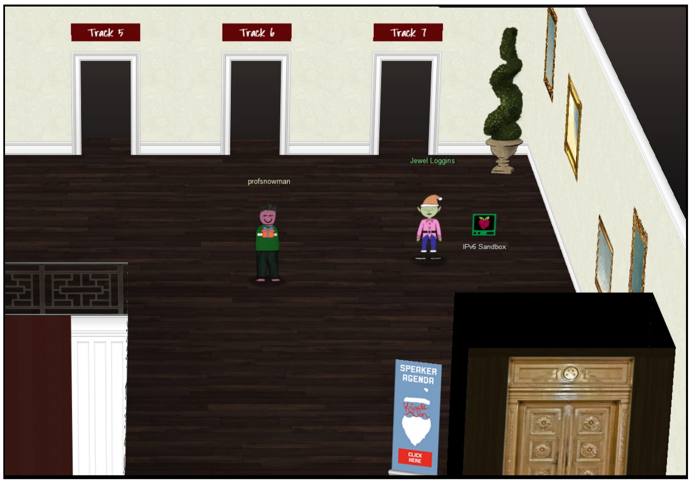
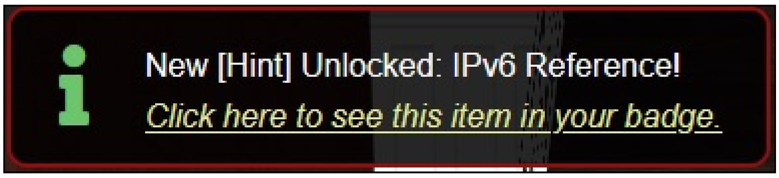
KringleCon 4: Calling Birds!

Talks Lobby



1. Click to talk to `Jewel Loggins`

```
Well hello! I'm Jewel Loggins.

I have to say though, I'm a bit distressed.

The con next door? Oh sure, I’m concerned about that too, but I was talking about the issues I’m
having with IPv6.

I mean, I know it's an old protocol now, but I've just never checked it out.

So now I'm trying to do simple things like Nmap and cURL using IPv6, and I can't quite get them
working!

Would you mind taking a look for me on this terminal?

I think there's a Github Gist that covers tool usage with IPv6 targets.
```



New [Hint] Unlocked: IPv6 Reference!

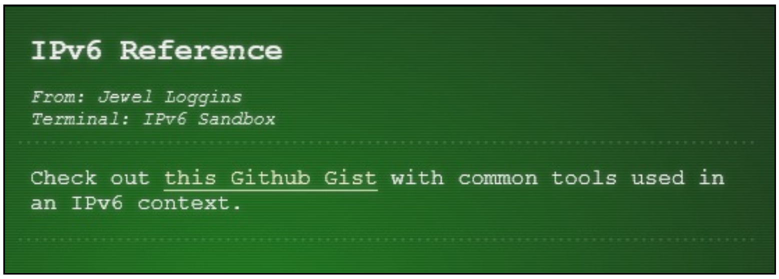
Click here to see this item in your badge.

2. Click to talk to `Jewel Loggins`

```
The tricky parts are knowing when to use [] around IPv6 addresses and where to specify the source
interface.

I’ve got a deal for you. If you show me how to solve this terminal, I’ll provide you with some
nice tips about a topic I’ve been researching a lot lately – Ducky Scripts! They can be really
interesting and fun!
```

