1 PERC VAGY 1 ÉV?

INFORMATIKAI TÁMADÁSOK KIVITELEZÉSE NEM HOLLYWOODI MÓDSZEREKKEL

Veres-Szentkirályi András 2019-11-12

$ whoami

Veres-Szentkirályi András

- OSCP, GWAPT, SISE, HAREC
- Silent Signal társalapító (2009-)
- pentester, toolmaker
- 15+ év tapasztalat

Menetrend

1. Bevezetés
2. 1. célpont: sima ügy
3. 2. célpont: kisebb nehézségek
4. 3. célpont: kemény dió

Egy fontos gondolat előszó helyett

“Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can’t break.”

– Bruce Schneier (1998. október 15.)
https://www.schneier.com/crypto-gram-9810.html#cipherdesign

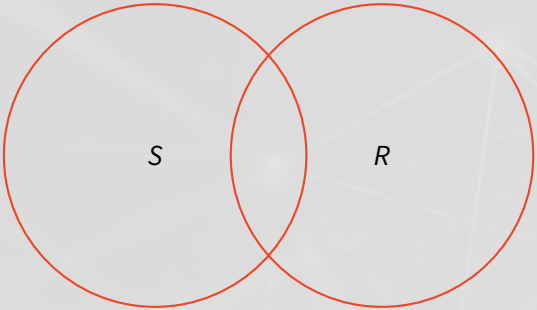
Grand Brighton Hotel, 1984

“Today we were unlucky, but remember **we only have to be lucky once. You will have to be lucky always.**”

– Provisional IRA (1984. október 13.)
Taylor, Peter (2001). Brits: The War Against the IRA. Bloomsbury Publishing. p. 265. ISBN 0-7475-5806-X.

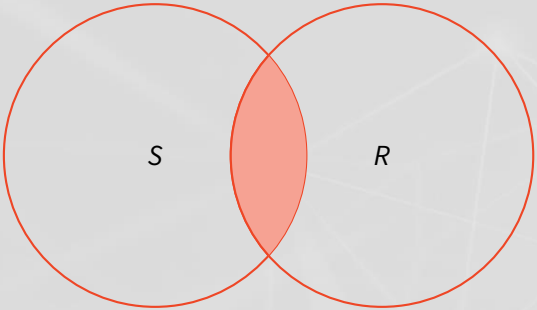
https://en.wikipedia.org/wiki/Brighton_hotel_bombing

Offenzív vs. defenzív megközelítés



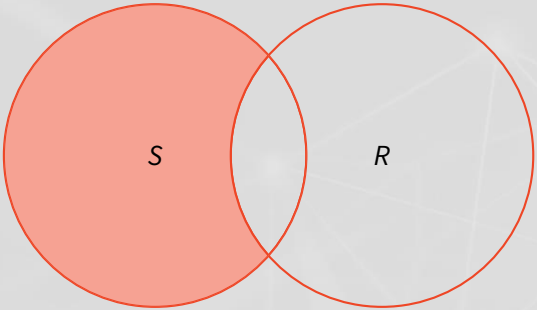
- *S* specifikáció
- *R* rendszer

Offenzív vs. defenzív megközelítés



- S specifikáció
- R rendszer
- $S \cap R$ specifikációnak megfelelően működő rendszer (ideálisan $S = R$)

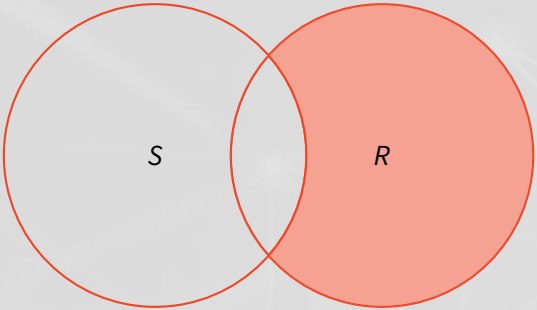
Offenzív vs. defenzív megközelítés



- S specifikáció
- R rendszer
- $S \cap R$ specifikációnak megfelelően működő rendszer (ideálisan $S = R$)
- $S - R$ specifikációban szereplő, de rendszer által **nem** nyújtott szolgáltatás
  - bug, funkcionális hiba

Offenzív vs. defenzív megközelítés

silent signal



- S specifikáció
- R rendszer
- $S \cap R$ specifikációnak megfelelően működő rendszer (ideálisan $S = R$)
- $S - R$ specifikációban szereplő, de rendszer által **nem** nyújtott szolgáltatás
  - bug, funkcionális hiba
- $R - S$ specifikációban **nem** szereplő, de rendszer által nyújtott szolgáltatás
  - feature, potenciális biztonsági hiba

