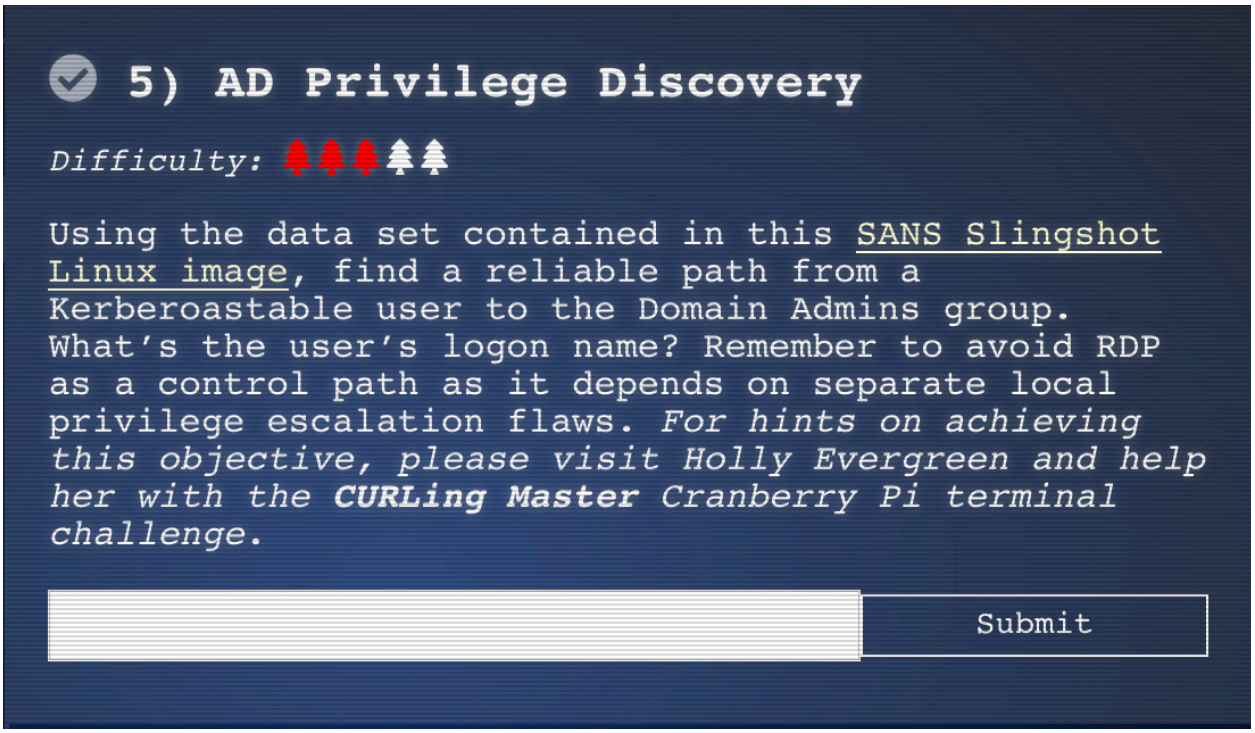
Main Challenge

AD Privilege Discovery



Hint Challenge

The CURLing Master

Cranberry Pi terminal challenge

Hint Challenge

The CURLing Master

Cranberry Pi terminal challenge

Holly Evergreen at 1nd floor go left enter lobby continue forward until you find him .

Hi, I'm Holly Everygreen.

Oh that Bushy!

Sorry to vent, but that brother of mine did something strange.

