NESSUS

IL
Security Scanner

Francesco M. Taurino
[taurino@na.infn.it]

La vostra RETE

- Quali servizi sono presenti?
- Sono configurati in modo sicuro?
- Su quali macchine girano?

Domanda...

Quanto e’ “sicura” la vostra rete?

...qui arriva NESSUS

NESSUS

e’ un security scanner capace, da remoto, di identificare il sistema operativo e i servizi che girano su una o piu’ macchine e di individuarne gli eventuali punti deboli

Cosa fa

- Cerca i servizi che girano su una macchina e le versioni dei programmi che li gestiscono
- Prova realmente gli exploit noti (~900 ad aprile 2002)
- A richiesta puo’ lanciare dei DOS

NESSUS non da nulla per scontato.

Alcuni servizi possono girare su una porta non standard

Es: un web server potrebbe girare sulla porta 1234

Alcuni riconoscimenti

- 6/2000 NESSUS e' risultato il primo classificato in un confronto fra prodotti commerciali e gratuiti, ed e' ATTUALMENTE in cima alla lista dei security tools sul sito

  http://www.insecure.org/tools.html

- 3/2002 NESSUS e' stato premiato come miglior tool gratuito di sicurezza da "Information Security Magazine"

  durante il "Security Excellence Award 2002"

  http://www.infosecuritymag.com

Caratteristiche principali

1. Architettura a plug-in
2. Database delle vulnerabilita' costantemente aggiornato (alcuni script vengono rilasciati dallo staff di NESSUS poche ore dopo la pubblicazione di un nuovo bug sulle mailing list della sicurezza)
3. I nuovi script di test vengono scaricati e installati facilmente (comando 'nessus-update-plugins')

1. Ricerca intelligente dei servizi (porte non standard, servizi multipli)
2. Test condizionali (se il servizio web non c’e’ gli attacchi CGI non vengono lanciati)
3. Velocita’ di esecuzione (scan in multithread)
4. NASL (Network Attack Scripting Language) e C come linguaggi per gli script

1. Client/Server
2. Client multipiattaforma (con criptazione del traffico)
3. Supporto CVE (Common Vulnerabilities and Exposures)
4. Report in Latex, ASCII, HTML, XML

Inoltre e’ Open Source, ed essendo rilasciato sotto la licenza GNU...

GRATUITO

La storia di NESSUS

- Apr/98 Alpha 1
- Nov/99 Nessus 0.99
- 1Q/2000 Nessus 1.0
- Giu/2001 Nessus 1.0.8 (681 test)
- Ago/2001 Nessus 1.1.3 (exp. version)
- Apr/2002 Nessus 1.2.0 (~900 test)

