RÁDIÓS HÁLÓZATOK ELLENI TÁMADÁSOK RENDSZERTANA

Varga Péter János

ZMNE KMDI doktorandusz

Probléma

- Vezeték nélküli hálózatok térhódítása ☺ ⇔ ☹
- A fő veszélyforrást az jelenti, hogy a hálózathoz való hozzáférés nem igényel fizikai kapcsolódást
- Támadó bárhol lehet az eszközünk rádiós hatósugarán belül
- Támadás esetén közel anonim hozzáférés

Célkitűzés

- Egy a gyakorlatban is alkalmazható Wi-Fi hálózatok támadását leíró rendszertan kidolgozása
- A támadási rendszertannak megfeleltetett védelmi rendszertan felállítása

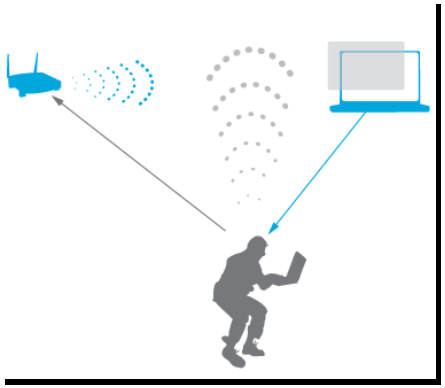
Elemzés – Átfogó rendszertanok

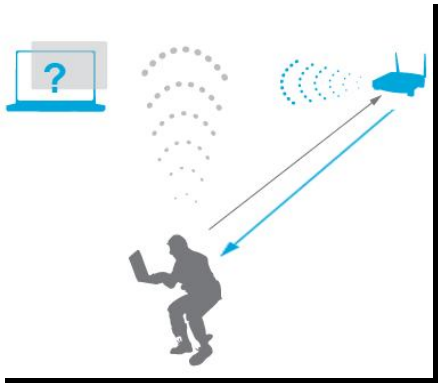
- CEH -
  Certified Ethical Hacking
- CERT -
  Computer Emergency Response
- IASTED -
  International Association of Science and Technology for Development
- CISCO
- INFORMÁCIÓS MŰVELETEK

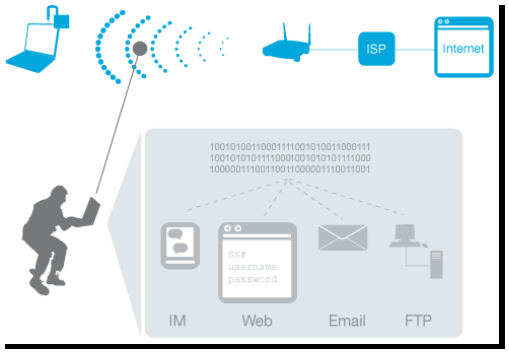
CEH

Certified Ethical Hacking

- WEP, WPA jelszó törés
- Evil Twin támadás (megszemélyesítés)
- Szolgáltatás blokkolás
- Felderítés
- Lehallgatás







http://www.careeracademy.com/index.asp?PageAction=VIEWPROD&ProdID=74

CERT

Computer Emergency Response Team

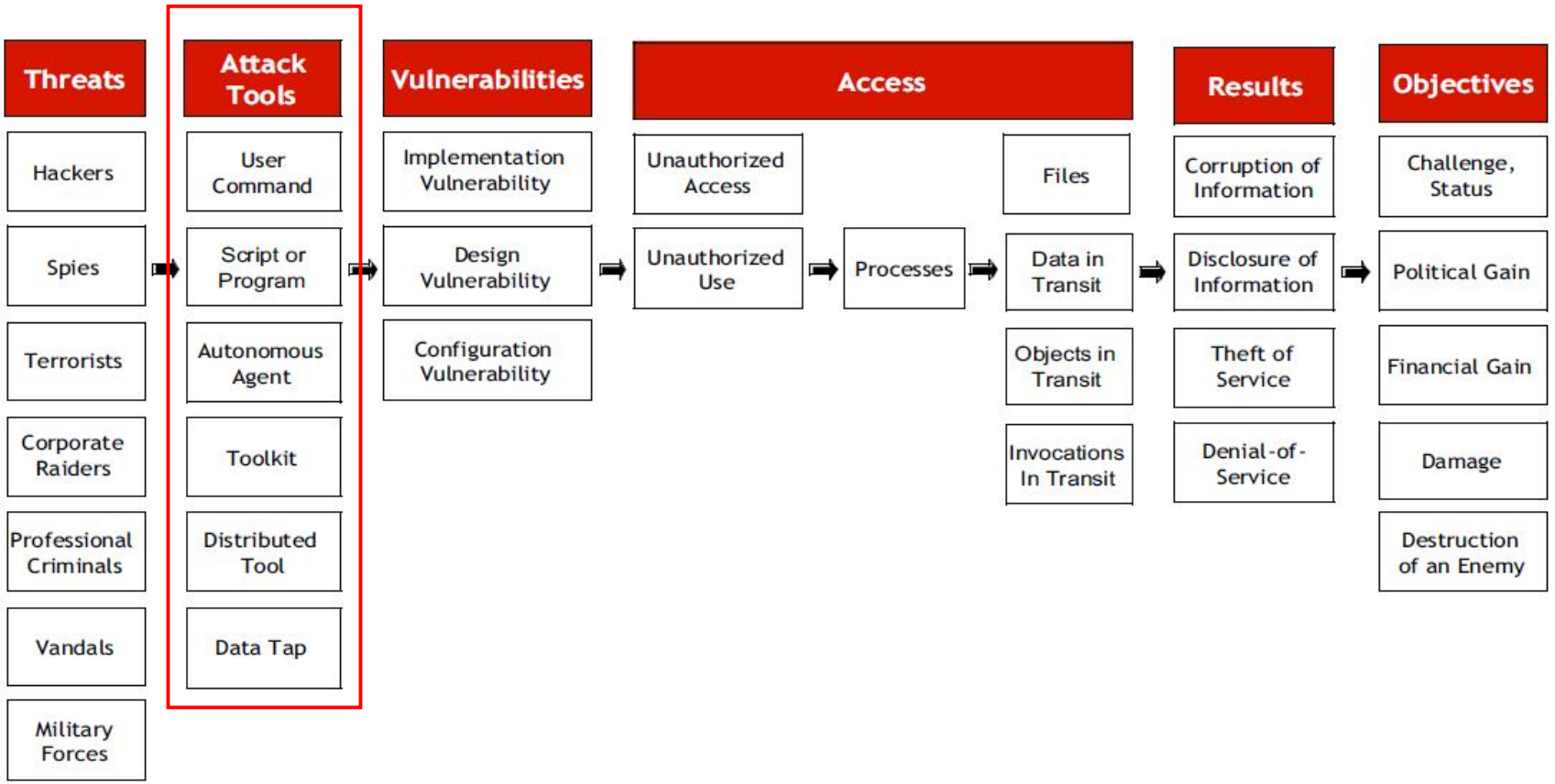
- Passzív támadások: más néven „lexikonépítő” támadás, amely a forgalom figyelése és statisztikai vizsgálatok alapján történő dekódolást jelenti
- Aktív támadás: a hozzáférési pont kijátszásával a kód dekódolása

