



# Test de intrusión y robustecimiento de la seguridad

Barcelona, 16 de febrero de 2006

- Cubrir los conceptos de integridad, confidencialidad, disponibilidad y no-repudio, mediante la implantación de un conveniente conjunto de controles, que pueden ser políticas, normas, procedimientos, estructuras organizativas y herramientas software.
- Estos controles se tienen que establecer para asegurar el cumplimiento de los objetivos de seguridad de la empresa.



- Se deben implantar herramientas de auditoría que permitan comprobar las políticas de seguridad tanto en los servidores y estaciones de trabajo como en bases de datos.
- Estas herramientas de se ejecutan periódicamente y realizan informes sobre el estado actual de los sistemas:
  - Herramientas de auditoría en servidores y estaciones de trabajo
  - Herramientas de auditoría en bases de datos
  - Herramientas de auditoría de vulnerabilidades de seguridad

- Son herramientas de ayuda en la administración de los riesgos de seguridad mediante un sistema de análisis y detecciones del sistema operativo, aplicaciones y puntos débiles de la seguridad controlados por el usuario. Identifican posibles puntos débiles de la seguridad comparando políticas de seguridad predefinidas con la actual configuración del sistema.
- **Comprobaciones realizadas:**
  - Detección de señales de intrusiones en un sistema.
  - Verificación de la integridad del sistema.
  - Comprobación de la seguridad de la configuración del sistema.
  - Comprobación de la seguridad de los servicios de redes.
  - Comprobación de de la Configuración Actual
  - Comprobación de la Propiedad y Permisos sobre Ficheros...
- Ejemplos: Microsoft Baseline Security Analyzer, Kane Security Analyst...

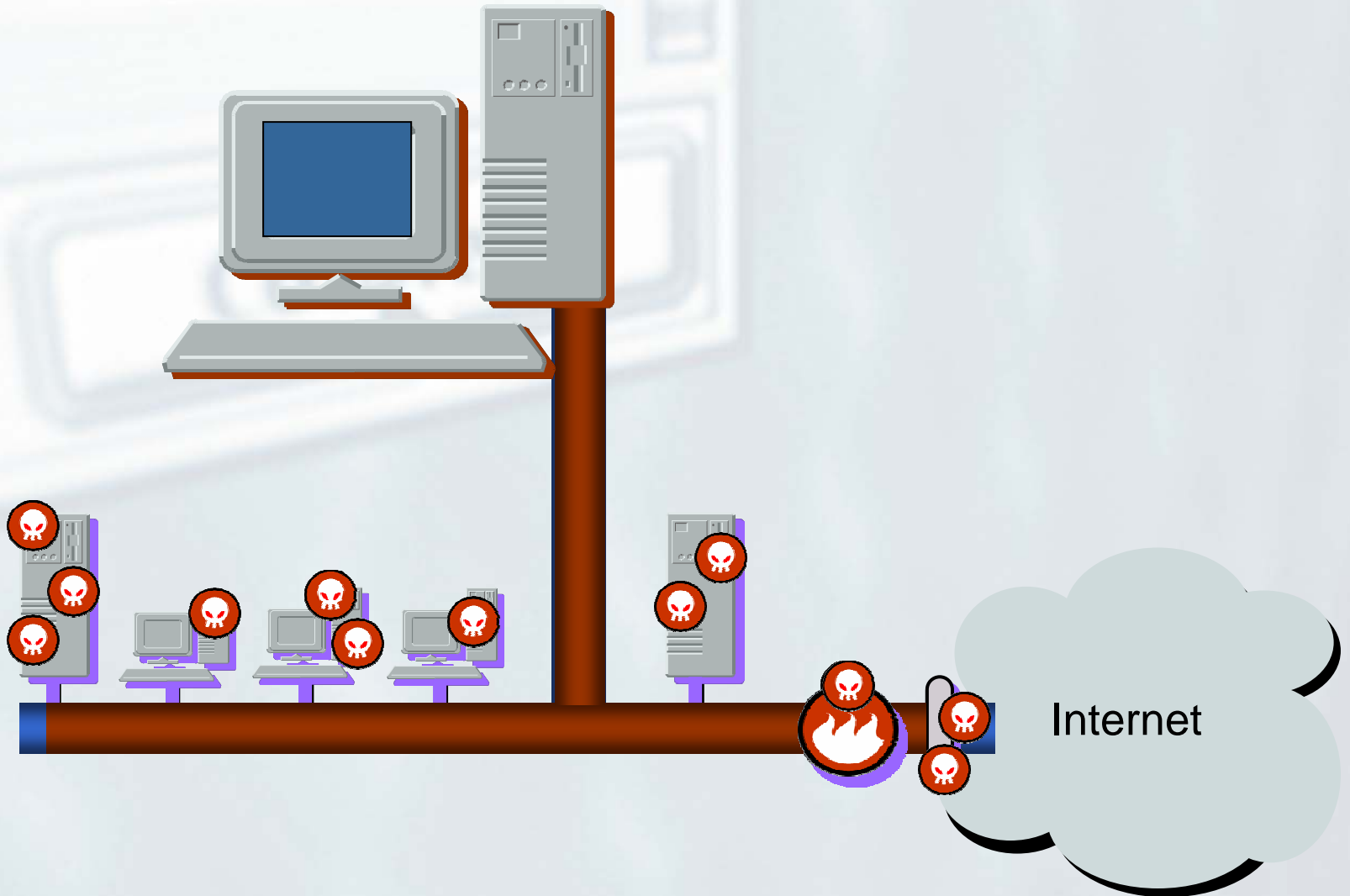


- Son aplicaciones que automatizan el proceso de asegurar los datos almacenados en servidores Oracle, Microsoft SQL Server o Sybase Adaptive Server database. Establecen políticas de seguridad cubriendo las vulnerabilidades potenciales y proporcionando un asesoramiento detallado de los riesgos y reparando la información para sistemas de bases de datos en sistemas UNIX o Windows NT.
- **Comprobaciones realizadas:**
  - Permisos de un role.
  - Conexiones fuera de hora.
  - Permisos de cuentas.
  - Propietarios de objetos no autorizados.
  - Conexiones en remoto y servidores.
  - Tabla de permisos del sistema.
  - Procedimientos de almacenamiento extensivo...
- Ejemplos: Database Scanner...

