

Bezpečnostní služby CESNETu v roce 2007

IDS a AUDIT

Pavel.Vachek@cesnet.cz

Bezpečnostní služby CESNETu

I. **System pro detekci útoků**

Intrusion Detection System (IDS)

Program LaBrea

<http://labrea.sourceforge.net> (Tom Liston)

- Jednoduchá a účinná odezva na útoky síťových červů a hackerů
- Na adresách dosud nealokovaných koncovým uživatelům vytváří virtuální servery, které:
 - akceptují pokusy o připojení
 - vzniklá spojení udržují co nejdéle – vytvoří tím virtuální “asfaltovou jámu” - **TARPIT**
 - reagují i na přijatý *PING* a *SYN+ACK*

Nejznámější asfaltové jámy: La Brea (Los Angeles, CA)



<http://www.tarpits.org>

LaBrea – princip činnosti

LaBrea zachycuje a brzdí přicházející spojení dvěma možnými způsoby:

1: Jednoduchý způsob - **tarpping**:

Na přijatý paket *SYN* LaBrea pouze odpoví paketem *SYN+ACK*; další útočnickovy pakety (*ACK*) ignoruje. Spojení skončí, jakmile uběhne *retransmission timeout* (obvykle po několika minutách).

LaBrea – princip činnosti

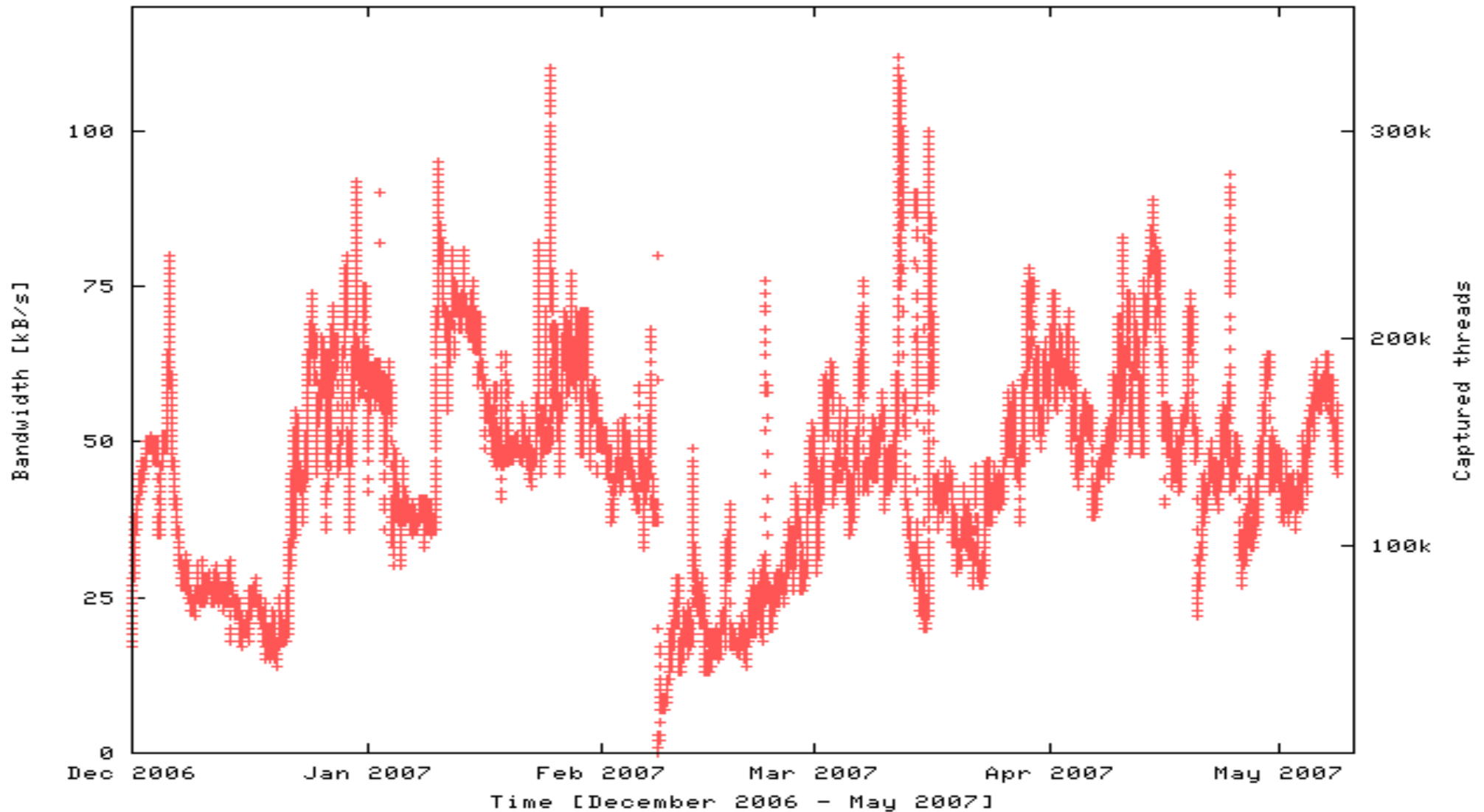
2: Pokročilý způsob – **trvalé zachycení spojení:**

