

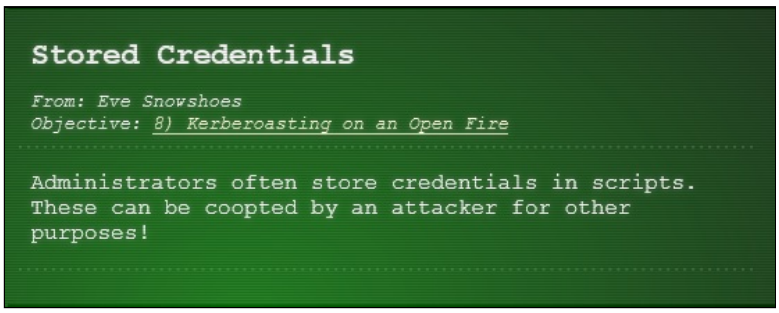
> Oh, and one last thing: once you've granted permissions to your user, it might take up to five minutes for it to propogate throughout the domain.

23. Click the i (Hints) icon

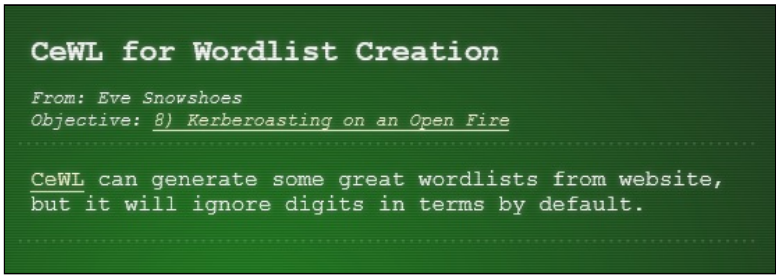
24. Click Active Directory Interrogation



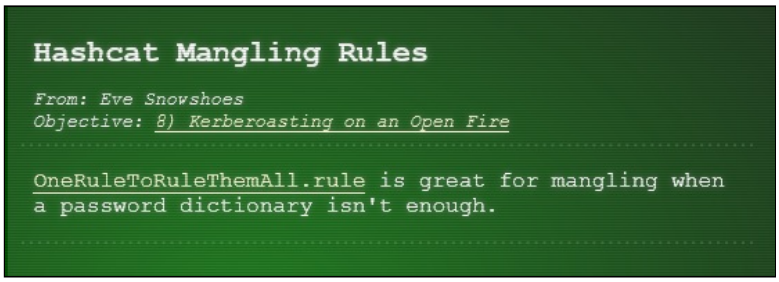
25. Click Stored Credentials



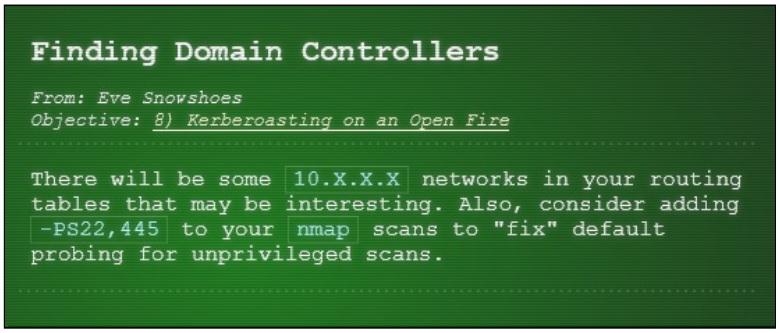
26. Click CeWL for Wordlist Creation



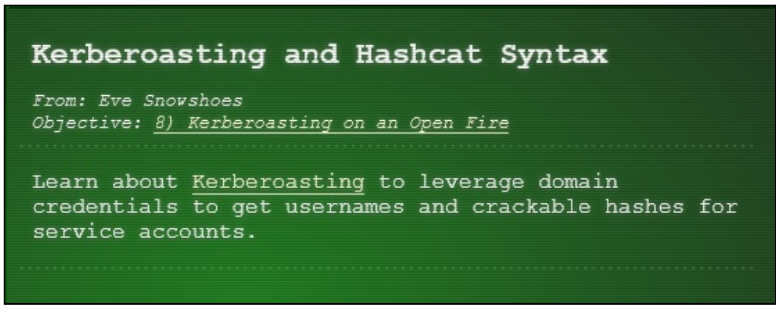
27. Click Hashcat Mangling Rules



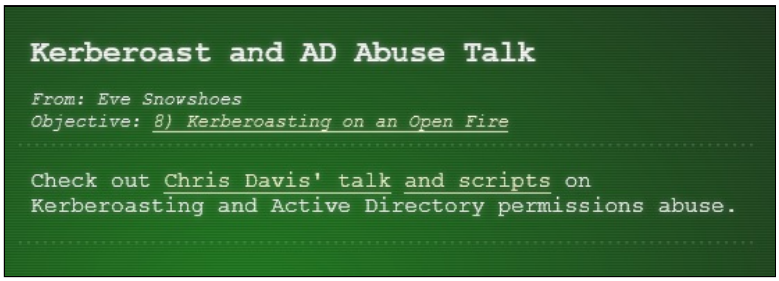
28. Click Finding Domain Controllers



29. Click Kerberoasting and Hashcat Syntax



30. Click `Kerberoast and AD Abuse Talk`



31. Click `[Exit]`

32. Click `Map` (Destinations) icon and then click `NetWars`