- Estas herramientas comprueban las vulnerabilidades de seguridad desde fuera, es decir, aquellas que puede encontrar un atacante de forma externa: escáner de puertos, bugs de seguridad...
- Su funcionamiento se basa en pasar varias baterías de pruebas buscando las vulnerabilidades que suelen aprovechar los hackers para investigar y atacar los sistemas de la empresa. Una vez que termina las pruebas realizan informes detallados sobre los problemas encontrados proporcionando acciones correctoras.
- Ejemplos: Qualysguard, Nessus, Languard...

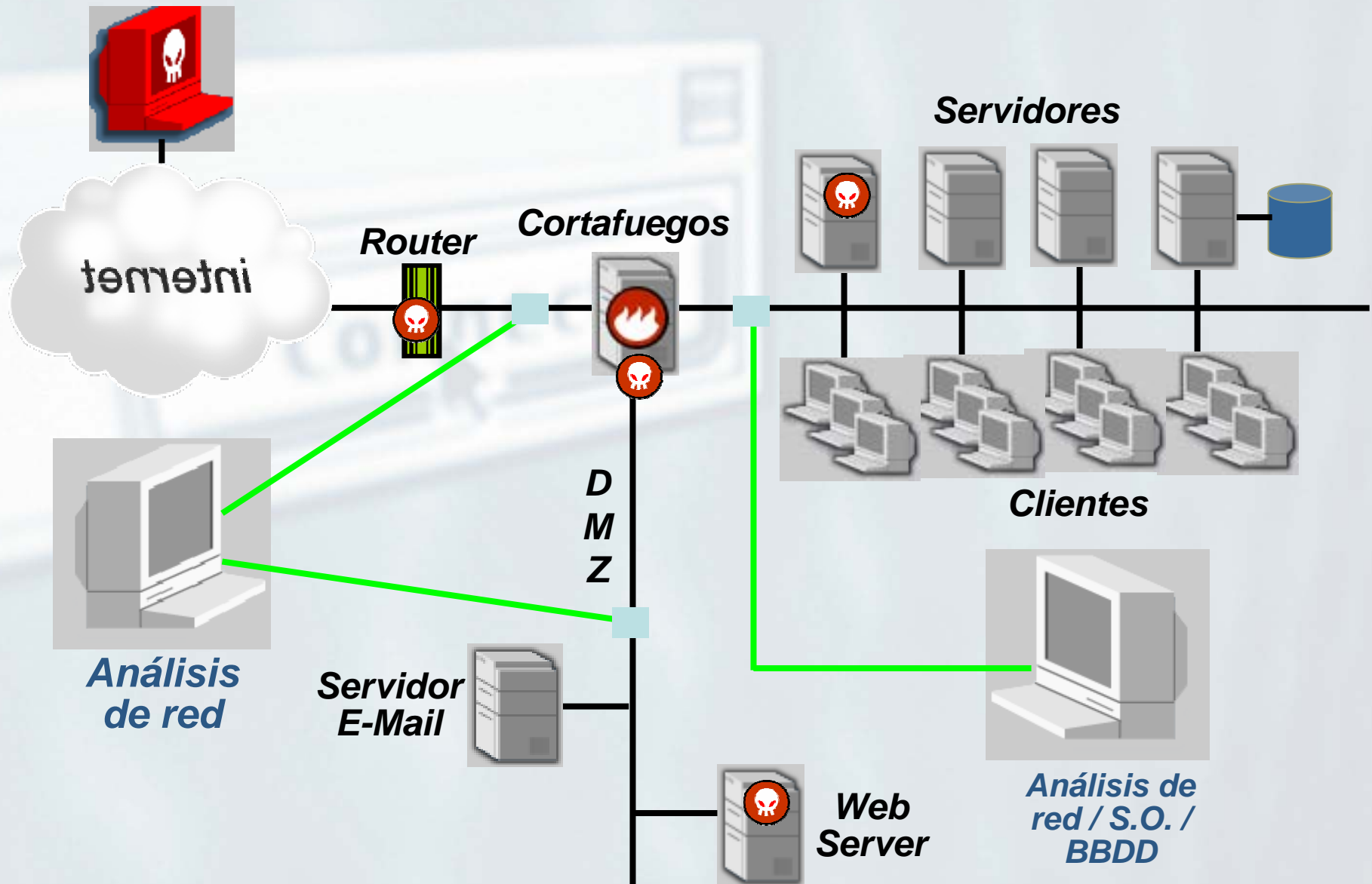
- Enfoque preventivo
- Se mantiene una base de datos de vulnerabilidades conocidas y se prueba su existencia en los sistemas
- Existen herramientas especializadas para:
  - Vulnerabilidades de Sistema Operativo
  - Vulnerabilidades de Bases de Datos
  - Vulnerabilidades de Servicios y elementos de red (cortafuegos, routers, switches, ...)
- Diversos tipos y formatos de informes (predefinidos y personalizados)
- Es imprescindible mantener actualizada la base de datos de vulnerabilidades de forma periódica



