Auditing e Sicurezza Informatica

Automazione di scansioni di servizi di rete remote finalizzate all'auditing per la sicurezza informatica.

Borsista: Dario Vettore

Tutor: Michele Michelotto

Auditing

- cos'è?
- perché farlo?
- scansioni perché?

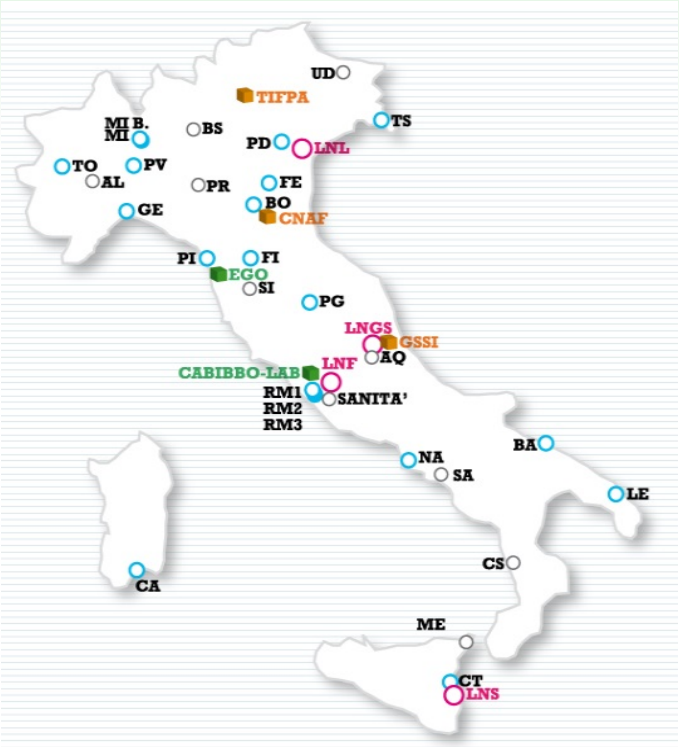
Auditing e Sicurezza Informatica

INFN

- Nmap
- Nessus
  - https://audiweb.infn.it

Garr

- Servizio Scarr
  - https://scarr.garr.it/



Auditing e Sicurezza Informatica

Ambiente di lavoro

- MV con Scientific Linux 6.5
  - bersaglio
- MV con Backbox Linux 3.13
  - attaccante

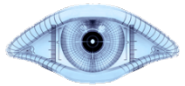
- ## Nmap: Network Mapper (1/2) ~ Caratteristiche

Scopo ↦ identifica le porte aperte (host/rete)

Metodo ↦ invio pacchetti TCP/UDP

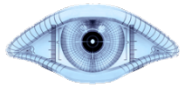
Uso ↦ linea di comando / UI (ZenMap)

Output ↦ grepable, xml, text



Nmap (1/2) ~ Alternative

- arp-scan
  - controllo solo su macchine accese, poche info
- pnscan
  - meglio di arp-scan, ma molto meno di nmap
- knocker
  - veloce, buona alternativa a nmap, non scala su grandi reti e porte



Auditing e Sicurezza Informatica

Nessus

- software per effettuare scansioni
- proprietario
- client/server/riga di comando
- output in HTML/PDF/XML
- propone soluzioni alle vulnerabilità
- patch?

OpenVAS, un alternativa a Nessus

- software per effettuare scansioni
- open source
- client/server/riga di comando
- output in HTML/PDF/XML/Latex
- propone soluzioni alle vulnerabilità
- patch?