- Eszközei:
  - Közbeékelt támadás
  - MAC cím visszaélés
  - WEP, WPA kódszó törés

http://www.cert.hu/images/stories/tanulmanyok/szalai.pdf

CERT

Computer Emergency Response Team



Adapted from *An Analysis Of Security Incidents On The Internet, 1989 - 1995*, Figure 6.9., Complete Computer and Network Attack Taxonomy, Co pyright John D. Howard, 1997, all rights reserved, a doctoral thesis submitted t o Carnegie Mellon University, as found at http:// www.cert.org/research/JHThesis/Start.html

- Passzív támadások
  - Lehallgatás
  - Forgalom elemzés
- Aktív támadások
  - Szolgáltatás megtagadás
  - Középreállásos támadás (megszemélyesítés)
  - Jogosultság kiterjesztés, lopás

http://www.cert.hu/images/stories/tanulmanyok/szalai.pdf

CISCO

- Passzív támadások
  - Lehallgatás
  - Forgalom elemzés
- Aktív támadások
  - Szolgáltatás megtagadás
  - Középreállásos támadás (megszemélyesítés)
  - Jogosultság kiterjesztés, lopás

saloperie.com/docs/cisco/BRKEWN-2020.pdf

Információs műveletek

- Számítógép – hálózati hadviselés
  - Számítógép – hálózati támadás
    - Adatok megszerzése, manipulálása, módosítása és tönkretétele
- Elektronikai hadviselés
  - Rádióelektronikai felderítés (Passzív támadás)
    - Felfedés
    - Iránymérés
    - Lehallgatás

Információs műveletek

- Elektronikai hadviselés
  - Elektronikai ellentevékenység (Aktív támadás)
    - Elektronikai zavarás
    - Elektronikai megtévesztés
    - Elektronikai pusztítás

Egyezőségek

	CEH	CERT	IASTED	CISCO	Információs műveletek
Passzív támadások	Felderítés	Lehallgatás	Lehallgatás	Lehallgatás	Felfedés
	Lehallgatás	Forgalom elemzés	Forgalom elemzés	Forgalom elemzés	Iránymérés
					Lehallgatás
Aktív támadás	Szolgáltatás megtagadás	Közbeékelt támadás	Szolgáltatás megtagadás	Szolgáltatás megtagadás	Elektronikai zavarás
	Megszemélyesítés	WEP, WPA kódszó törés	Megszemélyesítés	Megszemélyesítés	Elektronikai megtévesztés
	WEP, WPA jelszó törés	MAC cím visszaélés	Jogosultság kiterjesztés, lopás	Jogosultság kiterjesztés, lopás	Elektronikai pusztítás

Javaslat kiterjesztett rendszertanra

- Passzív támadások
  - Lehallgatás
  - Forgalom elemzés
  - Felderítés
- Aktív támadások
  - Szolgáltatás megtagadás
  - Megszemélyesítéses támadás
  - Jogosultság kiterjesztés, lopás
  - Elektronikai pusztítás

Összegzés

- A támadási rendszertan a Wi-Fi hálózatok biztonságosabbá tételének egyik kiindulópontja lehet
- Amennyiben tisztában vagyunk a hálózatunkat fenyegető veszélyekkel, a védekezést ennek megfelelően tudjuk kialakítani