2. óra: Az eszközök bemutatása: Kali Linux, a legfontosabb Linux parancsok pentesztereknek, VirtualBox, virtuális gépek hálózati beállításai.

Tartalom

---

1. VirtualBox, virtuális gépek hálózati beállításai

A VirtualBox (hivatalosan: Oracle VM Virtualbox) egy nyílt forráskódú, ingyenes alkalmazás, ami lehetővé teszi virtuális gépek (virtual machines - VMs) futtatását, a VM állapotainak elmentését (snapshotok) készítését, és azok visszaállítását. Letölthető innen: https://www.virtualbox.org/

1.1. Olvasnivaló

- Oracle VM VirtualBox User Manual (telepítés után elérhető itt: c:\Program Files\Oracle\VirtualBox\doc\UserManual.pdf)
- A VBoxManage parancs súgója (help)

1.2. Fogalmak

a. **Gazda op. rendszer (host OS)**: ez az op. rendszer fut a valódi hardveren, és ez futtatja a VirtualBox-ot. Lehet Windows, Mac OS X, Linux és Solaris.

b. **Vendég op. rendszerek (guest OS-es)**: ezek futnak a VirtualBoxban létrehozott virtuális gépeken (VM-ek). Ez bármelyik x86 alapú op. rendszer lehet (DOS, Windows, Linux, Solaris, Mac OS X, OS/2, FreeBSD, OpenBSD).

c. **Shared folder**: a gazda és a vendég gép által közösen használt könyvtár (mappa), ami állományok gépek közötti mozgatására használható.

d. **Guest additions**: a VM-be telepítendő komponensek (driverek, alkalmazások) ami lehetővé teszi a gazda és a vendég közötti a közös vágólapot, a megosztott könyvtár használatát és az egér integrációt.

1.3. Használata

1.3.1 GUI-val

1. A VirtualBox indítása: Start menüből.
2. A grafikus használói felület (GUI) részei
   - "Manager" ablak (Oracle VM VirtualBox Manager)
   - "VM" ablak: ami a VM képernyőjén jelenne meg, az ebben az ablakban látható.
3. VM létrehozását lásd a parancssoros résznél.

a. A VirtualBox beállításai: Menü: File > Preferences

b. Az éppen kijelölt VM beállításai: Ctrl + S

c. Snapshot (elmentett VM állapot) létrehozása, visszaállítása, törlése...

d. Host key (pl. jobb Ctrl), képernyőkép készítése: Host + E.

1.3.2 Parancssorosan (VBoxManage)

a. A VBoxManage.exe könyvtárát a PATH környezeti változóba kell tenni kézzel. Ha mégsincs ott, akkor először ezt kell futtatni:

```
@set path=%path%;c:\Program Files\Oracle\VirtualBox\
```

b. A VM-eket érdemes parancssorosan létrehozni. Lásd az órán kiosztott 01_create_pentest_win7.bat és 02_create_kali.bat állományokat. A pentest_win7-en jelszó: Alice/offensive2017, a Kalin: root/toor.

c. A gép BIOS órájának visszatekerése 1 nappal (86 400 000 ms-dal). Indítás előtt a pentest_win7-et vissza kell állítani 2019.02.20-ra.

```
VBoxManage modifyvm pentest_win7 \
--biossystemtimeoffset -86400000
```

d. Gép bekapcsolása (gui, egyéb mód: headless)

```
VBoxManage startvm pentest_win7 --type gui
```

e. Gép kikapcsolása és snapshot visszaállítása

```
VBoxManage controlvm pentest_win7 poweroff
VBoxManage snapshot  pentest_win7 restore crash_elott
```

f. Gép újraindítása. A várakozás - ismeretlen okból, de - szükséges.

```
VBoxManage controlvm pentest_win7 poweroff
VBoxManage snapshot  pentest_win7 restore crash_elott
timeout /t 1
VBoxManage startvm   pentest_win7
```

1.4. A virtuális gépek hálózati beállításai

1. A Manager ablakban bal oldalon a gép kijelölése, majd bill: Ctrl + S.
2. A felugró **<vm> - Settings** ablakban bal oldalon a "Network" kiválasztása.
3. A megfelelő adapter fült kiválasztva a **"Attached to"** legördülő listából választható ki a hálózati beállítás.

A VM-ek hálózati beállításai közül mi a "NAT"-ot és a "Host-only Adapter"-t fogjuk használni.

- **NAT**: a VM használja a gazdagép (host machine) internetkapcsolatát. A VM alapértelmezett IPv4 címe a 10.0.x.0/24 tartományba esik ahol az x 2-ről indul és minden újabb NAT hálózat eggyel nagyobb számot kap. Pl.: 10.0.2.15
- **Host-only Adapter**: a VM csak a gazdagépet és a gazdagépen futó más VM-eket látja, ha azok "Host-only Adapter" beállításban futnak. A VM alapértelmezett IPv4 címe 192.168.56.101 és egyesével növekszik minden új VM esetében pl. 192.168.56.**102** stb.

Az IP cím lekérdezésének parancsa Windowson: `ipconfig`, Linuxon: `ifconfig`.

---

2. Kali Linux

- A Kali Linux egy Debian Linux, több száz előre telepített alkalmazással.