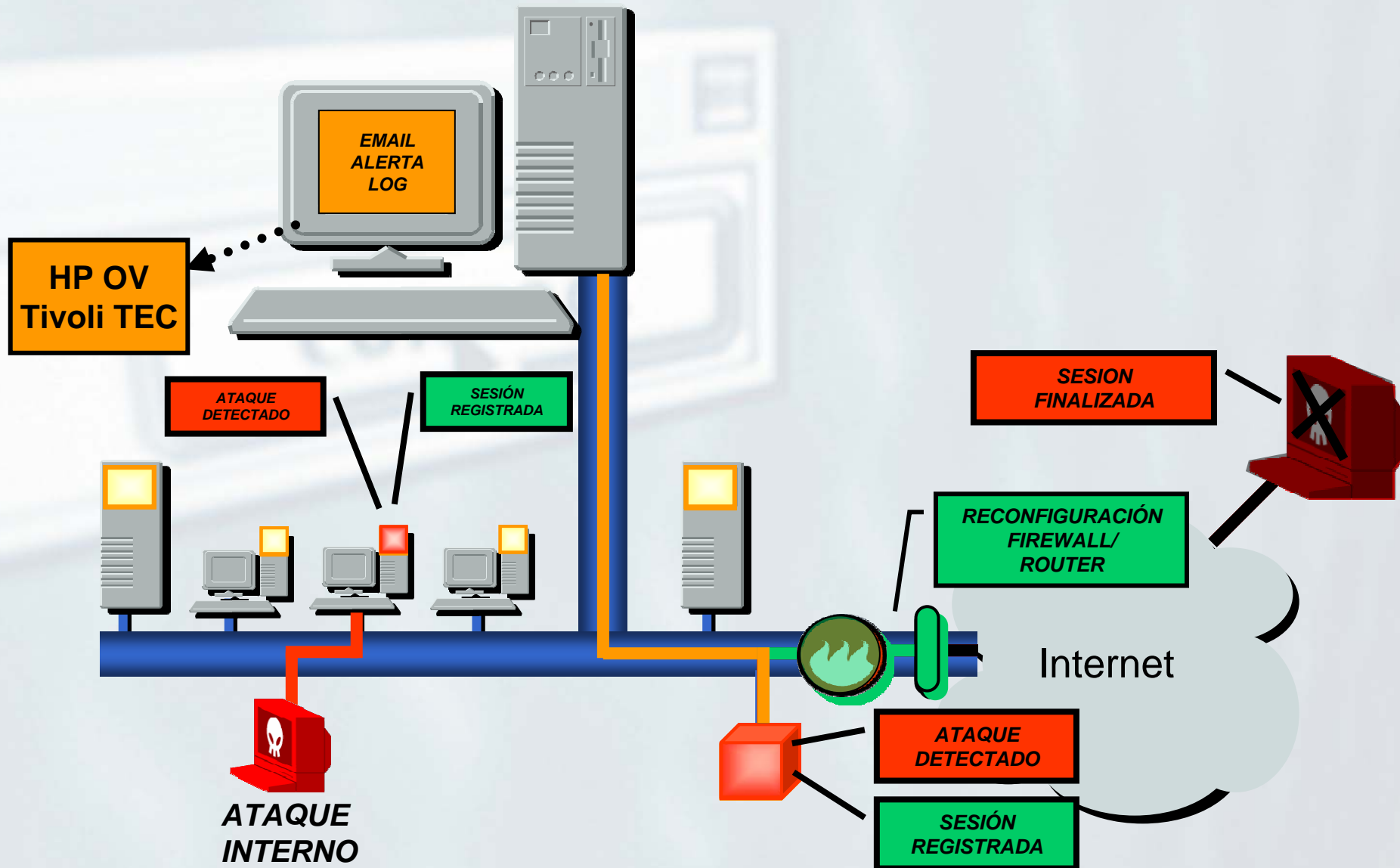


## **Categorías de vulnerabilidades analizadas:**

Backdoors	LDAP	O.S. Policy Issue
Browser	Network	O.S. Registry
Brute Force	Network Sniffers	O.S. Services
CGI-Bin	NFS	O.S. Users
Daemons	NIS	Protocol Spoofing
DCOM	O.S. Critical Issues	Router/Switch
DNS	O.S. Groups	RPC
E-mail	O.S. Networking	Share
Firewalls	O.S. Password	SNMP
FTP	O.S. Patches	Web Scan
Information Gathering		X Windows



- 1997
- Intrusion Detection Systems (IDS)
- Enfoque proactivo
- Se mantiene una base de datos de patrones de ataques conocidos y se analiza la actividad existente en tiempo real
- Dos tipos de sistemas IDS:
  - NDS (Network detection system). El análisis se enfoca a tráfico y servicios de red.
  - HDS (Host Detection System). El análisis se centra en máquinas específicas.
- Su implantación conlleva labores de parametrización con el fin de no alertar de falsos positivos
- Es imprescindible mantener actualizada la base de datos de patrones de ataque forma periódica



# **Peligros y Modos de Ataque**

**¿Cuáles son los tipos de ataque más comunes?**



- ***Sniffing:*** consiste en escuchar los datos que atraviesan la red, sin interferir con la conexión a la que corresponden, principalmente para obtener *passwords*, y/o *información confidencial*. **Protección:** basta con emplear mecanismos de autenticación y encriptación, red conmutada
- ***Barrido de puertos:*** utilizado para la detección de servicios abiertos en máquina tanto TCP como UDP (por ejemplo un telnet que no esté en el puerto 23, ..). **Protección:** filtrado de puertos permitidos y gestión de logs y alarmas.
- ***Bug de fragmentación de paquetes IP:*** con longitudes ilegales (*más pequeñas o más grandes*) de fragmentos, con solape entre ellos o saturación con multitud de fragmentos pequeños (*ej. ping de la muerte*) **Protección:** actualmente en los routers se limita el tráfico ICMP, incluso se analiza la secuencia de fragmentación, o bien parchear el SSOO

- ***Explotar bugs del software:*** aprovechan errores del software, ya que a la mayor parte del software se le ha añadido la seguridad demasiado tarde, cuando ya no era posible rediseñarlo todo y con ello puede adquirir privilegios en la ejecución, por ejemplo *buffers overflow (BOF o desbordamiento de pila)*
- Además, muchos programas corren con demasiados privilegios. La cadena o secuencia de órdenes para explotar esta vulnerabilidad del software se conoce como *exploit*.
- **Ataque:** los hackers se hacen con una copia del software a explotar y lo someten a una batería de pruebas para detectar alguna debilidad que puedan aprovechar. **Protección:** correcta programación o incluir parches actualizando los servicios instalados.

