T4. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

Apartados del BOE

- Herramientas del sistema operativo tipo Ping, Traceroute, etc
- Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc
- Herramientas de análisis de vulnerabilidades tipo Nessus
- Analizadores de protocolos tipo WireShark, Dsniff, Cain & Abel, etc
- Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy
- Ataques de diccionario y fuerza bruta tipo Brutus, Jhon the Ripper, etc

Herramientas de red de Windows

1. Ipconfig
2. Arp
3. Tracert
4. Route
5. Netstat
6. Nbtstat
7. Nslookup
8. Ping

- **ipconfig**
- IPConfig es una utilidad de línea de comandos que proporciona la configuración TCP-IP de un equipo.
- Cuando se utiliza con la opción /all, produce un informe detallado de la configuración de todas las interfaces de red presentes en el equipo, incluyendo los puertos serie configurados en el sistema (RAS).
- Las opciones /**release** [**adaptador**] y /**renew** [**adaptador**] liberan y renuevan respectivamente la dirección IP del adaptador especificado.
- Si no se especifica adaptador, el comando afectará a todas las direcciones de adaptadores enlazados a TCP/IP

- **ARP**
- El comando ARP resulta útil para visualizar la caché de resolución de direcciones.
- Muestra y modifica las tablas de traducción de direcciones IP a direcciones físicas usadas por el protocolo de resolución de direcciones ARP.
  - ARP -s dir_IP dir_eth [dir_if]
  - ARP -d dir_IP [dir_if]
  - ARP -a [dir_IP] [-N dir_if]Sus formatos de uso son:

- El comando presenta las siguientes opciones:
  - -a: Muestra las entradas actuales de ARP preguntando por los datos del protocolo. Si se especifica dir_IP, se muestran las direcciones IP y Física sólo para el equipo especificado. Cuando ARP se utiliza en más de una interfaz de red, entonces se muestran entradas para cada tabla ARP.
  - -g: Lo mismo que -a.
  - dir_IP: Especifica una dirección internet.
  - -N dir_if: Muestra las entradas de ARP para las interfaces de red especificadas por dir_if.
  - -d: Elimina el host especificado por dir_IP.
  - -s: Agrega el host y asocia la dirección internet dir_IP con la dirección física dir_eth. La dirección física se especifica con 6 bytes en hexadecimal separados por guiones. La entrada es permanente.
  - dir_eth: Especifica una dirección física.
  - dir_if: Si está presente, especifica la Dirección internet de la interfaz con la tabla de traducción de direcciones a modificar. Si no se especifica, se utiliza la primera interfaz aplicable.

- **Tracert**
- Tracert (trace route) es una utilidad que permite visualizar trazas. Utiliza el campo TTL del paquete IP en mensajes de petición de eco y de error (tiempo excedido)
- ICMP para determinar la ruta desde un host a otro a través de una red, para lo cual muestra una lista de las interfaces de routers por las que pasan dichos mensajes.
- Debe tenerse en cuenta que algunos routers eliminan de forma transparente paquetes con TTL expirado. Estos routers no aparecerán en la traza de Tracert.
- Su uso viene determinado por los siguientes formatos:
  - tracert [-d] [-h máximo_de_saltos] [-j lista_de_hosts]
  - tracert [-w tiempo_de_espera] nombre_de_destino

- Opciones:
  - -d: No convierte direcciones en nombres de hosts.
  - -h máximo_de_saltos: Máxima cantidad de saltos en la búsqueda del objetivo.
  - -j lista-de-host: Encaminamiento relajado de origen a lo largo de la lista de hosts.
  - -w tiempo_de_espera: Cantidad de milisegundos de espera por respuesta entre intentos.

- **Route**
- El comando Route se utiliza para visualizar y modificar la tabla de rutas.
- Route print muestra una lista con las rutas actuales conocidas por IP para el host.
- Route add se utiliza para añadir rutas a la tabla, y route delete se utiliza para borrar rutas de la tabla.
- Nótese que las rutas añadidas a la tabla no se harán persistentes a menos que se especifique el modificador –p, por lo que solo permanecerán en dicha tabla hasta el siguiente reinicio de la máquina.
- Para que dos hosts intercambien datagramas IP, ambos deberán tener una ruta al otro, o utilizar un gateway por omisión que conozca una ruta. Normalmente, los routers intercambian información entre ellos utilizando un protocolo como RIP (Routing Information Protocol) u OSPF (Open Shortest Path First).
- Puesto que NT no ha proporcionado tradicionalmente una implementación para estos protocolos, si se deseaba utilizar un equipo como router, debía configurarse manualmente su tabla de rutas.