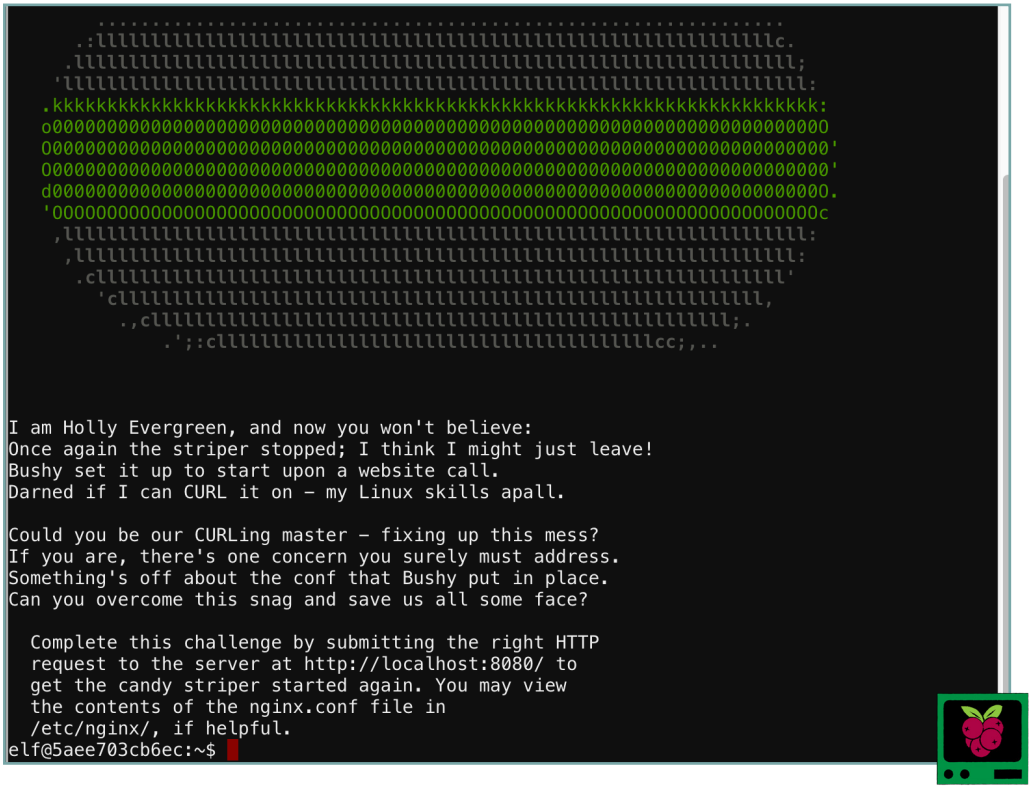
The trigger to restart the Candy Striper is apparently an arcane HTTP call or 2.

I sometimes wonder if all IT folk do strange things with their home networks.

HTTP/2.0 Basics > HTTP/2.0

https://developers.google.com/web/fundamentals/performance/http2/

Terminal Screen



Solution

1. Recommended watch KringleCon - Chris Davis & Chris Elgee talk about HTTP2:

   https://www.youtube.com/watch?v=9E-8HkDs-kQ

2. First let's view `nginx.conf` file in `/etc/nginx/` , write the command in terminal :

   `cat /etc/nginx/nginx.conf`

```
elf@fe1331e8f49b:/etc/nginx$ cat nginx.conf
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
        worker_connections 768;
        # multi_accept on;
}

http {

        sendfile on;
        tcp_nopush on;
        tcp_nodelay on;
        keepalive_timeout 65;
        types_hash_max_size 2048;
        # server_tokens off;

        # server_names_hash_bucket_size 64;
        # server_name_in_redirect off;

        include /etc/nginx/mime.types;
        default_type application/octet-stream;

        server {
        # love using the new stuff! -Bushy
                listen                  8080 http2;
                # server_name           localhost 127.0.0.1;
```

   You will find the server is using `http2` .

3. Let's use `curl` tool to get the server response:

   `curl --http2-prior-knowledge http://localhost:8080/`

```
<html>1331e8f49b:/etc/nginx$ curl --http2-prior-knowledge http://localhost:8080/
 <head>
  <title>Candy Striper Turner-On'er</title>
 </head>
 <body>
 <p>To turn the machine on, simply POST to this URL with parameter "status=on"


 </body>
</html>
elf@fe1331e8f49b:/etc/nginx$
```

   You will find a hint from server response :