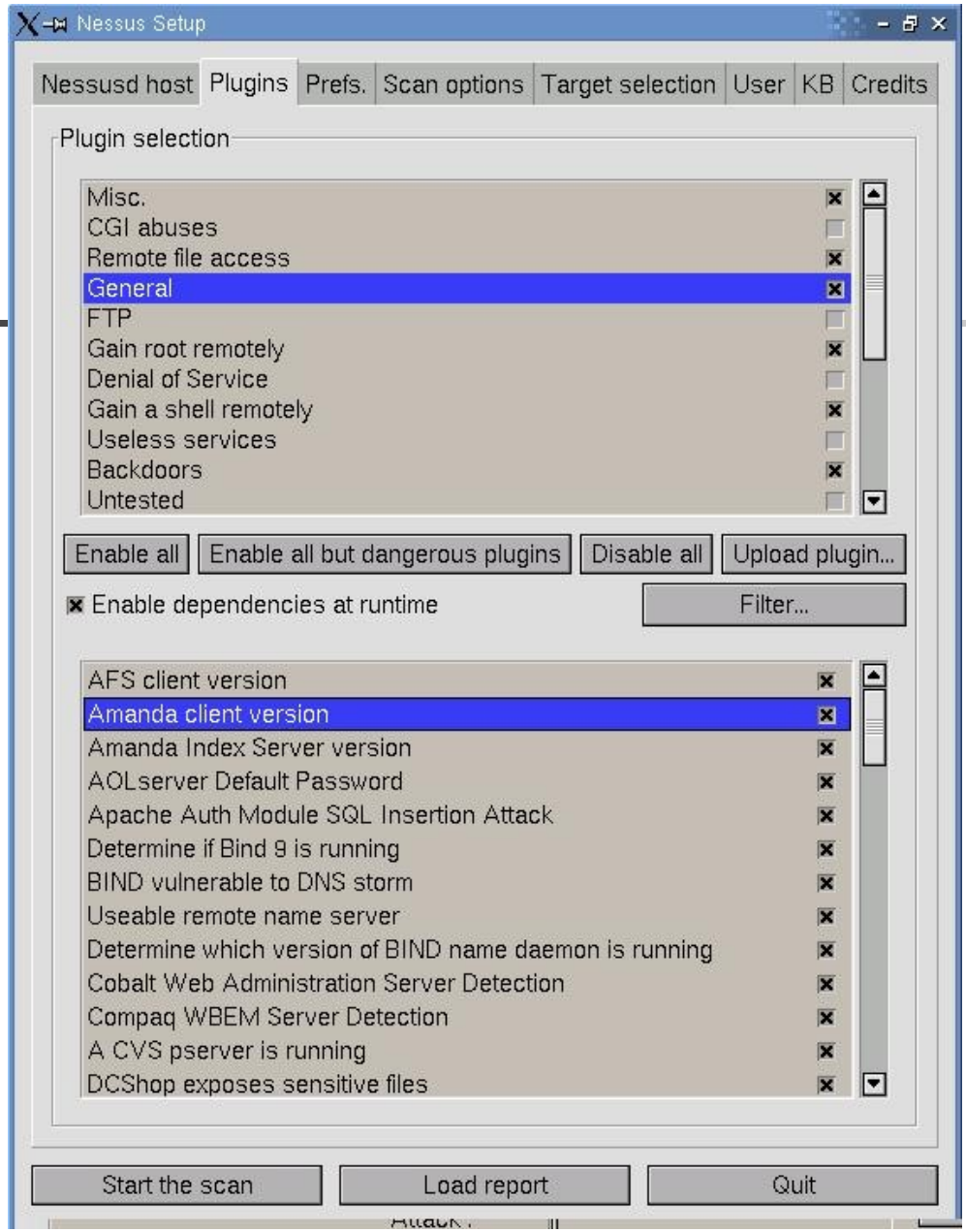
Installazione

- Il server Nessus gira su piattaforma unix
- Esistono client per unix e Windows
- Per la compilazione seguire le istruzioni del mini-howto disponibile su

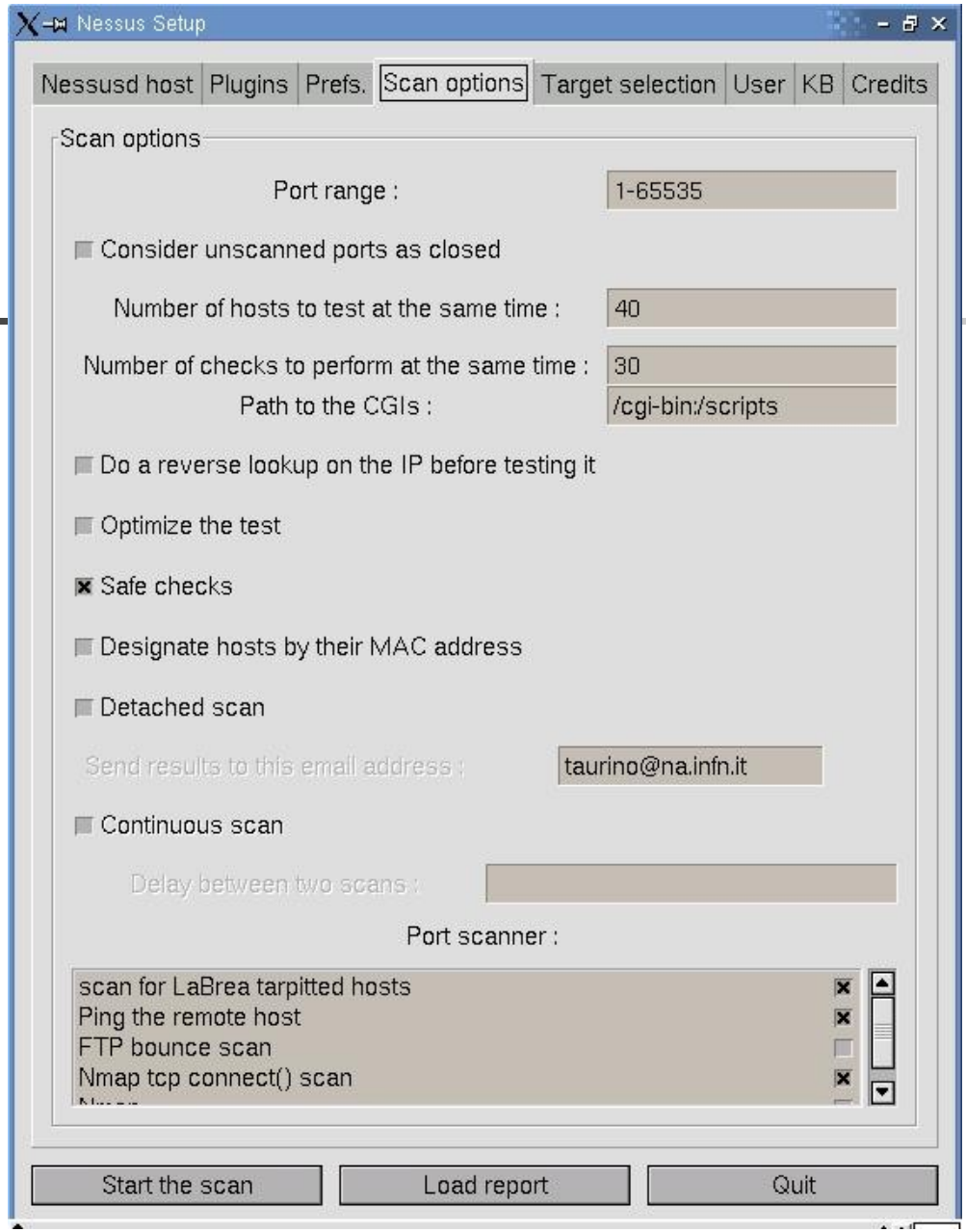
  http://www.na.infn.it/cdc/cdcdocuments.asp

