Virtualizált hackerek

Veres-Szentkirályi András

Silent Signal
vsza@silentsignal.hu

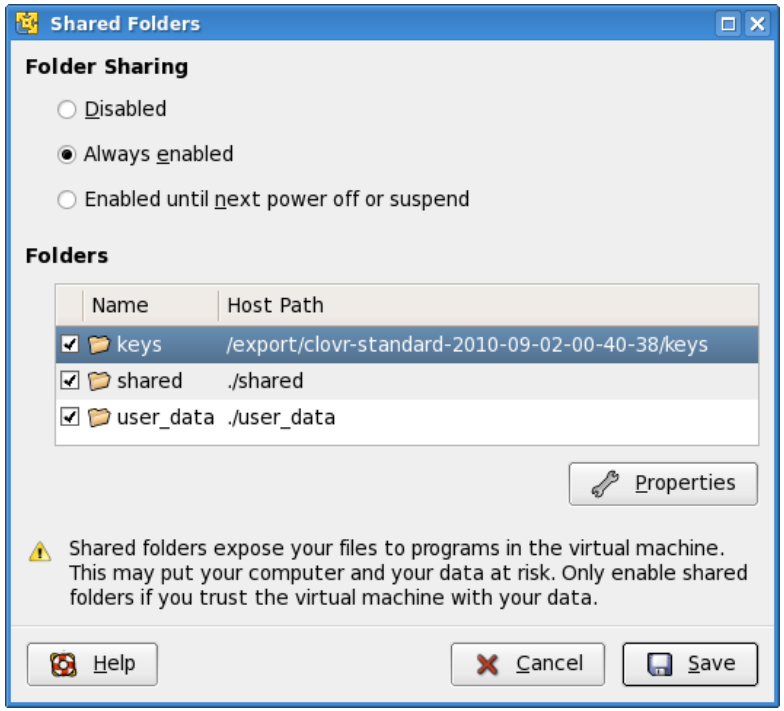
Virtualization Day
2010. november 5.

Tartalom

1. Biztonságos-e a virtualizáció?
   - Desktop példa: VMware shared folder bug (2008)
   - Szerver példa: VMware cloudburst (2009)
   - Ellenpélda: Qubes (2010)
2. Virtualizálhatók-e a hackerek?
   - Bevezetés
   - Tervezés
   - Megvalósítás
   - Tapasztalatok
3. Összefoglalás

Feature: shared folder

- szinte minden asztali virtualizációs termék alapszolgáltatása
- szegény ember fájlszervere
- izolációt és biztonságot ígér (ahogy maga a virtualizáció is)



Bug: CVE-2008-0923

- „Directory traversal vulnerability in the Shared Folders feature for VMWare ACE 1.0.2 and 2.0.2, Player 1.0.4 and 2.0.2, and Workstation 5.5.4 and 6.0.2 allows guest OS users to read and write arbitrary files on the host OS via a multibyte string that produces a wide character string containing .. (dot dot) sequences, which bypasses the protection mechanism, as demonstrated using a "%c0%2e%c0%2e" string." – CVE
- tipikus wide string hiba: a `PathName` változón azután hajtódik végre multibyte $\rightarrow$ widechar konverzió, miután lefutott a biztonsági ellenőrzés, amely .. karaktereket (%2e%2e) keres.
- webalkalmazás penteszterek számára triviális a kihasználás: a CVE idézetben látható bájtsorozat átmegy az ellenőrzésen, majd .. karakterré alakul a konverzió során.

Feature: VMware SVGA II

- fizikai megfelelővel nem rendelkező grafikus kártya
- sokaknak ismerős Windows vendég eszközkezelőjéből
- 2D/3D gyorsítás, gyakori vendég operációs rendszerekhez saját meghajtóprogrammal
- ezek közül a `xf86-video-vmware` (XFree86 meghajtó) nyílt forrású, tanulmányozható az architektúra

Bug: Cloudburst

- framebuffer a gazda memóriájában
- a vendég írhatja-olvashatja a framebuffert
- a `SVGA_CMD_RECT_COPY` művelet bugjai így hozzáférést engedhetnek a vendég részéről a gazda memóriájában
- érintett volt a Workstation, Fusion és ESX is
- további implementációs részletek Kostya Kortchinsky 2009-es Black Hat előadásában
- tanulság: a virtualizáció által adott réteg nem biztonsági, hanem egy újabb lehetőség bugvadászatra

