

Bezpečnostní služby CESNETu

IDS a AUDIT

Pavel.Vachek@cesnet.cz

Bezpečnostní služby CESNETu

- **I. Intrusion Detection system (IDS)**
- II. Audit zabezpečení strojů

La Brea (Los Angeles, CA): asfaltové jezero



<http://www.tarpits.org>

Program LaBrea

<http://labrea.sourceforge.net>

(autor: Tom Liston)

- monitoruje IP adresy CESNETu dosud nealokované uživatelům
- předstírá, že na všech těchto IP adresách existují funkční zařízení

Program LaBrea

LaBrea umí mnoho užitečného - např.:

- **TARPITTING**: zachytí přicházející pokus o navázání spojení *SYN* – odpoví na něj pomocí *SYN+ACK*. Spojení po určité době skončí na *retransmission timeout*
- **CONNECTION TRAPPING**: po úspěšně navázaném spojení LaBrea inseruje okno pro příjem dat s *nulovou délkou*. Takto navázané spojení samo o sobě nikdy neskonečí 😊

Program LaBrea

W. R. Stevens: TCP/IP Illustrated, Vol. 1,
chapter 22:

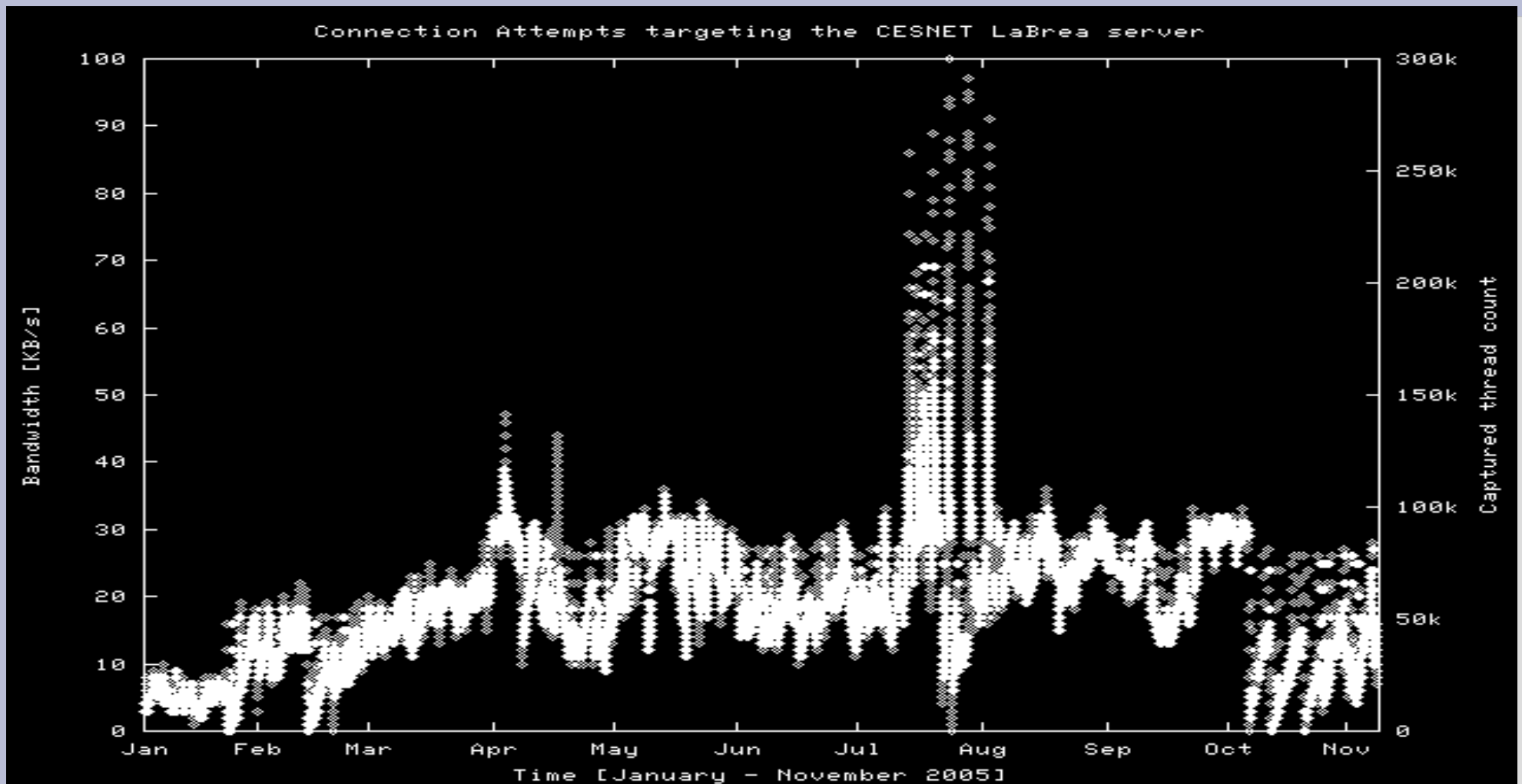
"The characteristic of the persist state that is different from the retransmission timeout [...] is that TCP *never* gives up sending window probes. These window probes continue to be sent at 60-second intervals until the window opens up or either of the applications using the connection is terminated."