- Standardní *TCP handshake* (*SYN* -
- *SYN+ACK* - *ACK*)
- LaBrea nastaví TCP okno pro příjem dat na nulu – útočník nemůže posílat žádná další data; musí se v pravidelných intervalech ptát, zda se okno znovu otevřelo
- Toto spojení samo o sobě nikdy neskončí a přitom spotřebuje jen nepatrnou šířku pásma

CESNET IDS

šířka pásma [kB/s] + počet vláken

Connection Attempts targeting the CESNET LaBrea server



LaBrea – princip činnosti: DDoS

Útoky typu *Distributed Denial of Service* v paketech často uvádějí zfalšované zdrojové IP adresy neexistujících strojů. Útok DDoS s využitím IP adres LaBrea probíhá takto:

Útočník: paket *SYN* → cíl (stroj C)

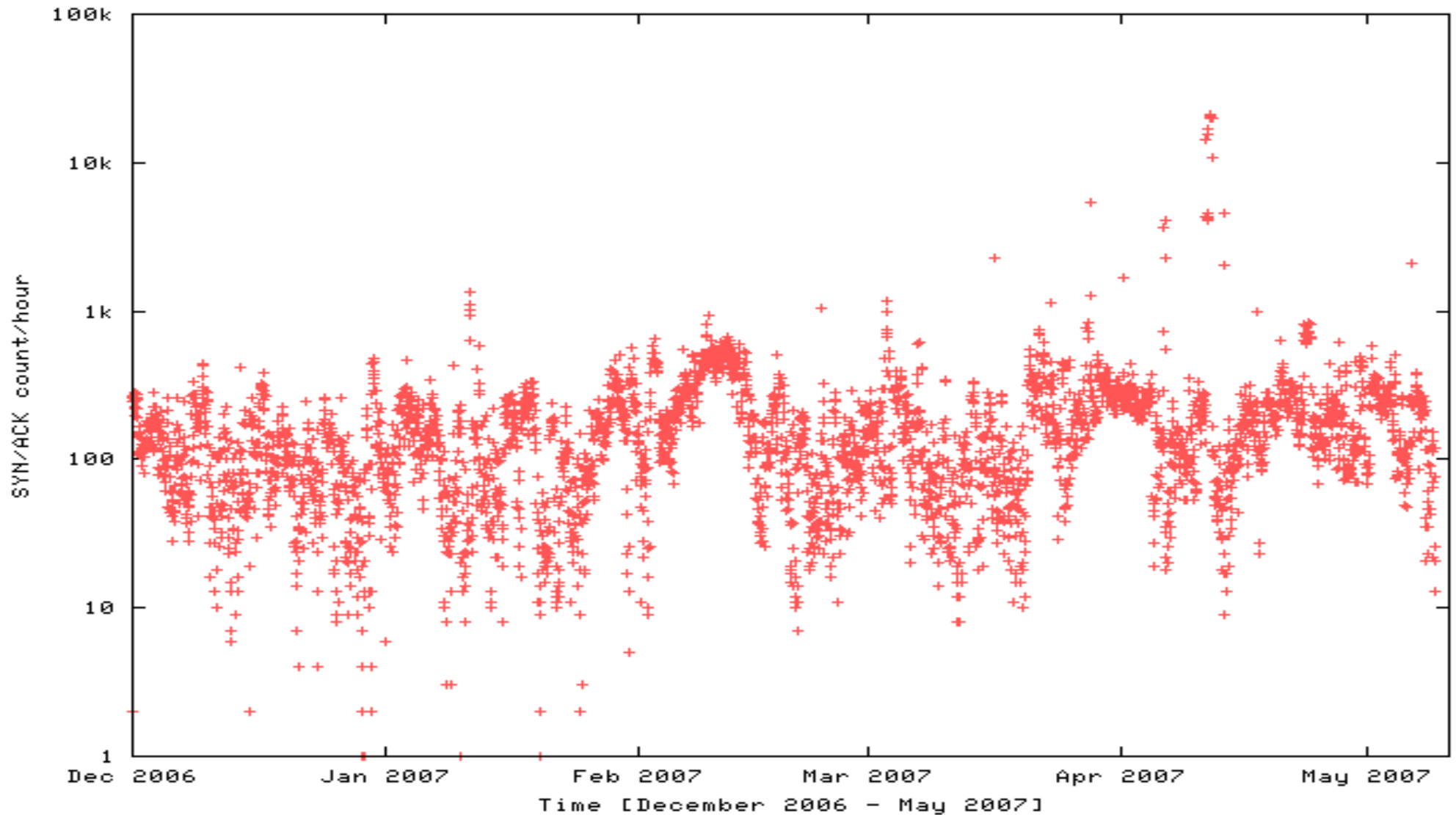
stroj C: paket *SYN+ACK* → server LaBrea

