Bezpečnost síťových 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

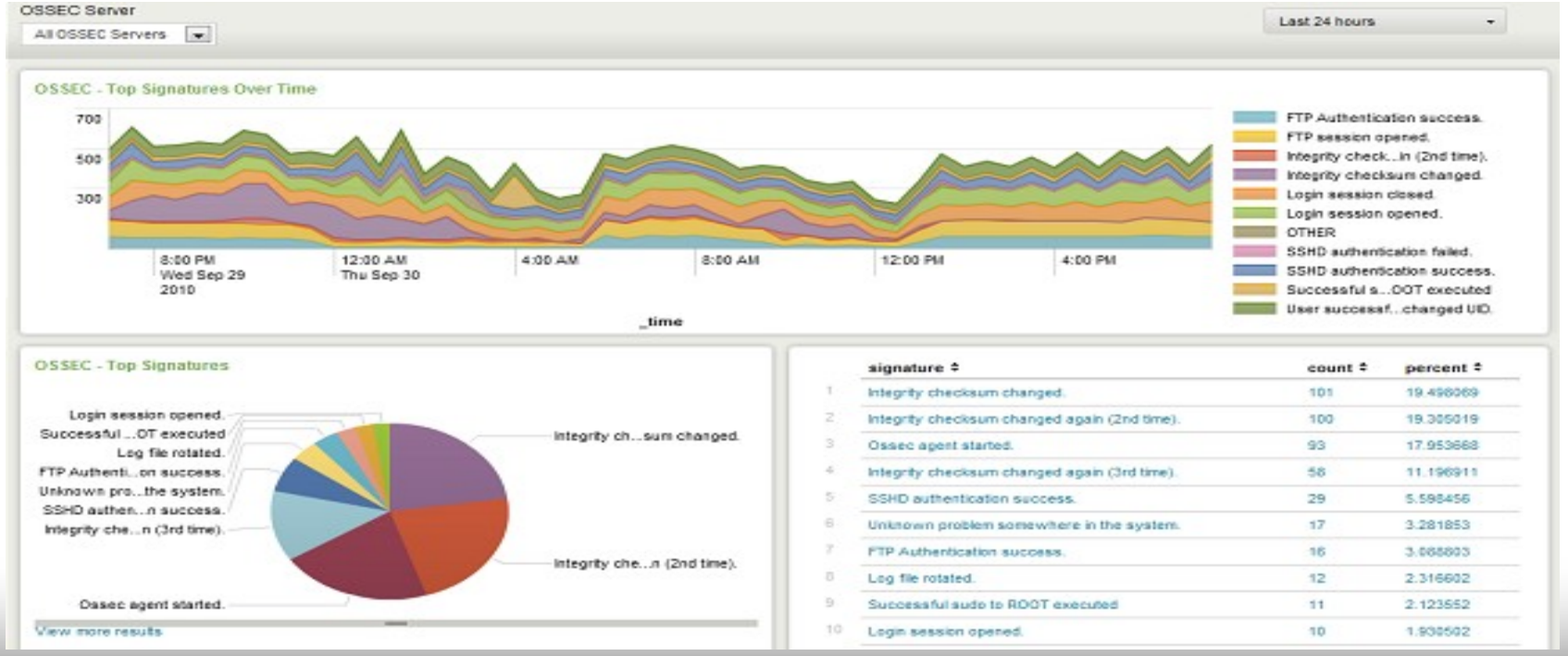
- Rotace
  - Snaha minimalizovat a rozdělit data
  - Rotace po číslech nebo lépe datumech
  - Post / Pre skripty – 0b!! Timestampy
- Integrita
  - Zajištění nezměnitelnosti-lokálně nelze
  - Remote syslog
  - Výhoda centrálního sběru

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, ...