Program LaBrea

Autor projektu LaBrea uvádí, že pro TCP/IP stack Windows NT je tento interval až 4 minuty; pro zachování spojení se vyžaduje přenos asi 1215 B/hod, tj. pouze 0.33 B/s! 😊

LaBrea umožňuje nastavit max. šířku pásma, která se smí využít pro zachycení pokusů o navázání spojení. 3 zachycené procesy spotřebují jen asi 1 B/s! 😊

Server LaBrea CESNETu



Server LaBrea CESNETu

**V nynější konfiguraci server LaBrea
CESNETu zachycuje max. datový tok
30 KB/s, tj. max. asi 90 tisíc vláken virů
nebo scannerů**

IDS server CESNETu

LaBrea generuje protokol s řadou užitečných informací. CESNET CSIRT jich využívá pro zřízení jednoduchého systému pro detekci útoků (Intrusion Detection System), který funguje zcela bez lidské obsluhy:

- LaBreaBackEnd analyzuje log LaBrey
- LaBreaReport rozesílá 2 * každý pracovní den upozornění správcům těch sítí (součástí sítě CESNET2), z nichž útoky vycházely

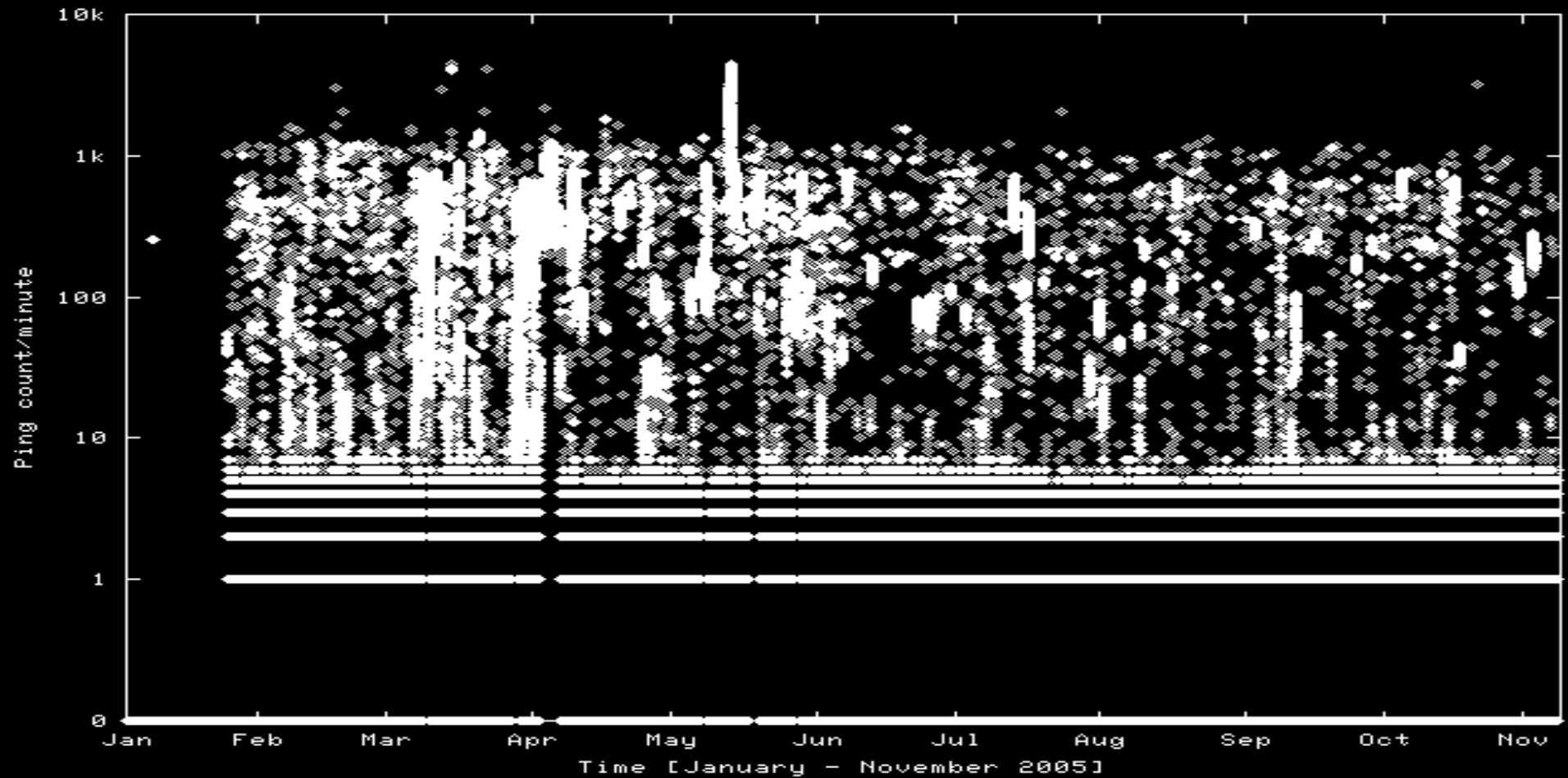
IDS server CESNETu

Do roku 2004 jsme zaznamenávali a hlásili útoky z celého světa. Nedoporučujeme to. Dnes zaznamenáváme pouze:

- úspěšné ukončení “TCP 3-way handshake” z IP adres alokovaných síti CESNET2
- přijetí *SYN+ACK*
- přijetí paketu ICMP ECHO (PING)
- hlášení o šířce datového toku

CESNET IDS - PING

Incoming PINGs on the CESNET LaBrea server



CESNET IDS - DDoS

Útoky typu Distributed Denial of Service běžně využívají zfalšovaných zdrojových IP adres neexistujících strojů

