SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

CYBERSECLAB

Etikus hackelés alapjai

Alapok, fogalmak, bevezető

Dr. Hidvégi Timót
egyetemi docens, IT biztonsági szakértő

Tartalomjegyzék

- Törvényi háttér
- Példák
- Pentest
- Virtuális környezet

Tiltott adatszerzés és az információs rendszer elleni bűncselekmények

- Büntető Törvénykönyv / 2012. évi C. törvény
  - információs rendszer: az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége
- 375. §: Információs rendszer felhasználásával elkövetett csalás
- 386. §: Védelmet biztosító műszaki intézkedés kijátszása
- 422. §: Tiltott adatszerzés
- 423. §: Információs rendszer vagy adat megsértése
- 424. §: Információs rendszer védelmét biztosító technikai intézkedés kijátszása

https://www.police.hu/sites/default/files/2012._evi_c._torveny.pdf

Néhány OT támadás

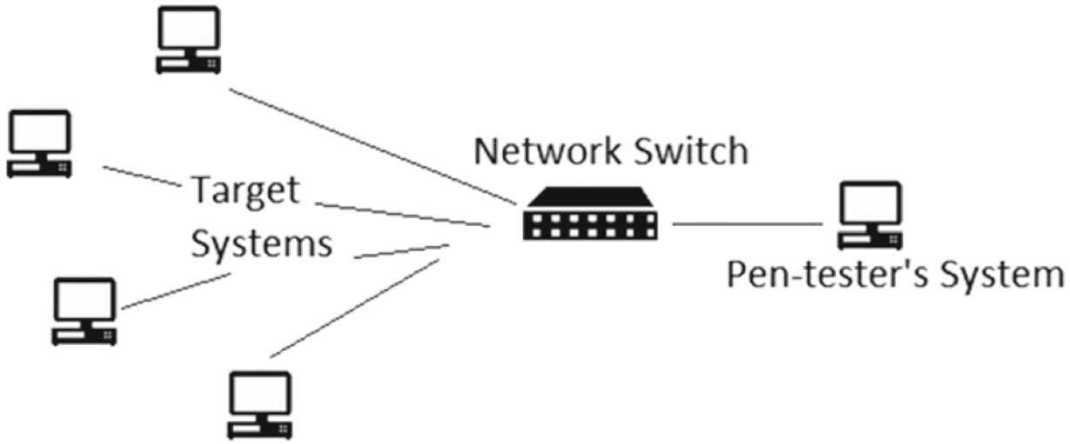
- 2012: Saudi Aramco
- 2016: Ukrenergo
- 2017: Merck, FedEx, Maersk
- 2018: Saudi Petrocherm, UK NHS
- 2019: Norsk Hydro, Duke Energy
- 2020: Cognzant, Honda, Solarwinds SC
- 2021: Oldsmar Florida, Colonial Pipelines

Biztonsági értékelés

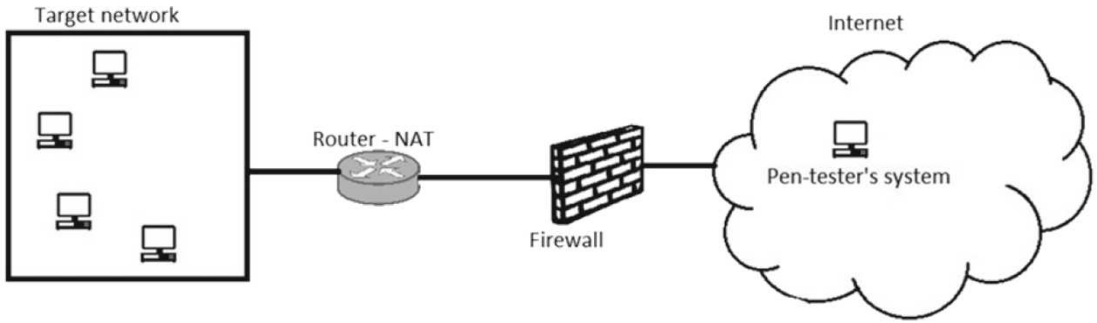
- Audit
- Sérülékenységvizsgálat
- Pentest

Behatolástesztelés

- Belső



- Külső



Behatolástesztelés

- A biztonsági értékelés egy tág fogalom, amely tovább osztályozható.
  - biztonsági auditokra, sebezhetőségi értékelések és behatolásvizsgálat
- A behatolásvizsgálat a valós világ által használt módszereket és technikákat szimulálja.
  - A behatolásvizsgálatnak különböző típusai vannak, mint például belső vagy külső, fekete dobozos /szürke doboz/fehér doboz, illetve bejelentett vagy előre be nem jelentett.
- A felderítés két típusba sorolható: aktív és passzív.
- A titoktartási megállapodás aláírása elengedhetetlen a vizsgálat megkezdése előtt. Ez biztosítja, hogy a vállalat bizalmas információi ne szivárogjanak ki a tesztelés során vagy azt követően.
- A teszt végén fontos, hogy elegendő információt tartalmazó jelentést készítsünk az érdekelt felek számára a sebezhetőségek megértéséhez és kijavításához.