Auditing e Sicurezza Informatica

Nessus/OpenVAS

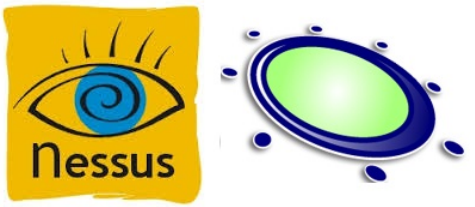
Criterio di confronto	Nessus	OpenVAS
Installazione	Facile	Difficile
UI	Semplice (Client/ Server)	Semplice
Qualità test	Molto Alta	Buona
N° plugin (05/14)	>60.000	~33.790
Costo (€)	1.200/anno + supporto	0/anno

Auditing e Sicurezza Informatica

Nessus/OpenVAS/ Altri [1]

	Rank	Open Source
Nessus	1°	NO
OpenVAS	2	SI
Core Impact	3	NO
Nexpose	4	NO

[1] http://sectools.org/tag/vuln-scanners/



Penetration-test

- cos'è?
- perché si fa?

Penetration-test – Fasi e Software (1/2)

- Information Gathering
  - Nmap/Whatweb
- Vulnerability Assessment
  - Nessus/OpenVAS/Nikto
- Exploitation
  - Sqlmap/msfconsole/joomscan

Penetration-test – Fasi e Software (2/2)

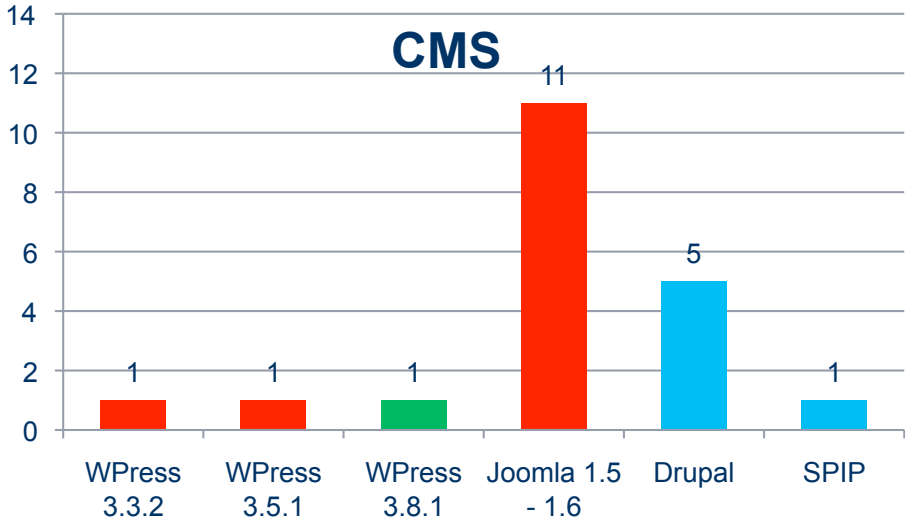
- Privilege Escalation
  - Whireshark
- Maintaining Access
  - Weevely (Web BackDoor),ptunnel
- Reporting
  - MagicTree
- Distribuzioni linux
  - BackBox, BackTrack, NodeZero, ecc

