Bezpečnost síťových aplikací

2019/2020

Př 5

Zabezpečení serverů v počítačové síti

- Instalace
  - Dělení disku, defaultní přístupy, minimalismus
- Firewall, Antivir
  - Aktualizace, centrální správa
- Limitace zdrojů a uživatelů
  - Chroot, limits.conf, virtualizace
- Obnovitelnost a dokumentace
  - Shadow copy, snapshoty

Instalace

- Ověřená media / síť
  - MD5
- Dělení disku
  - Systém a data zvlášť
    - Parted, partition magick, easeus
  - Dynamické disky – škálování
  - SW/HW raid
- Recovery CD + drivery
  - Je-li možnost vytvořit + zkusit

Instalace softwaru

- Během instalace jen to nejnutnější
- Každý balík může být hrozba
- Problém defaultních nastavení
  - /etc/default
- V základu stačí přístup
  - ssh/rdp/telnet
  - Ještě nebeží antivir / FW

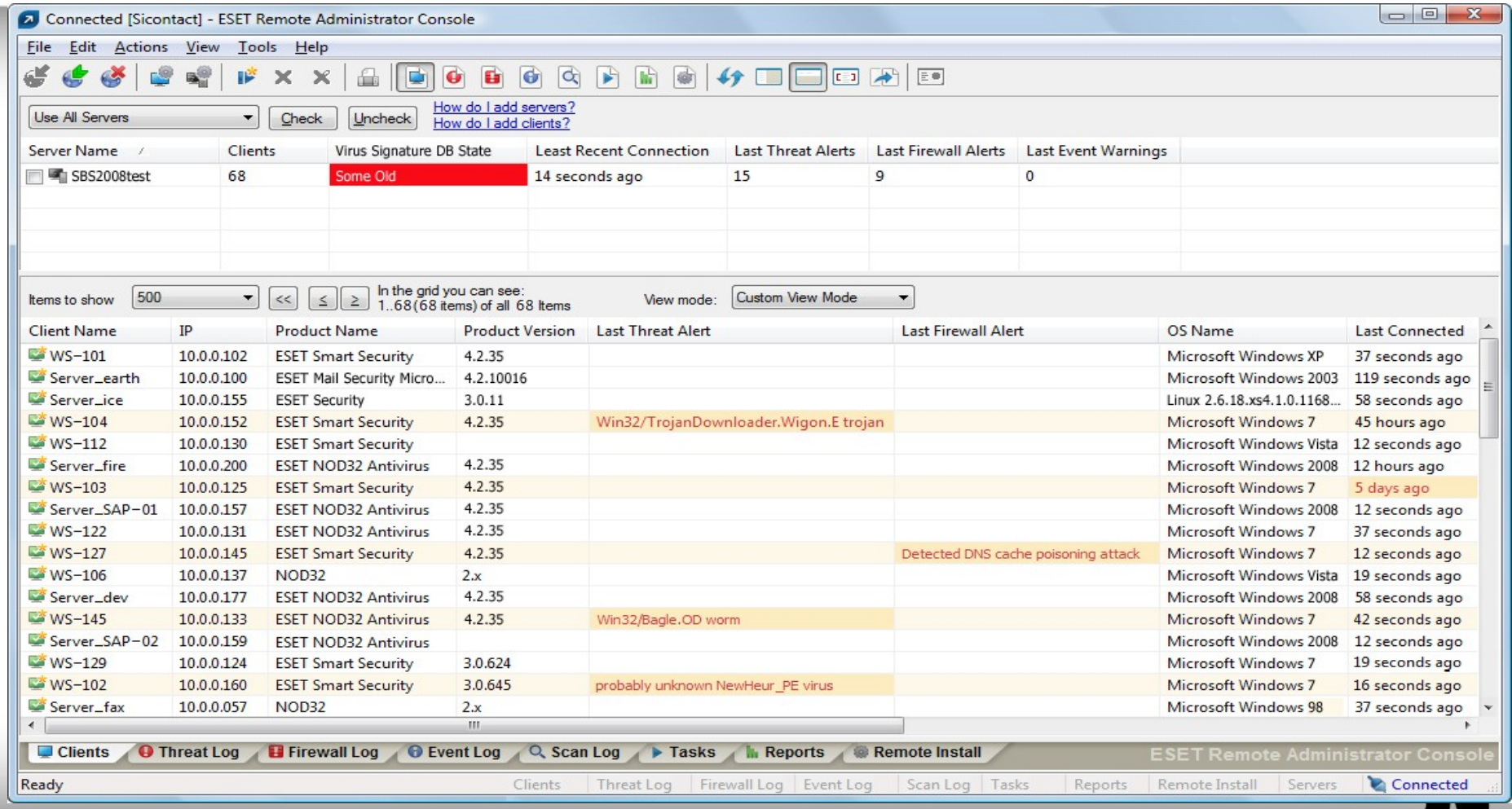
Firewall

- Input nastavit ihned po instalaci
  - Stroj může mít problem velmi brzo
- Ověřit z vnější sítě funkci
  - Nmap, telnet
- Maximálně omezit provoz
  - Default DROP, pak povolení
  - Povolit icmp + lo

Antivir

- Antivir - Jistá detekce problémů
- !!! VŽDY JEN JEDEN !!!
- Více výrobců
  - AVG, Avast, ESET, Clamav, Comodo
  - Cena / Licence
  - Aktualizace
  - Centrální správa
  - Požadavky na systémové zdroje