Mi rossz történhet? (©HBO)

silent signal

Közgáztámadás

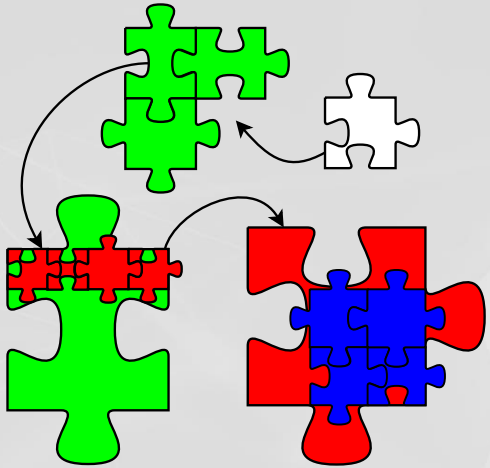
silent signal

- Védő: véges erőforrások
- Támadó: véges erőforrások
- $R - S$ halmaz
  - portok / tűzfalszabályok
  - ACL / `sudoers` bejegyzések
  - SUID binárisok
- Proaktív megközelítés: RDP NLA
  - MS12-020
  - CVE-2019-0708

Sérülékenységek forrásai

- Szervezeten kívülről
  - hosszú bizalmi lánc
  - szoftvergyártó hibát követ el
  - idővel kijavítja
- Szervezeten belülről ⇐ **ezzel kezdjük**
  - kiszervezett IT is ide tartozik
  - hibás beállítások
  - nem (időben) telepített frissítések

Az **információ** nem fizikai áru:
tetszőleges példányszámban másolható,
ellopása nem feltétlenül kelt feltűnést.

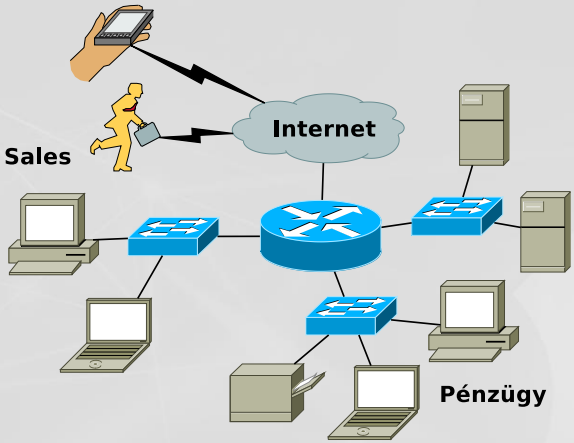


Menetrend

1. Bevezetés
2. 1. célpont: sima ügy
3. 2. célpont: kisebb nehézségek
4. 3. célpont: kemény dió

Cég IT-biztonsági érettségi szintje

- belső szolgáltatások saját szerveren
  - legyen elérhető futároknak és sales-eseknek kívülről bármikor
- biztonság nem visz magával csomagot
  - 0 költségvetés



Támadás

silent signal

- internet felőli felderítés
- gyenge pont azonosítása
- behatolás
- további védelem hiányában teljes hozzáférés

Intermezzo: Milyen a jó jelszó?

silent signal

Szerinted melyik a legerősebb jelszó az alábbiak közül?

1. `Micimacko2019!`
2. `correcthorsebatterystaple`
3. `SiX#e’9k`

Hányat kellene próbálkozni?

silent signal

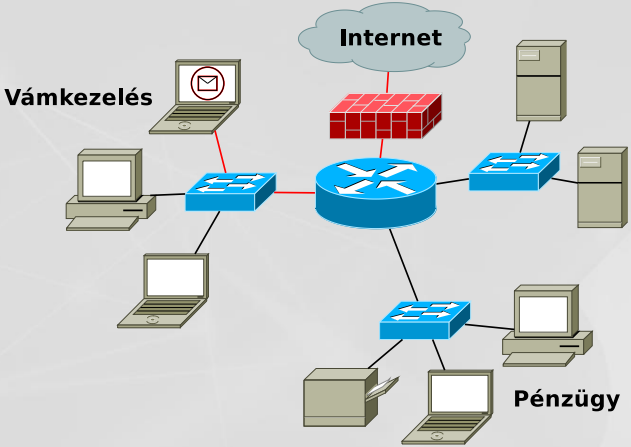
- `Micimacko2019!`
  100.000 szó $\times$10.000 szám $\times$16 szimbólum $=$ 16.000.000.000 $=$ $1{,}6 \cdot 10^{10}$ lehetőség
- `correcthorsebatterystaple`
  100.000^4 szó $=$ 100.000.000.000.000.000.000.000 $=$ 10^{20} lehetőség
- `SiX#e'9k`
  96^8 karakter (kis-/nagybetű/szám/speciális) $=$ 7.213.895.789.838.336 $\approx$ $7 \cdot 10^{15}$ lehetőség