Come fare uno scan

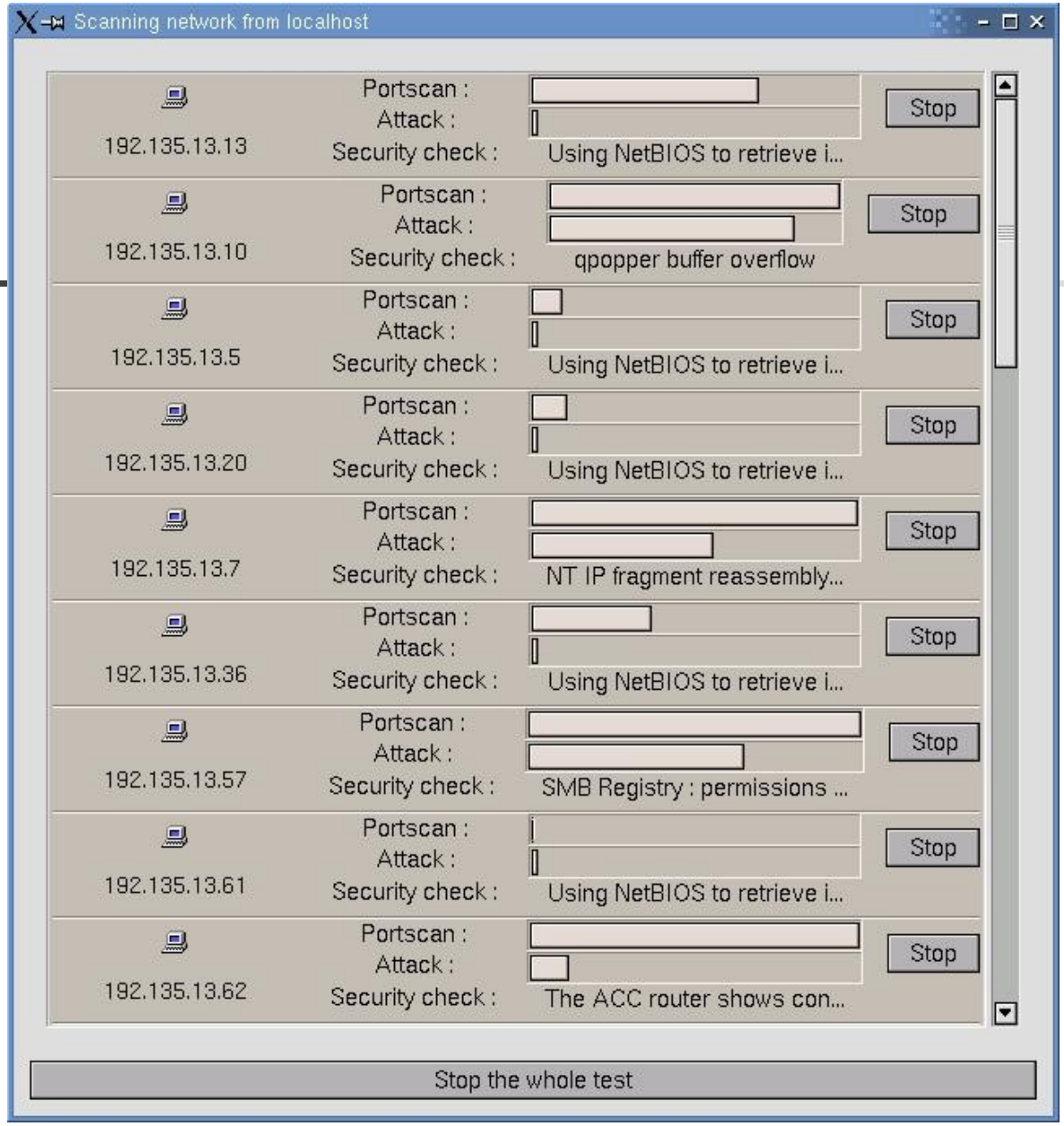
1. Lanciare il client ‘nessus’
2. Selezionare un server Nessusd
3. Selezionare i tipi di test da effettuare
4. Configurare le opzioni dei plug-in
5. Selezionare il port scanner
6. Inserire il target
7. Lanciare lo scan



