

# *Správa serverů a počítačových sítí*

2020/2021

Přednáška 9  
( ver. 2021-04-20-01 )



# Zabezpečení

- Typy zabezpečení a útoků
  - Lokální x Vzdálené
  - Lidské x Automatické
- Obecné principy zabezpečení
  - Znalost aplikací a systémů
  - Systémy autorizace a autentizace
  - Omezení pravomocí a prostoru
  - Role v rámci systému
- Detekce slabých míst
  - Automatická analýza systémů
  - Penetrační testování
  - Monitorování systémů



# 1. Zabezpečení

- Vždy je nutné vědět před kým se brání
- Detailní znalost systému a práce s ním
- Zabezpečení je vždy drahé
  - Výkonnější či specifické HW
  - Omezení možnosti práce se systémem
- Lokální napadení
  - Útoční do systému legálně smí
  - Vše co uživatel nemusí vidět to vidět nesmí
- Vzdálené napadení
  - Musí využívat síťovou komunikaci
  - Podle spuštěných služeb je omezen prostor
  - Služby neběží pod privilegovaným uživatelem



# 1.1 Typy přístupů

- Lokální napadení pomocí terminálu
  - Útočník nemusí mít v rámci systému konto
  - Útočník má fyzický přístup k zařízení
  - Typicky pracovní stanice či notebooky
  - Vzácně servery
  - Cílem jsou většinou lokální data
  - Šifrování souborového systému
  - Nenechávat přihlášené uživatele na terminálu
  - Dočasné odpojení systému k obejití ochran



# 1.1 Typy napadení

- Lokální útok pomocí vzdáleného přístupu
  - Útočník nemá k systému fyzický přístup
  - Útočník má konto v systému nebo jej získá
    - Defaultní uživatelé
    - Odhadnutá či odposlechnutá hesla
  - Cílů zde může být vícero
    - Uživatelské data
    - Zneužití stroje jako dočasné brány
    - Eskalace na správce systému a narušení chodu
  - Důsledné oddělení uživatelů a služeb
  - Důsledné logování
  - Aktualizace systému



# 1.1 Typy napadení

- Vzdálený přístup pomocí síťových služeb
  - Tři důvody
    - Získání lokálního přístupu
    - DoS, DDoS – odmítnutí služeb
    - Získání důvěrných informací
  - Napadení neaktualizovaných služeb
  - Využití zranitelnosti jádra OS či kombinace s předchozím
  - Odhadnutí či odposlechnutí hesla, nedostatečně omezený přístup
    - Nejtypičtější ssh, ftp, pop, imap
  - Vyčerpání systémových prostředků
    - Webové služby, poštovní služby
  - Podvržení identity služeb či uživatelů



# 1.2 Metody útoků

- **Hrubá síla**
  - Hádání hesel
  - Odmítnutí služby DoS, DDoS
  - Obranou jsou složitá hesla
- **Sociotechnika**
  - Vždy je chyba v lidech
  - Vydávám se na někoho kdo nejsem
  - Manipulace s lidmi
  - Nejjednodušší způsob útoku
- **Odposlechy**
  - Většinou na síťových službách
  - Cookie, sessions



# 1.2 Metody útoků

- Zneužití chyb v programech
  - Jedna z nejčastějších metod
  - Návodů a exploity volně na internetu
  - Využívané amatéry – vždy největší škody
- Neošetřená vstupní data programů
  - Typické pro webové služby
  - Zneužití serverů k spamům či dalším útokům
  - Infiltrace obsahu webu
  - Vykrádání údajů z počítačů návštěvníků
- Defaultní nastavení
  - Přednastavená hesla
  - Přednastavená konta





## 2. Základy zabezpečení Unixu

- Ošetření služeb systému
  - Extra uživatel pro každou službu
  - Pokud to není nezbytné běh bez admin oprávnění
  - Uzamčení služeb ve svém prostoru – chroot, jail
  - Služby se mezi sebou nevidí
- Maximální utajení informací
  - Práva na FS a na zálohy
  - Informace o verzích programů - phpinfo
  - Firewall a proxy
- Minimalizmus v systémech
  - Co nemusí běžet neběží
  - Kdo nepotřebuje účet nemá jej
  - Programy které nejsou nutné pro chod nejsou instalovány



