

Bezpečnost sít'ových aplikací

2019/2020

Př 9



Logování, monitoring a detekce útoků

- Logování a analýza logů
 - Syslog, Rsyslog, OSSEC, ...
- Monitoring služeb
 - Nagios, Icinga, Zabbix, SCOM, ...
- IDS / IPS
 - HIDS / NIDS
 - Snort, Dragon, Cisco Security, IDS, PortSentry, ...



Logování

- Kam logovat ?
 - txt logy aplikací
 - databáze
 - **syslog**
- Co logovat ?
 - Přístupy i neúspěšné!!
 - Požadavky – apache, DOS, DDOS
 - Rozlišovat error / warning



Rotace a integrita logů

- Rotace
 - Snaha minimalizovat a rozdělit data
 - Rotace po číslech nebo lépe datumech
 - Post / Pre skripty – Ob!! Timestampy
- Integrita
 - Zajištění nezměnitelnosti-lokálně nelze
 - Remote syslog
 - Výhoda centrálního sběru



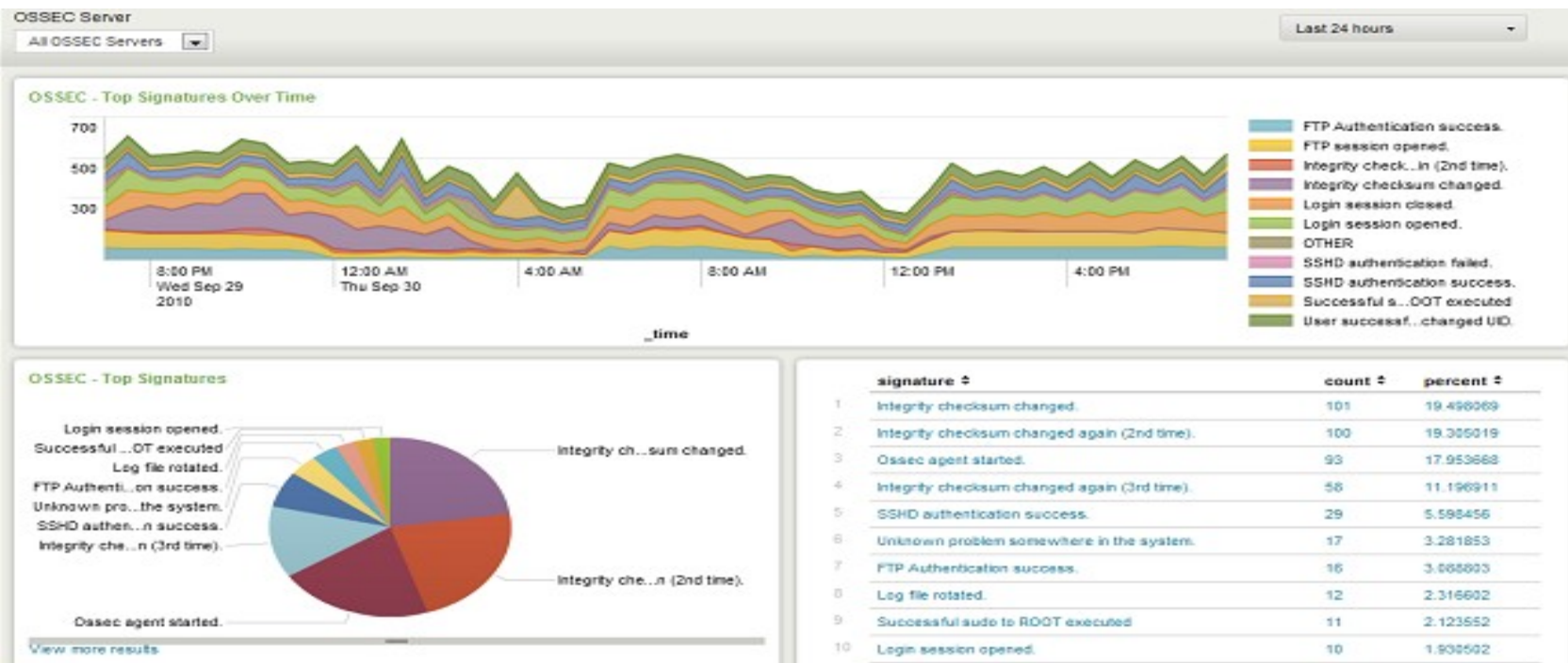
Metoda sběru

- Pasivní
 - Logy jsou posílané přes syslog
 - Musí být podporovaný
- Aktivní
 - Systém sám sbírá logy
 - agenti
 - Speciální programy SNMP



Visualizace logů

- Téměř vždy externí nástroje
- OSSEC, Graylog2, AlienVault



Monitoring

- Informace pro běh i bezpečnost
 - Zatížení může být i útok
- Průběžné sledování stavu
 - Serverů / Sítí
 - Služeb / HW Komponent
- Dostupná řešení
 - Nagios, Icinga, Zabbix
 - MS SCOM



Monitoring

- Nástroj
 - Serverů
 - Sítí
 - Služeb
 - komponent
- Notifikace stavu
 - Ok / Warning / Critical
 - WWW, Email, Jabber, SMS, GSM Call, ...



Nagios / Icinga

- Modulární Open Source
- Nastavujeme limity pro tři úrovně
- Free i placená verze Nagios XE
- Dostupné velké množství pluginů
- Možnost psaní vlastní pluginů
 - Bash, Perl, C/C++, PHP, ...