CONFIGURAZIONE



PORT SCANNER


Scanning network from localhost
192.135.13.13
Portscan :
Attack :
Security check :
Using NetBIOS to retrieve i...
Stop
192.135.13.10
Portscan :
Attack :
Security check :
qpopper buffer overflow
Stop
192.135.13.5
Portscan :
Attack :
Security check :
Using NetBIOS to retrieve i...
Stop
192.135.13.20
Portscan :
Attack :
Security check :
Using NetBIOS to retrieve i...
Stop
192.135.13.7
Portscan :
Attack :
Security check :
NT IP fragment reassembly...
Stop
192.135.13.36
Portscan :
Attack :
Security check :
Using NetBIOS to retrieve i...
Stop
192.135.13.57
Portscan :
Attack :
Security check :
SMB Registry : permissions ...
Stop
192.135.13.61
Portscan :
Attack :
Security check :
Using NetBIOS to retrieve i...
Stop
192.135.13.62
Portscan :
Attack :
Security check :
The ACC router shows con...
Stop
Stop the whole test

SCANNING

A test eseguito

Alla fine del test viene presentato un report con la situazione delle varie macchine ordinato per numero e gravita’ dei bachi

Nessus "NG" Report

Subnet

192.135.13

Port

ssh (22/tcp)
netbios-ssn (139/tcp)
netbios-ns (137/udp)

Severity

Security Warning
Security Note
Security Hole

Host

192.135.13.232
192.135.13.233
192.135.13.234
192.135.13.235
192.135.13.236
192.135.13.237
192.135.13.239
192.135.13.240
192.135.13.241
192.135.13.245
192.135.13.247
192.135.13.248
192.135.13.249
192.135.13.250
192.135.13.251
192.135.13.252
192.135.13.253
192.135.13.254

You are running a version of OpenSSH which is older than 3.0.2.

Versions prior than 3.0.2 are vulnerable to an environment variables export that can allow a local user to execute command with root privileges.
This problem affect only versions prior than 3.0.2, and when the UseLogin feature is enabled (usually disabled by default)

Solution : Upgrade to OpenSSH 3.0.2 or apply the patch for prior versions. (Available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH)

Risk factor : High (If UseLogin is enabled, and locally)

You are running a version of OpenSSH which is older than 3.0.1.