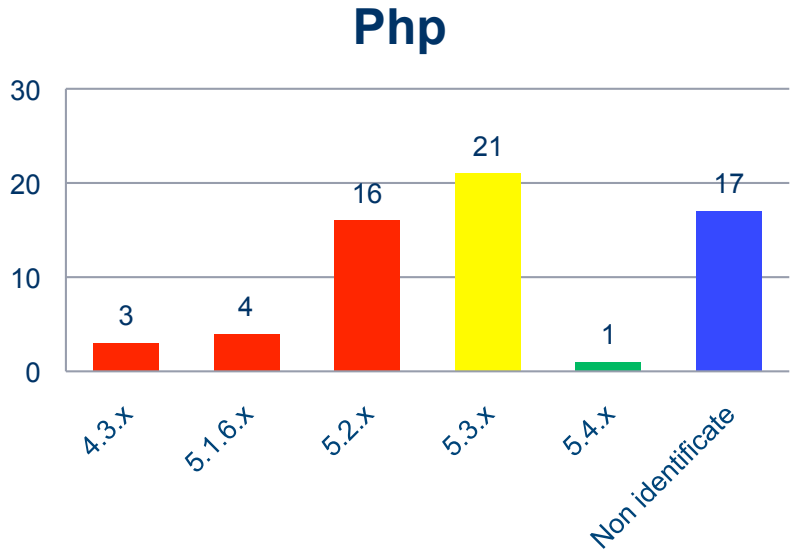
Impiego dei tool

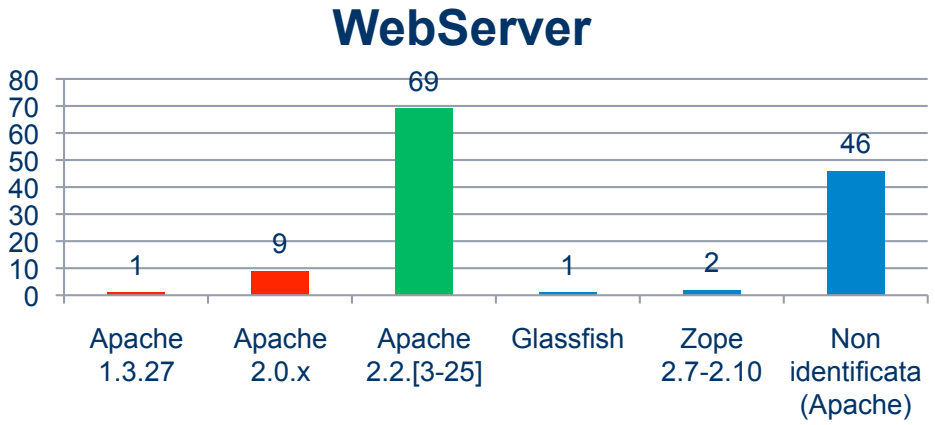
- Nessus vs OpenVAS
  - dominio: pd.infn.it, cnaf.infn.it ~ confronto??
- Nmap
  - dominio: pd.infn.it
- Nikto, joomscan
  - dominio: pd.infn.it
- Whatweb
  - dominio: *.infn.it

Auditing e Sicurezza Informatica

Risultati: **130** siti web analizzati

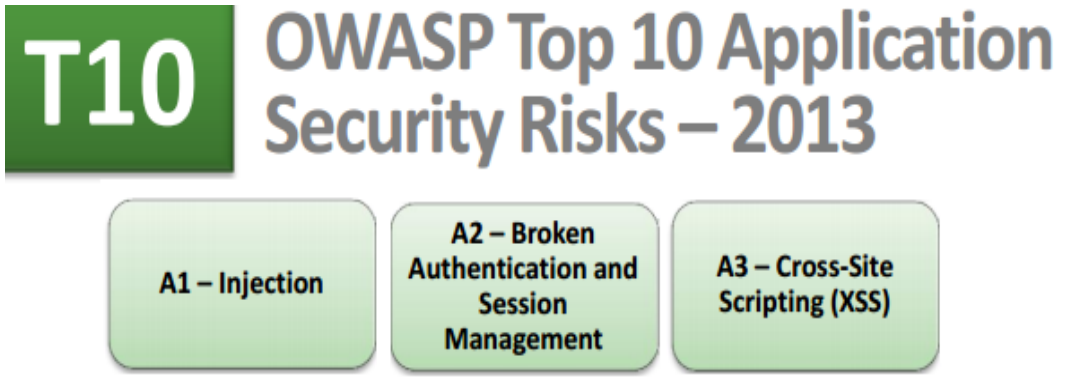






Auditing e Sicurezza Informatica

In futuro (1/2)

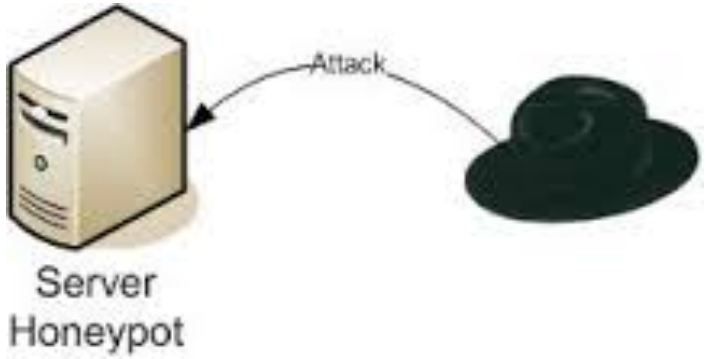


- Sql Injection
  - **SELECT** * **FROM** users
    WHERE USER='pippo' **AND** pwd='' **OR USER**='pippo'
- XSS
  - <**script** type="text/javascript">alert('XSS')</**script**>

