1. A kurzus követelményeinek és menetének ismertetése, az IT biztonság fogalma, a sérülékenység-vizsgálatok erkölcsi és jogi háttere

Tartalom

1. A kurzus követelményeinek és menetének ismertetése
2. Az IT biztonság fogalma
3. A sérülékenység-vizsgálatok erkölcsi és jogi háttere
4. Feladatok

---

1. A kurzus követelményeinek és menetének ismertetése

1.1. A kurzus követelményei

a. 6 db kis beadandó, amiket hetente kell elkészíteni, és emailben elküldeni. Ha ezeket elfogadom, a biztos kettes megvan.

b. 1 db nagyobb beadandó (egy működő exploit megírása), amire 2 hét áll rendelkezésre. Ennek megírása szükséges az ötöshöz.

1.2. A beadandókkal kapcsolatos követelmények

- Az állomány formátuma: PDF,
- az állomány neve: *vezeteknev_keresztnev*_ora*xx_éééé-hh-nn*.pdf, ahol
  - a vezetéknév és a keresztnév ékezetek nélkül van, *xx*: a hét száma; a többi pedig a készítés dátuma: *éééé*: év, *hh*: hónap sorszáma, *nn*: nap (a dátum jelzi majd a verziókat, ha esetleg újra el kellene küldeni).
  - Pl. lengyel_robert_ora01_2019-02-12.pdf
- A megfelelően elnevezett PDF-et 7-zip-pel, "betonlufi" jelszóval rejtjelezzük, majd töltsük fel a http://len.uw.hu /szerda/feltolto.php oldalon.
- Segéd batch állomány:

```
set datum=2019-02-12
set ora_sorszama=01
rem *************************
set nev=lengyel_robert
set allomanynev=%nev%_ora%ora_sorszama%_%datu
del feltolteni_%datum%.7z
ren a.pdf %allomanynev%.pdf
"c:\Program Files\7-Zip\7z.exe" a feltolteni_
 -mhe=on -pbetonlufi %allomanynev%.pdf
curl -i -F allomany=@feltolteni_%datum%.7z \
http://len.uw.hu/szerda/feltolto.php
```

Tartalmi követelmények

1. Tartalmazza, hogy mi volt a feladat.
2. Tartalmazza a lépéseket, amikkel megkaptad az eredményt.
   - Olyan részletesen írd le, hogy ha ezzel évekig nem foglalkoznál, akkor azután is el tudd újra végezni a feladatot a leírásod alapján (reprodukálhatóság), de ne részletesebben. Törekedj a tömörségre, a lényeg leírására. Ami nem kapcsolatos a lépések reprodukálásával, az valószínűleg nem is lényeges.
   - Minden egyes lépésnél szerepeljen a használt parancs és az arra kapott kimenet.
     - Grafikus használói felületű (GUIs) eszköznél ha a parancs leírható szövegesen (pl. Menü: File > Save), akkor elég úgy is, a kimenete viszont képernyőképpel szerepeljen.
     - Parancssoros eszköz kimenetét rád bízom, lehet szövegesen bemásolva és képernyőképpel is, de mindenképpen látszódjon a prompt, a parancs, és a kimenet is pl.

```
root@kali:~# ps -e | grep tty1
  307 tty1     00:00:00 login
  419 tty1     00:00:00 bash
root@kali:~#
```

3. Tartalmazza az eredményt.
   - Egy eszköz kimenetének szöveges, vagy képernyőképes beillesztése nem elég eredményként. Ha a kimenet tartalmazza a feladatban megválaszolandó kérdésre a választ, akkor elég, ha kiemeled azt valamilyen színnel, ha nem tartalmazza, le kell írni szavakkal is az eredményt. Ez azért fontos, mert így látom, hogy tudod, hogyan kell az egyes kimeneteket értelmezni.