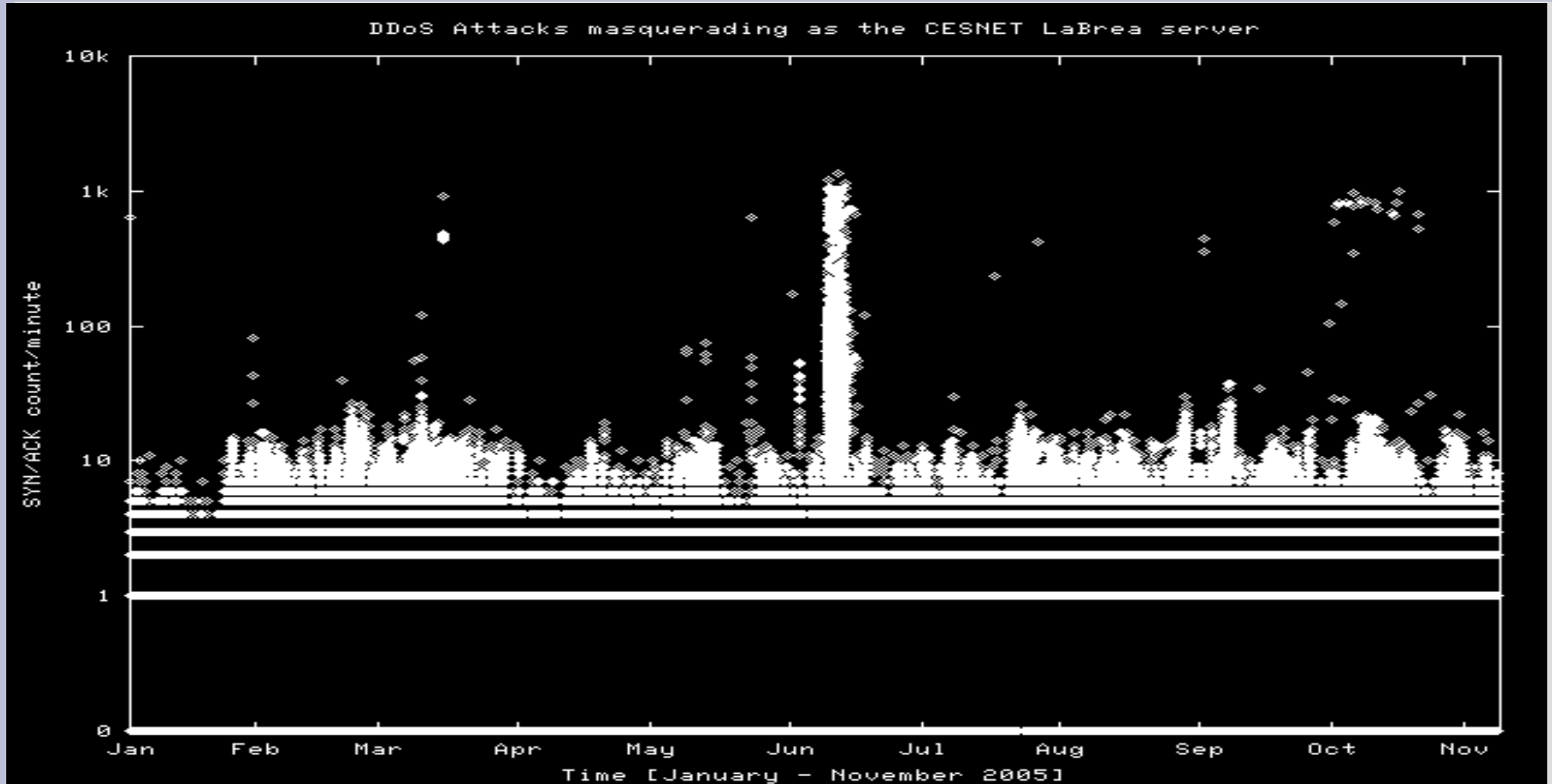
Útok DDoS (*SYN* flood):

útočník: paket *SYN* se zdroj. adresou LaBrea
→ cíl (stroj T)

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

LaBrea: paket *RST* → stroj T
=> útok zneškodněn 😊

CESNET IDS - DDoS



IDS server CESNETu

Provoz serveru IDS (LaBrea, LaBreaBackEnd, LaBreaReport) po instalaci nevyžaduje lidskou údržbu

Je velmi vhodný pro instituce, které mají v alokaci nevyužité adresové rozsahy (např. university s alokacemi “třídy B” = /16)

Prospívá celému Internetu

Bezpečnostní služby CESNETu

I. Intrusion Detection System (IDS)

II. Audit zabezpečení strojů

Program NESSUS

<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
- plugins
- přes 75 000 instalací po celém světě
(v CESNETu od r. 2001)