LaBrea: paket *RST* → stroj C

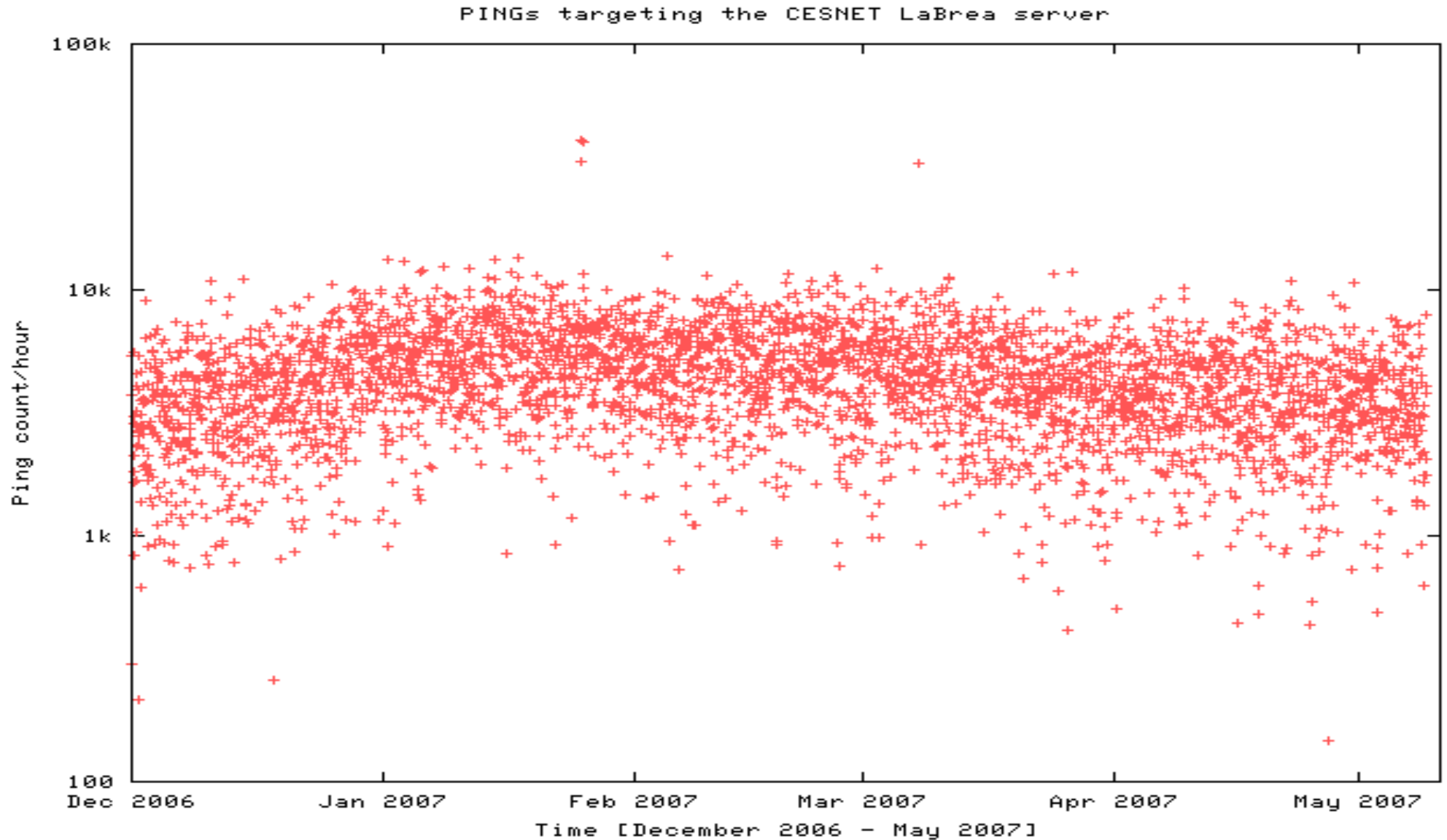
=> útok zneškodněn :-)

CESNET IDS: DDoS/hod.