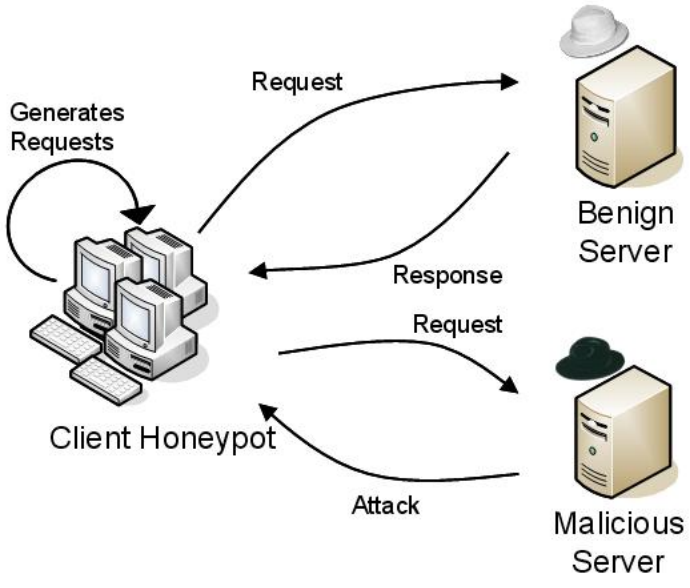
Auditing e Sicurezza Informatica

In futuro (2/2)