1.3. A kurzus menete

1. Az IT biztonság fogalma, a kurzus követelményeinek és menetének ismertetése, sérülékenység-vizsgálatok erkölcsi és jogi háttere, a laborkörnyezet ismertetése, a pentesztelés folyamata.
2. Az eszközök bemutatása: Kali Linux, a legfontosabb Linux parancsok penteszteréknek, VirtualBox, virtuális gépek hálózati beállításai.
3. Hálózati eszközök (Netcat, Wireshark, Tcpdump) és alapfogalmak (bind shell, reverse shell, helyi tűzfal, NAT).
4. Passzív információgyűjtés: Google hacking, web scraping, közösségi oldalak használata, email harvesting (harvester), netcraft, whois.
5. Aktív információgyűjtés: DNS enumeráció, hálózat szkennelése, portok szkennelése, szkennelési módok, szolgáltatások azonosítása, Nmap.
6. Aktív információgyűjtés 2.: SMB enumeráció, SMTP enumeráció, SNMP enumeráció, NetBIOS. Nmap szkriptek.
7. Sérülékenység-vizsgálati módszerek, sérülékenység szkennerek és pentesztelés, sérülékenység-adatbázisok, searchsploit, Metasploit alapok.
8. Puffer túlcsorduláson alapuló támadások: Memória-kezelés, a stack működése, Assembly alapok, fuzzing, memóriavédelmek (DEP, ASLR), Immunity Debugger, mona.py.
9. Puffer túlcsordulás kihasználása Windows rendszerekben, az Immunity debugger használata, BoF exploit fejlesztés.
10. Puffer túlcsordulás kihasználása Linux rendszerekben, a gdb debugger használata, edb, BoF exploit fejlesztés.
11. A hozzáférés fenntartása: állományok fel- és letöltése, Meterpreter, Netcat, Metasploit post modulok, backdoorok, anti-vírus alkalmazások megkerülése.
12. A pentesztelés gyakorlata, beszélgetés egy vendégelőadóval.

---

2. Az IT biztonság fogalma

Az IT rendszer biztonságának feltételei

1. Titkosság (confidentiality): csak az arra illetékesek olvashassák az adatokat,
2. épség (integrity): csak az arra illetékesek módosíthassák az adatokat,
3. működőképesség (availability): a működésének meghiúsítására irányuló támadások (pl. denial-of-service támadások) megakadályozása,
4. hitelesség (authenticity): minden szereplő (használó, szerver, szoftverpéldány) valóban az, akinek mondja magát,
5. letagadhatatlanság (nonrepudiation): az adatokon végzett módosításokat, vagy elküldött üzeneteket a módosító ill. küldő ne tudja letagadni.

---

3. A sérülékenység-vizsgálatok erkölcsi és jogi háttere

A kurzus során megismert eszközöket és parancsokat csak a tananyagban leírt laboratóriumi körülmények között szabad használni. A legtöbb támadás illegális, ha olyan gépeken hajtjuk végre, amikre nincs írásbeli engedélyünk. Nem vállalok felelősséget azért, ha valaki ezeket a kurzuson kívül végzi el.

Egy támadás etikusságának ("legálisságának") feltételei

1. A támadónak legyen előzetes engedélye (írásbeli szerződés, "bug bounty" program) a rendszer megtámadására, és
2. a támadó a talált sérülékenységeket nem osztja meg harmadik féllel addig az időtartamig ami a szerződésben vagy a "bug bounty" program feltételei között szerepel, vagy vitás kérdésben addig amíg nincs elegendő ideje az érintett szoftver fejlesztőinek vagy rendszer üzemeltetőinek az adott hiba kijavítására. Itt hetekről, akár hónapokról van szó.

---

4. Feladatok

1. Küldj egy pár sor bemutatkozást, majd mentsd el PDF-ben a fentiek szerint és töltsd fel a http://len.uw.hu /szerda/feltolto.php címre. A PDF tartalmazza a neved, az emailcímed, szakod, hanyadik féléved, szakmai érdeklődésedet, és hogy mit vársz a kurzustól. Határidő: holnapután 8:00.
2. Következő órára hozz egy külső HDD-t, vagy USB-t a VM-ek hazaviteléhez (min. 8 GB)