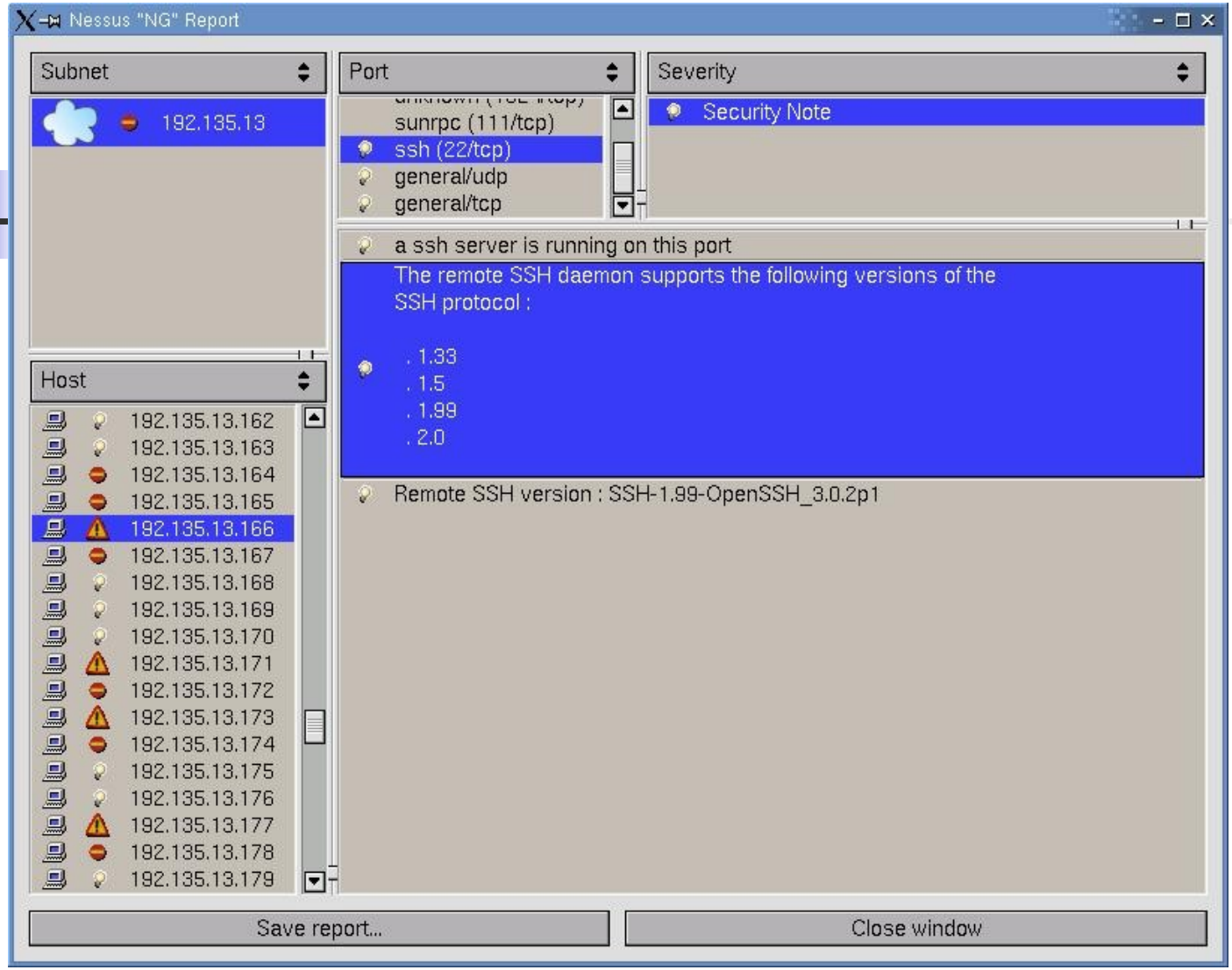
Versions older than 3.0.1 are vulnerable to a flaw in which an attacker may authenticate, provided that Kerberos V support has been enabled (which is not the case by default).
It is also vulnerable as an excessive memory clearing bug, believed to be unexploitable.

*** You may ignore this warning if this host is not using
*** Kerberos V

Save report...

Close window

N O N S I C U R A


Nessus "NG" Report
Subnet
192.135.13
Port
sunrpc (111/tcp)
ssh (22/tcp)
general/udp
general/tcp
Severity
Security Note
a ssh server is running on this port
The remote SSH daemon supports the following versions of the SSH protocol :
. 1.33
. 1.5
. 1.99
. 2.0
Remote SSH version : SSH-1.99-OpenSSH_3.0.2p1
Host
192.135.13.162
192.135.13.163
192.135.13.164
192.135.13.165
192.135.13.166
192.135.13.167
192.135.13.168
192.135.13.169
192.135.13.170
192.135.13.171
192.135.13.172
192.135.13.173
192.135.13.174
192.135.13.175
192.135.13.176
192.135.13.177
192.135.13.178
192.135.13.179
Save report...
Close window