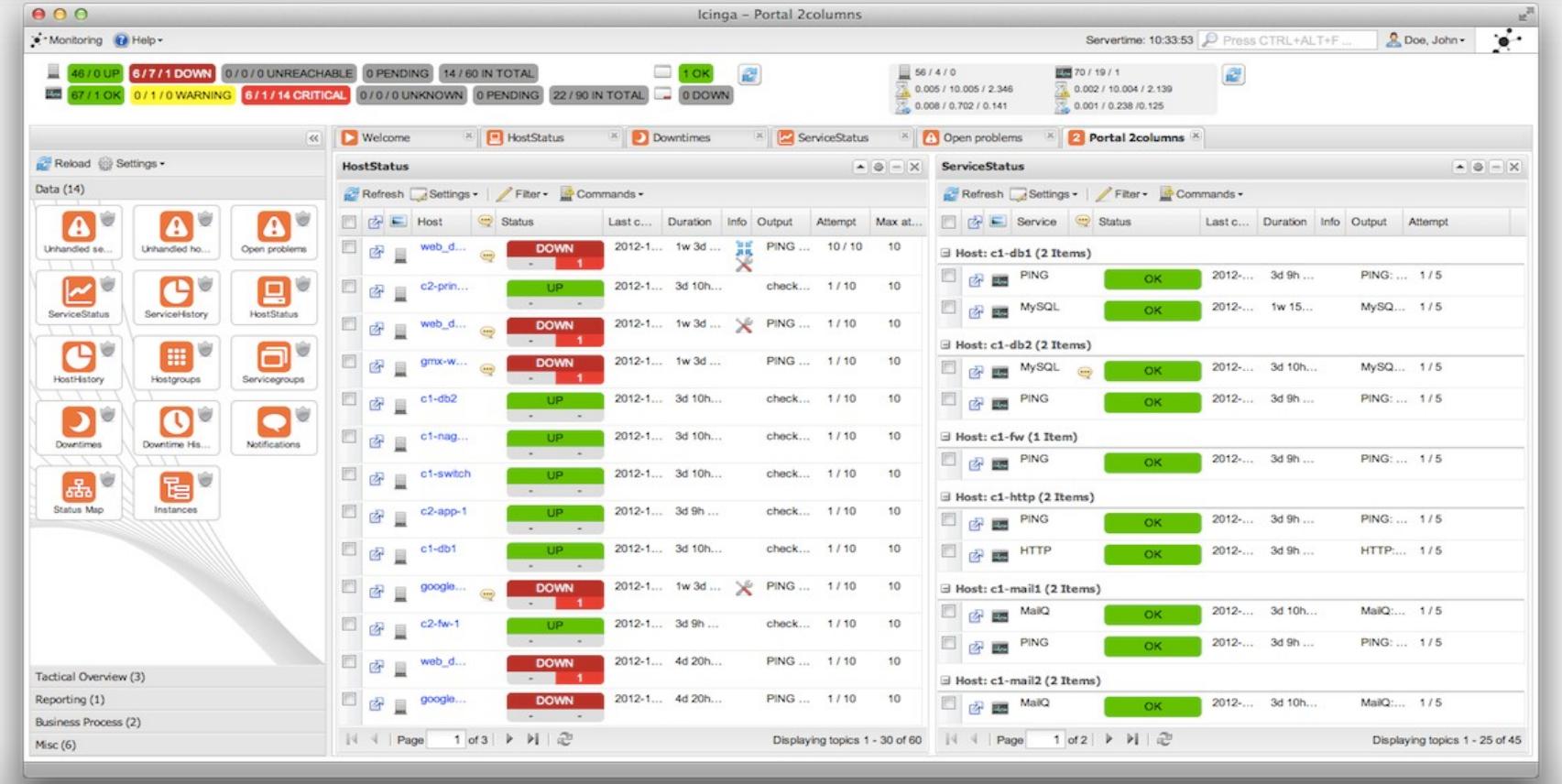
Nagios / Icinga

- 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, ...