- ***Caballo de Troya:*** un programa que se enmascara como algo que no es, normalmente con el propósito de conseguir acceso a una cuenta o ejecutar comandos con los privilegios de otro usuario. **Ataque:** el atacante por ejemplo sabotea algún paquete de instalación o saboteando una máquina, modifica las aplicaciones, p.ej “ls”, “ps”, .. **Protección:** revisión periódica de *compendios*, firma digital, comprobación del sistema de ficheros (ejemplo aplicación “*tripware*”), etc
- ***Ataques dirigidos por datos:*** son ataques que tienen lugar en modo diferido, sin la participación activa por parte del atacante en el momento en el que se producen. El atacante se limita a hacer llegar a la víctima una serie de datos que al ser interpretados (en ocasiones sirve la visualización previa típica de MS. Windows) ejecutarán el ataque propiamente dicho, como por ejemplo un virus a través del correo electrónico o código JavaScript maligno. **Protección:** firma digital e información al usuario (lecturas off-line, o en otro servidor o instalar antivirus en el servidor de correo)

- **Denegación de servicio:** estos ataques no buscan ninguna información si no a impedir que sus usuarios legítimos puedan usarlas. Ejemplos:
- **SYN Flooding**, realizando un número excesivo de conexiones a un puerto determinado, bloqueando dicho puerto. Un caso particular de este método es la generación masiva de conexiones a servidores http o ftp, a veces con dirección origen inexistente para que no pueda realizar un RST. **Protección:** en el servidor aumentar el límite de conexiones simultáneas, acelerar el proceso de desconexión tras inicio de sesión medio-abierta, limitar desde un cortafuegos el número de conexiones medio abiertas
- **mail bombing**, envío masivo de correos para saturar al servidor SMTP y su memoria. **Protección:** similar a SYN Flooding
- **pings** (o envío de paquetes UDP al puerto 7 de echo) a direcciones broadcast con dirección origen la máquina atacada. Estas técnicas son conocidas como Smurf (si pings), Fraggle (si UDP echo). **Protección:** parchear el SSOO para que no realice pings broadcasts y que limite el procesamiento de paquetes ICMP

- **Ingeniería social:** son ataques que aprovechan la buena voluntad de los usuarios de los sistemas atacados. Un ejemplo de ataque de este tipo es el phishing: se envía un correo con el remite "root" a un usuario con el mensaje "por favor, cambie su password a "informatica". El atacante entonces entra con ese password. A partir de ahí puede emplear otras técnicas de ataque. O incitando a ver determinadas páginas web, descargar fotos, ...**Protección:** educar a los usuarios acerca de qué tareas no deben realizar jamás, y qué información no deben suministrar a nadie, salvo al administrador en persona.
- **Acceso físico:** a los recursos del sistema y pudiendo entrar en consola, adquirir información escrita, etc **Protección:** políticas de seguridad, dejar servidores bajo llave y guardia de seguridad, tal como se vigila alguna cosa de valor.
- **Adivinación de passwords:** la mala elección de passwords por parte de los usuarios permiten que sean fáciles de adivinar (*o por fuerza bruta*) o bien que el propio sistema operativo tenga passwords por defecto. Ejemplo: muchos administradores utilizan de password "administrador"). **Protección:** políticas de seguridad



- ***Spoofing:*** intento del atacante por ganar el acceso a un sistema haciéndose pasar por otro, ejecutado en varios niveles, tanto a nivel MAC como a nivel IP:
- ***ARP Spoofing*** (que una IP suplantada tenga asociada la MAC del atacante). **Ataque:** el atacante falsifica paquetes ARP indicando gratuitamente su MAC con la IP de la máquina suplantada. Los hosts y los switches que escuchan estos mensajes cambiarán su tabla ARP apuntando al atacante
- ***IP Spoofing*** (suplanta la IP del atacante). **Ataque:** el atacante debe de estar en la misma LAN que el suplantado, y modifica su IP en combinación con ARP spoofing, o simplemente “sniffee” todo el tráfico en modo promiscuo.
- ***DNS Spoofing*** (el nombre del suplantado tenga la IP del atacante ), donde el intruso se hace pasar por un DNS. **Ataque:** el atacante puede entregar o bien información modificada al host, o bien engañar al DNS local para que registre información en su cache (poisoning). P.ej, puede hacer resolver [www.banesto.com](http://www.banesto.com) a una IP que será la del atacante, de forma que cuando un usuario de Banesto se conecta, lo hará con el atacante.
- **Protección ante Spoofing:** introducir autenticación y cifrado de las conexiones para ARP e IP Spoofing. Aunque la intrusión se realice en capa 2 ó 3 se puede detectar en capa 7. En el caso de ARP, configurar que el host o switch aprenda MAC's sólo de paquetes ARP unicast. Para DNS Spoofing, utilizar certificados para comprobar fidedignamente la identidad del servidor.





