- El comando route presenta los siguientes formatos:

  route [-f] [-p] [comando [destino]] [MASK máscara de red] [puerta de acceso] [METRIC métrica] [IF interfaz]

  - -f: Borra las tablas de enrutamiento de todas las entradas de la puerta de acceso. Si se usa éste junto con uno de los comandos, las tablas se borran antes de ejecutar el comando.
  - -p: Cuando se usa con el comando ADD, hace una ruta persistente en el inicio del sistema. De forma predeterminada, las rutas no se conservan cuando se reinicia el sistema. Cuando se usa con el comando PRINT, muestra la lista de rutas persistentes registradas. Se omite para todos los otros comandos, que siempre afectan las rutas persistentes apropiadas.
  - Comando: Puede ser uno de los siguientes:

- PRINT <destino>: Imprime una ruta
- ADD <destino> <máscara> <gateway> Metric <métrica> if <interfaz>: Agregar una ruta
- DELETE <destino>: Elimina una ruta
- CHANGE <destino> <máscara> <gateway> Metric <métrica> if <interfaz>: Modifica una ruta existente
- MASK <máscara>: Especifica que el siguiente parámetro es el valor "máscara de red".
- METRIC <métrica>: Especifica la métrica, es decir, el costo para el destino.
- if <interfaz>: Especifica la dirección IP de la interfaz sobre la que es accesible el destino.
- máscara de red: Especifica un valor de máscara de subred para esta entrada de ruta. Si no se especifica, el valor predeterminado es 255.255.255.255.
- destino: Especifica el host.
- puerta de acceso: Especifica la puerta de acceso.
- Interfaz: El número de interfaz para la ruta especificada.

- Todos los nombres simbólicos usados para el destino se buscan en el archivo de la base de datos de la red NETWORKS. Los nombres simbólicos para la puerta de acceso se buscan en el archivo de la base de datos de nombres de hosts HOSTS.
- Si el comando es **PRINT** o **DELETE**. El destino o la puerta de acceso pueden ser un comodín (el comodín se especifica como una estrella "*") o bien se puede omitir el argumento de la puerta de acceso.
- Si **Dest** contiene un carácter * o ?, se le considera como un modelo de núcleo y sólo se imprimen las rutas de destino coincidentes. El carácter "*" coincide con cualquier cadena y "?" coincide con cualquier carácter. Ejemplos: 157.*.1, 157.*, 127.*, *224*.
- Si no se da **IF**, intenta buscar la mejor interfaz para una puerta de acceso determinada.

- **netsat**
- Netstat muestra estadísticas relativas al protocolo y las conexiones TCP/IP en curso. **Netstat –a** muestra todas las conexiones, y **netstat –r** muestra la tabla de rutas, además de las conexiones que se encuentren activas.
- El modificador **–n** indica a netstat que no convierta direcciones y números de puertos a nombres.
- La sintaxis del comando tiene el siguiente formato:

  netstat [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalo]

- A continuación se describen las diferentes opciones con que se puede invocar este comando:
  - **-a**: Mostrar todas las conexiones y puertos escucha. (Normalmente, el extremo servidor de las conexiones no se muestra).
  - **-e**: Mostrar estadísticas Ethernet. Se puede combinar con la opción -s.
  - **-n**: Mostrar números de puertos y direcciones en formato numérico.
  - **-p proto**: Mostrar conexiones del protocolo especificado por proto; que puede ser **tcp** o **udp**. Si se usa con la opción **-s** para mostrar estadísticas por protocolo, **proto** puede ser **tcp**, **udp** o **ip**.
  - **-r**: Mostrar el contenido de la tabla de rutas.
  - **-s**: Mostrar estadísticas por protocolo. En forma predeterminada, se muestran para TCP, UDP e IP; se puede utilizar la opción **–p** para especificar un subconjunto de lo predeterminado.
  - - **Intervalo**: Vuelve a mostrar las estadísticas seleccionadas, haciendo pausas en un intervalo de segundos entre cada muestra. Pulse CTRL+C para detener el refresco de estadísticas. Si se omite, netstat imprimirá la información de configuración actual una única vez.

- **nbtstat**
- Muestra estadísticas del protocolo y conexiones TCP/IP actuales utilizando NBT (NetBIOS sobre TCP/IP). NBTStat es una herramienta que resulta de utilidad para solucionar problemas con la resolución de nombres llevada a cabo por NetBIOS.
- **NBTStat –n** muestra los nombres que fueron registrados de forma local en el sistema por aplicaciones, tales como el servidor y el redirector. **NBTStat –c** muestra la caché de nombres NetBIOS, que contiene las traslaciones nombredirección para otras computadoras. **NBTStat –R** purga la caché de nombres y la carga de nuevo desde el fichero LMHOSTS. **NBTStat –a <nombre>** realiza un comando de estado del adaptador NetBIOS contra la computadora especificada por **nombre**.
- El comando de estado de adaptador devuelve la tabla de nombres NetBIOS para esa computadora además de la dirección MAC de la tarjeta adaptadora. **NBTStat –S** lista las sesiones NetBIOS en curso y sus estados, incluyendo estadísticas.