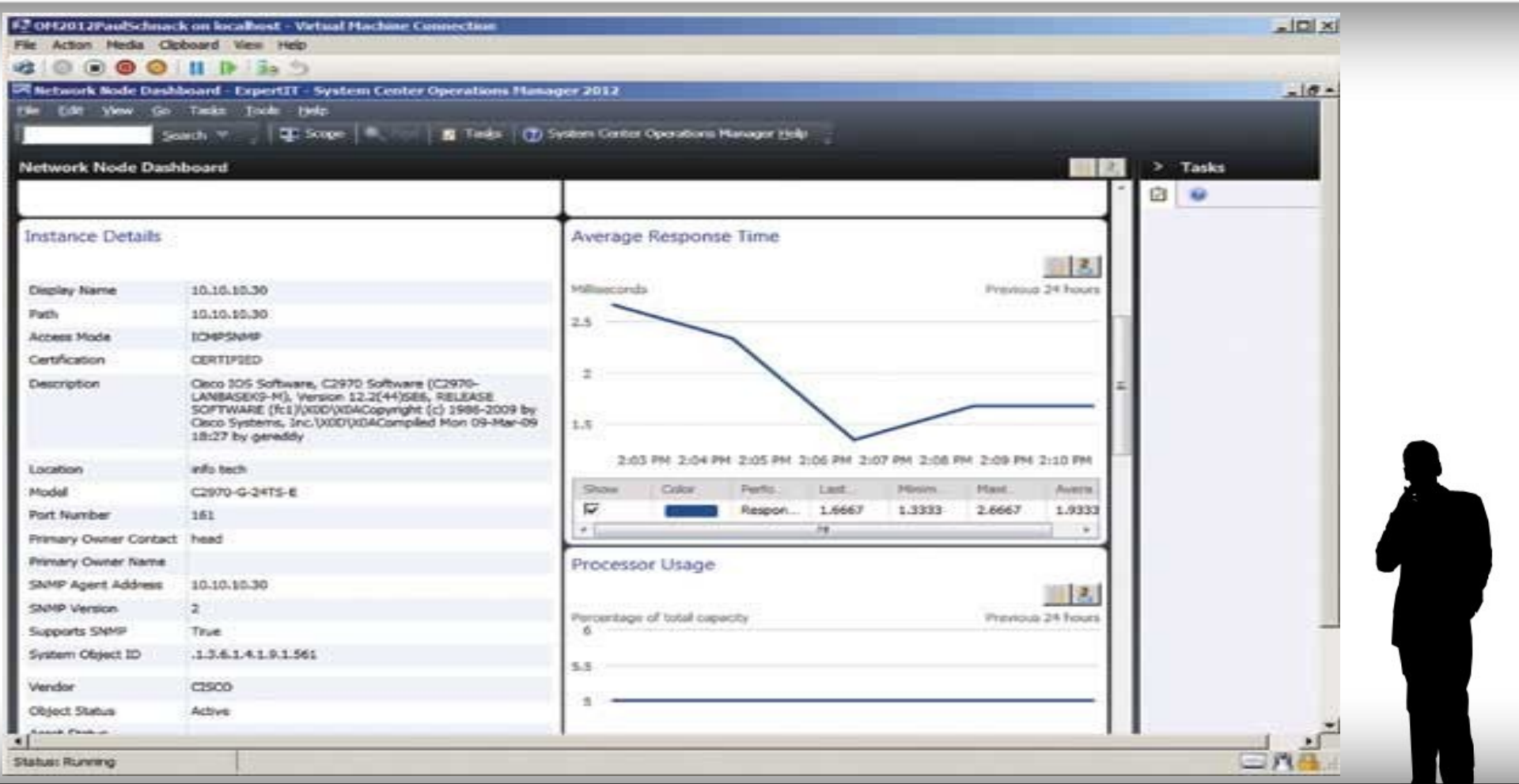
NRPE / NSCA

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

Icinga



SCOM



IDS / IPS

- Intrusion Detection System
- Poslouchá na sítí / 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)