- Honeypot server
  - di produzione
  - di ricerca



- Honeypot client



Grazie per l'attenzione

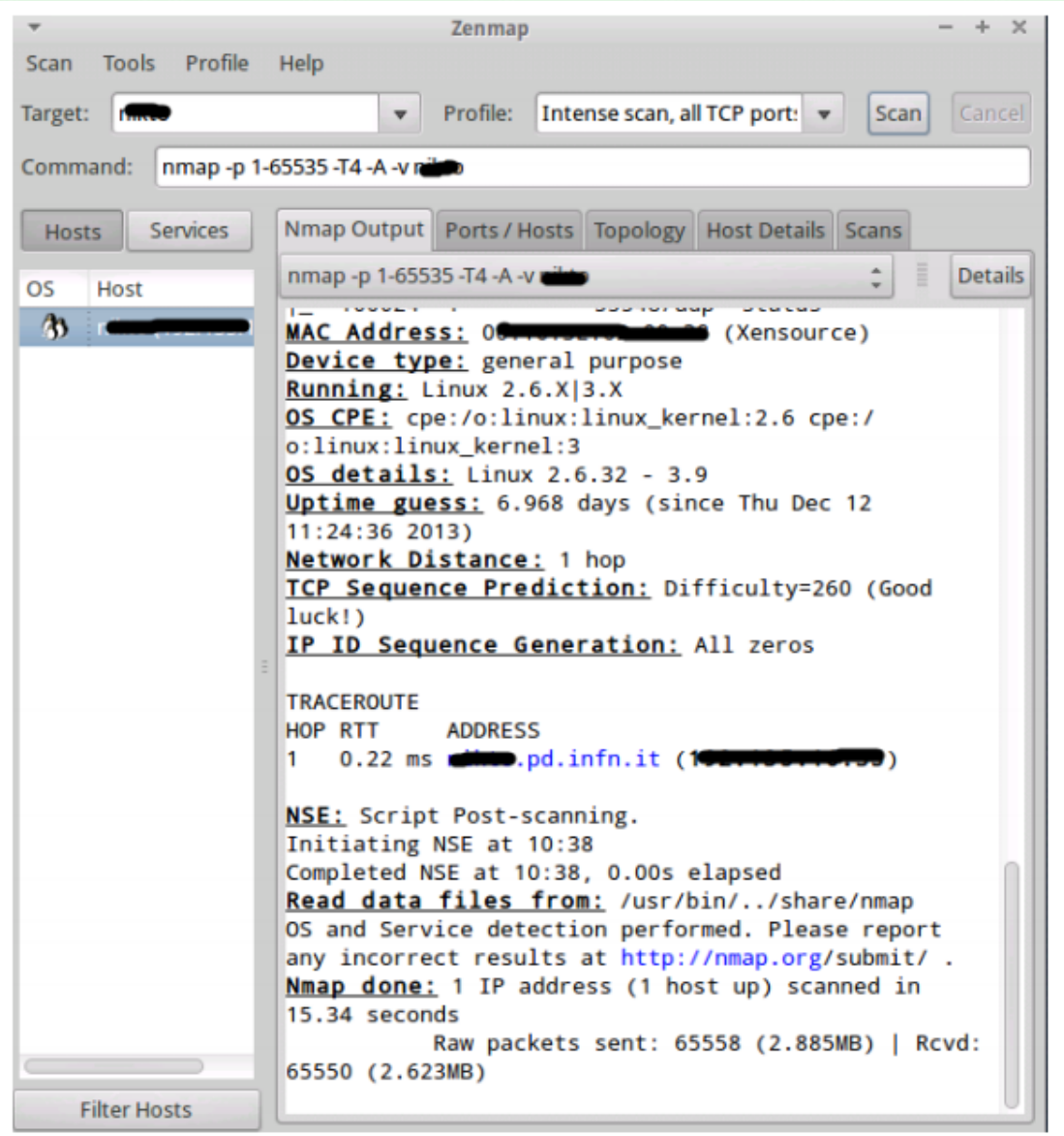
FINE

Nmap

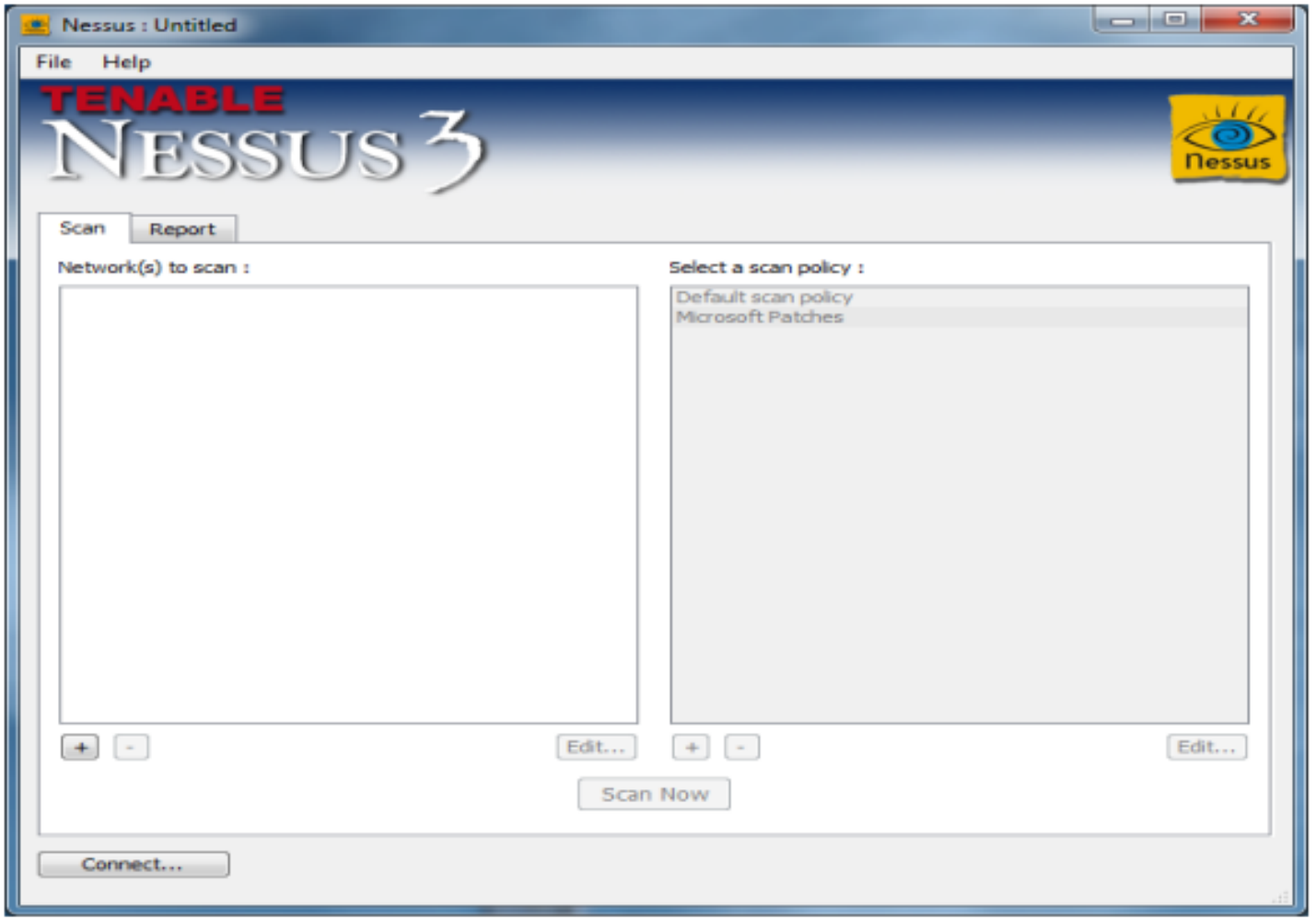
```
PORT     STATE  SERVICE         REASON       VERSION
21/tcp   closed ftp             conn-refused
22/tcp   open   ssh             syn-ack      OpenSSH 5.3 (protocol 2.0)
23/tcp   closed telnet          conn-refused
25/tcp   closed smtp            conn-refused
53/tcp   closed domain          conn-refused
80/tcp   open   http            syn-ack      Apache httpd 2.2.15 ((Scientific Linux))
109/tcp  closed pop2            conn-refused
110/tcp  closed pop3            conn-refused
143/tcp  closed imap            conn-refused
443/tcp  closed https           conn-refused
465/tcp  closed smtps           conn-refused
587/tcp  closed submission      conn-refused
993/tcp  closed imaps           conn-refused
995/tcp  closed pop3s           conn-refused
1080/tcp closed socks           conn-refused
1443/tcp closed ies-lm          conn-refused
8000/tcp closed http-alt        conn-refused
8080/tcp closed http-proxy      conn-refused
8081/tcp closed blackice-icecap conn-refused
53/udp   closed domain          port-unreach
69/udp   closed tftp            port-unreach
161/udp  closed snmp            port-unreach
162/udp  closed snmptrap        port-unreach
MAC Address: [redacted] (Xensource)
Final times for host: srtt: 1301 rttvar: 801  to: 100000

Read from /usr/bin/../share/nmap: nmap-mac-prefixes nmap-payloads nmap-service-probes nmap-services.
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.34 seconds
           Raw packets sent: 5 (212B) | Rcvd: 5 (324B)
root@backbox:~#
```