Fejlesztő: Invisible Things Lab

- 2007-ben alapította Joanna Rutkowska
- „érdekesebb" támadásokkal foglalkoznak
  - Blue Pill: OS ultravékony VM-be zárása újraindítás nélkül
  - Vista UAC kijátszás
  - Xen Owning Trilogy
  - TXT (Trusted Execution Technology) támadások
  - TrueCrypt FDE Evil Maid
  - AMT rootkitek (ring -3?)
- rámutatnak a jelenlegi „lakossági" operációs rendszerek alapbető biztonsági hiányosságaira

Qubes: lakosági virtualizáció

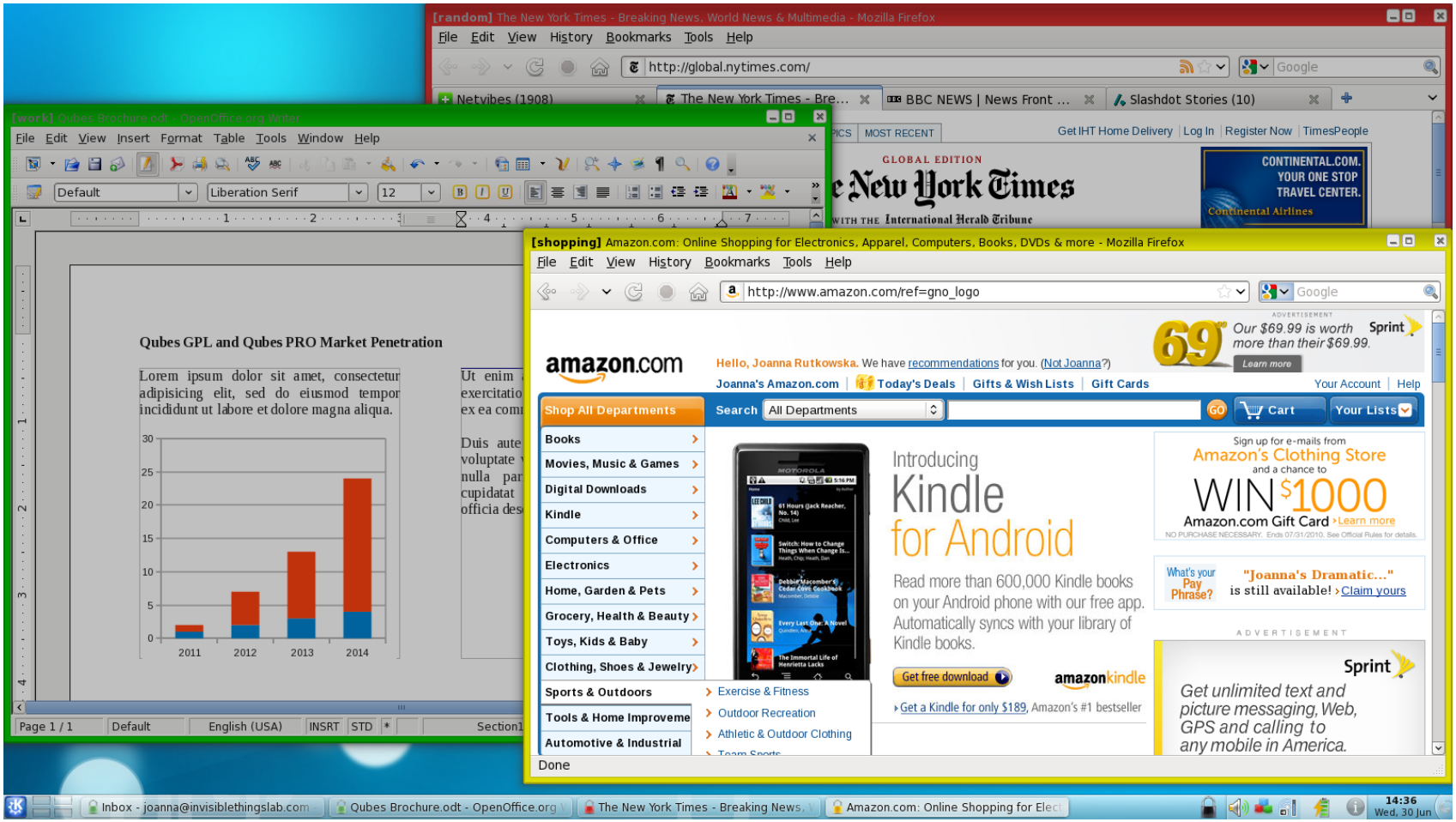
- Xen, X, Linux alapok
- külön VM ablakok egy közös desktopon