- **Confianza transitiva:** en sistemas Unix existen los conceptos de *confianza entre hosts y entre usuarios (red de confianza)*, y por tanto pueden conectarse entre sí diferentes sistemas o usuarios sin necesidad de autenticación de forma “oficial”, utilizando sólo como identificativo la IP. **Ejemplo** en Linux las aplicaciones *r\** (*rsh*, *rlogin*, *rcp*,...), *Xwindow*, *RPC*, ... utilizan el fichero */etc/hosts.equiv* o el fichero en *\$HOME/.rhost*. **Ataque:** cualquier atacante que tome el control de una máquina o bien suplante la IP (*spoofing*), podrá conectarse a otra máquina gracias a la confianza entre hosts y/o entre usuarios sin necesidad de autenticación. **Protección:** encriptación del protocolo y exigir siempre autenticación, evitar redes de confianza.
- **Hijacking:** consiste en robar una conexión después de que el usuario (a suplantar) ha superado con éxito el proceso de identificación ante el sistema remoto. Para ello el intruso debe *sniffear* algún paquete de la conexión y averiguar las direcciones IP, los ISN y los puertos utilizados. Además para realizar dicho ataque, el atacante deberá utilizar la IP de la máquina suplantada. **Ataque:** en un momento determinado, el intruso se adelanta una respuesta en la conexión TCP (con los ISN correctos, lo cual lo obtiene por sniffing) y por tanto el que estaba conectado no cumple con los ISN debido a que el intruso mandó información válida y queda excluido de la conexión (su conexión TCP aparente se ha colgado), tomando el control el intruso. Otra acción adicional, sería inutilizar al suplantado con una ataque DoS. **Protección:** uso de encriptación o uso de una red conmutada.











- **Enrutamiento fuente:** los paquetes IP admiten opcionalmente el enrutamiento fuente, con el que la persona que inicia la conexión TCP puede especificar una ruta explícita hacia él. La máquina destino debe usar la inversa de esa ruta como ruta de retorno, tenga o no sentido, lo que significa que un atacante puede hacerse pasar (spoofing) por cualquier máquina en la que el destino confíe (obligando a que la ruta hacia la máquina real pase por la del atacante). **Protección:** dado que el enrutamiento fuente es raramente usado, la forma más fácil de defenderse contra esto es deshabilitar dicha opción en el router.
- **ICMP Redirect:** con la opción redirect, alguien puede alterar la ruta a un destino para que las conexiones en las que esté interesado pasen por el atacante, de forma que pueda intervenirlas. Los mensajes “redirect” deben obedecerlos sólo los hosts, no los routers, y sólo cuando estos provengan de un router de una red directamente conectada. **Protección:** filtrado de paquetes.
- **Modificación de los protocolos de routing:** RIP, BGP, ... de forma que redirige la información por otras rutas del atacante. Esta técnica es poco habitual y compleja. **Protección:** utilizar rutas estáticas o protocolos de routing con encriptación.

# Herramientas de Seguridad










**Enumeración de las herramientas más comunes**






- **Nmap**   
  - Herramienta de exploración de red "Open Source" .
  - Utiliza distintos paquetes IP para determinar qué hosts se encuentran disponibles en la red, qué servicios (aplicación y versión) ofrecen, qué sistemas operativos (y versiones) corren en las máquinas, qué tipo de filtros/firewalls usan, etc.
- **Nessus**  
  - Herramienta de evaluación de seguridad "Open Source" de mayor renombre.
  - Escáner de seguridad remoto para Linux, BSD, Solaris y otros Unix.
  - Permite generar reports en HTML, XML, LaTeX, y texto ASCII; también sugiere soluciones para los problemas de seguridad
- **Security Expressions** 
  - Permite Evaluar el grado de cumplimiento de determinadas políticas de seguridad (nist, nsa, etc) de uno o varios equipos










- **Ethereal**   
  - Analizador de protocolos de red para Unix y Windows, y es libre (free).
- **Snort**   
  - Sistema de detección de intrusiones de red de poca carga (para el sistema), capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP.
- **Netcat**   
  - Una utilidad simple y potente que lee y escribe datos a través de conexiones de red usando los protocolos TCP o UDP.
- **TCPDump / WinDump**   
  - El sniffer clásico para monitoreo de redes y adquisición de información.











- **Hping2**  
  - Ensambla y envía paquetes de ICMP/UDP/TCP hechos a medida y muestra las respuestas
  - Particularmente útil al tratar de utilizar funciones como las de traceroute/ping o analizar de otra manera, hosts detrás de un firewall que bloquean los intentos de las herramientas estándar.
- **Dsniff**   
  - Set de herramientas para la monitorización pasiva de redes, la interceptación de tráfico en red y la implementación de ataques en PKI débiles (monkey-in-the-middle).
- **GFI LANguard**  
  - Escanea redes y reporta información como el nivel de "service pack" de cada máquina, ausencia de parches, recursos compartidos, puertos abiertos, servicios/aplicaciones activos, datos del registro ("key registry entries"), passwords débiles, usuarios y grupos; etc.
- **Ettercap**   
  - Interceptor/sniffer para LANs con ethernet basado en terminales (terminal-based).











- **Whisker/Libwhisker y Nikto**   
  - Escáners de servidores HTTP con respecto a agujeros de seguridad conocidos, particularmente, la presencia de peligrosos scripts/programas que usen CGI.
- **John the Ripper**   
  - Poderoso, flexible y rápido cracker de hashes de passwords multi-plataforma
- **Sam Spade** 
  - Incluye herramientas como ping, nslookup, whois, dig, traceroute, finger, explorador de web crudo, transferencia de zona de DNS {"DNS zone transer"}, comprobación de "relay" de SMTP, búsqueda en sitios web, y más.
- **ISS Internet Scanner**  
  - Evaluación de vulnerabilidades a nivel de Aplicación.