3. Click the `i` (Hints) icon

4. Click `IPv6 Reference`



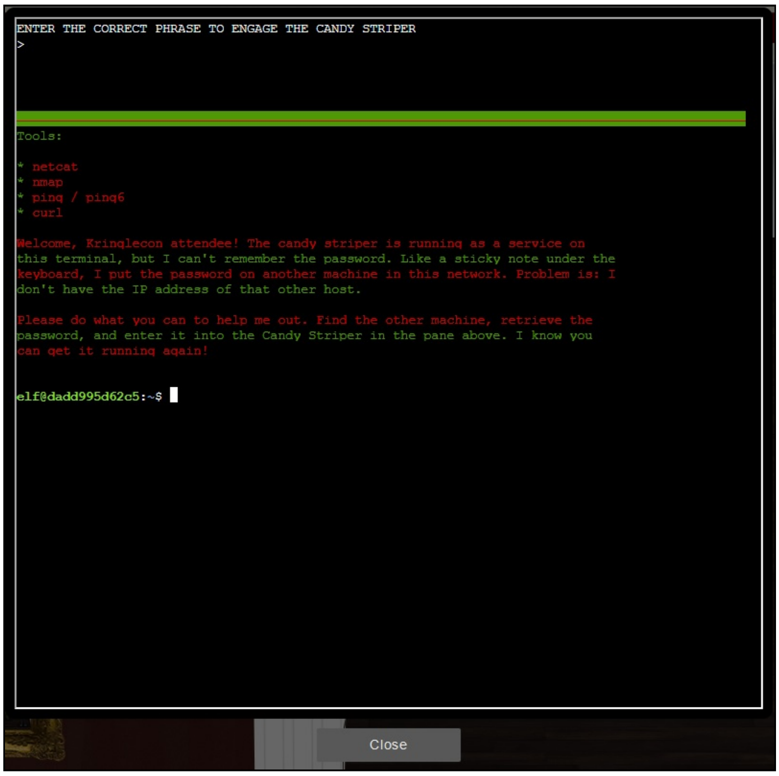
IPv6 Reference

From: Jewel Loggins
Terminal: IPv6 Sandbox

Check out this Github Gist with common tools used in an IPv6 context.

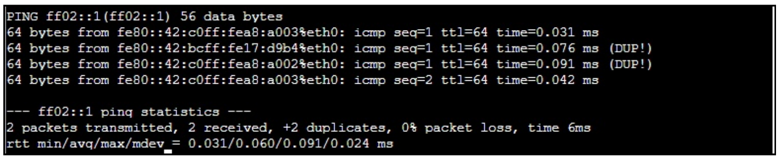
5. Click `[Exit]`

6. Click `IPv6 Sandbox` Cranberry Pi terminal



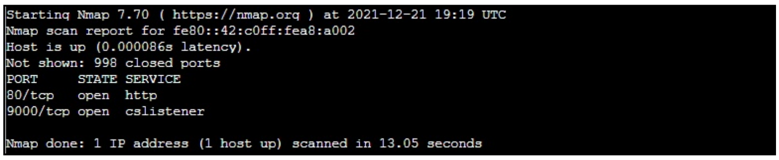
```
ENTER THE CORRECT PHRASE TO ENGAGE THE CANDY STRIPER
>

Tools:

* netcat
* nmap
* ping / ping6
* curl

Welcome, Kringlecon attendee! The candy striper is running as a service on
this terminal, but I can't remember the password. Like a sticky note under the
keyboard, I put the password on another machine in this network. Problem is: I
don't have the IP address of that other host.

Please do what you can to help me out. Find the other machine, retrieve the
password, and enter it into the Candy Striper in the pane above. I know you
can get it running again!


elf@dadd995d62c5:~$
```

7. Type `ping6 ff02::1 -c2`



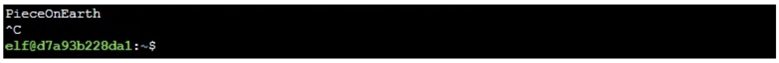
```
PING ff02::1(ff02::1) 56 data bytes
64 bytes from fe80::42:c0ff:fea8:a003%eth0: icmp seq=1 ttl=64 time=0.031 ms
64 bytes from fe80::42:bcff:fe17:d9b4%eth0: icmp seq=1 ttl=64 time=0.076 ms (DUP!)
64 bytes from fe80::42:c0ff:fea8:a002%eth0: icmp seq=1 ttl=64 time=0.091 ms (DUP!)
64 bytes from fe80::42:c0ff:fea8:a003%eth0: icmp seq=2 ttl=64 time=0.042 ms

--- ff02::1 ping statistics ---
2 packets transmitted, 2 received, +2 duplicates, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 0.031/0.060/0.091/0.024 ms
```

8. Type `nmap -6 fe80::42:c0ff:fea8:a002%eth0`



```
Starting Nmap 7.70 ( https://nmap.org ) at 2021-12-21 19:19 UTC
Nmap scan report for fe80::42:c0ff:fea8:a002
Host is up (0.000086s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
9000/tcp open  cslistener

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
```