## 2. Základy zabezpečení Unixu

- Volba vhodných síťových služeb
  - Postfix x Sendmail
  - Vsftpd x proftpd
  - inetd x standalone
- Monitorování systému
  - Nestandardní chování – nagios, icinga, zabbix, scom,..
  - Změny důležitých důležitých souborů – tripware
  - Změny ve viditelnosti služeb – nmap nessus
- Automatické penetrační testy
  - Testování útoků – nessus, nmap, satan,saint
  - Detekce útoků – snort, portsentry, scanlog



## 2.1 Nagios/Icinga2

- Monitorování stavu systémů a služeb
- Umožňuje předcházet kritickým stavům systému
- Umožňuje vzdálené i lokální testování
- Modulární systém, jednotlivé je možné dopisovat, modifikovat či tvořit vlastní: Perl, C
- Rozsáhlá uživatelská základna
- Webový frontend – php, cgi
- Stavby typu : Ok, Warning, Critical
- Notifikace : web, email, sms, jabber ...



# 2.1 Icinga2 - příklad

The screenshot displays the Icinga2 web interface. At the top, there are summary statistics for hosts and services. The main content area is divided into three panels: a left sidebar with navigation icons, a central 'HostStatus' table, and a right 'ServiceStatus' table.

**Summary Statistics:**

- Hosts: 46 / 0 UP, 6 / 7 / 1 DOWN, 0 / 0 / 0 UNREACHABLE, 0 PENDING, 14 / 60 IN TOTAL, 1 OK
- Services: 56 / 4 / 0, 70 / 19 / 1, 0.005 / 10.005 / 2.346, 0.002 / 10.004 / 2.139, 0.008 / 0.702 / 0.141, 0.001 / 0.238 / 0.125

**HostStatus Table:**

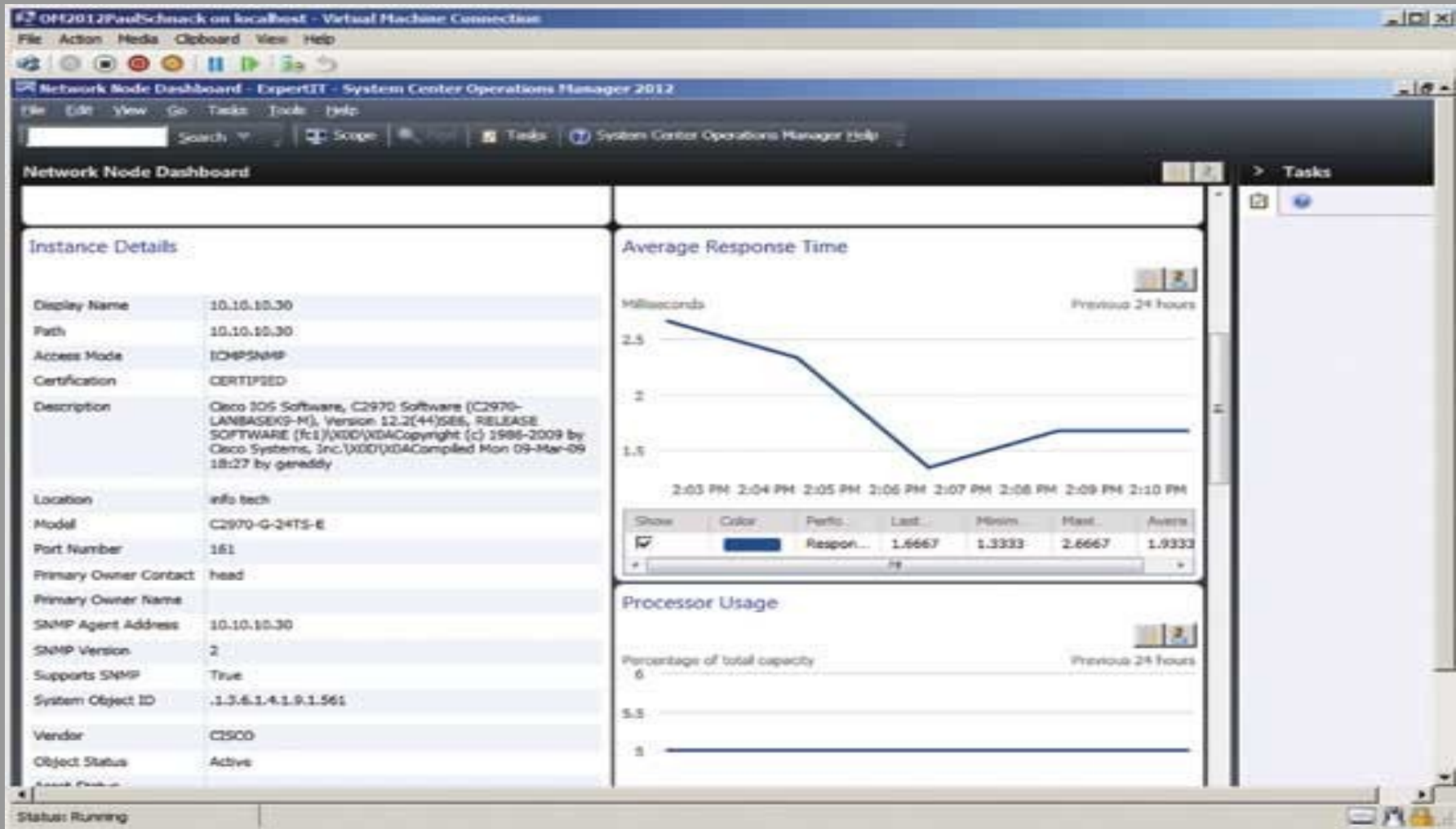
Host	Status	Last c...	Duration	Info	Output	Attempt	Max at...
web_d...	DOWN	2012-1...	1w 3d ...		PING ...	10 / 10	10
c2-prin...	UP	2012-1...	3d 10h...		check...	1 / 10	10
web_d...	DOWN	2012-1...	1w 3d ...		PING ...	1 / 10	10
gmx-w...	DOWN	2012-1...	1w 3d ...		PING ...	1 / 10	10
c1-db2	UP	2012-1...	3d 10h...		check...	1 / 10	10
c1-nag...	UP	2012-1...	3d 10h...		check...	1 / 10	10
c1-switch	UP	2012-1...	3d 10h...		check...	1 / 10	10
c2-app-1	UP	2012-1...	3d 9h ...		check...	1 / 10	10
c1-db1	UP	2012-1...	3d 10h...		check...	1 / 10	10
google...	DOWN	2012-1...	1w 3d ...		PING ...	1 / 10	10
c2-fw-1	UP	2012-1...	3d 9h ...		check...	1 / 10	10
web_d...	DOWN	2012-1...	4d 20h...		PING ...	1 / 10	10
google...	DOWN	2012-1...	4d 20h...		PING ...	1 / 10	10

