Analyzátory síťového provozu

Zařízení pro detekci a vyhodnocování síťového provozu

Praktické využití

Jiří Richter
Michal Vymazal

Požadavky

- Otevřený zdrojový kód
- Nekomerční licence
- Nasazení na běžný HW
- Reference od národních bezpečnostních autorit EU
- Dostupný popis jednotlivých modulů analyzátoru (dekodér, preprocesor, signatury)

Reference BSI

BSI Forum
2015#5 23. Jahrgang

BSI Forum

offizielles Organ des BSI
Bundesamt
für Sicherheit in der
Informationstechnik

Messepräsenz

Das BSI auf der it-sa 2015

Vom 6. bis 8. Oktober 2015 ist das BSI mit einem Stand auf der IT-Security Messe it-sa in Nürnberg vertreten. Wie in den vorangegangenen Jahren unterstützt das BSI gemeinsam mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM e. V.) die Messe als ideeller Träger.

Am BSI-Stand in Halle 12, Stand 736 können sich Besucher zu zahlreichen Themen der IT- und Informationssicherheit informieren. Präsentationsschwerpunkte sind in diesem Jahr:

_____ Allianz für Cyber-Sicherheit
_____ Cloud-Computing
_____ IT-Grundschutz
_____ Sicheres mobiles Arbeiten
_____

Inhalt

Impressum

Redaktion:
Matthias Gärtner (verantwortlich)
E-Mail: matthias.gaertner@bsi.bund.de

Sebastian Bebel
E-Mail: sebastian.bebel@bsi.bund.de

Bundesamt für Sicherheit

Analyzátory síťového provozu

Toto zařízení je relevantní k bezpečnostním opatřením subjektů (právnické osoby, fyzické osoby) na něž se vztahuje zákon 181/2014 Sb. (Zákon o kybernetické bezpečnosti).

Jedná se o zařízení, které je součástí technických opatření dle Hlavy II, §22 a §23 Vyhlášky 316/2014 Sb. (Vyhláška k zákonu o kybernetické bezpečnosti, Nástroj pro detekci kybernetických bezpečnostních událostí a Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí).

Analyzátory síťového provozu

- Zjištění stávajících datových toků v měřeném segmentu sítě
- Kontrola „regulérnosti“ jednotlivých spojení (nekorektní provoz nemusí znamenat napadení útočníkem)
- Detekce „neregulérních“ spojení, možnost analýzy jednotlivých paketů a odpovídajících signatur
- Tvorba vlastních signatur

