Wireshark

Bevezetés

Mire is jó ez?

- hálózati problémák felderítése rendszergazdák számára
- hálózati biztonsági szakembereknek biztonsági rések felderítése
- fejlesztők használhatják a protokoll implementációk tesztelésére, debuggolására
- segítségével megérthető a hálózatok működése

És végül: mire nem jó a Wireshark?

- Nem akadályozza meg, illetve nem figyelmeztet külső behatolás esetén.
- Ennek ellenére, felhasználhatók a "különös" dolgok felderítésére.
- Nem lehet vele manipulálni a hálózatot, hanem csak mérni, megfigyelni lehet azt.

Wireshark wiki nagyon hasznos

1. Hacktivity wargame-s feladatom megoldása

2. SSL https://wiki.wireshark.org/SSL

- RSA Kulcs és cert generálása:

```
openssl req -new -x509 -out server.crt -nodes -keyout server.pem -subj
/CN=localhost
```

- Ezzel a kulccsal szerver indítása

```
openssl s_server -www -cipher AES256-SHA -key server.pem -cert server.crt
```

- https://localhost:4433/ -on fut a szerver
- Wiresharkban kulcs megadása, forgalom monitorozása

```
printf 'GET / HTTP/1.0\r\n\r\n' | openssl s_client -ign_eof
```

- Follow TCP Stream vs folloq SSL Stream

3. http POST üzenetek elfogása http://www.blackmoreops.com/2015/04/11/website-password-hacking-using-wireshark/

http.request.method==POST

jelszó -> plaintext

4. Wifi adatforgalom rögzítése

- Szépen megy wiresharkkal
- Wifi kártya monitor módban -> csak linux alól
- fontos, hogy legyen rögzítve 4-way handsake WPA-nál (eapol-lal tudjuk ellenőrízni), hogy tudjuk dekódolni a csomagokat

ifconfig wlan0 down

iwconfig wlan0 mode monitor

ifconfig wlan0 up