**ServiceStatus Table:**

Service	Status	Last c...	Duration	Info	Output	Attempt
Host: c1-db1 (2 Items)						
PING	OK	2012-...	3d 9h ...		PING: ...	1 / 5
MySQL	OK	2012-...	1w 15...		MySQL...	1 / 5
Host: c1-db2 (2 Items)						
MySQL	OK	2012-...	3d 10h...		MySQL...	1 / 5
PING	OK	2012-...	3d 9h ...		PING: ...	1 / 5
Host: c1-fw (1 Item)						
PING	OK	2012-...	3d 9h ...		PING: ...	1 / 5
Host: c1-http (2 Items)						
PING	OK	2012-...	3d 9h ...		PING: ...	1 / 5
HTTP	OK	2012-...	3d 9h ...		HTTP:...	1 / 5
Host: c1-mail1 (2 Items)						
MailQ	OK	2012-...	3d 10h...		MailQ:...	1 / 5
PING	OK	2012-...	3d 9h ...		PING: ...	1 / 5
Host: c1-mail2 (2 Items)						
MailQ	OK	2012-...	3d 10h...		MailQ:...	1 / 5



# 2.1 MS SCOM - příklad



## 2.2 Tripwire

- Inventarizace systému
- Eviduje stav jednotlivých souborů a hlásí změny
- Náročný na výkon
- Neocenitelný po napadení systému
- Častá chybná konfigurace a plané poplachy
- Každou změnu je třeba potvrzovat
- Hlášení mailem



## 2.3 NMAP

- Síťový scanner
- Patrně nejkompaktnější dostupný nástroj
- Detekce běžících služeb
- Detekce verzí služeb či jádra systému