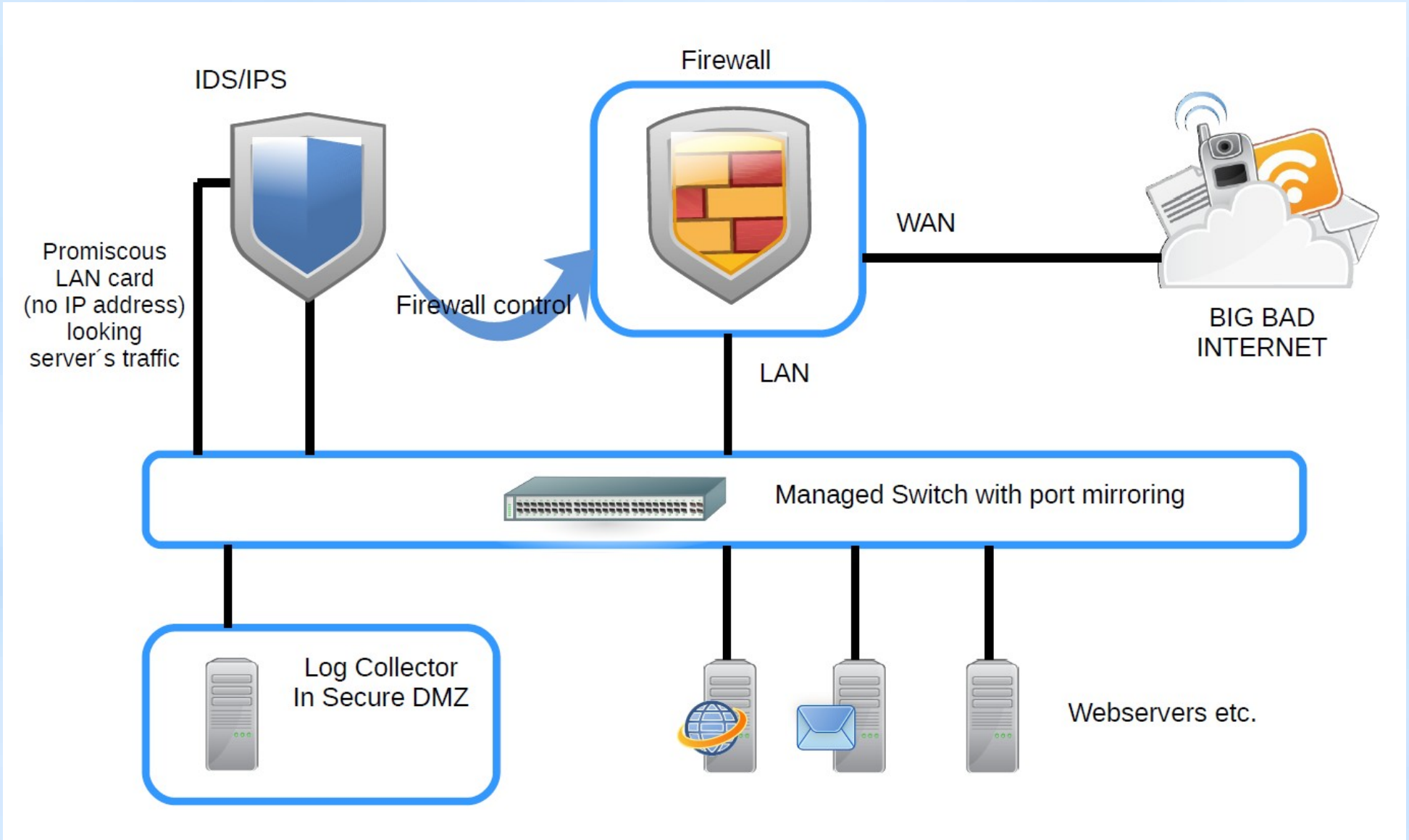
Schopnosti detekce

- Monitorování protokolů TCP, UDP, ICMP
- Detekce portscanů
- Tři stupně analýzy provozu (dekodér, preprocesor, signatury)
- Možnost monitorování dalších protokolů (AH, ESP)