   `To turn the machine on, simply POST to this URL with parameter "status=on"`

4. Let's run our `curl` tool again and add "`status=on`" parameter to turn the machine on :

   `curl --http2-prior-knowledge -d "status=on" http://localhost:8080/`

The CURLing Master Cranberry Pi terminal challenge

```
</head>
<body>
<p>To turn the machine on, simply POST to this URL with parameter "status=on"

                                                        okkd,
                                                       OXXXXX,
                                                      oXXXXXXo
                                                     ;XXXXXXX;
                                                    ;KXXXXXXx
                                                   oXXXXXXXO
                                                 .lKXXXXXXX0.
 ''''''      .''''''      .''''''      .::::;   ':okKXXXXXXXX0Oxcooddool,
'MMMMMO',,,,,;WMMMMM0',,,,,;WMMMMMK',,,,,,occccoOXXXXXXXXXXXXxxXXXXXXXXXX.
'MMMMN;,,,,,'0MMMMMW;,,,,,'OMMMMMW:,,,,,'kxcccc0XXXXXXXXXXXXXxx0KKKKK000d;
'MMMMl,,,,,,oMMMMMMo,,,,,,lMMMMMMd,,,,,,cMxcccc0XXXXXXXXXXXXXXOdkO000KKKKK0x.
'MMMO',,,,,;WMMMMM0',,,,,,NMMMMMK',,,,,,XMxcccc0XXXXXXXXXXXXXxxXXXXXXXXXXX:
'MMN,,,,,,'OMMMMMW;,,,,,'kMMMMMW;,,,,,'xMMxcccc0XXXXXXXXXXXXKkkxxO00000OOx;.
'MMl,,,,,,lMMMMMMo,,,,,,cMMMMMMd,,,,,,:MMMxcccc0XXXXXXXXXXKOOkd0XXXXXXXXXO.
'M0',,,,,;WMMMMM0',,,,,,NMMMMMK,,,,,,XMMMxcccckXXXXXXXXXX0KXKxOKKXXXXXXXXk.
.c.......'cccccc.......'cccccc.......'cccc:ccc: .c0XXXXXXXXX0xO00000000c
                                                  ;xKXXXXXXX0xKXXXXXXXXK.
                                                     ..,:ccllc:cccccc:'


Unencrypted 2.0? He's such a silly guy.
That's the kind of stunt that makes my OWASP friends all cry.
Truth be told: most major sites are speaking 2.0;
TLS connections are in place when they do so.

-Holly Evergreen
<p>Congratulations! You've won and have successfully completed this challenge.
<p>POSTing data in HTTP/2.0.

 </body>
</html>
elf@0c18a7e91032:~$
```

Unencrypted HTTP/2? What was he thinking? Oh well.

Have you ever used Bloodhound for testing Active Directory implementations? It's a merry little tool that can sniff AD and find paths to reaching privileged status on specific machines.

AD implementations can get so complicated that administrators may not even know what paths they've set up that attackers might exploit.

Have you seen anyone demo the tool before?

Bloodhound Tool

https://github.com/BloodHoundAD/BloodHound

Bloodhound Demo

https://youtu.be/gOpsLiJFI1o

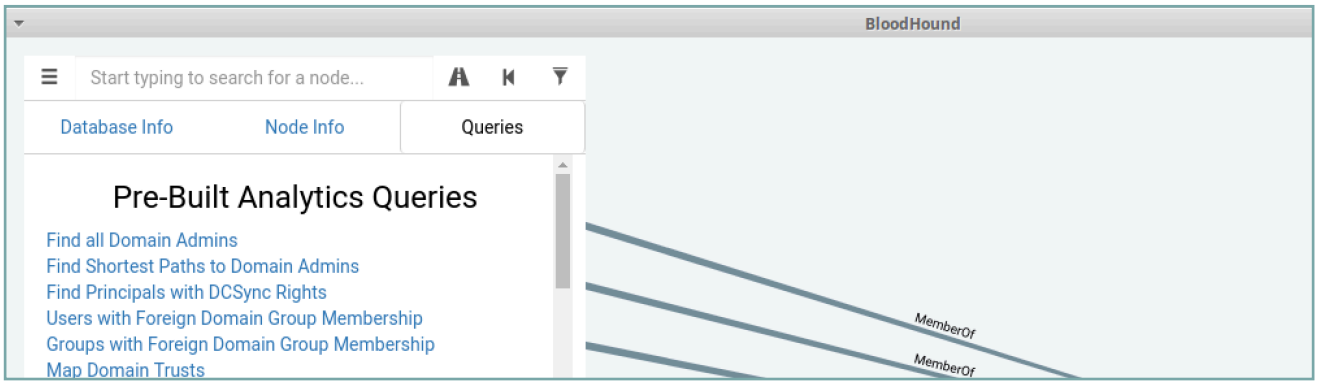
AD Privilege Discovery

SANS Slingshot Linux image .