## 2.3 NMAP

```
root@proteus:~# nmap -A -sV ares.fav.zcu.cz
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2009-04-15 06:48 CEST
Interesting ports on ares.fav.zcu.cz (147.228.63.10):
Not shown: 1671 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh         (protocol 2.0)
80/tcp    open  http        Apache httpd 2.2.9 ((Debian) mod_auth_kerb/5.3 DAV/2 SVN/
1.5.1 PHP/5.2.6-3 with Suhosin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g)
113/tcp   open  ident       OpenBSD identd
443/tcp   open  ssl/http    Apache httpd 2.2.9 ((Debian) mod_auth_kerb/5.3 DAV/2
SVN/1.5.1 PHP/5.2.6-3 with Suhosin-Patch mod_ssl/2.2.9 OpenSSL/0.9.8g)
1521/tcp  open  oracle-tns  Oracle TNS Listener 10.2.0.4.0 (for Linux)
3306/tcp  open  mysql       MySQL 5.0.51a-24-log
5432/tcp  open  postgresql  PostgreSQL DB
8009/tcp  open  ajp13?
SF:0,"SSH-2\0-OpenSSH_5\1p1\x20Debian-5\r\n");
MAC Address: 00:15:C5:89:18:B2 (Dell)
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20
Service Info: OS: OpenBSD
Nmap finished: 1 IP address (1 host up) scanned in 21.267 seconds
```





## 2.4 Nessus

- Systém na detekci zranitelnosti systému
- Aplikace typu klient-server, kde klientů je více : GUI-GTK, web, konzolová aplikace
- Klient zadává nastavení a spouští testy, server je vykonává
- Detekuje už známé zranitelnosti
- Je třeba konfigurovat testy opatrně
- Moduly jsou psané v extra jazyce
  - NASL (Nessus Attack Scripting Language)



# 2.4 Nessus - příklad

The screenshot displays the Nessus web interface. The top navigation bar includes the Nessus logo, 'Scans', and 'Settings' menus, along with a notification bell and a user profile icon. The left sidebar contains 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Customized Reports, Scanners). The main content area is titled 'Live Results Scan' and includes a 'Back to My Scans' link. Below this, there are filters for 'Hosts' (1), 'Vulnerabilities' (45), and 'History' (1). A search bar for vulnerabilities is present, showing '45 Vulnerabilities'. The central table lists various vulnerabilities with columns for severity, name, family, and count. The right sidebar features a 'Scan Details' section with metadata and a 'Vulnerabilities' donut chart showing the distribution of severity levels.

Sev	Name	Family	Count
CRITICAL	Mozilla Foundation Unsupported Application ...	MacOS X Local Security Checks	1
HIGH	Mozilla Firefox < 59 Multiple Vulnerabilities (m...	MacOS X Local Security Checks	1
HIGH	Mozilla Firefox < 59.0.1 Multiple Code Executi...	MacOS X Local Security Checks	1
HIGH	Mozilla Firefox < 59.0.2 Denial of Service Vuln...	MacOS X Local Security Checks	1
HIGH	Mozilla Firefox < 60 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
HIGH	Mozilla Firefox < 61 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
HIGH	Mozilla Firefox < 62 Multiple Critical Vulnerabili...	MacOS X Local Security Checks	1
MEDIUM	SSL Certificate Cannot Be Trusted	General	1
INFO	Netstat Portscanner (SSH)	Port scanners	16
INFO	Service Detection	Service detection	4
INFO	HTTP Server Type and Version	Web Servers	2
INFO	Additional DNS Hostnames	General	1

**Scan Details**

Name: Live Results Scan  
Status: Completed  
Policy: Advanced Scan  
Scanner: Local Scanner  
Modified: Today at 6:03 PM (Live Results)

**Vulnerabilities**

Legend: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue)

Zdroj: <https://www.tenable.com/products/nessus>



## 2.5 PortSentry, Scanlogd

- Programy detekující scanování portů
- PortSentry
  - Umožňuje TCP i UDP
  - Umí na detekovaný útok reagovat změnou FW
  - Umí ochránit jen lokální systém
- Scanlogd
  - Umožňuje detekci jen TCP scanů
  - Umí detekovat útok v rámci celé sítě
  - Útok pouze detekuje a informuje o něm
  - Detekce zaplnění logu



## 2.6 Snort

- OpenSource IDS systém
  - Intrusion Detection System
- Funguje na principu detekce signatur
- Má vysokou míru paranoii
- Dostupný pro mnoho systémů
- Nevyžaduje patch kernelu jako například LIDS
- Má webový i gui interface
- Při větších datových tocích náročný na zdroje



# 2.6 Snort - příklad

Snort IDS Console - Microsoft Internet Explorer

Address: https://[redacted]

Snort IDS Console Unfilter Refresh every 30 secs. View alerts since 6 AM or on [redacted]