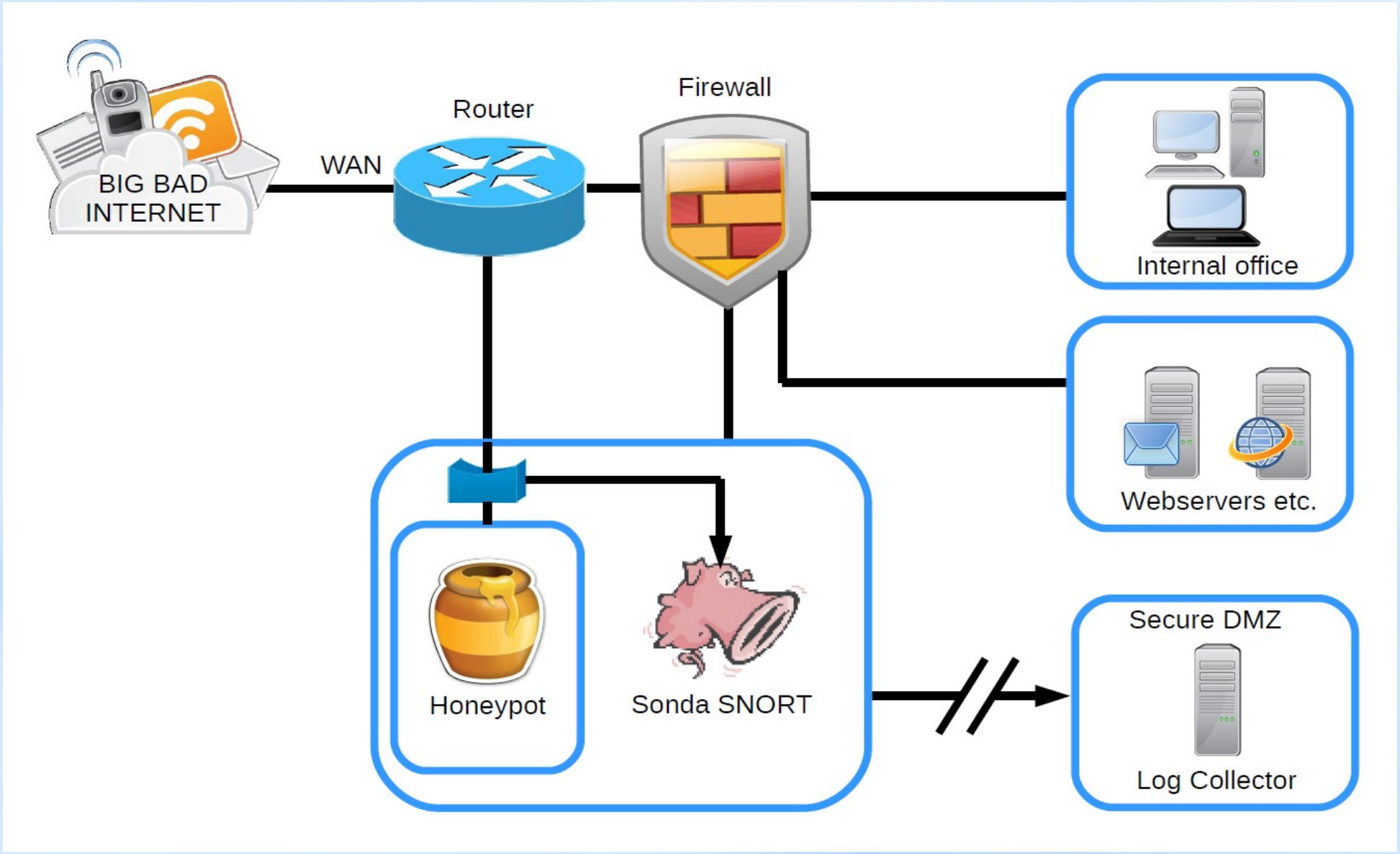
Možnosti reportování událostí

- Ukládání dat do binárního formátu na filesystém sondy
- Export dat do formátu SYSLOG
- Export dat do vzdáleného log serveru
- Ukládání událostí do databáze
- Řada přehledných front-end aplikací