  NetVM hálózati kártyában sem bízunk

  AppVM védelmi szintek szerint bontva („utca, lakás, munkahely”)

  Eldobható egy-egy PDF megnyitásához
- tervek: külön tároló VM, biztonságos boot TXT alapokon
- tanulság: a biztonsági célú virtualizáció nem feltétlenül kényelmetlen

Qubes screenshot (forrás: `http://qubes-os.org`)



WTF wargame

- military és játékos körökben háborúszimulációt jelent

WTF wargame

- military és játékos körökben háborúszimulációt jelent
- hacker szlengbe kerülés: WarGames (Háborús játékok, 1983)
  - (vö. wardialing, wardriving, warbiking, warboating, . . .)
- „a server that is set up specifically for the purpose of being hacked into. This allows the hacker to have a server to hack into, without the need to worry about the legal issues, as the owner is knowingly allowing this to happen."

  – WordIQ.com

Történelem

2003. július 5–6. első Hacktivity

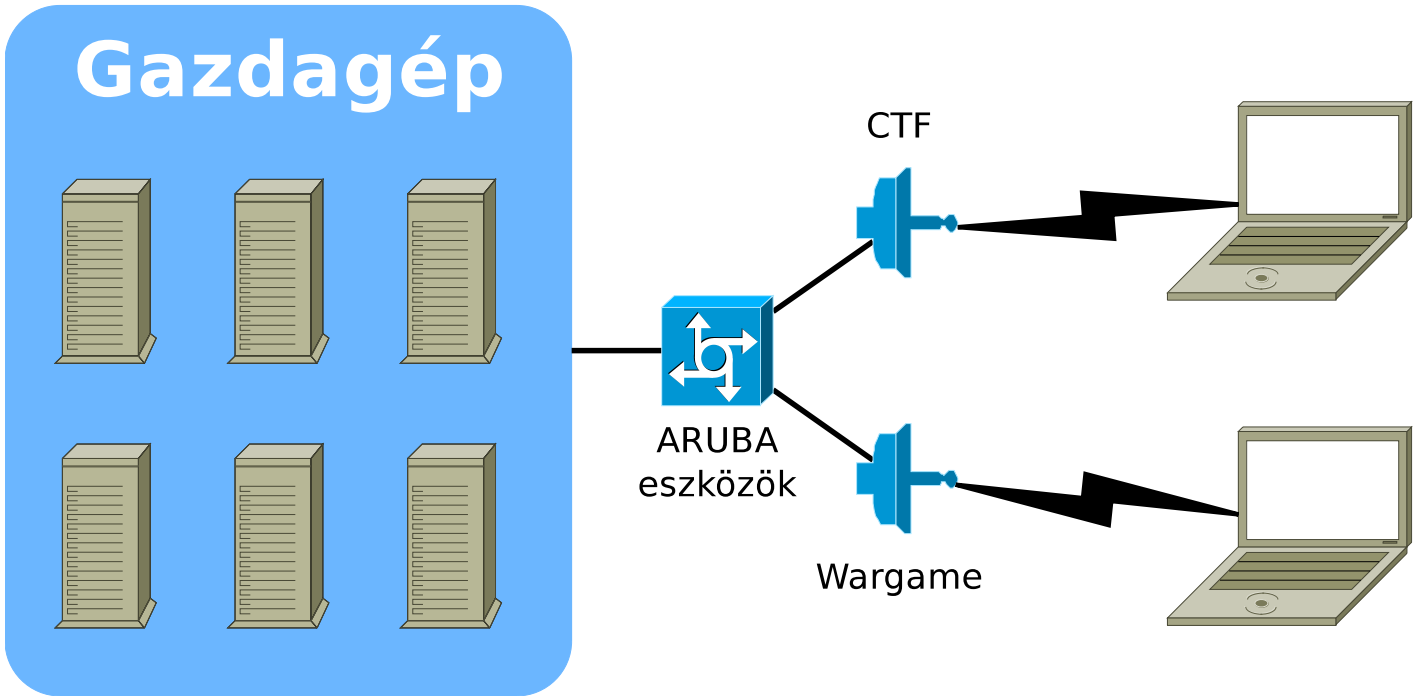
2004. augusztus 14–15. első wargame-es Hacktivity