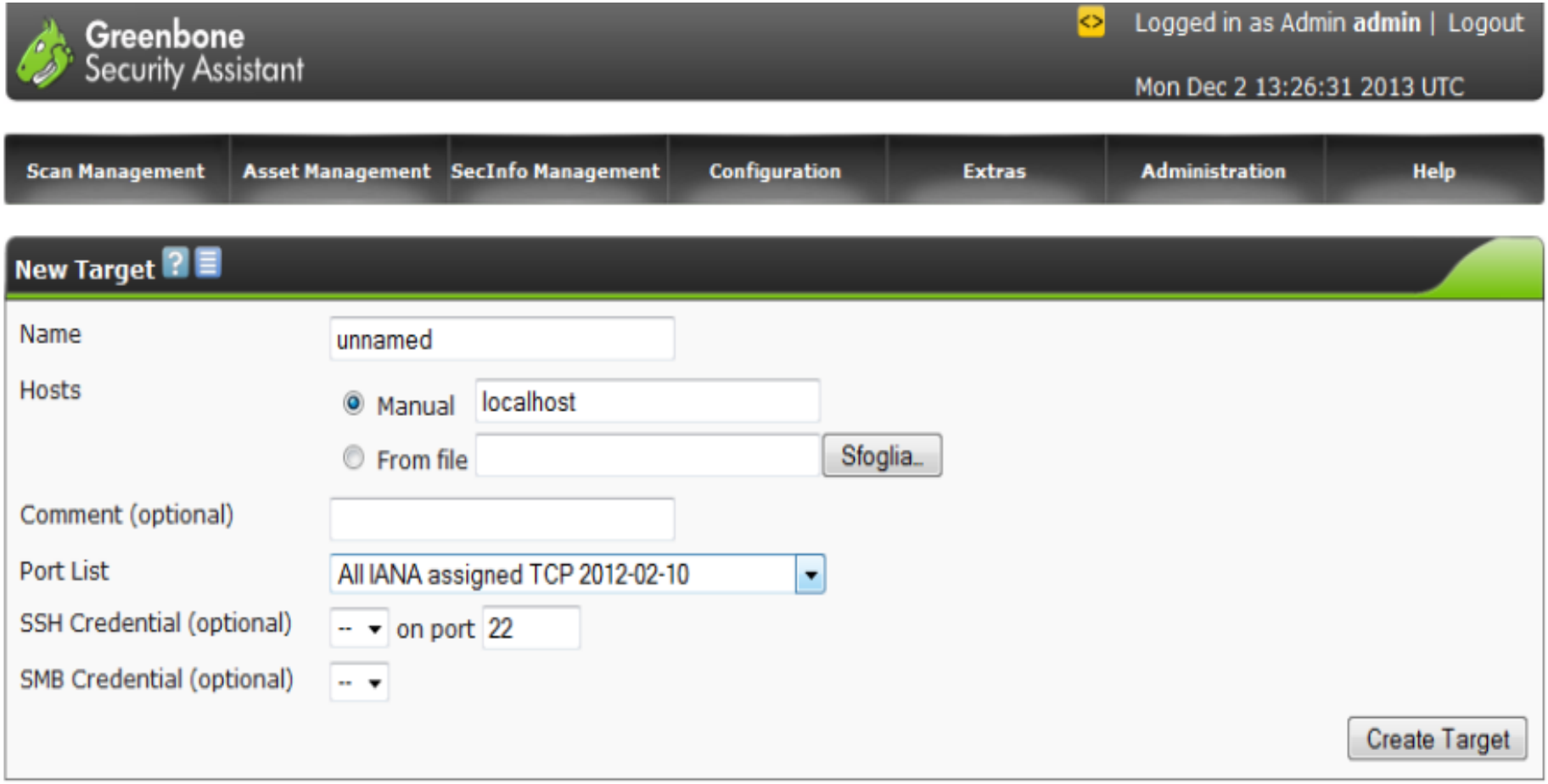
ZenMap


Zenmap
Scan Tools Profile Help
Target:
Profile: Intense scan, all TCP port:
Scan
Cancel
Command: nmap -p 1-65535 -T4 -A -v
Hosts
Services
OS Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -p 1-65535 -T4 -A -v
Details
MAC Address: (Xensource)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.9
Uptime guess: 6.968 days (since Thu Dec 12 11:24:36 2013)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
TRACEROUTE
HOP RTT ADDRESS
1 0.22 ms .pd.infn.it (
NSE: Script Post-scanning.
Initiating NSE at 10:38
Completed NSE at 10:38, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.34 seconds
Raw packets sent: 65558 (2.885MB) | Rcvd: 65550 (2.623MB)
Filter Hosts

Nessus client



OpenVAS: new target



OpenVAS: new task