Behatolástesztelés

- Fontos a penetrációs teszt helyes elvégzése.
- Minden fontos eszközt tesztelni kell. A pentesztelőnek a célszervezet érintett érdekelt feleivel együtt át kell tekintenie a szervezet eszközlistáját, és kritikusságuk alapján kategorizálni és rangsorolni kell az eszközöket.
  - Az eszközök a korábbi biztonsági incidensek alapján is rangsorolhatók.
- Szinte kötelező:
  - Webszerverek- FTP-kiszolgáló- DNS- Mail szerverek- Tűzfalak- IDS és IPS eszközök- Távoli hozzáférési eszközök, például VPN- Kommunikációs kapcsolatok- Nyilvános weboldalak- Érzékeny adatokat tároló belső rendszerek (például bérszámfejtő rendszerek)
- Behatolástesztelés fajtái
  - külső vagy belső, fekete dobozos , szürke dobozos vagy fehér dobozos, valamint bejelentett vagyelőre be nem jelentett.

Behatolástesztelés - típusok

- Fekete doboz
  - A tesztelőnek nincs előzetes ismerete a célpontról -> támadások valós szimulációja -> csökkenti a hamis pozitív eredményeket.
  - Jellemzően több időt, erőfeszítést és költséget emészt fel a fekete dobozos behatolásvizsgálat elvégzése.
- Szürke doboz
  - A tesztelő korlátozott vagy részleges ismeretekkel rendelkezik a célinfrastruktúráról, a meglévő biztonsági mechanizmusokról és a tesztelendő kommunikációs csatornákról.
  - A valós világot szimulálja, ahol a támadásokat belső személy vagy egy külső támadó (korlátozott ismeretekkel rendelkező) hajthat végre a célrendszeren.
- Fehér dobozos
  - A tesztelő teljes és mélyreható ismeretekkel rendelkezik a célinfrastruktúráról, a meglévő biztonsági mechanizmusokról és a tesztelendő kommunikációs csatornákról.
  - Ez a fajta tesztelés segít szimulálni egy olyan támadást, amelyet egy olyan bennfentes hajthat végre, aki teljes körű ismeretekkel és jogosultságokkal rendelkezik az adott rendszerben.