DDoS Attacks using IP addresses of the CESNET LaBrea server



CESNET IDS: *ICMP Ping/hod.*



CESNET IDS

12/2002 - 11/2004

CESNET Intrusion Detection System zaznamenával útoky **z celého světa** a správčům nakažených strojů rozesílal varování. Vhodnější je účastnit se např. těchto distribuovaných projektů:

- DSHIELD: <http://www.dshield.org>
- MyNetWatchman:
<http://www.mynetwatchman.com>

CESNET IDS od 11/2004

CESNET IDS nyní zaznamenává pouze útoky přicházející ze sítí zákazníků a členů sdružení CESNET (AS 2852)

Přesvědčili jsme správce téměř všech sítí připojených k CESNETu, aby definovali adresy pro hlášení incidentů **`abuse@domain.tld`** podle RFC 2142. Tyto adresy jsme zaregistrovali v RIPE DB:

Ukázka záznamů v RIPE DB

inetnum: 10.0.0.0 – 10.0.0.127
netname: MOJE-FIRMA
descr: Moje firma, s.r.o.
descr: Brno
country: CZ
admin-c: JN9876-RIPE
tech-c: JN9876-RIPE
(...)

**remarks: Please report network
abuse -> abuse@moje-firma.cz**

changed:
source: RIPE

person: Josef Novak
address: Moje firma, s.r.o.
address: Firemni 123
address: Brno
address: 616 00
prone: +420 543214321
fax-no: +420 543214123
e-mail: Josef.Novak@moje-firma.cz

