Fábián Zoltán – Hálózatok elmélet

IT Biztonság

Kell-e erről beszélni?

- Az IT eszközökön tárolt adatok értéke sokszorosa maguknak az eszközöknek az értékéhez képest.

Fogalmak

- Esemény – Egy IT rendszer szokásos működését megzavaró művelet
- Incidens – Olyan esemény, amely veszélyezteti egy szervezet informatikai rendszerét
- Behatolás – Olyan incidens, amelynek során információ szivárgott ki, illetéktelenül módosították vagy törölték az IT rendszeren tárolt információkat
- Behatolási kísérlet – Sikertelenül végződött behatolás.
- Social Engineering – az emberek természetes bizalomra való hajlamának kihasználása

Hardveres biztonság

- Szerverek – fizikailag elzárva, szerverszobában, zárolt helyen
- Munkaállomások – jelszóval, biztonságos helyen
- Biztonságos adattárolás
  - Alapszabály: Minden fontos adat két példányban legyen
- Biztonsági szintek
  - Két adatpartíció – véletlen törlés ellen véd
  - Két HDD – tükörbe szervezve vagy RAID 3,RAID 5-ben – Ha az egyik HDD megsérül
  - Két hardver egy szobában – Ha az egyik gép leég
  - Két hardver egy épületben – Ha az egyik szobát kirabolják, kigyullad
  - Két hardver két telephelyen – Ha a telephely leég, felrobban, stb…
- Hálózat lehallgathatósága
  - Rézkábelek lehallgathatósága
  - Optikai kábelek lehallgathatósága
  - Telephelyek közti forgalom lehallgathatósága
- Munkaállomások lehallgathatósága
  - Keylogger
  - Képernyőscanner
  - Bármilyen elektromágneses sugárzás lehallgatható
- Mobil eszközök biztonsága
  - Jelszóval védett
  - Távoli kapcsolat védelme

Szoftveres biztonság

- A felhasznált szoftverek beállításainak szabályozása
  - Csak megadott és kipróbált szoftverek használata
  - Jogtiszta szoftverek használata
  - Nyílt forráskódú szoftverek használata
- Vírusvédelem
  - Mindegy, hogy milyen víruskereső – irtó
  - Több féle és/vagy integrált rendszer használata
- Határvédelem
  - Cél a cég digitális adatvagyonának védelme
  - A cég üzletvitelének ésszerű keretekbe szorítása
  - A magánhasználat szükséges mértékű korlátozása
  - Távoli használat szabályozása (VPN)
  - URL-ekhez való hozzáférés korlátozása (proxy, tűzfal)
  - Szolgáltatások korlátozása (tűzfal)
- Security Scanner program használata
  - GFI LANGuard
    - Patch kezelés (Microsoft OS és nem Microsoft OS és alkalmazások
    - Biztonsági rések kezelése
    - Hálózati és szoftver auditálás
    - Eszközök kezelése (beállítások, biztonság, stb)
    - Változáskezelés
    - Rizikó kezelés és támogatás
- Ethical Hacker felkérése
  - http://www.ethicalhacker.net/

HackerWatch
Anti-Hacker Community

Tűzfal portscan

GFI LANguard

Biztonsági másolatok

- Backupok fajtái
  - Szinkronizálás (módosítási időpont, méret alapján)
  - Inkrementális
  - Teljes
- Backupok időzítése
  - Napi backup – inkrementális
  - Időszakonként – Havonta, negyed évente - inkrementális
  - Félévente, évente - Teljes
- Backup és szinkronizáló eszközök
  - Windows – előző verziók kezelése
  - Windows Backup
  - GFI Backup
  - Levelek:
    - Exchange
    - PST Sync
  - Fájlok
    - Microsoft Groove, Groove Server
    - Free FileSync
    - Windows: XCOPY parancs
    - Linux: TAR/GZ
- Egyéb backup és szinkronizáló szoftverek: http://www.fzolee.hu/framework/backup_szoftverek

GFI Backup HOME EDITION

Ügyviteli biztonság

- Portaszolgálat szabályozása
- Tiszta íróasztal politika
- Nem digitális adatok bizalmas kezelésének módja
- Biztonsági zónák az épületben
- Kitűzők használata
- Új dolgozókkal kapcsolatos teendők szabályozása