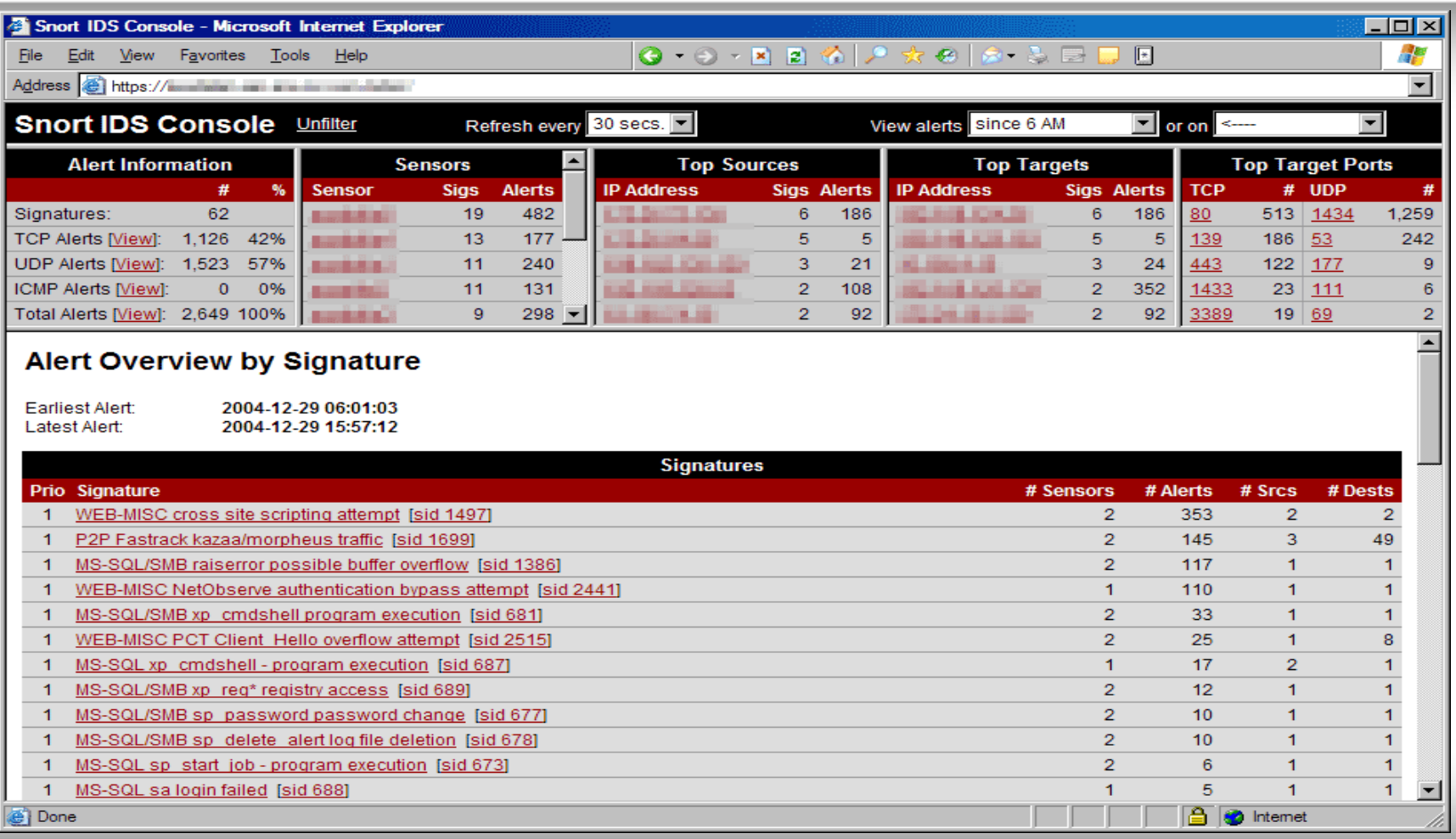
IDS - princip

- 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 modů – 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 - Nadstavba