abuse-mailbox: abuse@moje-firma.cz

nic-hdl: JN9876-RIPE
notify: notify@moje-firma.cz
changed:
source: RIPE

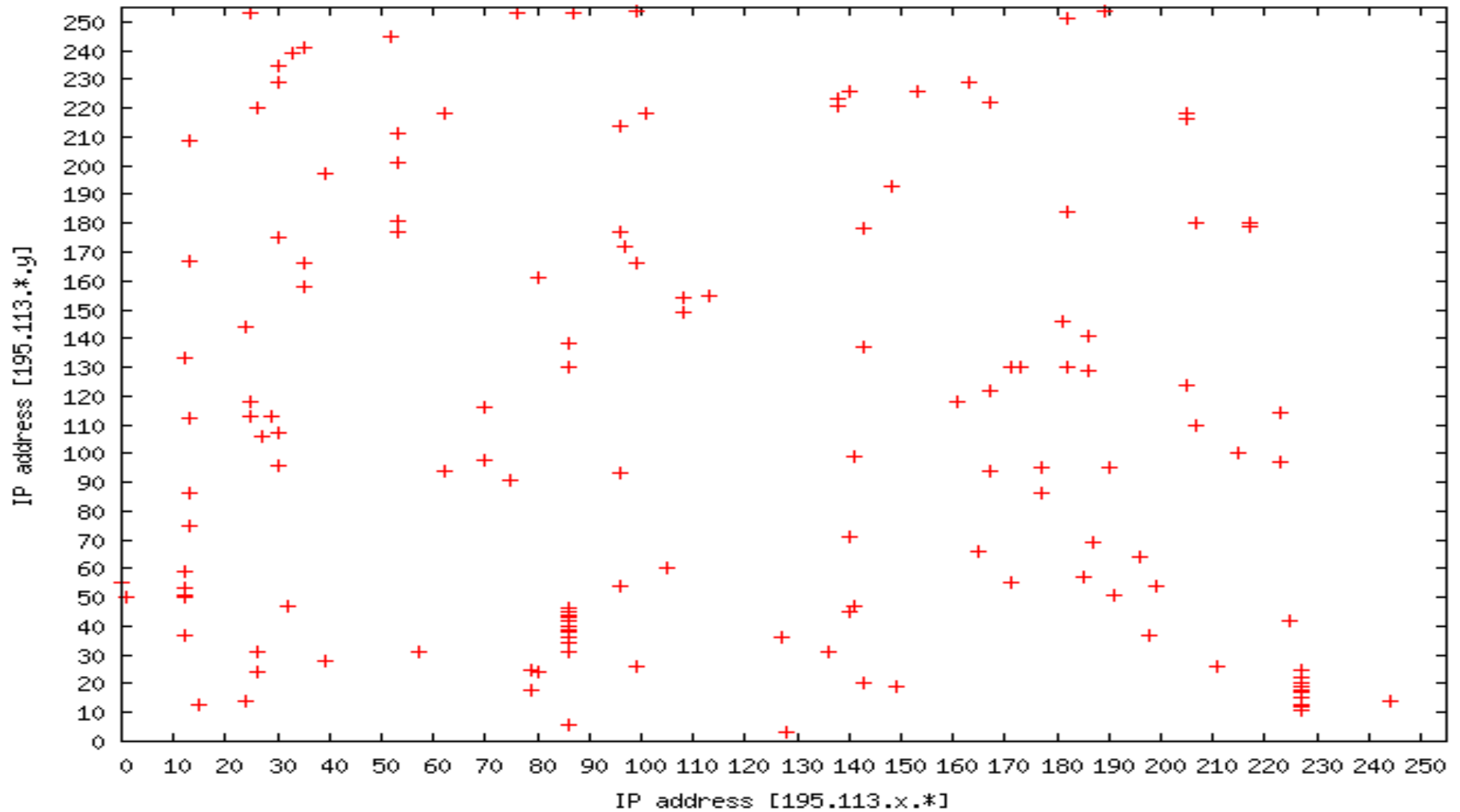
CESNET IDS od 11/2004

Na uvedené adresy **abuse@domain.tld**, **abuse@domain2.tld**, ... rozesílá CESNET IDS každý pracovní den (6.05 – 16.05 hodin GMT) každé 2 hodiny upozornění správcům těch sítí (součástí CESNETu), z nichž útoky pocházejí.

CESNET IDS: 2005

Útoky ze sítě CESNET/16

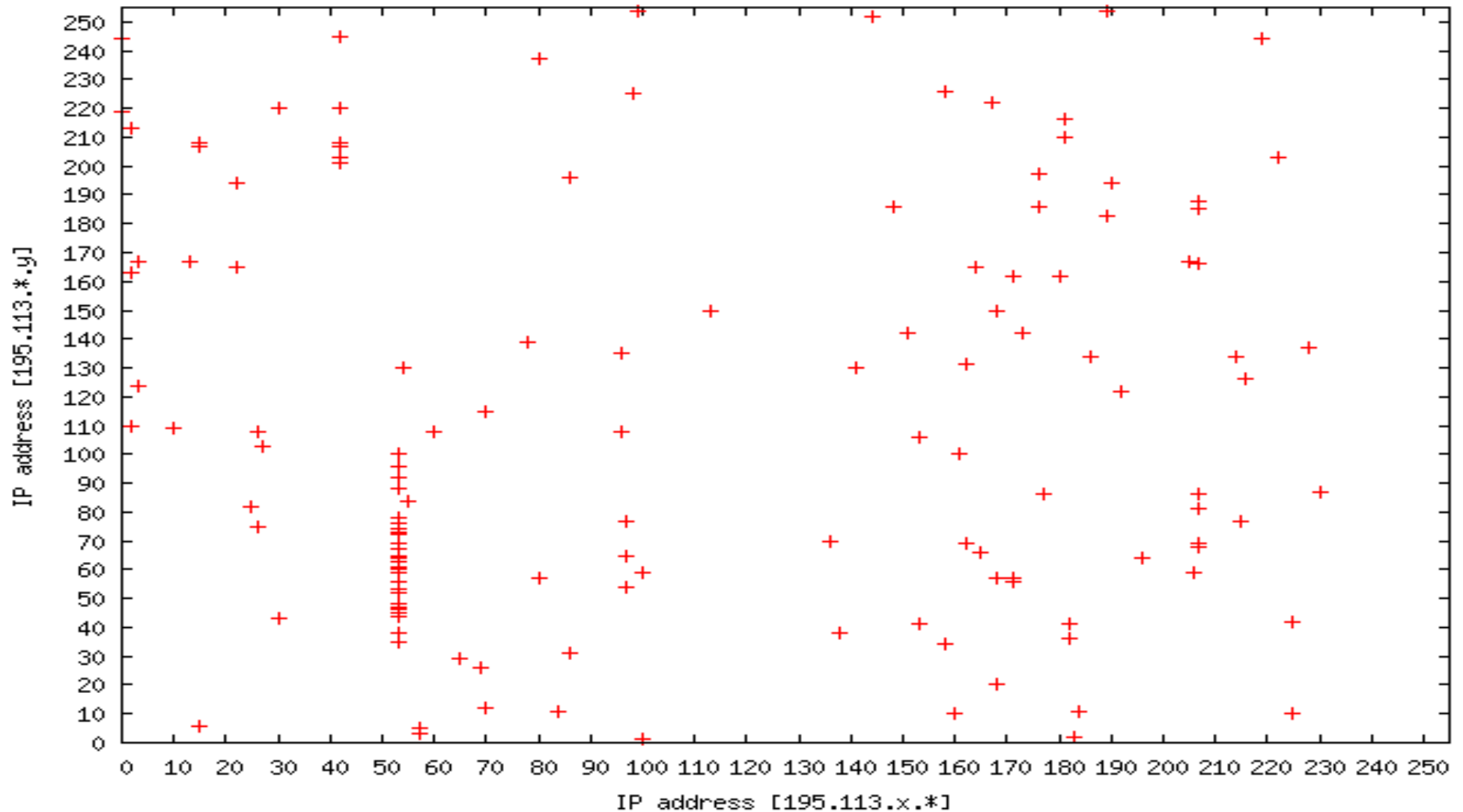
CESNET machines targeting the CESNET IDS - 2005