Jelszavak, azonosítók biztonságos használata

- Jelszóházirend (hossza, tartalma, érvényessége, csréje)
- Mester jelszó (lezárt borítékban, páncélszekrényben)
- Rendszergazdai jelszavakat élesben nem használunk
- Titkosított protokollok használata
  - https://, ftps://, sftp://, VPN
- Azonosítók jelszavak tárolási eszközei:
  - Kee-Pass Password Safe http://keepass.info/
  - AZZ Card File http://www.azzcardfile.com/
  - Total Commander plugin: http://www.totalcmd.net/plugring/darkcrypttc.html

Jogosultságok kezelése

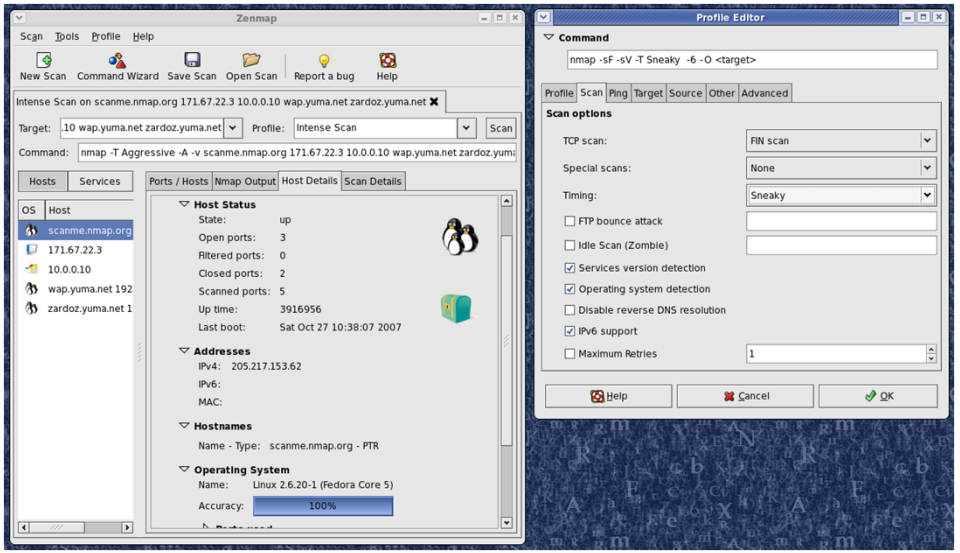
- A feladat ellátásához, megfelelő feladathoz a minimálisan szükséges és elégséges jogosultság
- Egyéni jogosultság és csoportos jogosultságok rendszere
- Legalább két rendszergazdai jogú felhasználó (személy)
- Rendszergazdai jelszó a páncélban
- A rendszergazdát is ellenőrizze egy felhasználó

Dokumentálás

- Szoftverek beállításainak dokumentálása
  - Biztonsági szoftverek (tűzfalak, switchek, routerek, szerverek)
  - Alkalmazói programok (Office, más szoftverek)
  - Fejlesztői programok (jogosultságok)
  - Jogosultságok rendszerének dokumentálása
- Hardverek beállításainak dokumentálása
- Szoftverleltár
  - Adatok összegyűjtése
  - Licencek tárolása
  - A ténylegesen használt és dokumentált leltár különbségeinek kezelése
    - Steel Inventory
    - Microsoft Szoftverleltár Elemző

Behatolási / védekezési módszerek 1

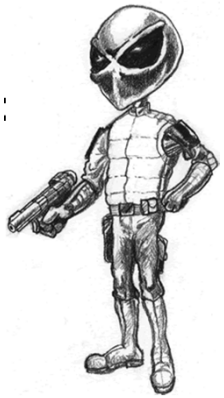
- DDOS támadás
- Szolgáltatások támadása
  - Portscan
    - TCP Connect
    - Syn Scan
    - TCP Idle Scan (Zombie scan)
      - Pl: http://www.radmin.com/
  - WEB támadás
    - Acunetix Vulnerability Scanner
    - Webserver Stress Tool
  - Általános scanner
    - NMAP Security Scanner
  - WIFI felderítés
    - http://www.netstumbler.com/downloads/

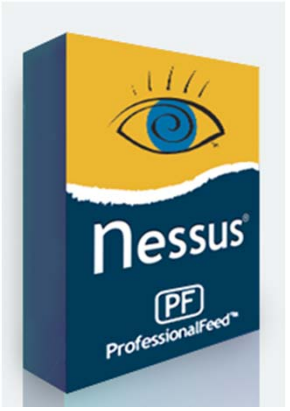


Behatolási/védekezési módszerek 2 (http://regulation.hu)

- Túlcsordulási tesztek
  - DoS (Denied of Service, Szolgáltatás Megtagadása) támadási tesztek
  - SQL Injection lehetőségek keresése
  - XSS (Cross Site Scripting) hibák
  - Nem publikus URL-ek autentikáció nélküli elérhetőségének vizsgálata
  - stb.