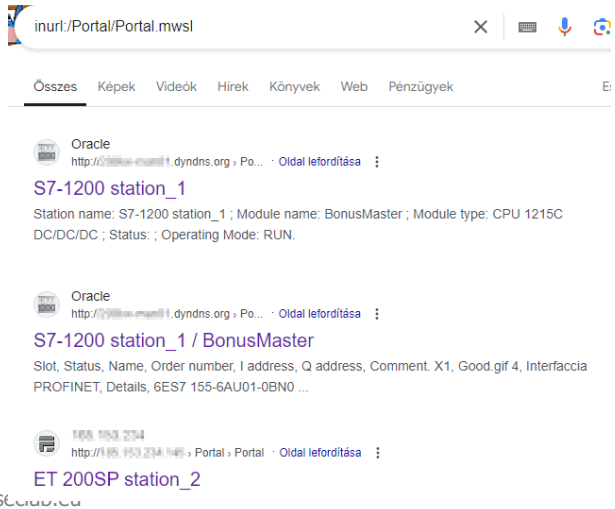
Behatolástesztelés – automata / kézi

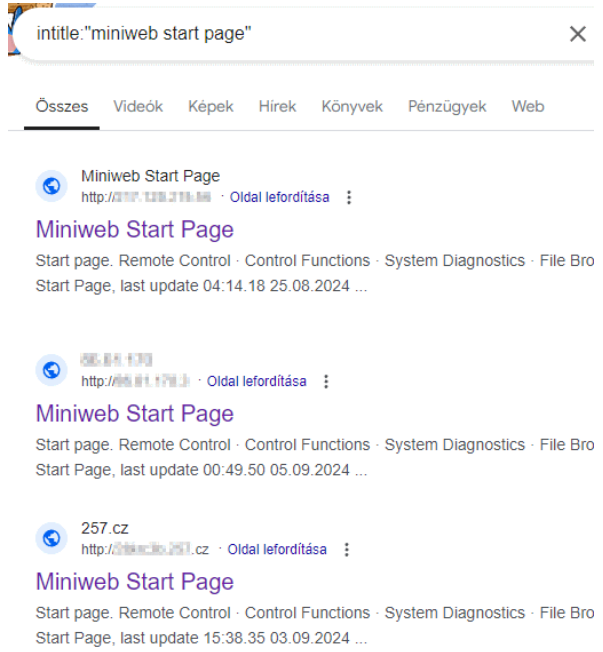
- Automatizált
  - A penetrációs tesztelés sok feladatot foglal magában, és a támadási felület is időnként összetett, néhány szervezet inkább az automatizált penetrációs teszteléshez használt eszközöket részesítik előnyben. Egyszerűen lefuttatják a scan-t az infrastruktúrán, majda jelentéseket megosztják az érintett csapatokkal a problémák kezelése érdekében.
  - Korlátok
    - *Csak az előre meghatározott sebezhetőségeket ellenőrzi, és több hamis pozitív eredmény lehet. Emellett nem tudja biztonsági szempontból felülvizsgálni az architektúrát és a rendszerintegrációt.*
    - *Alkalmas azonban több célpont ismételt vizsgálatára és a kézi tesztelés kiegészítésére.*
- Kézi tesztelés
  - A kézi tesztelés során a tesztelő saját szakértelmét és készségeit használja a célrendszerbe való behatoláshoz. Kisebb az esélye a hamis pozitív eredményeknek, a tesztek végrehajtása ellenőrzöttebb módon történik.

Open Source Intelligence (OSINT)

- Shodan
  - https://www.shodan.io/
- Censys
  - https://search.censys.io/
- ZoomEye
  - https://www.zoomeye.hk/project?id=industry
- Recon-NG
- Google
  - Operátorok alkalmazása
    - *inurl:/Portal/Portal.mwsl*
    - *intitle:"miniweb start page"*

- Wireshark
- GreyNoise
- CIRCL OTX
- ICS-CERT



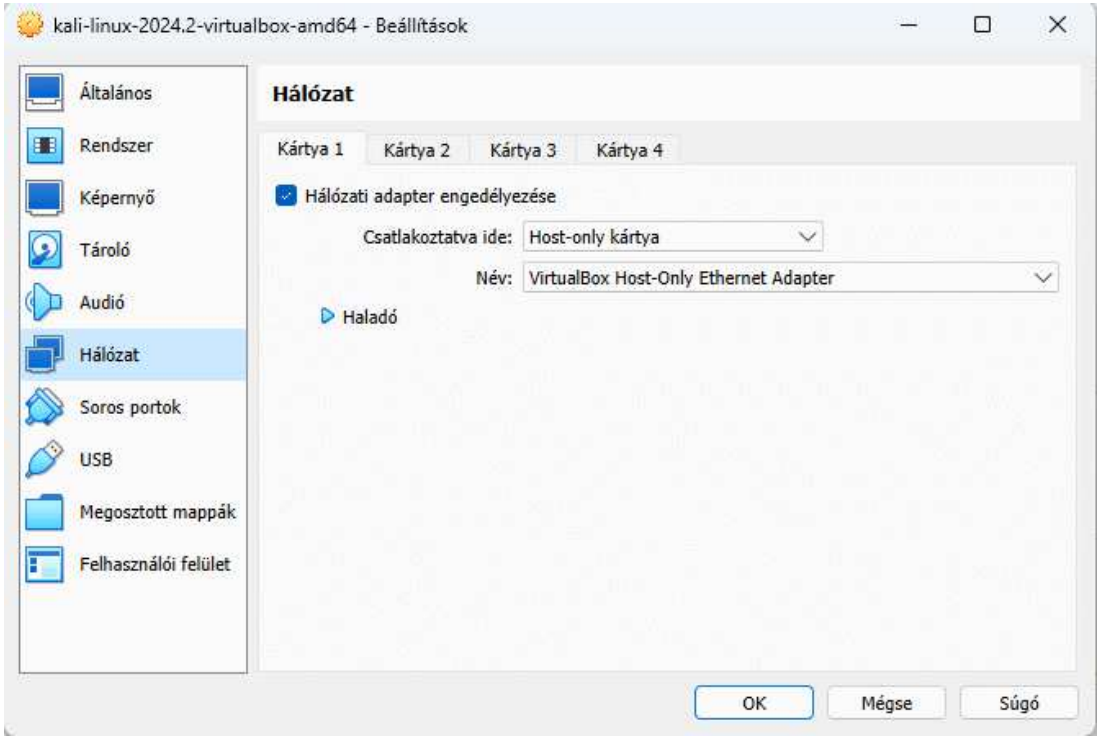


Néhány pentest eszköz

- Információszerzés
  - nmap
    - *nmap IP cím*
    - *nmap -p portszám --script scriptnév IP cím*
  - Metasploit
  - Shodan, zoomeye
- SCADA specifikus
  - Pl.: különböző fuzzerek
- ICS sérülékenységkereső eszközök
  - Metasploit
  - Nessus

