

Bezpečnost sít'ových 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 nejnútnejší
- 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

Connected [Sicontact] - ESET Remote Administrator Console

File Edit Actions View Tools Help

Use All Servers [Check] [Uncheck] [How do I add servers?](#) [How do I add clients?](#)

Server Name	Clients	Virus Signature DB State	Least Recent Connection	Last Threat Alerts	Last Firewall Alerts	Last Event Warnings
SBS2008test	68	Some Old	14 seconds ago	15	9	0

Items to show: 500 In the grid you can see: 1.68 (68 items) of all 68 items View mode: Custom View Mode

Client Name	IP	Product Name	Product Version	Last Threat Alert	Last Firewall Alert	OS Name	Last Connected
WS-101	10.0.0.102	ESET Smart Security	4.2.35			Microsoft Windows XP	37 seconds ago
Server_earth	10.0.0.100	ESET Mail Security Micro...	4.2.10016			Microsoft Windows 2003	119 seconds ago
Server_ice	10.0.0.155	ESET Security	3.0.11			Linux 2.6.18.xs4.1.0.1168...	58 seconds ago
WS-104	10.0.0.152	ESET Smart Security	4.2.35	Win32/TrojanDownloader.Wigon.E trojan		Microsoft Windows 7	45 hours ago
WS-112	10.0.0.130	ESET Smart Security				Microsoft Windows Vista	12 seconds ago
Server_fire	10.0.0.200	ESET NOD32 Antivirus	4.2.35			Microsoft Windows 2008	12 hours ago
WS-103	10.0.0.125	ESET Smart Security	4.2.35			Microsoft Windows 7	5 days ago
Server_SAP-01	10.0.0.157	ESET NOD32 Antivirus	4.2.35			Microsoft Windows 2008	12 seconds ago
WS-122	10.0.0.131	ESET NOD32 Antivirus	4.2.35			Microsoft Windows 7	37 seconds ago
WS-127	10.0.0.145	ESET Smart Security	4.2.35		Detected DNS cache poisoning attack	Microsoft Windows 7	12 seconds ago
WS-106	10.0.0.137	NOD32	2.x			Microsoft Windows Vista	19 seconds ago
Server_dev	10.0.0.177	ESET NOD32 Antivirus	4.2.35			Microsoft Windows 2008	58 seconds ago
WS-145	10.0.0.133	ESET NOD32 Antivirus	4.2.35	Win32/Bagle.OD worm		Microsoft Windows 7	42 seconds ago
Server_SAP-02	10.0.0.159	ESET NOD32 Antivirus				Microsoft Windows 2008	12 seconds ago
WS-129	10.0.0.124	ESET Smart Security	3.0.624			Microsoft Windows 7	19 seconds ago
WS-102	10.0.0.160	ESET Smart Security	3.0.645	probably unknown NewHeur_PE virus		Microsoft Windows 7	16 seconds ago
Server_fax	10.0.0.057	NOD32	2.x			Microsoft Windows 98	37 seconds ago

Clients Threat Log Firewall Log Event Log Scan Log Tasks Reports Remote Install

Ready Clients Threat Log Firewall Log Event Log Scan Log Tasks Reports Remote Install Servers Connected

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 před 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

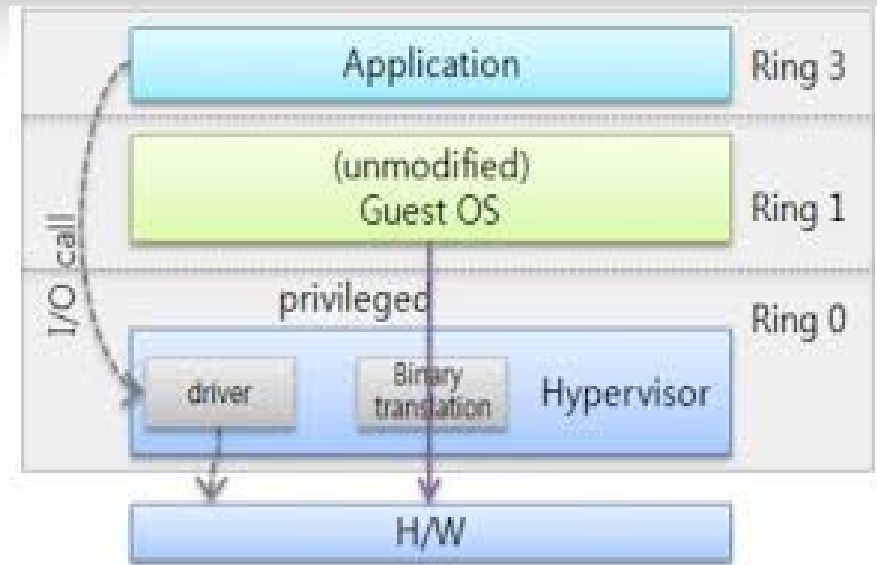
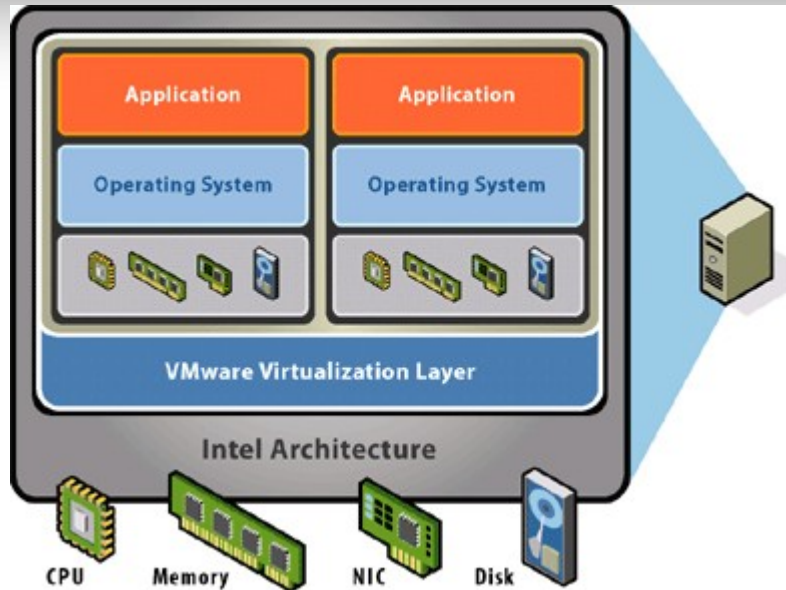


Oddělení uživatelů

- 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
- Smazání 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 služeb
 - Administrátoři služeb a dokumentace
 - Evidence servisních oken

