

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

```
Jack is trying to break into Santa's workshop!

Santa's elves are working 24/7 to manually look through logs, identify the
malicious IP addresses, and block them. We need your help to automate this so
the elves can get back to making presents!

Can you configure Fail2Ban to detect and block the bad IPs?

* You must monitor for new log entries in /var/log/hohono.log
* If an IP generates 10 or more failure messages within an hour then it must
  be added to the naughty list by running naughtylist add <ip>
  /root/naughtylist add 12.34.56.78
* You can also remove an IP with naughtylist del <ip>
  /root/naughtylist del 12.34.56.78
* You can check which IPs are currently on the naughty list by running
  /root/naughtylist list

You'll be rewarded if you correctly identify all the malicious IPs with a
Fail2Ban filter in /etc/fail2ban/filter.d, an action to ban and unban in
/etc/fail2ban/action.d, and a custom jail in /etc/fail2ban/jail.d. Don't
add any nice IPs to the naughty list!

*** IMPORTANT NOTE! ***

Fail2Ban won't rescans any logs it has already seen. That means it won't
automatically process the log file each time you make changes to the Fail2Ban
config. When needed, run /root/naughtylist refresh to re-sample the log file
and tell Fail2Ban to reprocess it.

root@4c075b33cdd0:~#
```

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`

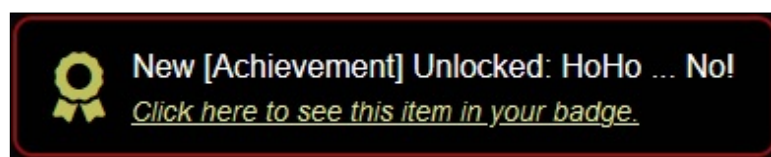
* Restarting Authentication failure monitor fail2ban

[OK]

12. Type `/root/naughtylist refresh`

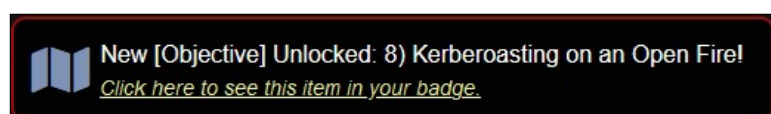
```
Refreshing the log file...
root@073a147ace98:~# Log file refreshed! It may take fail2ban a few moments to re-process.
68.61.202.91 has been added to the naughty list!
155.174.179.182 has been added to the naughty list!
191.242.85.38 has been added to the naughty list!
196.7.137.96 has been added 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 identified 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** button14. 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!



New [Hint] Unlocked: Kerberoast and AD Abuse Talk!

[Click here to see this item in your badge.](#)

16. Click to talk to **Eve Snowshoes**

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



New [Hint] Unlocked: Kerberoasting and Hashcat Syntax!

[Click here to see this item in your badge.](#)

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.



New [Hint] Unlocked: Finding Domain Controllers!

[Click here to see this item in your badge.](#)

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.



New [Hint] Unlocked: Hashcat Mangling Rules!

[Click here to see this item in your badge.](#)

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.



New [Hint] Unlocked: CeWL for Wordlist Creation!

[Click here to see this item in your badge.](#)

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!



New [Hint] Unlocked: Stored Credentials!

[Click here to see this item in your badge.](#)

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.



New [Hint] Unlocked: Active Directory Interrogation!

[Click here to see this item in your badge.](#)

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 propagate throughout the domain.

23. Click the **i** (Hints) icon24. Click **Active Directory Interrogation**

Active Directory Interrogation

From: Eve Snowshoes

Objective: 8) Kerberoasting on an Open Fire

Investigating Active Directory errors is harder without Bloodhound, but there are native methods.

25. Click **Stored Credentials****Stored Credentials**

From: Eve Snowshoes

Objective: 8) Kerberoasting on an Open Fire

Administrators often store credentials in scripts. These can be coopted by an attacker for other purposes!

26. Click **CeWL for Wordlist Creation****CeWL for Wordlist Creation**

From: Eve Snowshoes

Objective: 8) Kerberoasting on an Open Fire

CeWL can generate some great wordlists from website, but it will ignore digits in terms by default.

27. Click **Hashcat Mangling Rules****Hashcat Mangling Rules**

From: Eve Snowshoes

Objective: 8) Kerberoasting on an Open Fire

OneRuleToRuleThemAll.rule is great for mangling when a password dictionary isn't enough.

28. Click **Finding Domain Controllers****Finding Domain Controllers**

From: Eve Snowshoes

Objective: 8) Kerberoasting on an Open Fire

There will be some `10.X.X.X` networks in your routing tables that may be interesting. Also, consider adding `-PS22,445` to your `nmap` scans to "fix" default probing for unprivileged scans.

29. Click **Kerberoasting and Hashcat Syntax****Kerberoasting and Hashcat Syntax**

From: Eve Snowshoes

Objective: 8) Kerberoasting on an Open Fire

Learn about Kerberoasting to leverage domain credentials to get usernames and crackable hashes for service accounts.

30. Click **Kerberoast and AD Abuse Talk**



31. Click **[Exit]**

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