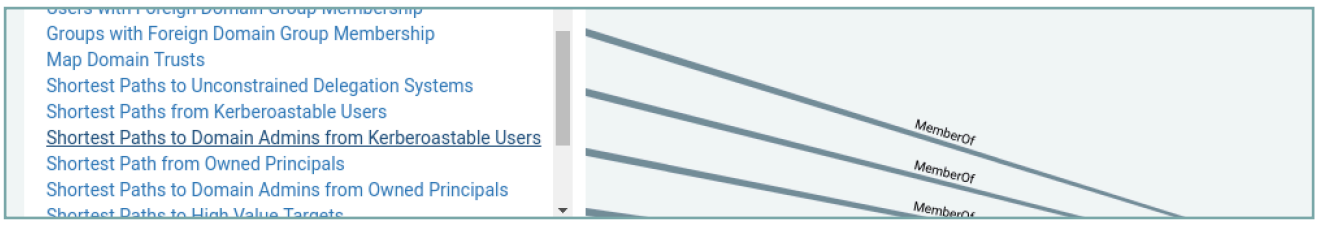
Solution

1. Watch Bloodhound Demo :
   https://youtu.be/gOpsLiJFI1o
2. Download SANS Slingshot Linux image then start the image using VirtualBox or any similar software :
   https://download.holidayhackchallenge.com/HHC2018-DomainHack_2018-12-19.ova
3. Run Bloodhound tool from desktop shortcut :

4. We are looking for a reliable path from a Kerberoastable user to the Domain Admins group with avoiding RDP as a control path:
   a. Select Queries from search panel on the left