S
I
C
U
R
A

Report in html

Questo report rende visibili le vulnerabilita’ delle macchine testate in pagine html con link ai riferimenti CVE e ai siti con gli eventuali aggiornamenti da applicare

http://people.na.infn.it/~taurino/nessus

Nessus Report - Netscape

File Edit View Go Communicator Help

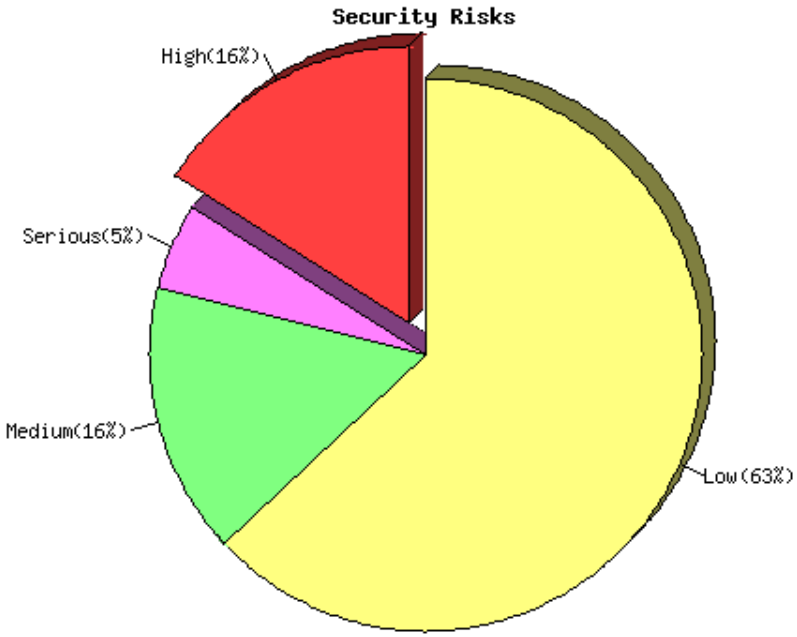
Back Forward Reload Home Search Netscape Print Security Shop Stop

Bookmarks Location: http://people.na.infn.it/~taurino/nessus/ What's Related

The Nessus Security Scanner was used to assess the security of 8 hosts

- **11 security holes have been found**
- **70 security warnings have been found**
- **42 security notes have been found**

Part I : Graphical Summary :



Document: Done

Start Microsoft PowerPoint - [NE... Nessus Report - Nets... 12:50

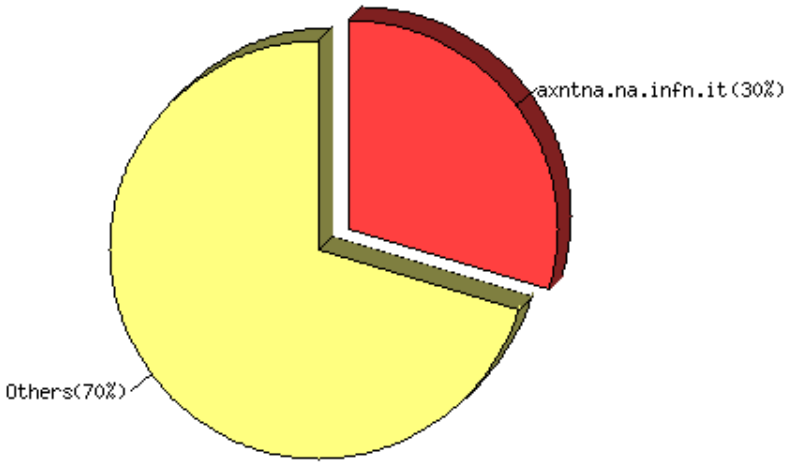
Nessus Report - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

Bookmarks Location: http://people.na.infn.it/~taurino/nessus/ What's Related

Most dangerous host weight in the global insecurity



Part II. Results, by host :

axntna.na.infn.it	(found 6 security holes)
axntmsa.na.infn.it	(found 2 security holes)
lxtest.na.infn.it	(found 1 security hole)
luxna2.na.infn.it	(found 1 security hole)

Document: Done

Start Microsoft PowerPoint - [NE... Nessus Report - Nets... 12.56

Novita’ di NESSUS 1.2

- Safe checks
- IDS Evasion
- Knowledge Base saving
- Test “mirati”
- Scalabilita’ migliorata
- Nuovo formato dei file di report

Riferimenti

- Nessus
  http://www.nessus.org
- NMAP
  http://www.insecure.org/nmap
- GTK
  http://www.gtk.org
- CVE
  http://cve.mitre.org/