- Gyakran használt eszközök:
  - Nikto
  - Wikto
  - Sandcat
  - Paros proxy
  - SQL power injector
  - Blackwidow – Spy program
  - Nessus – Általános Security
  - Appscan





Social Engineering

Már Virág elvtárs is megmondta Pelikán József gátőrnek, hogy „… az a gyanús, ami nem gyanús…”

- Elektronikus manipulációk
  - Adathalászat – Megtévesztő email és weboldal
  - Célzott adathalászat – Látszólag ismerőstől származó kérés, üzenet, email
  - E-mailes csalások – Könnyű pénzt ígérő ajánlatok
- A támadás fázisai
  - Adatgyűjtés – A cég olyan dolgozóinak megkeresése, akik bizalmas információ birtokában vannak
  - Információ ellenőrzése
  - Az igazi kapcsolatfelvétel – az adatok felhasználása
- Módszerek az első lépéshez
  - Kiadja magát az ember egy külső partner alkalmazottjának (szállító, ügyfél)
  - Halászat – A halászó kiadja magát külső partner emberének és emailben kér bizalmas adatokat
  - Telefonos adathalászat – Telefonon felhívja a kiszemelt dolgozót, külső partner nevében és bizalmas információkat kér.
  - Visszahívást kér véletlen számokról a technikai személyzettől, és kiadja magát külső partnernek, a technikai személyzet már tényleg elhiszi az előadását és valamenniy jogot ad neki.
  - Előtte megfelelően felkészül a várható ellenőrző kérdésekre, esetleg preparálja a cég kimenő telefonvonalait
  - Trójai faló beküldése (disk, Pendrive, CD-ROM, Preparált CD-n, amivel ráveszi az alkalmazottat, hogy indítsa el a rajta lévő anyagot)
  - Turkálás a szemétben cetlik után
- Híres Social Engineer-ek (Kevin Mitnick, Badir Brothers)
- Előadás:
  - http://www.axonic.hu/regulation/regulak_1_SocialEngineering
- Hacker című film egyes jelenetei

DOS, DDOS

- Elárasztásos támadás
- Egy szerveralkalmazást olyan mennyiségű kéréssel bombáznak, amelytől előbb-utóbb megfekszik
- Védekezés
  - Csak azok a szolgáltatások menjenek ki, amelyek szükségesek
  - Tűzfal alkalmazása
  - Update, patch

SQL Injection

- SELECT * FROM users WHERE id='.$x.';
- Normál eset: $x= 5 => 1 user jön vissza
- Pl:
  - $x = 5 .' OR 10=10' => Minden user visszajön
  - $x=5.'; INSERT INTO user (id,name, pwd) VALUES (6,\'fz\',\'fz\');' => Új felhasználó jön létre
- Védekezés
  - A fejlesztett kódban az adatbevitel ellenőrzése
  - A bevitt adatok tisztítása

XSS – Cross Site Scripting

- Egy közönséges weboldalon elhelyezek olyan scriptet, amely egy másik weboldalról tölt be kódot (pl. Hozzászólás oldalon)
- A felhasználó gépén lefut az idegen forrásból származó javascript kód és AJAX technikával lehívja az ártó kódot (JAVA, FLASH, ActiveX, EXE)
- Védekezés
  - Idegen tartalmak felvitele csak szűrt módon (csak bizonyos TAG-ek vihetők be)
  - Moderált tartalomkezelés

Nem publikus URL-ek autentikáció nélküli elérhetőségének vizsgálata

- Behatolás módja
  - Felderítés, hogy milyen rendszer fut a szerveren
  - A rendszer nyílt forráskódú
  - Az ismert rendszerek hibáinak listája alapján
  - Speciális URL-ek meghívása
  - Speciális kérések beküldése
- Védekezés
  - PATCH, Update
  - Nem default telepítés
  - Nem default usernév, jelszó használata