CESNET IDS: 2006

Útoky ze sítě CESNET/16

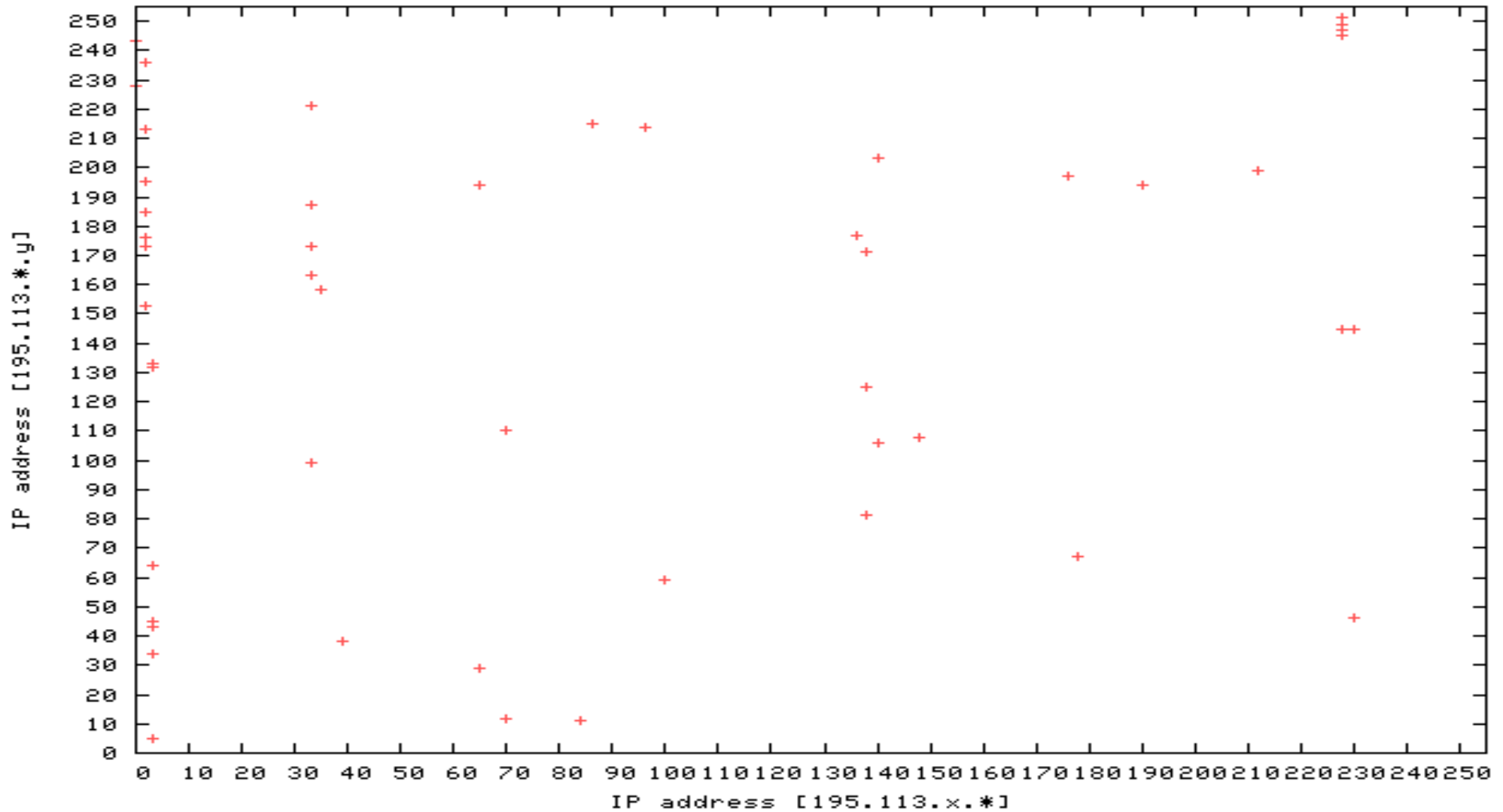
CESNET machines targeting the CESNET IDS - 2006