Antivir - ESET



Antivir – nedostatky

- Vždy opožděný za viry
  - Viry často mění signatury
- Více antivirů
  - Nestabilita, ztráta výkonu
- Přepisování údajů v OS
  - Stahování pošty
- V napadnutém systému nedůvěryhodný
  - Sken po bootu / Live CD

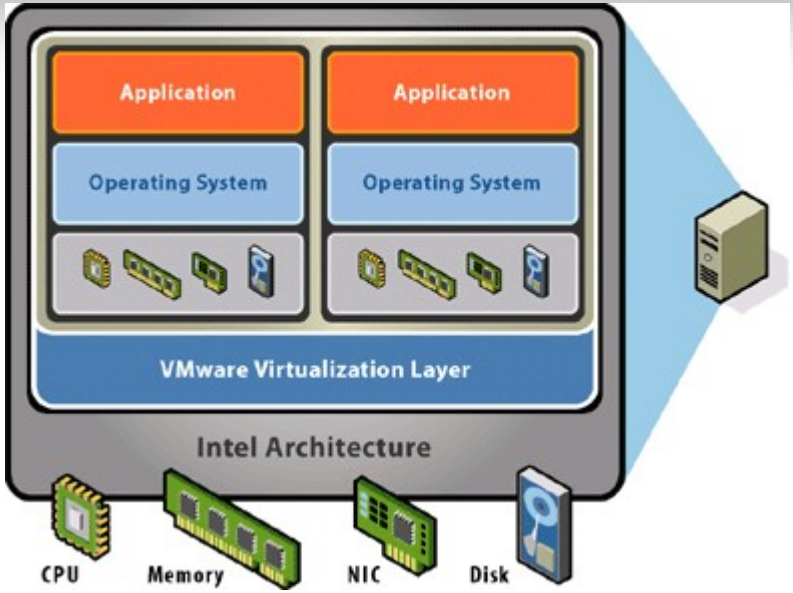
Limitace zdrojů

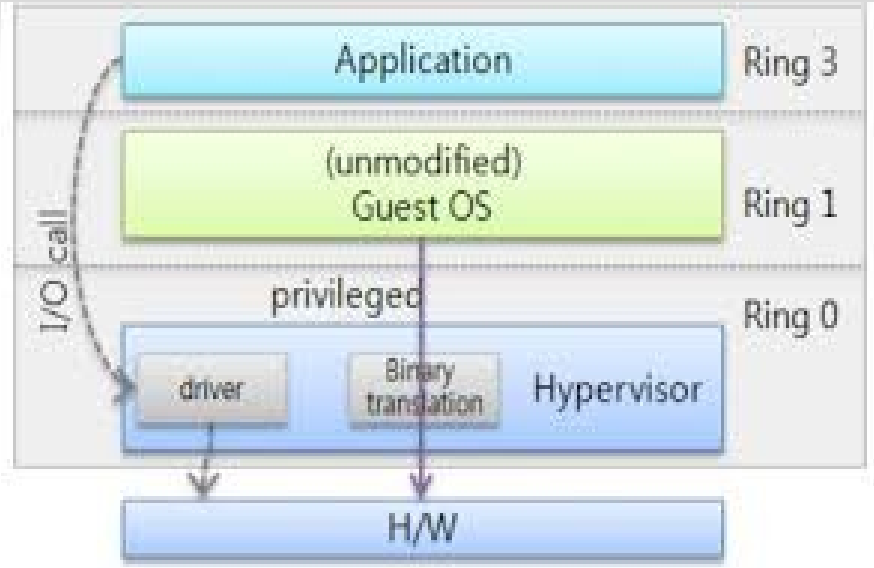
- Prevence pred DOS, DDOS
  - CPU, paměť, disk, síť
- Možnosti podle OS
  - /etc/security/limits.conf
  - aplikační - java,php,...
  - Limit podle uživatele x procesu
  - Patche do jádra OS - grsecurity

Oddělení uživatelů

- ACL, filesystem
  - Kam nepotřebuju nesmím vidět
- Chroot
  - Přenesení kořene FS - ftp, ssh, apache
  - Může být na úrovni jádra či aplikace
- Kontejnery
  - “systém v systému” - se společným jádrem
  - Docker, LXC,...

Virtualizace





Virtualizace

- Hypervisor
  - Zajišťuje řízení zdrojů a přístup k HW
  - Vmware, HyperV, Xen, KVM
- Dom0
  - Prostředí pro ovládání virtualizace
- DomU
  - Virtuální stroje

Virtualizace

- Pro aplikace či celé OS
- Běh v emulovaném nebo hybridním prostředí
- Téměř dokonalé oddělení systémů
- Snadná přenositelnost
- Live migrace mezi hypervisory
- Problém I/O

Obnovitelnost

- Příprava rychlého návratu o krok zpět
- Smazaní dokumentů, VIRY, chyby SW
  - Shadow copy
  - Snapshot
  - LVM backup
  - OwnCloud – kopie při změně

Dokumentace

- Evidence HW i SW
- Automatická aktualizace
  - PC Audit, shell skripty, tex
- Návaznost systémů
  - Jaké služby běží na jakém stroji
  - Provázanost zdrojů – jeden server více služe
  - Administrátorři služeb a dokumentace
  - Evidence servisních oken