NESSUS a OpenVAS

- od r. 2002 → Tenable Network Security
- NESSUS v. 2.x volně šiřitelný pod GPL
nejnovější: v. 2.2.6 (8.11.2005)
- plugins:
 - Direct Feed = bez zpoždění, nutnost platby
 - Commercial Direct Feed = pro audit zákazníků
 - Registered Feed = zpoždění 7 dní, nutnost registrace, zdarma
 - Commercial Registered Feed = pro audit zákazníků
 - GPL Feed (nezahrnuje plugins od firmy Tenable)

NESSUS a OpenVAS

- Připravuje se nová větev NESSUS v. 3.x – stále zdarma, ale non-GPL !!
- V reakci na toto oznámení vzniká projekt **OpenVAS (OpenSource Vulnerability Assessment Scanner)** – NESSUS má být dále vyvíjen pod GPL; základ = v. 2.2.5
- Bližší informace: <http://www.openvas.org>

AUDIT server CESNETu

Původní architektura (2002 – 2004):

- dávkový režim – 2 seznamy strojů
 - testy úplné včetně potenciálních DoS
 - testy pouze bezpečné (non-DoS)
- testy probíhaly každé 2 týdny
- výsledky zobrazovány na zabezpečeném webu přístupném pomocí HTTPS
- souhrnné výsledky (změny proti minulému běhu) rozesílány elektronickou poštou

AUDIT server CESNETu

Nový systém auditu (2005):

Server je přístupný prostřednictvím el. pošty na adrese ***audit@audit.ces.net***

Každý uživatel CESNETu, z.s.p.o., ho může kdykoli požádat o otestování svých strojů

Výsledky auditu odešle server elektronickou poštou – podepsané, popř. i zašifrované

AUDIT server CESNETu

Komunikace zabezpečená pomocí PGP

pub 1024D/CBC98E74 2005-10-06 CESNET AUDIT <audit@audit.ces.net>
Key fingerprint = 40E8 4E54 607C 41D5 7F12 9DEA FF54 3E02 CBC9 8E74

Zájemce o audit svých strojů předá svůj PGP klíč a seznam strojů, které bude oprávněn testovat

Server AUDIT přijímá poštu jen z adresových rozsahů CESNETu

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:]
```

AUDIT server CESNETu: žádost o audit

Date: Sun, 9 Oct 2005 10:14:54 +0200 (CEST)
To: Audit <audit@audit.ces.net>
Subject: REAL TEST # 40

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

target 195.113.205.91

config full

format html

delay 1 h 20 m

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.0 (GNU/Linux)

Comment: For info see http://quantumlab.net/pine_privacy_guard/

(...)

-----END PGP SIGNATURE-----

AUDIT server CESNETu: výsledky auditu

From: CESNET AUDIT <audit@audit.ces.net>
Subject: Re: REAL TEST # 40
Date: Sun, 9 Oct 2005 09:41:28 +0000

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

This audit request has been queued on Sun Oct 9 08:15:07 2005 GMT.
Audit request processing advanced by 6 seconds.
Parameters supplied in `1128850507.1128845707.17621':
CONFIG: full
FORMAT: html
TARGET: 195.113.205.91

Best regards,
the CESNET AUDIT robot.

AUDIT server CESNETu

- nyní = zkušební provoz
- přejdeme na rychlejší hardware
- zpřístupníme WWW stránku
- vydáme technickou zprávu
- další vývoj podle požadavků uživatelů:
 - stručný přehled dalších možností NNESSUSu v češtině ??
 - zpřístupnění dalších typů konfiguračních souborů ??

AUDIT server CESNETu: zkušenosti z provozu

- Na strojích dostupných autorovi teď trvá úplný bezpečnostní audit od 7 minut (Windows 98) do 12 minut (Linux + iptables)
- při testování strojů ve vzdálených sítích může nastavení firewallů a routerů zkreslit výsledky testů
- autor bude vděčen za připomínky a náměty ke zlepšení. 😊

Bezpečnostní služby CESNETu

Děkuji Vám za pozornost a trpělivost.