NRPE / NSCA

- Ne vše jde monitorovat vzdáleně
 - Disku, CPU, paměť, lokální aplikace
- NRPE
 - Na hostu je aplikace, která dělá “proxy”
 - Musí být veřejně dostupné
- NSCA
 - Na hostu je aplikace co posílá data na server
 - Iniciativu přebírá testovaný - nevýhodné



Icinga

The screenshot displays the Icinga web interface in a browser window titled "Icinga - Portal 2columns". The interface is divided into several sections:

- Monitoring Summary:** Located at the top, it shows overall system health with statistics for UP, DOWN, UNREACHABLE, PENDING, and OK states. For example, it shows "6 / 7 / 1 DOWN" and "1 OK".
- Navigation Panel:** On the left side, there is a "Data (14)" section with icons for Unhandled problems, ServiceStatus, HostHistory, Downtimes, Status Map, and Instances. Below it is a "Tactical Overview (3)" section with Reporting and Business Process links.
- HostStatus Panel:** The central panel displays a table of host statuses. The table has columns for Host, Status, Last c..., Duration, Info, Output, Attempt, and Max at... The status is color-coded: red for DOWN and green for UP. Several hosts are shown as DOWN, including web_d..., gm-x..., and google....
- ServiceStatus Panel:** The right panel displays a table of service statuses. It is organized by host, such as "Host: c1-db1 (2 Items)" and "Host: c1-http (2 Items)". Services like PING, MySQL, and MailQ are listed with their status (OK or DOWN) and last check details.

At the bottom of each panel, there are pagination controls: "Page 1 of 3" for HostStatus and "Page 1 of 2" for ServiceStatus. The footer of the interface indicates "Displaying topics 1 - 30 of 60" and "Displaying topics 1 - 25 of 45".



SCOM

The screenshot shows the SCOM Network Node Dashboard for a Cisco IOS device. The interface is divided into several sections:

- Instance Details:** A table listing various attributes of the device.
- Average Response Time:** A line graph showing response time in milliseconds over the previous 24 hours. A data table below the graph provides specific values.
- Processor Usage:** A bar chart showing the percentage of total capacity used by the processor over the previous 24 hours.

Display Name	10.10.10.30
Path	10.10.10.30
Access Mode	ICMP/SNMP
Certification	CERTIFIED
Description	Cisco IOS Software, C2970 Software (C2970-LANBASEK9-M), Version 12.2(44)SEB, RELEASE SOFTWARE (fc1)(X00)X0ACopyright (c) 1996-2009 by Cisco Systems, Inc.(X00)X0ACompiled Mon 09-Mar-09 18:27 by gredddy
Location	info tech
Model	C2970-G-24TS-E
Port Number	161
Primary Owner Contact	head
Primary Owner Name	
SNMP Agent Address	10.10.10.30
SNMP Version	2
Supports SNMP	True
System Object ID	.1.3.6.1.4.1.9.1.561
Vendor	CISCO
Object Status	Active

Show	Color	Perfo.	Last	Minim	Max	Avera
<input checked="" type="checkbox"/>	Blue	Respon...	1.6667	1.3333	2.6667	1.9333

Percentage of total capacity
6



IDS / IPS

- Intrusion Detection System
- Poslouchá na síti / serveru co se děje
 - HIDS (Host-based intrusion detection system)
 - Dragon Squire, Intruder Alert, OSSEC, ...
 - NIDS (Network intrusion detection system)
 - **Snort**, Cisco Secure IDS, Hogwash, ...
- Intrusion Prevention System (IPS)
- Intrusion Detection and Prevention System (IDPS)



IDS - princip

- Transparentnost / neviditelnost
- Sondy – sběr z více míst
- Sběr na jedno místo
 - Velké objemy dat, složitá filtrace
- Detekce známých operací či chování
 - `/?site=/etc/passwd`
- Problém jednoznačné detekce
 - FTP v aktivním modu – detekce otevírání portů



Snort

- Nejznámější zástupce IDS v open source
- Široká konfigurovatelnost
- Možnost definovat více cílu logů
 - TXT, DB, syslog,
- Více rozhraní pro přístup
 - WWW, cmd, GUI
- Náročný na chod CPU/Mem
 - sběr a analýza velkého různých dat



Snort - WWW

Snort IDS Console - Microsoft Internet Explorer

Address: https://

Snort IDS Console [Unfilter](#) Refresh every View alerts or on

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			19	482		6	186		6	186	80	513	1434	1,259
TCP Alerts [View] :	1,126	42%		13	177		5	5		5	5	139	186	53	242
UDP Alerts [View] :	1,523	57%		11	240		3	21		3	24	443	122	177	9
ICMP Alerts [View] :	0	0%		11	131		2	108		2	352	1433	23	111	6
Total Alerts [View] :	2,649	100%		9	298		2	92		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	WEB-MISC cross site scripting attempt [sid 1497]	2	353	2	2
1	P2P Fastrack kazaa/morpheus traffic [sid 1699]	2	145	3	49
1	MS-SQL/SMB raiserror possible buffer overflow [sid 1386]	2	117	1	1
1	WEB-MISC NetObserve authentication bypass attempt [sid 2441]	1	110	1	1
1	MS-SQL/SMB xp_cmdshell program execution [sid 681]	2	33	1	1
1	WEB-MISC PCT Client Hello overflow attempt [sid 2515]	2	25	1	8
1	MS-SQL xp_cmdshell - program execution [sid 687]	1	17	2	1
1	MS-SQL/SMB xp_req* registry access [sid 689]	2	12	1	1
1	MS-SQL/SMB sp_password password change [sid 677]	2	10	1	1
1	MS-SQL/SMB sp_delete_alert log file deletion [sid 678]	2	10	1	1
1	MS-SQL sp_start_job - program execution [sid 673]	2	6	1	1
1	MS-SQL sa login failed [sid 688]	1	5	1	1

Done Internet



Snort - Nadstavba