Minta Apache logjából

- 203.252.243.163 - - [01/Feb/2011:00:19:11 +0100] "GET //phpmyadmin/ HTTP/1.1" 301 230
- 203.252.243.163 - - [01/Feb/2011:00:19:16 +0100] "GET //phpMyAdmin/ HTTP/1.1" 301 230
- 203.252.243.163 - - [01/Feb/2011:00:19:21 +0100] "GET //pma/ HTTP/1.1" 404 202
- 203.252.243.163 - - [01/Feb/2011:00:19:26 +0100] "GET //dbadmin/ HTTP/1.1" 404 206
- 203.252.243.163 - - [01/Feb/2011:00:19:37 +0100] "GET //phppgadmin/ HTTP/1.1" 404 209
- 203.252.243.163 - - [01/Feb/2011:00:19:42 +0100] "GET //PMA/ HTTP/1.1" 301 230
- 203.252.243.163 - - [01/Feb/2011:00:19:47 +0100] "GET //admin/ HTTP/1.1" 404 204
- 118.129.166.97 - - [01/Feb/2011:01:28:35 +0100] "GET HTTP/1.1 HTTP/1.1" 400 226
- 118.129.166.97 - - [01/Feb/2011:01:28:37 +0100] "GET /phpmyadmin/scripts/setup.php HTTP/1.1" 301 230
- 118.129.166.97 - - [01/Feb/2011:01:29:21 +0100] "GET HTTP/1.1 HTTP/1.1" 400 226
- 118.129.166.97 - - [01/Feb/2011:01:29:22 +0100] "GET /phpmyadmin/scripts/setup.php HTTP/1.1" 301 230
- 118.129.166.97 - - [01/Feb/2011:01:30:15 +0100] "GET HTTP/1.1 HTTP/1.1" 400 226
- 118.129.166.97 - - [01/Feb/2011:01:30:21 +0100] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 301 230
- 202.155.208.243 - - [01/Feb/2011:05:09:11 +0100] "GET /3rdparty/phpMyAdmin/scripts/setup.php HTTP/1.1" 301 230
- 202.155.208.243 - - [01/Feb/2011:05:09:23 +0100] "GET /PMA/scripts/setup.php HTTP/1.1" 301 230
- 202.155.208.243 - - [01/Feb/2011:05:09:28 +0100] "GET /PMA2005/scripts/setup.php HTTP/1.1" 404 223
- 202.155.208.243 - - [01/Feb/2011:05:09:33 +0100] "GET /SQL/scripts/setup.php HTTP/1.1" 404 219
- 202.155.208.243 - - [01/Feb/2011:05:09:39 +0100] "GET /SSLMySQLAdmin/scripts/setup.php HTTP/1.1" 404 229
- 202.155.208.243 - - [01/Feb/2011:05:10:17 +0100] "GET /cpanelmysql/scripts/setup.php HTTP/1.1" 404 227
- 202.155.208.243 - - [01/Feb/2011:05:10:22 +0100] "GET /cpanelphpmyadmin/scripts/setup.php HTTP/1.1" 404 232
- 202.155.208.243 - - [01/Feb/2011:05:10:44 +0100] "GET /db/scripts/setup.php HTTP/1.1" 301 230
- 202.155.208.243 - - [01/Feb/2011:05:11:21 +0100] "GET /mysqlmanager/scripts/setup.php HTTP/1.1" 404 228
- 202.155.208.243 - - [01/Feb/2011:05:11:31 +0100] "GET /pMA/scripts/setup.php HTTP/1.1" 404 219
- 202.155.208.243 - - [01/Feb/2011:05:11:37 +0100] "GET /php-my-admin/scripts/setup.php HTTP/1.1" 404 228
- 202.155.208.243 - - [01/Feb/2011:05:11:42 +0100] "GET /php-myadmin/scripts/setup.php HTTP/1.1" 404 227
- 202.155.208.243 - - [01/Feb/2011:05:11:48 +0100] "GET /phpMyAdmin-2.2.3/scripts/setup.php HTTP/1.1" 301 230
- 202.155.208.243 - - [01/Feb/2011:05:11:53 +0100] "GET /phpMyAdmin-2.2.6/scripts/setup.php HTTP/1.1" 301 230
- 202.155.208.243 - - [01/Feb/2011:05:15:32 +0100] "GET /phpMyAdmin-2.6.4/scripts/setup.php HTTP/1.1" 301 230
- 202.155.208.243 - - [01/Feb/2011:05:15:55 +0100] "GET /phpMyAdmin-2.7.0-rc1/scripts/setup.php HTTP/1.1" 301 230
- 202.155.208.243 - - [01/Feb/2011:05:16:01 +0100] "GET /phpMyAdmin-2.7.0/scripts/setup.php HTTP/1.1" 301 230
- 202.155.208.243 - - [01/Feb/2011:05:16:12 +0100] "GET /phpMyAdmin-2.8.0-rc1/scripts/setup.php HTTP/1.1" 301 230
- 202.155.208.243 - - [01/Feb/2011:05:16:17 +0100] "GET /phpMyAdmin-2.8.0-rc2/scripts/setup.php HTTP/1.1" 301 230
- 202.155.208.243 - - [01/Feb/2011:05:16:25 +0100] "GET /phpMyAdmin-2.8.0.1/scripts/setup.php HTTP/1.1" 301 230
- 202.155.208.243 - - [01/Feb/2011:05:19:24 +0100] "GET /~/admin/scripts/setup.php HTTP/1.1" 404 223
- wolf.serverffs.com - - [01/Feb/2011:09:29:36 +0100] "GET /user/soapCaller.bs HTTP/1.1" 404 216
- wolf.serverffs.com - - [01/Feb/2011:09:30:07 +0100] "GET /user/soapCaller.bs HTTP/1.1" 404 216
- wolf.serverffs.com - - [01/Feb/2011:09:30:16 +0100] "GET /user/soapCaller.bs HTTP/1.1" 404 216