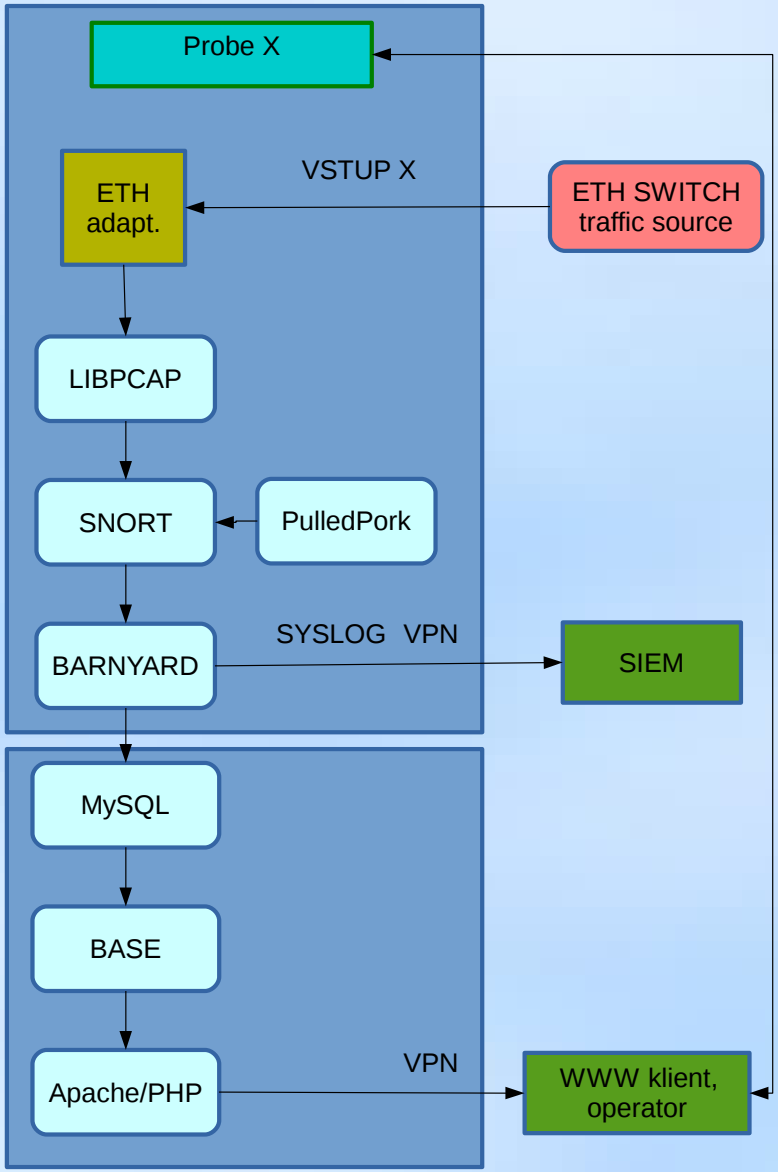
Topologie IDS/IPS



Topologie Honeypotu



Blokové schema sondy



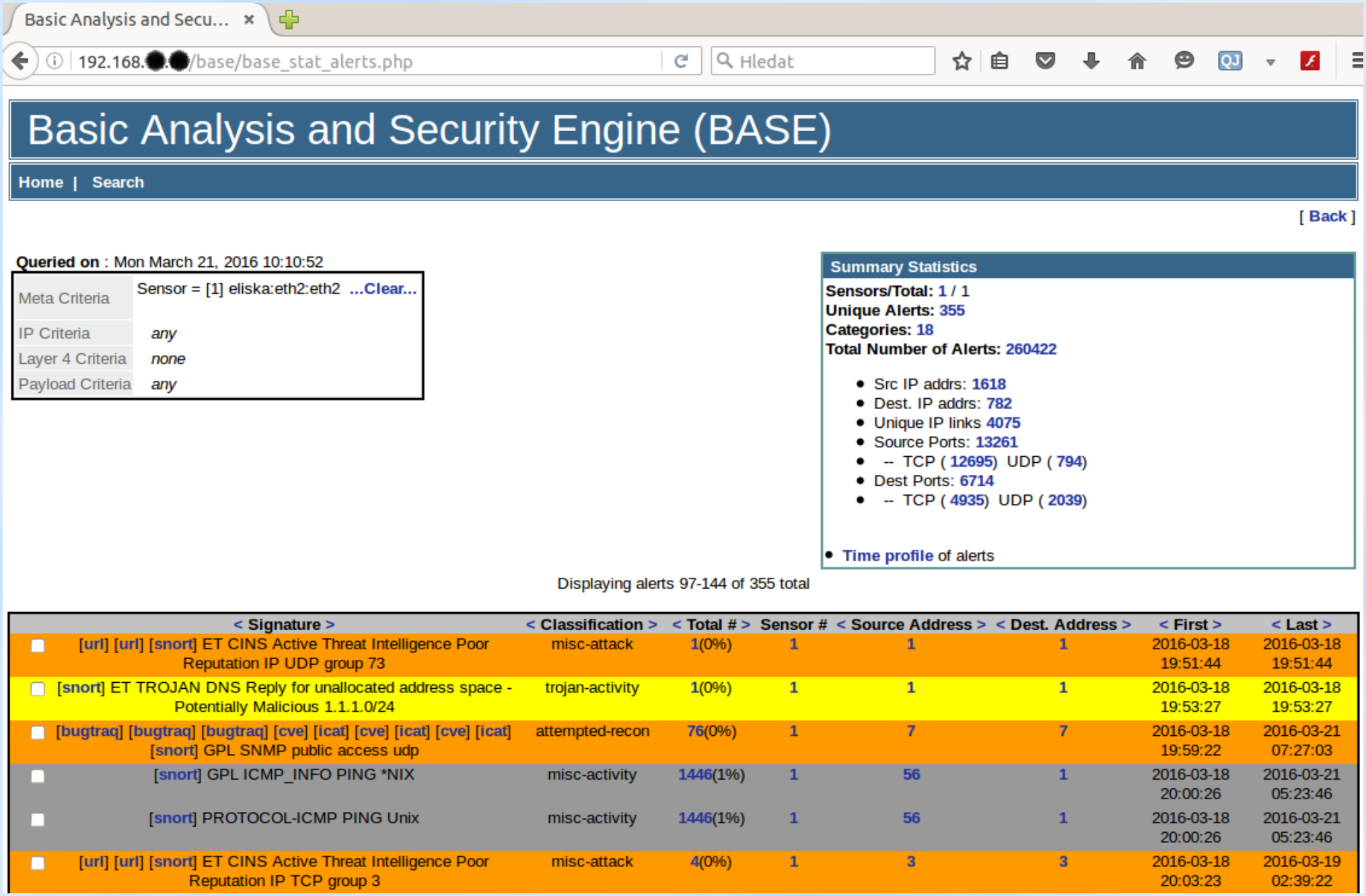
Programové vybavení - sondy

- SNORT - network intrusion detection system
- Suricata - high performance Network IDS