CESNET IDS: 1-5/2007

Útoky ze sítě CESNET/16

CESNET machines targeting the CESNET IDS - 2007



CESNET IDS 2005-2007: počet útočících strojů

Institute	2005	2006	1-5/2007
Universita 1 /16	1	1	1
Universita 2 /16	26	7	7
Universita 3 /16	0	0	0
Universita 4 /16	6	5	0
Universita 5 /16	3	0	3
Universita 6 /16	9	8	1
Universita 7 /16	1	3	2
Universita 8 /16	4	3	1
Universita 9 /16	0	0	2
Universita 10 /16	0	0	0
Universita 11 /16	0	0	0
Universita 12 /16	3	2	0
CESNET /16	144	136	49
CESNET /19	18	3	0

CESNET IDS: část výstražného dopisu

Data od `St 18.04.2007, 16:05:05' do `Čt 19.04.2007, 06:05:02'.

230 pokusů o připojení z 10.1.2.3 (host.domain.tld)

Začátek útoku: 1176948217 = Čt 19.04.2007, 02:03:37

1176948217 10.1.2.3 59125 -> 195.113.aaa.20 445

1176948217 10.1.2.3 59126 -> 195.113.aaa.21 445

1176948217 10.1.2.3 59127 -> 195.113.aaa.22 445

1176948217 10.1.2.3 59128 -> 195.113.aaa.23 445

... vynecháno 222 řádek ...

1176948280 10.1.2.3 3542 -> 195.113.aaa.227 445

1176948280 10.1.2.3 3543 -> 195.113.aaa.228 445

1176948282 10.1.2.3 3544 -> 195.113.aaa.229 445

1176948282 10.1.2.3 3545 -> 195.113.aaa.230 445

Konec útoku: 1176948282 = Čt 19.04.2007, 02:04:42.

Útok trval: 0:01:05 [h:m:s]. Frekvence: 212.308 [pokusů/min].

CESNET IDS – shrnutí: nevýhody

- Je málo účinný při detekci virů přicházejících ze “vzdálených” sítí, protože viry se snaží infikovat zejména stroje v “blízkých” sítích – viz např.

<http://www.viruslist.com/en/viruslist.html?id=4226>

- Nedokáže detekovat útoky UDP.

CESNET IDS – shrnutí: výhody

- Zvláště vhodný pro instituce s velkými, částečně nevyužitými alokacemi adres – např. pro university se sítěmi /16 (“třída B”)
- Rychle a spolehlivě detekuje zavirované nebo jinak zkompromitované stroje na “blízkých” IP adresách
- Větší rozsah adres přidělených IDSu zlepšuje schopnost detekce útoků
- Žádná falešná positiva
- Snadná instalace, nepotřebuje údržbu
- **Prospívá celému Internetu!**

CESNET IDS – shrnutí

- CESNET IDS byl navržen pro monitorování jedné velké sítě zahrnující mnoho menších sítí různých koncových uživatelů – viz Technická zpráva CESNETu

<http://www.cesnet.cz/doc/techzpravy/2006/ids>

- ČVUT Praha ve své síti /16 provozuje svůj vlastní IDS s webovým rozhraním, také založený na programu LaBrea:

<http://ids.vc.cvut.cz>

Bezpečnostní služby CESNETu

II. Audit zabezpečení strojů

Program NISSUS

<http://www.nessus.org>

= program pro bezpečnostní audit strojů

- získal řadu ocenění u odborné veřejnosti
- ve srovnávacích testech bývá na předních místech
- architektura klient – server
- 10.5.2007: 14602 bezpečnostních testů (*plugins*)
- přes 75 000 instalací NISSUSu po celém světě (v CESNETu od r. 2001)