Képzés

- Ethical Hacking tanfolyam (NetAcademia)
- Hacker kézikönyv
- Google a hacker legjobb barátja

White HAT hackerek

- **1. Stephen Wozniak:**
"Woz" is famous for being the "other Steve" of Apple . Wozniak, along with current Apple CEO Steve Jobs, co-founded Apple Computer. He has been awarded with the National Medal of Technology as well as honorary doctorates from Kettering University and Nova Southeastern University. Additionally, Woz was inducted into the National Inventors Hall of Fame in September 2000.
Woz got his start in hacking making blue boxes, devices that bypass telephone-switching mechanisms to make free long-distance calls. After reading an article about phone phreaking in Esquire, Wozniak called up his buddy Jobs. The pair did research on frequencies, then built and sold blue boxes to their classmates in college. Wozniak even used a blue box to call the Pope while pretending to be Henry Kissinger.

- **2. Tim Berners-Lee:**
Berners-Lee is famed as the inventor of the World Wide Web, the system that we use to access sites, documents and files on the Internet. He has received numerous recognitions, most notably the Millennium Technology Prize.
While a student at Oxford University, Berners-Lee was caught hacking access with a friend and subsequently banned from University computers. w3.org reports, "Whilst [at Oxford], he built his first computer with a soldering iron, TTL gates, an M6800 processor and an old television." Technological innovation seems to have run in his genes, as Berners-Lee's parents were mathematicians who worked on the Manchester Mark1, one of the earliest electronic computers.

- **3. Linus Torvalds:**
Torvalds fathered Linux, the very popular Unix-based operating system. He calls himself "an engineer," and has said that his aspirations are simple, "I just want to have fun making the best damn operating system I can."
Torvalds got his start in computers with a Commodore VIC-20, an 8-bit home computer. He then moved on to a Sinclair QL. Wikipedia reports that he modified the Sinclair "extensively, especially its operating system." Specifically, Torvalds hacks included "an assembler and a text editor…as well as a few games."

- **4. Richard Stallman:**
Stallman's fame derives from the GNU Project, which he founded to develop a free operating system. For this, he's known as the father of free software. His "Serious Bio" asserts, "Non-free software keeps users divided and helpless, forbidden to share it and unable to change it. A free operating system is essential for people to be able to use computers in freedom."
Stallman, who prefers to be called rms, got his start hacking at MIT. He worked as a "staff hacker" on the Emacs project and others. He was a critic of restricted computer access in the lab. When a password system was installed, Stallman broke it down, resetting passwords to null strings, then sent users messages informing them of the removal of the password system.

- **5. Tsutomu Shimomura:**
Shimomura reached fame in an unfortunate manner: he was hacked by Kevin Mitnick. Following this personal attack, he made it his cause to help the FBI capture him.
Shimomura's work to catch Mitnick is commendable, but he is not without his own dark side. Author Bruce Sterling recalls: "He pulls out this AT&T cellphone, pulls it out of the shrinkwrap, finger-hacks it, and starts monitoring phone calls going up and down Capitol Hill while an FBI agent is standing at his shoulder, listening to him."