Alert Information		Sensors			Top Sources			Top Targets			Top Target Ports				
	#	%	Sensor	Sigs	Alerts	IP Address	Sigs	Alerts	IP Address	Sigs	Alerts	TCP	#	UDP	#
Signatures:	62		[redacted]	19	482	[redacted]	6	186	[redacted]	6	186	80	513	1434	1,259
TCP Alerts <a href="#">View</a> :	1,126	42%	[redacted]	13	177	[redacted]	5	5	[redacted]	5	5	139	186	53	242
UDP Alerts <a href="#">View</a> :	1,523	57%	[redacted]	11	240	[redacted]	3	21	[redacted]	3	24	443	122	177	9
ICMP Alerts <a href="#">View</a> :	0	0%	[redacted]	11	131	[redacted]	2	108	[redacted]	2	352	1433	23	111	6
Total Alerts <a href="#">View</a> :	2,649	100%	[redacted]	9	298	[redacted]	2	92	[redacted]	2	92	3389	19	69	2

### Alert Overview by Signature

Earliest Alert: 2004-12-29 06:01:03  
Latest Alert: 2004-12-29 15:57:12

Signatures					
Prio	Signature	# Sensors	# Alerts	# Srcs	# Dests
1	<a href="#">WEB-MISC cross site scripting attempt [sid 1497]</a>	2	353	2	2
1	<a href="#">P2P Fastrack kazaa/morpheus traffic [sid 1699]</a>	2	145	3	49
1	<a href="#">MS-SQL/SMB raiserror possible buffer overflow [sid 1386]</a>	2	117	1	1
1	<a href="#">WEB-MISC NetObserve authentication bypass attempt [sid 2441]</a>	1	110	1	1
1	<a href="#">MS-SQL/SMB xp_cmdshell program execution [sid 681]</a>	2	33	1	1
1	<a href="#">WEB-MISC PCT Client_Hello overflow attempt [sid 2515]</a>	2	25	1	8
1	<a href="#">MS-SQL xp_cmdshell - program execution [sid 687]</a>	1	17	2	1
1	<a href="#">MS-SQL/SMB xp_req* registry access [sid 689]</a>	2	12	1	1
1	<a href="#">MS-SQL/SMB sp_password password change [sid 677]</a>	2	10	1	1
1	<a href="#">MS-SQL/SMB sp_delete alert log file deletion [sid 678]</a>	2	10	1	1
1	<a href="#">MS-SQL sp_start_job - program execution [sid 673]</a>	2	6	1	1
1	<a href="#">MS-SQL sa login failed [sid 688]</a>	1	5	1	1

Done Internet



# 3. Zabezpečení kernelu

- Nejdůležitější a základní zabezpečení
- Minimalismus
- Verze jádra jdou poznat vzdáleně
- Na jádra existují lokální i vzdálené exploity
- Bezpečnostní doplňky systému
  - Grsecurity
  - SELinux
  - Medusa DS9



# 3.1 GRSECURITY

- Patch pro kernely 2.X
  - RBAC - Role Based Access Control
  - Zavádí MAC - Mandatory Access Control
  - Postaven nad klasickým DAC Discrete Access Control, který doplňuje
- Velké množství omezení
  - Práva na privilegované porty
  - Práva nahlížet na zbytek systému
  - Omezení konkrétních příkazů např. Dmesg, chroot
  - Monitorování konkrétních operace např mount, chroot atd



## 3.2 PAX

- Patch pro kernel distribuovaný s GRSECURITY
- Nespustitelné stránky v paměti
- Randomizace adresního prostoru
- Problém s některými programy jako java či openoffice
- Možné za chodu modifikovat příkazem chpax pro jednotlivé programy





## 3.3 SELinux

- Součást linuxového kernelu od verze 2.6.X
- Stejně jako GRSECURITY zavádí MAC
- Výhodou je implementace v rámci kernelu pomocí LSM - Linux Security Module
- Složitě na konfiguraci
- Komerční podpora v rámci Redhat Enterprise Linux



# 4. Šifrování

- Brání nebezpečí odposlechnutí především hesel, ale i citlivých dat
- Pro některé služby defaultně zapnuté
  - SSH, IMAPS, HTTPS
- Nutné používat tam, kde se předávají citlivá data
- Služby které nemají podporu je možné tune-  
lovat
  - Stunnel, OpenSSH
  - OpenVPN, IPSEC