- **Kismet** 
  - Sniffer para redes inalámbricas
- **MBSA, Dumpsec, Dumprec** 
  - Proporcionan información sobre el nivel de parches instalados, políticas de auditoría, políticas de cuentas, servicios habilitados, recursos compartidos...
- **SuperScan** 
  - Un escáner de puertos de TCP, pinger y hostname resolver basado en connect()
- **L0phtCrack4** 
  - Aplicación de recuperación y auditoría de passwords para Windows
- **Retina** 
  - Al igual que Nessus y ISS Internet Scanner, la función de Retina es escanear todos los hosts en una red y reportar cualquier vulnerabilidad encontrada.








- **traceroute/ping/telnet/whois/dig: Lo básico.**   
- **Saint**   
  - Saint es otra herramienta no-libre de evaluación de seguridad (al igual que [ISS Internet Scanner](#) o [Retina de eEye](#)).
- **Network Stumbler** 
  - Netstumbler es la más conocida herramienta para Windows utilizada para encontrar "access points" inalámbricos abiertos (802.11)
- **SARA**  
  - Herramienta de evaluación de vulnerabilidades derivada del escáner SATAN.







- **N-Stealth**  
  - Escáner de seguridad de servidores web no-libre.
- **AirSnort**   
  - Herramienta para WLAN que crackea las llaves de cifrado mediante monitorización pasiva de paquetes
- **NBTScan**   
  - Herramienta de scanning de redes IP que lista direcciones, nombre de NetBIOS, nombre de usuario con sesión iniciada en la máquina y dirección de MAC.
- **Firewalk**  
  - Herramienta para determinar mapas de redes y filtros de listas de control de acceso (ACL) empleadas por gateways.

- **Cain & Abel** 
  - Aplicación de recuperación de passwords para Windows
- **XProbe2**  
  - Herramienta que sirve para determinar el sistema operativo de un host remoto (OS Fingerprinting)
- **SolarWinds Toolsets**  
  - Herramientas de descubrimiento/monitorización/ataque para redes
- **THC-Amap**  
  - Escáner de identificación de aplicaciones ("application fingerprinting").
- **Enum:** 
  - Proporciona mucha información de un equipo que permite conexiones nulas

- **NTop**   
  - Herramienta para monitorizar el uso de tráfico de red
- **Nemesis**  
  - Herramienta para la inyección de paquetes IP. Se complementa con hping2.
- **LSOF: LiSt Open Files**  
  - Lista información acerca de cualquier archivo abierto por procesos que estén ejecutándose en el sistema. También puede listar sockets de comunicaciones abiertos por cada proceso.
- **Hunt** 
  - “Packet sniffer” y “connection intrusion” para Linux



- **Achilles y Paros** 
  - Servidores proxy, que actúan como una persona-en-el-medio {man-in-the-middle} durante una sesión de HTTP.
- **Brutus** 
  - Un cracker de autenticación de fuerza bruta para redes. Soporta HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP, y más. El código fuente no está disponible.
- **Paketto Keiretsu**  
  - Set de herramientas que utilizan nuevas e inusuales estrategias para manipular redes con TCP/IP
- **Fragroute**   
  - Permite retrasar, duplicar, descartar, fragmentar, reordenar, segmentar, especificar source-routing y otras operaciones en los paquetes IP salientes destinados a un host en particular

- **SPIKE Proxy**   
  - Proxy de HTTP "open source" que sirve para encontrar fallos de seguridad en sitios web
- **THC-Hydra**   
  - Un cracker de autenticación de fuerza bruta para redes. Soporta HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP, y más. El código fuente no está disponible.
- **Herramientas Web:**
  - Permiten obtener mucha información acerca de una dirección web o dirección ip:
    - Domtools.com, Netcraft.com
    - Ripe.net, arin.com, Esnic.es
    - Visualroute.it, Google

- Hyena 
  - Herramienta de descubrimiento de redes muy versatil y completa
- Otras herramientas: pwdump3, IpTraf, LibNet, hfnetchk, dig, Crack/Cracklib, snoop, The Coroner's Toolkit...

# ¿Dónde buscar herramientas?

- [www.packetstormsecurity.org](http://www.packetstormsecurity.org)
  - [neworder.box.sk/](http://neworder.box.sk/)
- [www.securiteam.com/exploits](http://www.securiteam.com/exploits)
- [www.hoobie.net/security/exploits/](http://www.hoobie.net/security/exploits/)
- [www.insecure.org/sploits.html](http://www.insecure.org/sploits.html)
  - [www.astalavista.com/tools](http://www.astalavista.com/tools)
  - [www.securityfocus.com](http://www.securityfocus.com)
    - [www.cve.mitre.org](http://www.cve.mitre.org)
    - [www.somarsoft.com](http://www.somarsoft.com)

- [www.hackthissite.org](http://www.hackthissite.org)
- [www.hackerslab.org](http://www.hackerslab.org)
- [www.hdcwargame.com](http://www.hdcwargame.com)