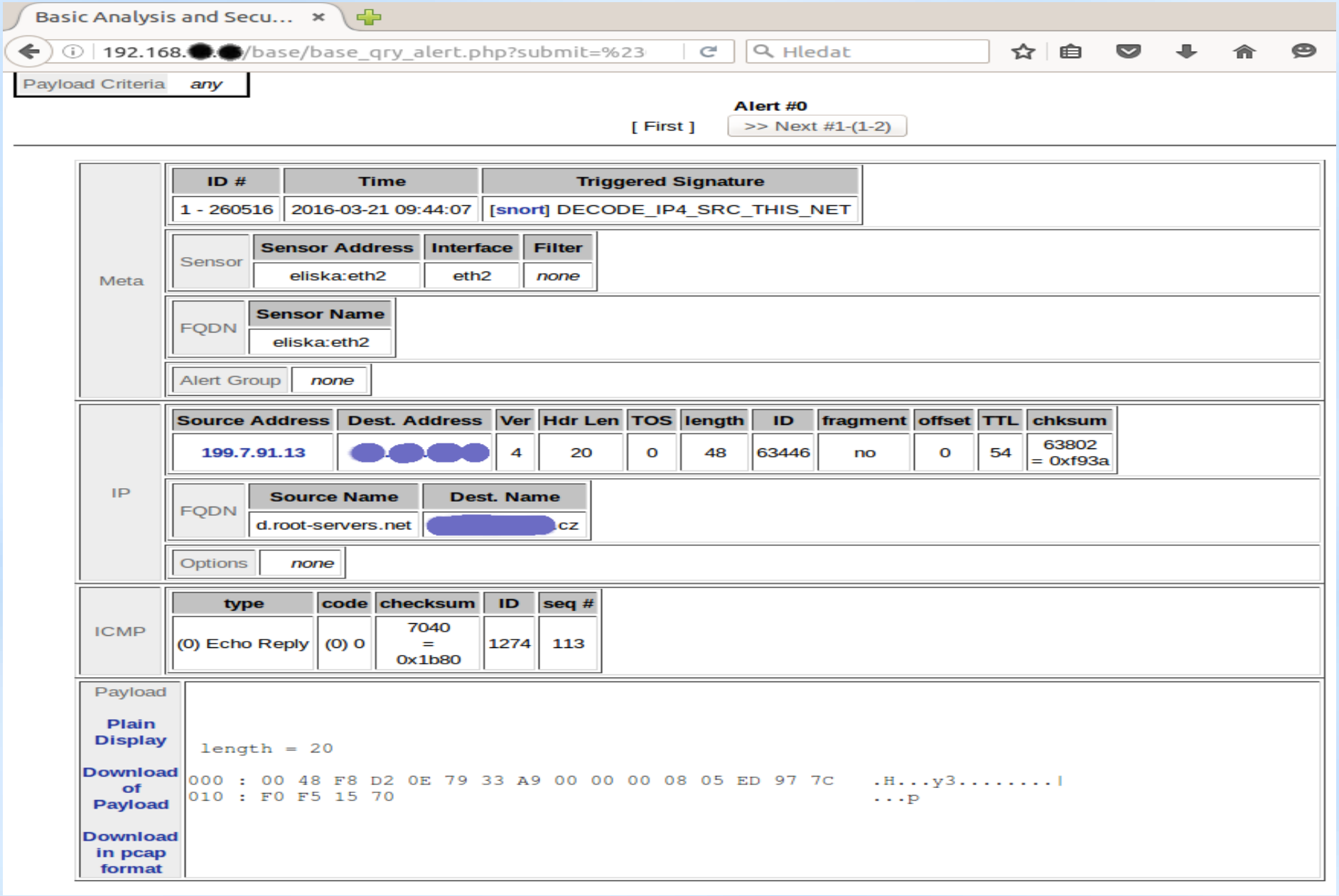
Programové vybavení – front-endy

- BASE - Basic Analysis and Security Engine
- Snorby - modern Snort IDS front-end
- Squert - Simple QUEry and Report Tool
- ELSA - centralized syslog framework
- Aanval - Snort, Suricata, and Syslog console