9. Type `nc -6 fe80::42:c0ff:fea8:a002%eth0 9000` and then press `CTRL + C`



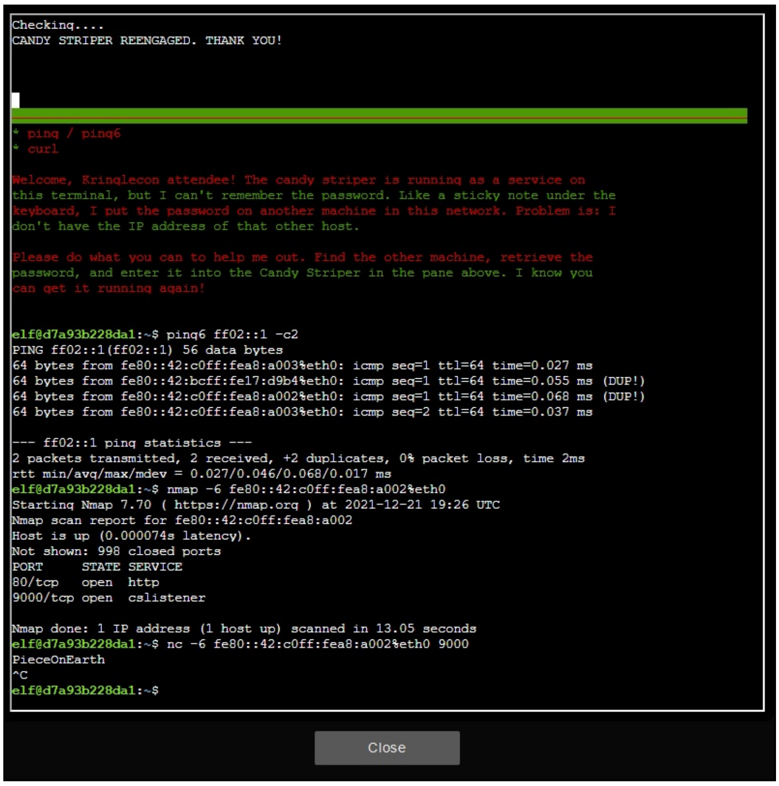
```
PieceOnEarth
^C
elf@d7a93b228da1:~$
```

10. Click in the `Top` windows

11. Type `PieceOnEarth`

New [Achievement] Unlocked: IPv6 Sandbox!

Click here to see this item in your badge.



```
Checking....
CANDY STRIPER REENGAGED. THANK YOU!



* ping / ping6
* curl

Welcome, Kringlecon attendee! The candy striper is running as a service on
this terminal, but I can't remember the password. Like a sticky note under the
keyboard, I put the password on another machine in this network. Problem is: I
don't have the IP address of that other host.

Please do what you can to help me out. Find the other machine, retrieve the
password, and enter it into the Candy Striper in the pane above. I know you
can get it running again!


elf@d7a93b228da1:~$ ping6 ff02::1 -c2
PING ff02::1(ff02::1) 56 data bytes
64 bytes from fe80::42:c0ff:fea8:a003%eth0: icmp seq=1 ttl=64 time=0.027 ms
64 bytes from fe80::42:bcff:fe17:d9b4%eth0: icmp seq=1 ttl=64 time=0.055 ms (DUP!)
64 bytes from fe80::42:c0ff:fea8:a002%eth0: icmp seq=1 ttl=64 time=0.068 ms (DUP!)
64 bytes from fe80::42:c0ff:fea8:a003%eth0: icmp seq=2 ttl=64 time=0.037 ms

--- ff02::1 ping statistics ---
2 packets transmitted, 2 received, +2 duplicates, 0% packet loss, time 2ms
rtt min/avg/max/mdev = 0.027/0.046/0.068/0.017 ms
elf@d7a93b228da1:~$ nmap -6 fe80::42:c0ff:fea8:a002%eth0
Starting Nmap 7.70 ( https://nmap.org ) at 2021-12-21 19:26 UTC
Nmap scan report for fe80::42:c0ff:fea8:a002
Host is up (0.000074s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
9000/tcp open  cslistener

Nmap done: 1 IP address (1 host up) scanned in 13.05 seconds
elf@d7a93b228da1:~$ nc -6 fe80::42:c0ff:fea8:a002%eth0 9000
PieceOnEarth
^C
elf@d7a93b228da1:~$
```

12. Click the `Close` button

13. Click to talk to `Jewel Loggins`

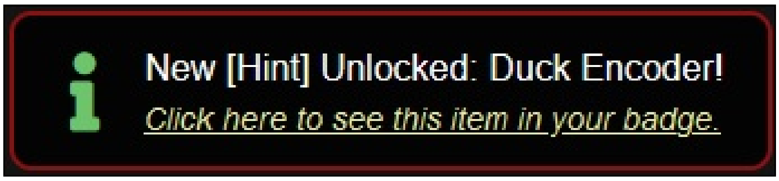
```
Great work! It seems simpler now that I've seen it once. Thanks for showing me!

Prof. Petabyte warned us about random USB devices. They might be malicious keystroke injectors!

A troll could program a keystroke injector to deliver malicious keystrokes when it is plugged in.
```

New [Hint] Unlocked: Ducky Script!

Click here to see this item in your badge.

14. Click to talk to `Jewel Loggins`

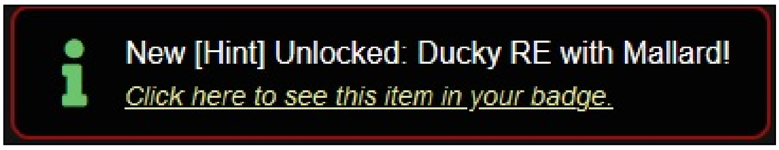
```
Ducky Script is a language used to specify those keystrokes.
```



New [Hint] Unlocked: Duck Encoder!
Click here to see this item in your badge.