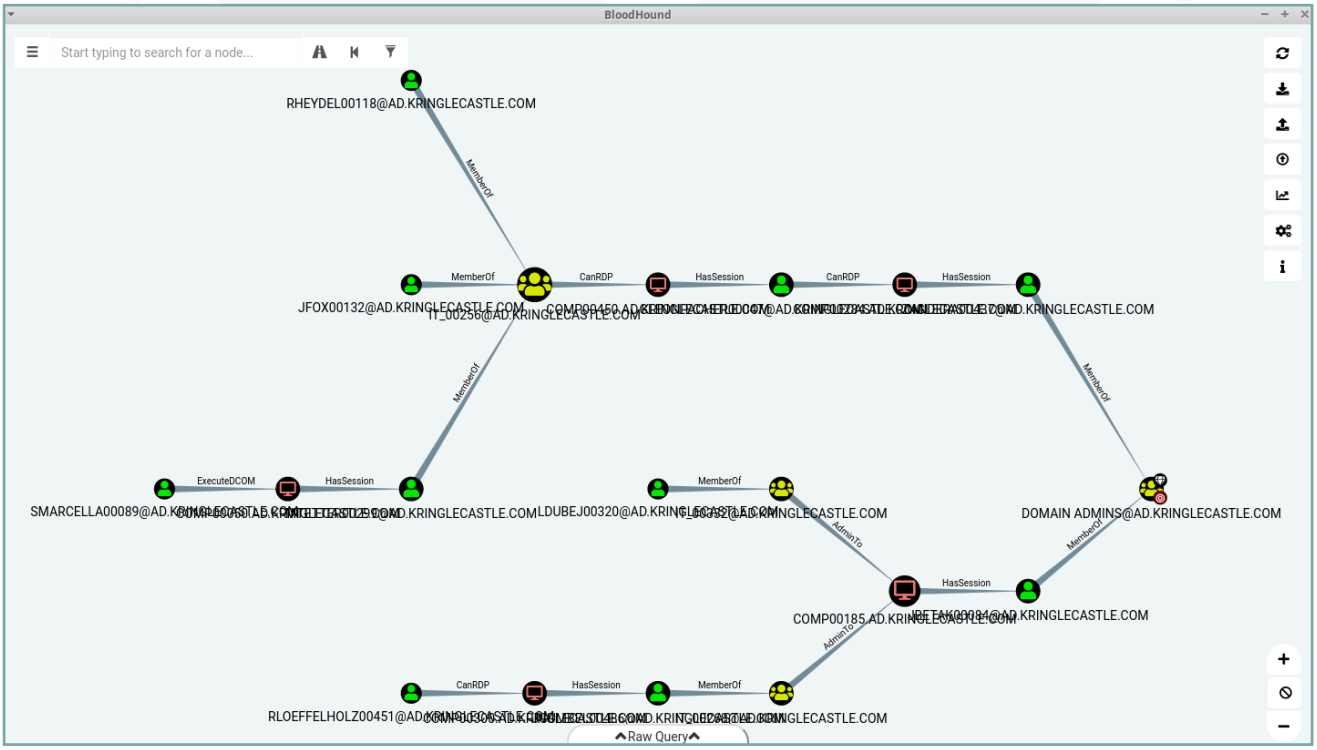


   b. Scroll down until you find Shortest Paths to Domain Admins from Kerberoastable Users then click on it