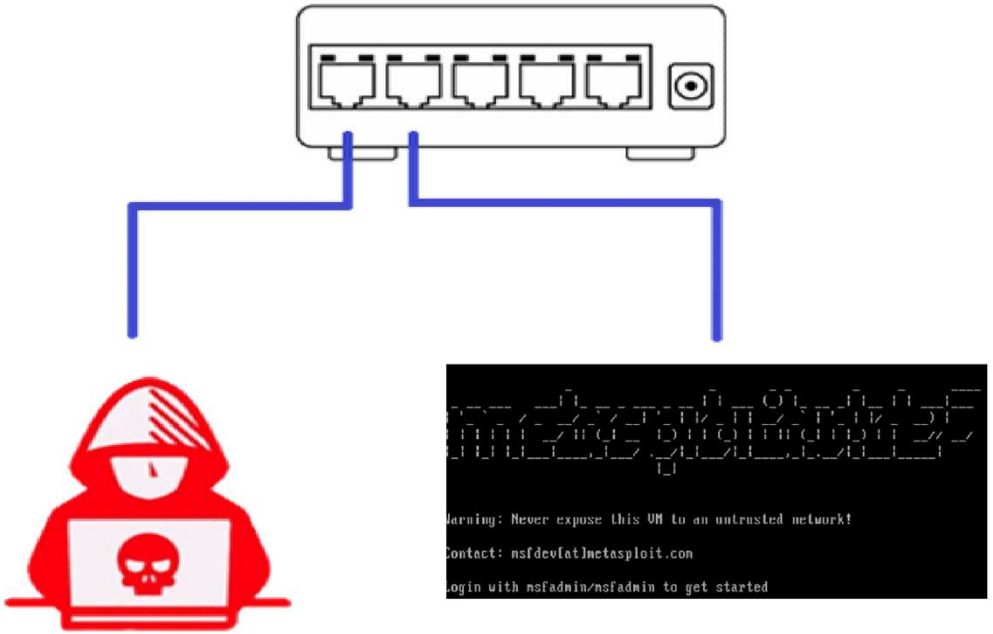
Saját virtuális környezet kialakítása

- Virtuális gépek alkalmazása
  - Virtuális környezet
    - *Hyper-V*
    - *VirtualBox*
    - *VmWare*
  - Tesztelő gép
    - *Kali Linux (https://www.kali.org)*
    - *Parrot OS (https://www.parrotsec.org)*
  - Virtuális gép (áldozatgép)
    - *Ubuntu 22.04*
    - *Metasploitable 2*
    - *Raspberry Pi*



Saját virtuális környezet kialakítása

- Operációs rendszer
  - Kali Linux (vizsgálógép)
    - *kali / kali*
  - Metasploitable 2 (áldozat)
    - *msfadmin / msfadmin*
- Hálózati beállítások
  - A szükséges telepítések után javasolt a „Host only” alkalmazása



Virtuális gép készítése Virtualbox alá

- Kali Linux letöltése
  - https://kali.org
- Kali Linux VM importálása
  - https://www.youtube.com/watch?v=5SAQPsKcPvA&list=PLy9LTKNPuJ5YsRijY8DJ19-o3N2K3_28i
- Ubuntu virtuális gép készítése
  - https://webelektronika.com/article/20180709Virtualis-kep-keszites
- Metasploitable 2 letöltése
  - https://sourceforge.net/projects/metasploitable/files/Metasploitable2
- Metasploitable 2 telepítése Virtualbox alá
  - https://www.geeksforgeeks.org/how-to-install-metasploitable-2-in-virtualbox
  - https://www.youtube.com/watch?v=yyf131KILaU

Linkek

- Information Trust Institute
  - https://github.com/ITI
- ICS-Security-Tools
  - https://github.com/automayt/ICS-Security-Tools
- ICS pcap file-ok
  - https://github.com/automayt/ICS-pcap
- Pcap file-ok
  - https://gitlab.com/wireshark/wireshark/-/wikis/SampleCaptures
- Google keresés
  - https://webelektronika.com/article/20180619google-hacking

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
GÉPÉSZMÉRNÖKI, INFORMATIKAI ÉS VILLAMOSMÉRNÖKI KAR

CYBERSECLAB

Industrial and Research Lab for Cybersecurity

- Web
  - https://cyberseclab.eu
- Facebook
  - https://www.facebook.com/IndustrialandResearchLab
- Github
  - https://github.com/cyberseclabor
- Linkedin
  - https://www.linkedin.com/company/industrial-and-research-lab-for-cybersecurity

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR
GÉPÉSZMÉRNÖKI, INFORMATIKAI ÉS VILLAMOSMÉRNÖKI KAR

CYBERSECLAB

Industrial and Research Lab for Cybersecurity