Program NISSUS

- Od r. 2002 → Tenable Network Security
- NISSUS v. 2.x volně šiřitelný pod GPL; nejnovější + jediná verze podporovaná od 15.6.2007 = 2.2.9
- NISSUS v. 3.x distribuován stále zdarma, ale non-GPL (bez zdrojové verze) nejnovější verze = 3.0.5 (beta: 3.1.3)
- plugins:
 - Direct Feed = bez zpoždění; nutnost platby
 - Registered Feed = zpoždění 7 dní; nutnost registrace; zdarma
 - GPL Feed (nezahrnuje plugins od firmy Tenable) ²⁵

Klienty programu NISSUS

- Grafický klient pro Un*x i MS Windows umožňuje nejdokonalejší využití všech možností NISSUSu (*host-based + network-based security audit*) podle potřeb uživatele
- Řádkový klient je využit v projektu CESNET AUDIT pro rychlé a snadné otestování bezpečnosti strojů bez nutnosti instalovat NISSUS a studovat rozsáhlou dokumentaci

AUDIT server CESNETu: komunikace zabezpečená pomocí PGP

- Zájemci o bezpečnostní audit musí předat svůj veřejný PGP klíč a seznam strojů, které chtějí testovat
- Pak mohou kdykoli požádat o bezpečnostní audit těchto strojů - odesláním dopisu podepsaného klíčem PGP na adresu audit@audit.cesnet.cz
- Server odešle výsledky auditu elektronickou poštou, podepíše je svým PGP klíčem.

AUDIT server CESNETu: poštovní rozhraní

Formát dopisu se žádostí o audit:

```
CONFIG: [previous] | full | safe
FORMAT: [previous] | html | text | ...
TARGET: [previous] | IP_add... Dom.ain.add...
[DELAY: hh H mm M]
[VERBOSE:]
[END:]
```

PGP klíč serveru:

```
pub 1024D/6279F9C4 2007-01-03 CESNET AUDIT <audit@audit.cesnet.cz>
Fingerprint=EB6E 4EB8 973B F265 5248 4FEF F40F F75F 6279 F9C4
```

AUDIT server CESNETu: žádost o audit

From: test@example.cz
To: audit@audit.cesnet.cz
Subject: TEST U15
Date: Tue, 30 Jan 2007 15:34:38 +0100

config full
format html
target 10.0.0.127
delay 1h 5m
end

Server odpoví dvěma dopisy ...

AUDIT server CESNETu: výsledky auditu (1)

From: CESNET AUDIT <audit@audit.cesnet.cz>
To: test@example.cz
Subject: Re: TEST U15
Date: Tue, 30 Jan 2007 14:34:48 +0000

AUDIT v. 41 start: Tue Jan 30 14:34:43 2007 GMT
Permitted TARGET:
10.0.0.127 10.0.1.25 10.0.2.3

Audit configuration requested in Qfile:
CONFIG: full
FORMAT: html
TARGET: 10.0.0.127
DELAY: 3900 seconds (-> Tue Jan 30 15:39:46 2007 GMT)

Audit request `1170171586.1170167686.27889' queued.

AUDIT server CESNETu: výsledky auditu (2)

From: CESNET AUDIT <audit@audit.cesnet.cz>
To: test@example.cz
Subject: Re: TEST U15
Date: Tue, 30 Jan 2007 15:50:28 +0000

Hello,
please find the results of your NESSUS security audit
in the attached file.

Audit request queued on Tue Jan 30 14:34:46 2007 GMT.
Launch scheduled for Tue Jan 30 15:39:46 2007 GMT.
Launching audit on Tue Jan 30 15:40:01 2007 (15 second(s) late).
Parameters supplied in `1170171586.1170167686.27889':
CONFIG: full
FORMAT: html
TARGET: 10.0.0.127

Best regards,
the CESNET AUDIT robot.

AUDIT server CESNETu: zkušenosti z provozu

- Na strojích dostupných autorovi trvá úplný bezpečnostní audit od 7 minut (Windows 98) do 12 minutes (Linux + IPTables)
- Při testování strojů ve vzdálených sítích může nastavení mezilehlých routerů a firewallů zkreslit výsledky testů.

AUDIT server CESNETu: shrnutí

- Server umožňuje snadno a rychle otestovat zabezpečení strojů prostřednictvím poštovního rozhraní
- I nadále lze spouštět pokročilé bezpečnostní testy prostřednictvím grafického rozhraní (Un*x nebo MS Windows)
- Další informace jsou obsaženy v Technické zprávě CESNETu:

<http://www.cesnet.cz/doc/techzpravy/2005/lansec/>

Bezpečnostní služby CESNETu

Děkuji Vám za pozornost. :-)