# **Cómo realizar un test de intrusión**

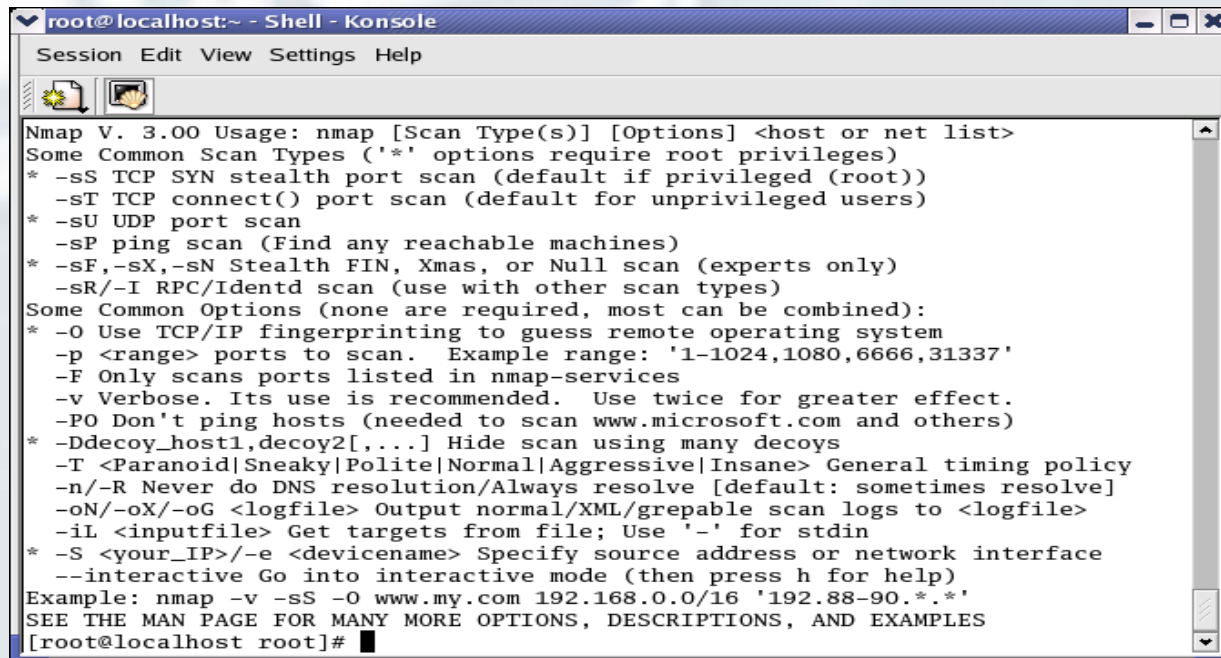
## **Pasos Básicos**



- Etapas de un test de intrusión:
  - Obtención de información pública
  - Escaneo de puertos / Enumeración de servicios
  - Detección de vulnerabilidades
  - Explotación controlada de vulnerabilidades

- **Obtención del rango de direcciones del objetivo:**
  - Los organismos oficiales de registro tienen esta información: ripe, arin, esnic.
  - También nos permite conocer los DNS
- **Intento de transferencia de zona:**
  - Permite conocer estructura interna del objetivo
  - Comando dig en linux.
  - Domtools.com
- **Información sobre sistemas y aplicaciones:**
  - Netcraft.com nos indica el sistema operativo y las aplicaciones que corren en una determinada IP.

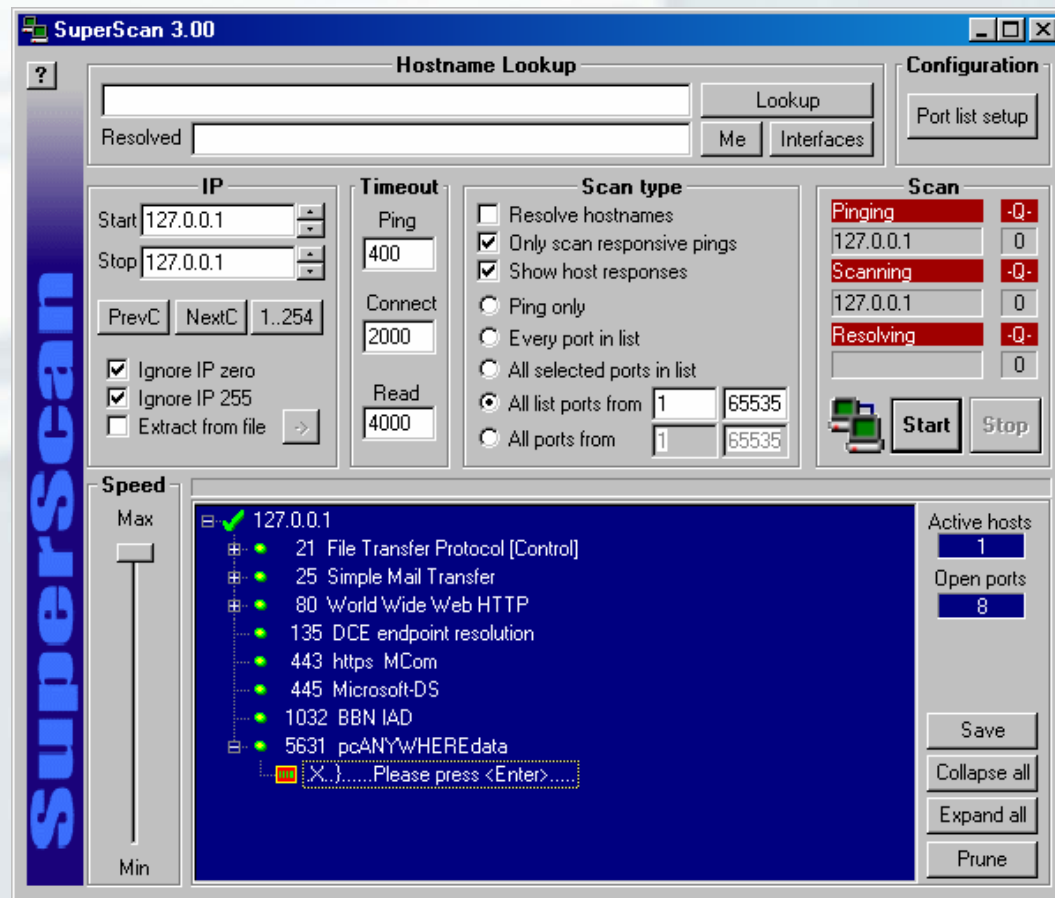
- **Nmap:** Permite conocer los servicios accesibles en los servidores objetivo, además de proporcionar información sobre el sistema operativo
  - `nmap -g 53 -T aggressive -n -O -sS -sV -sR -P0 -oN salida.nmap -iL ips_objetivo.txt`