BASE


Basic Analysis and Secu...
192.168.●.●/base/base_stat_alerts.php
Hledat
Basic Analysis and Security Engine (BASE)
Home | Search
[Back]
Queried on : Mon March 21, 2016 10:10:52
Meta Criteria
Sensor = [1] eliska:eth2:eth2 ...Clear...
IP Criteria
any
Layer 4 Criteria
none
Payload Criteria
any
Summary Statistics
Sensors/Total: 1 / 1
Unique Alerts: 355
Categories: 18
Total Number of Alerts: 260422
Src IP addrs: 1618
Dest. IP addrs: 782
Unique IP links 4075
Source Ports: 13261
-- TCP (12695) UDP (794)
Dest Ports: 6714
-- TCP (4935) UDP (2039)
Time profile of alerts
Displaying alerts 97-144 of 355 total
< Signature > < Classification > < Total # > Sensor # < Source Address > < Dest. Address > < First > < Last >
[url] [url] [snort] ET CINS Active Threat Intelligence Poor Reputation IP UDP group 73 misc-attack 1(0%) 1 1 1 2016-03-18 19:51:44 2016-03-18 19:51:44
[snort] ET TROJAN DNS Reply for unallocated address space - Potentially Malicious 1.1.1.0/24 trojan-activity 1(0%) 1 1 1 2016-03-18 19:53:27 2016-03-18 19:53:27
[bugtraq] [bugtraq] [bugtraq] [cve] [icat] [cve] [icat] [cve] [icat] [snort] GPL SNMP public access udp attempted-recon 76(0%) 1 7 7 2016-03-18 19:59:22 2016-03-21 07:27:03
[snort] GPL ICMP_INFO PING *NIX misc-activity 1446(1%) 1 56 1 2016-03-18 20:00:26 2016-03-21 05:23:46
[snort] PROTOCOL-ICMP PING Unix misc-activity 1446(1%) 1 56 1 2016-03-18 20:00:26 2016-03-21 05:23:46
[url] [url] [snort] ET CINS Active Threat Intelligence Poor Reputation IP TCP group 3 misc-attack 4(0%) 1 3 3 2016-03-18 20:03:23 2016-03-19 02:39:22

BASE


Basic Analysis and Secu...
192.168.●.●/base/base_qry_alert.php?submit=%23
Hledat
Payload Criteria any
Alert #0
[First]
>> Next #1-(1-2)
Meta
ID # | Time | Triggered Signature
1 - 260516 | 2016-03-21 09:44:07 | [snort] DECODE_IP4_SRC_THIS_NET
Sensor | Sensor Address | Interface | Filter
eliska:eth2 | eth2 | none
FQDN | Sensor Name
eliska:eth2
Alert Group none
IP
Source Address | Dest. Address | Ver | Hdr Len | TOS | length | ID | fragment | offset | TTL | chksum
199.7.91.13 | ●●●● | 4 | 20 | 0 | 48 | 63446 | no | 0 | 54 | 63802 = 0xf93a
FQDN | Source Name | Dest. Name
d.root-servers.net | ●●●●●●●●cz
Options none
ICMP
type | code | checksum | ID | seq #
(0) Echo Reply | (0) 0 | 7040 = 0x1b80 | 1274 | 113
Payload
Plain Display
Download of Payload
Download in pcap format
length = 20
000 : 00 48 F8 D2 0E 79 33 A9 00 00 00 08 05 ED 97 7C .H...y3.....|
010 : F0 F5 15 70 ...p

Využití

- Monitorování síťového provozu (pasivní režim)
- Aktivní spolupráce se síťovými prvky (firewall). Vyžaduje standardní API.
- Nástroj pro penetrační testování (scénář penetračních testů)

Signatury

- Volně dostupné, nekomerční licence
- Možnost rozšíření (úpravy) signatur
- Ukázky signatur pro detekci IPSEC provozu (IKE, ESP)
- alert ip any any -> any any (msg:"IPSec ESP traffic detected"; ip_proto:50; classtype:encrypted-protocol; sid:500001; rev:1;)
- alert udp any any -> any 500 (msg:"ISAKMP Key Exchange"; classtype:encrypted-protocol; sid:500003; rev:1;)

Licence – GPL

- Nekomerční licence (GPL, AGPL, MIT, FreeBSD)
- Otevřený kód
- Možnost dokoupit komerční rozšíření (např. SNORT rošíření služeb pro signatury nebo Aanval neomezený počet senzorů)

Závěr

Děkuji za pozornost

Jiří Richter

Michal Vymazal

richter@linuxservices.cz

vymazal@linuxservices.cz