Menetrend

1. Bevezetés
2. 1. célpont: sima ügy
3. 2. célpont: kisebb nehézségek
4. 3. célpont: kemény dió

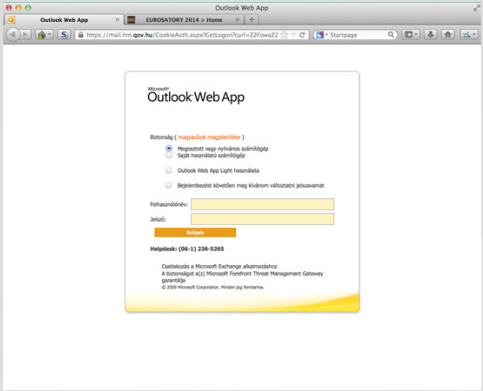
Cég IT-biztonsági érettségi szintje

- internet felől semmi látnivaló
- munkatársak megfelelő jelszavakat használnak
- vámkezelés miatt e-mail lehetőség
- nincsenek belső „válaszfalak”



Támadás

- alapos céges felderítés
- belépési pont azonosítása
- phishing oldal létrehozása
- phishing levél beküldése
- felhasználó megszemélyesítése

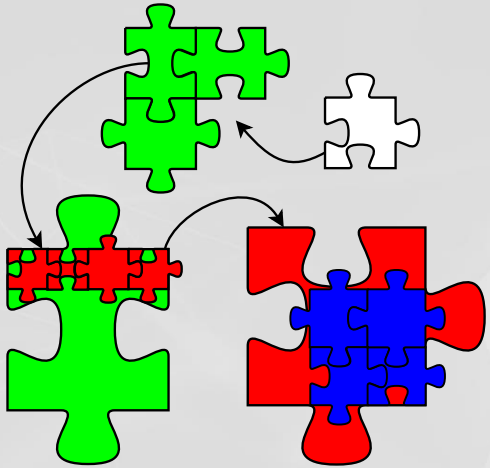


https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-pawn-storm.pdf

Sérülékenységek forrásai

- Szervezeten kívülről ⇐ **itt folytatjuk**
  - hosszú bizalmi lánc
  - szoftvergyártó hibát követ el
  - idővel kijavítja
- Szervezeten belülről
  - kiszervezett IT is ide tartozik
  - hibás beállítások
  - nem (időben) telepített frissítések

Az **információ** nem fizikai áru:
tetszőleges példányszámban másolható,
ellopása nem feltétlenül kelt feltűnést.



Intermezzo: Mennyi időnk van?

silent signal

Szerinted átlagosan mennyi idő egy gyártói javítás megjelenése után elkészíteni a javított sérülékenységet kihasználó támadást?

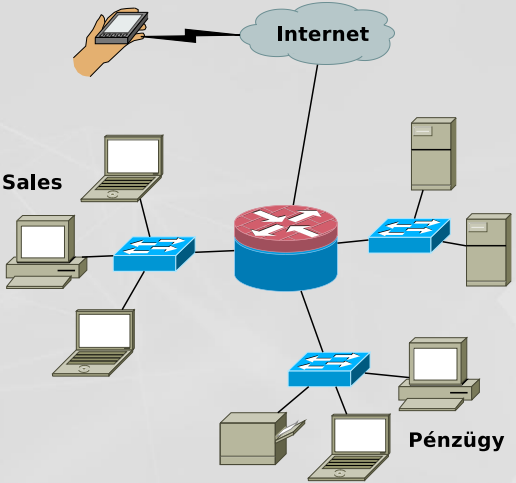
- **11 nap**
- **22 nap**
- **44 nap**
- **88 nap**

Menetrend

1. Bevezetés
2. 1. célpont: sima ügy
3. 2. célpont: kisebb nehézségek
4. 3. célpont: kemény dió

Cég IT-biztonsági érettségi szintje

- hálózat izolált részekre van szedve
  - ezek között ellenőrzött átjárás
- modern kétfaktoros azonosítás
  - phishingnek esélye sincs



Támadás

- lassú és nagyon alapos céges felderítés
  - rendszergazdák IT fórumokon azonosítható kérdései
  - álláshirdetésekben megjelölt technológiák
  - nyilvános sajtóbejelentések, beszállítói marketinganyagok
  - alacsonynak besorolt információszivárgás sérülékenységek
- sok-sok várakozás
  - mikor települ egy frissítés későn
  - mikor kerül engedélyezésre valami ideiglenesen
  - „A gép forog, az alkotó pihen.”
- lépésről-lépésre haladás
  - minden lépés és perc magában hordozza a lebukás esélyét

Összefoglalás

silent signal

- ezek fikcionális cégek voltak
- mindenki máshol helyezkedik el ezen a skálán
- konkrétumok is hasznosak lehetnek…
- …de mindenki a saját lehetőségein belül tud egy kicsit előre menni
- cél: támadói siker kockázat csökkentése

KÖSZÖNÖM!

VERES-SZENTKIRÁLYI ANDRÁS

vsza@silentsignal.hu

facebook.com/silentsignal.hu

@SilentSignalHU

@dn3t

silent signal