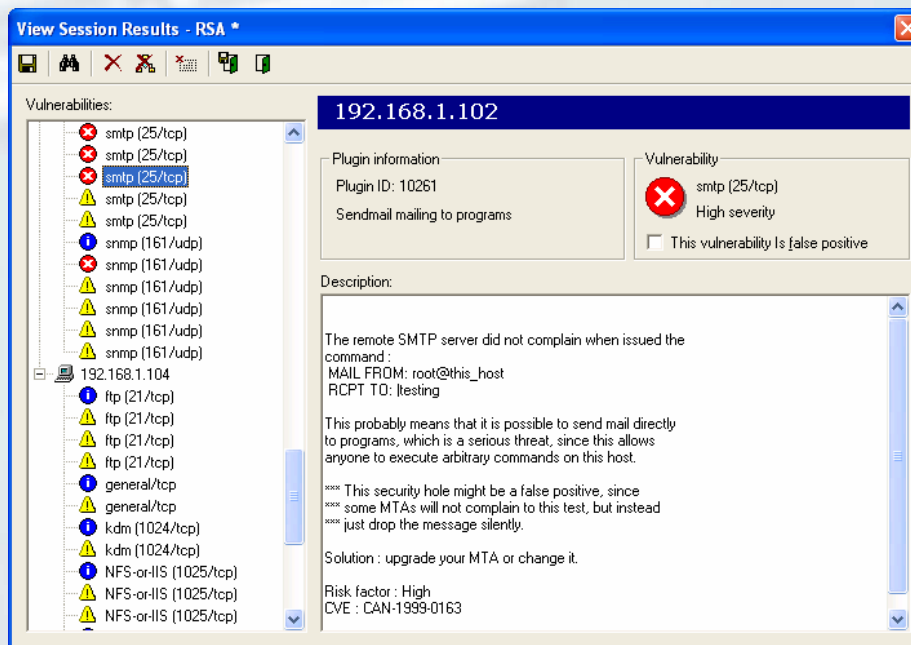
```
root@localhost:~ - Shell - Konsole
Session Edit View Settings Help

Nmap V. 3.00 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
[root@localhost root]#
```

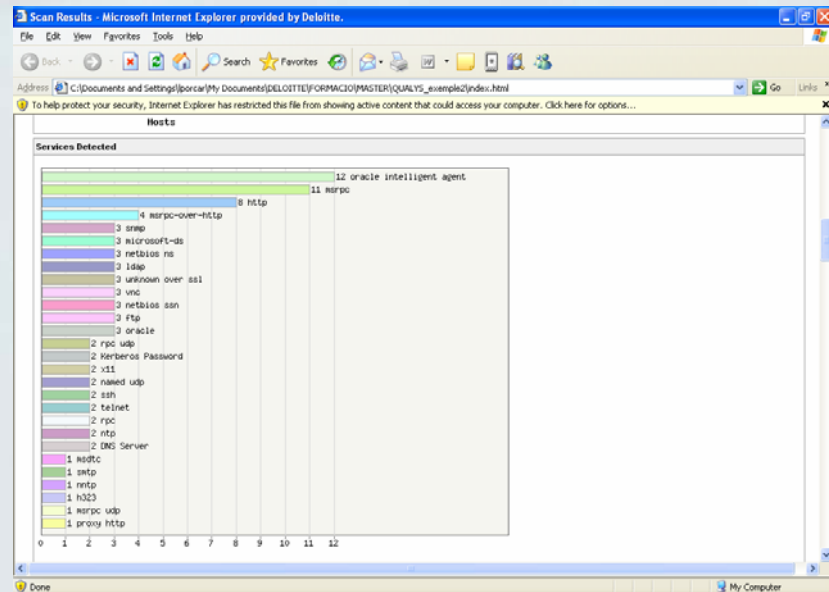
- **Superscan:** Parecido a nmap pero con GUI en Windows.



- **Nessus:** Una de las herramientas libres más potentes para la identificación de vulnerabilidades.
  - Añade información sobre el código de la vulnerabilidad (CVE), su código BID, e incluso la forma de explotarla
  - Buena presentación de resultados
  - A veces proporciona falsos positivos



- **Qualysguard:** Una de las herramientas de pago más potentes para la identificación de vulnerabilidades.
  - Base de vulnerabilidades completa y permanentemente actualizada
  - Añade información sobre criticidad, impacto de la vulnerabilidad, forma de explotarla y su solución
  - Óptima presentación de resultados: gráficas, informes personalizables...





- Con la información proporcionada por las herramientas intentar explotar las vulnerabilidades detectadas, además de realizar pruebas manuales que nos permitan encontrar debilidades adicionales.
- Para la búsqueda de exploits:
  - [www.securityfocus.com/bid/xxx/](http://www.securityfocus.com/bid/xxx/)
  - [www.packetstormsecurity.org](http://www.packetstormsecurity.org)
  - [neworder.box.sk/](http://neworder.box.sk/)
  - [www.securiteam.com/exploits](http://www.securiteam.com/exploits)
  - [www.hoobie.net/security/exploits/](http://www.hoobie.net/security/exploits/)
  - [www.insecure.org/sploits.html](http://www.insecure.org/sploits.html)
  - [www.astalavista.com/tools](http://www.astalavista.com/tools)
  - Google

# Deloitte.