15. Click to talk to `Jewel Loggins`

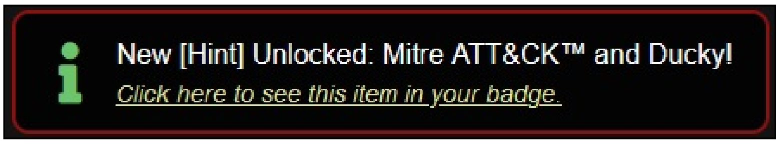
```
What commands would a troll try to run on our workstations?
```



New [Hint] Unlocked: Ducky RE with Mallard!
Click here to see this item in your badge.

16. Click to talk to `Jewel Loggins`

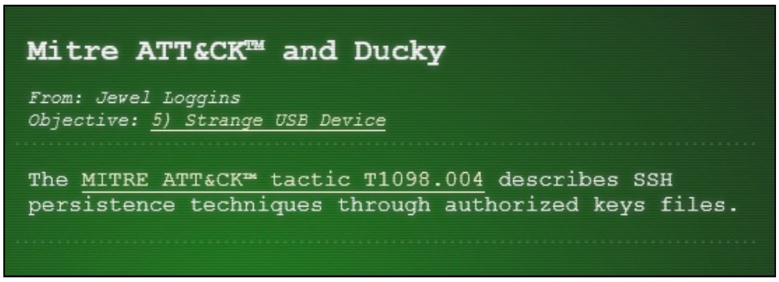
```
I heard that SSH keys can be used as backdoors. Maybe that's useful?
```



New [Hint] Unlocked: Mitre ATT&CK™ and Ducky!
Click here to see this item in your badge.

17. Click the `i` (Hints) icon

18. Click `Mitre ATT&CK™ and Ducky`

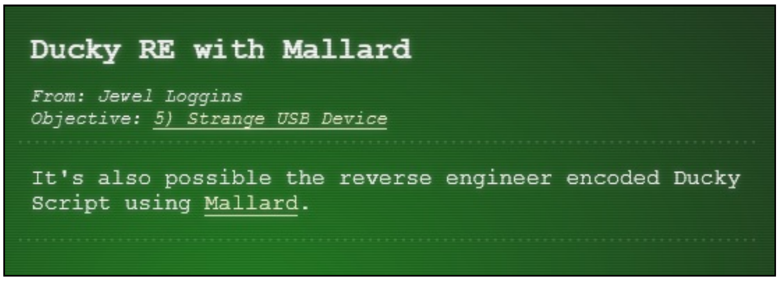


Mitre ATT&CK™ and Ducky

From: Jewel Loggins
Objective: 5) Strange USB Device

The MITRE ATT&CK™ tactic T1098.004 describes SSH persistence techniques through authorized keys files.

19. Click `Ducky RE with Mallard`

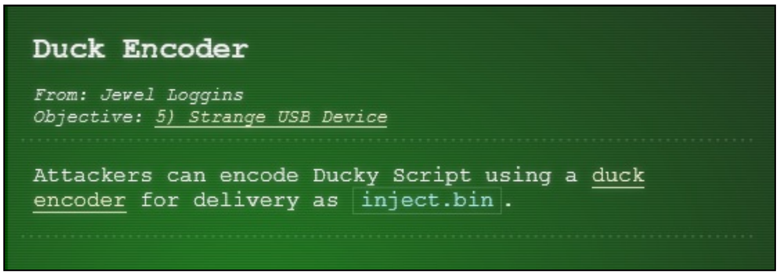


Ducky RE with Mallard

From: Jewel Loggins
Objective: 5) Strange USB Device

It's also possible the reverse engineer encoded Ducky Script using Mallard.

20. Click `Duck Encoder`

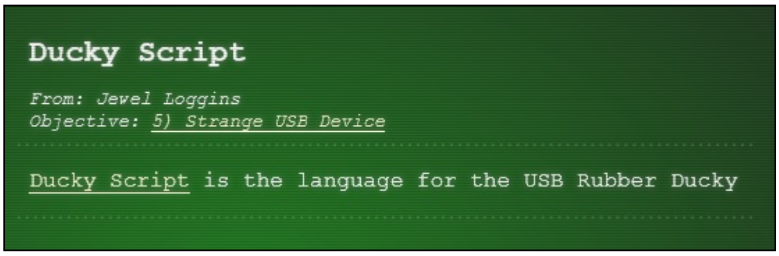


Duck Encoder

From: Jewel Loggins
Objective: 5) Strange USB Device

Attackers can encode Ducky Script using a duck encoder for delivery as `inject.bin`.

21. Click `Ducky Script`



Ducky Script

From: Jewel Loggins
Objective: 5) Strange USB Device

Ducky Script is the language for the USB Rubber Ducky

22. Click `[Exit]`

23. Move `Left` and enter the `Speaker UNPrepareness Room`