2.1. Telepítése

1. "Kali Linux Vm 32 Bit 7z" (2,4 GB) letöltése innen: <https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>
2. Kitömörítés
3. Írtam egy létrehozó szkriptet a VirtualBox-hoz
4. Alapértelmezett jelszó: root/toor ~~toor~~ toor123

---

3. Legfontosabb Linux parancsok pentesztereknek

Olvasnivaló

1. man parancs

```
man ls
```

2. http://www.mediacollege.com/linux/command/linux-command.html
3. http://www.mediacollege.com/linux/command/shell-command.html

3.1. Általános

Mit?	Hogyan?
Jelszó megváltoztatása	`passwd`
Terminálablak törlése	`clear`
A gép lekapcsolása	`shutdown now`
A gép újraindítása	`shutdown -r now`
Kernel verzió lekérdezése	`uname -r`
Distro lekérdezése	`cat /etc/issue`
Egy `alice` nevű felhasználó létrehozása.	`adduser alice`

3.2. Állományok, könyvtárak

Mit?	Hogyan?
Jelenlegi könyvtár nevének kiírása	`pwd`
A jelenlegi könyvtár tartalmának kilistázása	`ls -al`
Egy `ujdir` nevű könyvtár létrehozása	`mkdir ujdir`
Az `ujdir` könyvtárba lépés	`cd ujdir`
Egy `a.txt` nevű állomány létrehozása echo-val.	`echo Valami > a.txt`
Az `a.txt` állomány kilistázása.	`cat a.txt`
Az `a.txt` állomány szerkesztése	`nano a.txt`
Az `a.txt` állomány másolása `b.txt`-té.	`cp a.txt b.txt`
A `b.txt` állomány mozgatása a szülőkönyvtárba és átnevezése `a.txt`-té.	`mv b.txt ../a.txt`
A `/bin/pwd` állományról információk kiírása.	`file /bin/pwd`
Az `a.txt` állomány törlése	`rm a.txt`

3.3. Állományok keresése

Mit?	Hogyan?
Az `ls` nevű állomány megkeresése a `/usr/lib` könyvtárban, vagy bármelyik alkönyvtárában (a névre pontos egyezés)	`find /usr/lib -name ls`
Az `ls` szövegre végződő nevű állományok megkeresése a `/bin` könyvtártól lefelé.	`find /bin -name *ls`
Az `ls` nevű állomány megkeresése az elérési útban (PATH)	`which ls`
Az `mlocate` csomag telepítés a `locate` parancs használatához.	`apt-get install mlocate`
Az állománynéveket tároló adatbázis frissítése a `locate` parancs használatához.	`updatedb`
Az `ls` nevű állomány megkeresése az adatbázisban (pontos egyezés).	`locate -b '\ls'`
Az `openvpn` szöveget tartalmazó nevű állomány megkeresése az adatbázisban (nem pontos egyezés).	`locate -b 'openvpn'`

3.4. Hálózat

Mit?	Hogyan?
A nyitva lévő portok listázása	`netstat -antup`
Hálózati adapterek és IP címük listázása	`ifconfig`
Az `eth0` nevű hálózati adapter kikapcsolása.	`ifdown eth0`
Az `eth0` nevű hálózati adapter bekapcsolása.	`ifup eth0`
Az SSH szerver elindítása	`service ssh start`
Az SSH szerver leállítása	`service ssh stop`
Az SSH szerver induljon el minden bootoláskor.	`systemctl enable ssh`
Az SSH szerver ne induljon el minden bootoláskor.	`systemctl disable ssh`

3.5. Adatfeldolgozás

Mit?	Hogyan?
A nevükben `lr` szöveget tartalmazó állományok teljes elérési útjainak a `b.txt`-be gyűjtése.	`locate -b 'lr' > b.txt`
A `b.txt` sorainak száma.	`wc -l b.txt`
A `b.txt` utolsó 10 sorának kiírása	`tail b.txt`
A `b.txt` első 10 sorának kiírása	`head b.txt`
A `b.txt` sorainak kiírása számozva.	`cat -n b.txt`
A `b.txt` sorainak száma, amik tartalmazzák az `openvas` szöveget.	`grep openvas b.txt | wc -l`
A `b.txt` sorainak száma, amik NEM tartalmazzák az `openvas` szöveget.	`grep -v openvas b.txt | wc -l`
Reguláris kifejezés használata	`grep -o 'openv[^/]*' b.txt`
Az `/etc/passwd` állomány sorainak felosztása a ":" karakter szerint (`-d:`, és ezekből az első mezőt kiemelni.`-f1`.	`cut -d: -f1 /etc/passwd`
A `b.txt`-ben szereplő második könyvtárainak sorba rendezése, és az ismétlődések kiszedése.	`cut b.txt -d "/" -f3 | sort -u`
Az előző az előfordulási számokkal. Az `uniq` parancshoz kell egy `sort`	`cut b.txt -d "/" -f3 | sort | uniq -c`

The Art of Linux

3.6. Bash szkripting

- Egy `a.sh` nevű állomány létrehozása és szerkesztése

```
nano a.sh
```

```
#!/bin/bash # Shebang
runid=$1    # parancssoros argumentum $1 első arg
task=nmap   # értékadás változónak
echo ${task}_${runid} # változók használata
for line in $(head /etc/passwd); do # ciklus1
    echo ${line}
    echo ${line} | cut -d: -f1
done
# ciklus2
for ip in $(seq 50 55); do echo 195.56.100.${ip}; done
# chmod 755 a.sh
# ./a.sh 01
```

---

4. Feladatok

4.1. A 2. heti beadandó feladat

Határidő: jövő hétfő 8:00

1. Telepítsd otthon a Kali és a Pentest_win7 gépeket. Elég az eredményről 1-1 kép.
2. Mlocate-tel (`locate` parancs) keress olyan állományokat, amelyeknek nevében (nem az elérési útjában) szerepel a monogramod, rendezd azokat sorrendbe

---