2008. szeptember 20–21. első „általunk tervezett” wargame

2010. május 8–9. „How Strong is Your Fu?” – inspiráció

2010. szeptember 18–19. első hivatalos Silent Signal wargame

Játéktér



- egy gazdagép
- több vendég VM (célpontok és eredménytábla)
- két hálózat (Wargame és CTF)

Célpontok

- célpont: VM, amin a játékosnak root / rendszergazda jogosultságot kell szereznie pontok reményében
- jogosultság megszerzése bizonyítékkal igazolható
  - UNIX-szerű rendszereken `/root/proof.txt`
  - Windowson Rendszergazda asztaláról ugyanez
- bizonyítékot megoszthatják egymással a játékosok
  - rendszeresen cserélni kell
  - lehetőleg automatizált módon
  - mind a célponton, mind az elfogadó oldalon
- magas megszerezhető jogosultság $\rightarrow$ félóránként vissza kell állítani a gépeket „szűz” állapotba

Gazdagép

- vas: 8 mag, 12 GB memória
- OS: VMware vSphere Hypervisor 4.1 (korábban „free ESXi”)
- ingyenes, gyorsan települ, sokan ismerik
- rengeteg leírás található weben az automatizálási lehetőségeiről (félóránkénti visszaállításhoz)

Hálózat

- helyszínen külön SSID → külön VLAN
- ideális megoldás: külön VLAN-ban a gépek is
- idei időtakarékos megoldás:
  - egy VLAN
  - L3 szeparáció (tűzfal)
  - rengeteg hibalehetőség
  - gépek egymásról támadhatók
- lehetséges problémaforrás: eredménytábla elérhetősége

Automatizált visszaállítás a'la vSphere

- félóránként visszaállításra lenne szükség, vSphere automatizálható, nyert ügy
- Java alkalmazáson keresztül minden adat kiolvasható

Automatizált visszaállítás a'la vSphere

- félóránként visszaállításra lenne szükség, vSphere automatizálható, nyert ügy
- Java alkalmazáson keresztül minden adat kiolvasható
- `com.vmware.vim25.RestrictedVersion` kivétel
- ingyenes változat esetén csak olvasható a távoli interfész

Automatizált visszaállítás a'la vSphere

- félóránként visszaállításra lenne szükség, vSphere automatizálható, nyert ügy
- Java alkalmazáson keresztül minden adat kiolvasható
- `com.vmware.vim25.RestrictedVersion` kivétel
- ingyenes változat esetén csak olvasható a távoli interfész
- megoldás: SSH bekapcsolása (Google a barátom), `vim-cmd vmsvc/snapshot.revert`

Az elkészült szkript

- választott nyelv: Python (vö. `import antigravity`)
- felhasznált könyvtárak:
  - libssh2 visszaállítás és bizonyíték frissítés (SCP)
  - mysqldb központi adatbázis (bizonyíték- és géptár)
- cronból futtatható félóránként
- visszaállítja a gépet a megfelelő állapotba
- lecseréli a bizonyítékokat (kivárja az SSH feléledését)
- frissíti a pontszámokat (CTF esetén)

Tapasztalatok

- ESXi-be Workstation telepítése nem triviális (fordítva igen)
- vSphere SSHd egy kapcsolat alatt csak egy visszaállítást tud végrehajtani
- végrehajtás sikeressége egyszerűen ellenőrizhető (ROOT)
- kulcsos belépés nincs implementálva a Python libssh2 modulban

Összefoglalás

- a virtualizáció nem feltétlenül ad biztonságot
- a biztonságos virtualizáció nem feltétlenül kényelmetlen
- a hackerek virtualizálhatók
- az ingyenes termékek is használhatóvá tehetők

Köszönöm a figyelmet!