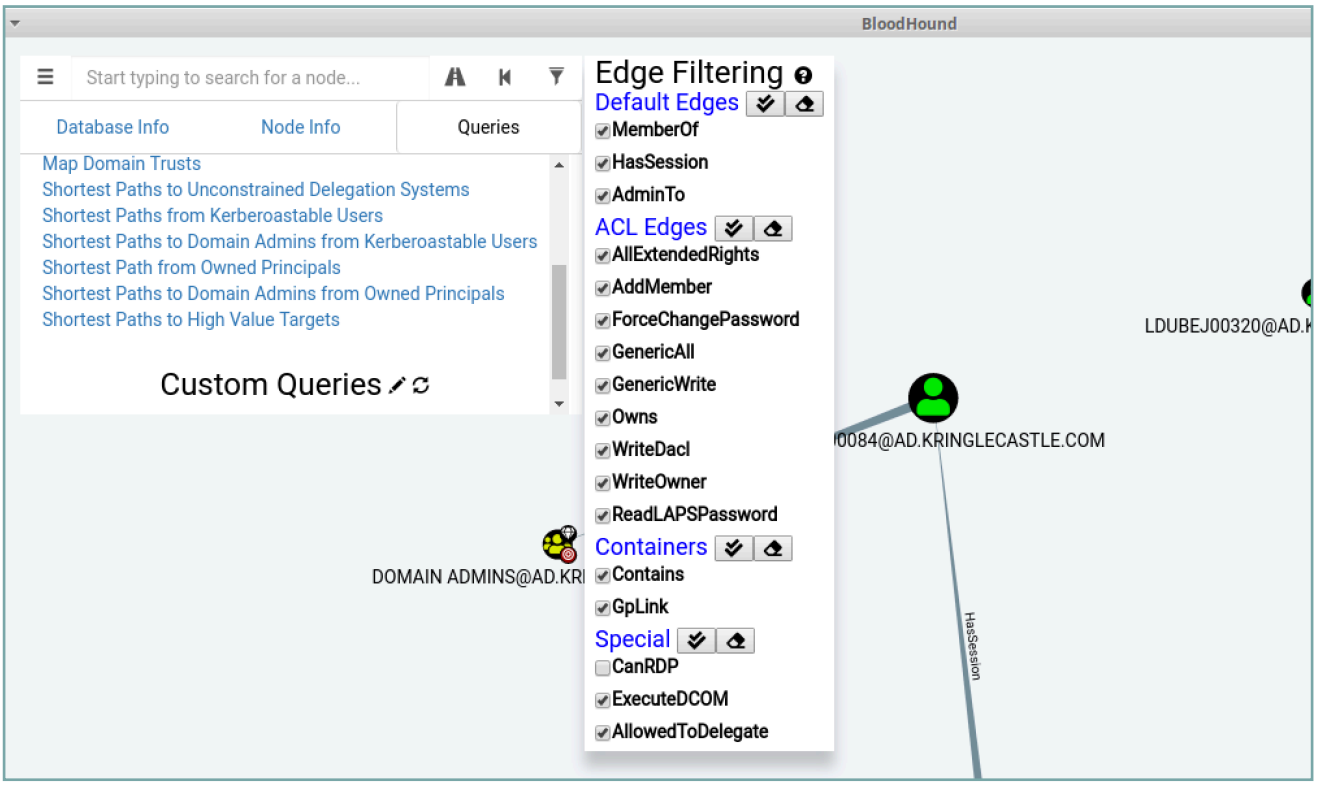


   c. Click on DOMAIN ADMINS@AD.KRINGLECASTLE.COM

AD Privilege Discovery

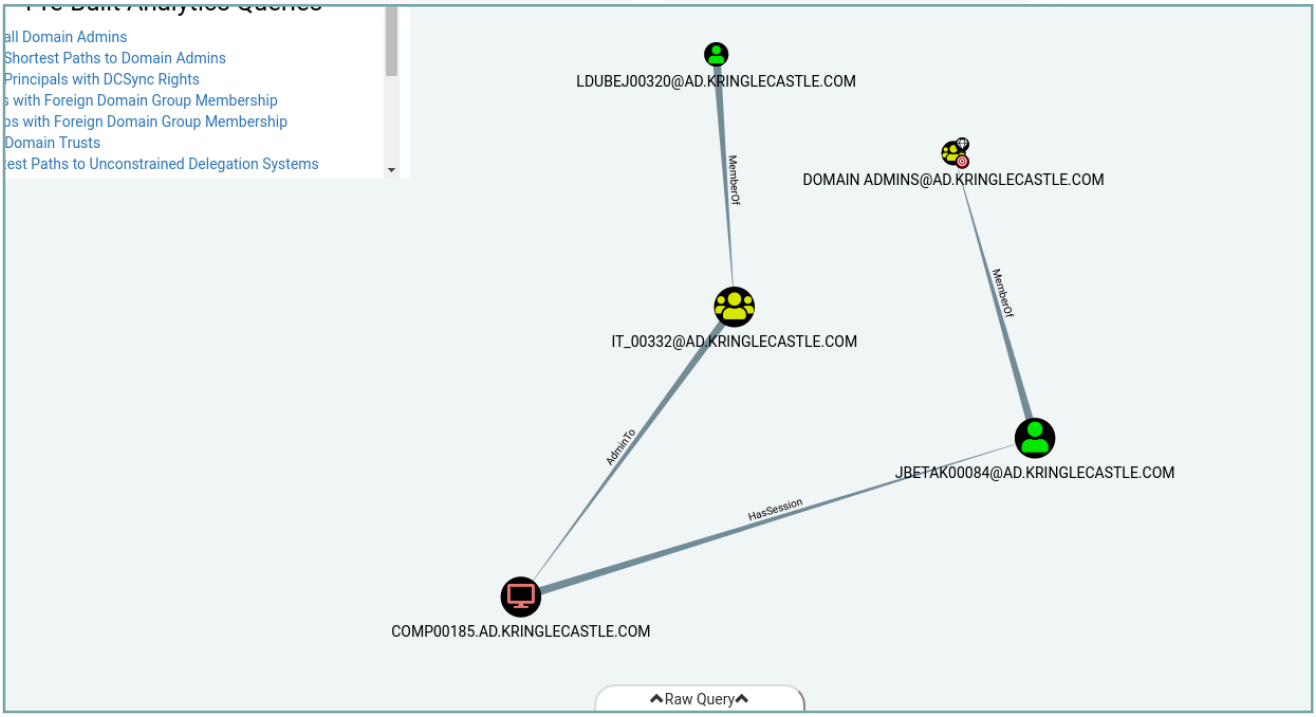


d. To remove users with RDP as a control path ,Click on filter then unselect canRDP



e. Our User is : LDUBEJ00320@AD.KRINGLECASTLE.COM

AD Privilege Discovery



Go to your Badge > Objectives > Enter LDUBEJ00320@AD.KRINGLECASTLE.COM