- A continuación se describe el formato de este comando:

  nbtstat [-a Nombre remoto] [-A dirección IP] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [intervalo]]

- El comando puede utilizarse con las siguientes opciones:
  - **-a**: (estado del adaptador) Lista la tabla de nombres de máquinas remotas dado su nombre.
  - **A**: (estado del adaptador) Lista la tabla de nombres de máquinas remotas dada su dirección IP.
  - **-c**: (caché) Muestra la caché global de nombres remotos incluyendo las direcciones IP
  - **-C**: (caché) Muestra la caché global de nombres remotos con direcciónes IP por dispositivo
  - **-n**: (nombres) Muestra nombres locales NetBIOS.
  - **-r**: (resueltos) Muestra los nombres resueltos por difusión y vía WINS
  - **-R**: (Recargar) Purga y vuelve a cargar la tabla caché de nombres remotos

- **(Cont)**
  - **-S**: (Sesiones) Muestra tablas de sesiones con las direcciones IP de destino
  - **-s**: (sesiones) Muestra las tablas de sesiones para convertir las direcciones IP de destino a nombres de host usando el archivo hosts.
  - **-RR**: (LiberarActualizar) Envía paquetes de liberación de nombres a WINS y luego inicia la actualización
  - **Nombre remoto**: Nombre de la máquina de host remota.
  - **Dirección IP**: Representación de la dirección IP con separación de punto decimal.
  - **Intervalo**: Vuelve a mostrar las estadísticas seleccionadas, indicando la pausa en segundos entre cada muestra. Presione Ctrl+C para interrumpir el ciclo de estadísticas.

- **Nslookup**
- Nslookup se añadió a Windows NT 4. y es una herramienta muy útil para resolver problemas con el Servicio de Nombres de Dominio (DNS), tales como la resolución del nombre de un equipo. Cuando se inicia nslookup, éste muestra el nombre de host y la dirección IP del servidor DNS que haya sido configurado en el sistema local, pasando a continuación a mostrar un prompt >. Tecleando **?**, se mostrarán las diferentes opciones que se encuentran disponibles para este comando.
- Par buscar la dirección IP de un host a través de DNS, teclee el nombre del host y pulse INTRO. Nslookup utilizará por omisión el servidor DNS configurado para la computadora en que está ejecutando, pero, si lo desea, el comando puede configurarse para que utilice cualquier otro servidor DNS a través del formato **nslookup server <nombre>**, en el que **nombre** es el nombre simbólico del servidor que se desee utilizar. Una de las principales características que presenta esta herramienta para resolución de problemas con el servicio de nombres es su modo de depuración, el cual puede ser invocado tecleando **nslookup set debug** o, para conseguir un mayor detalle, **nslookup set d2**.
- En modo depuración, nslookup detalla los pasos por los que va pasando en el procesamiento de sus comandos.

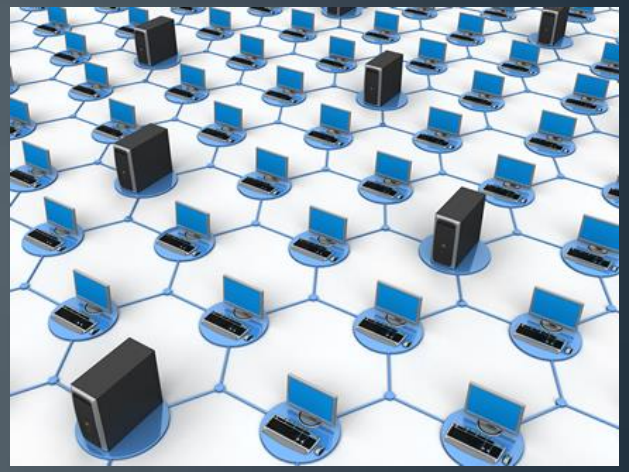
- A continuación se detallan las diferentes opciones y modos presentes en el comando nslookup, los identificadores se muestran en mayúsculas:
  - **NAME**: imprime información acerca del host o dominio NAME usando el servidor predeterminado
  - **NAME1 NAME2**: igual que el anterior, pero usa NAME2 como servidor
  - **ayuda** o **?**: imprime información acerca de comandos comunes disponibles
  - en nslookup
  - **set OPTION**: establecer una opción
  - **all**: imprime opciones, servidor y host actuales
  - **[no]debug**: imprime información de depuración. Precedido de **no** deja de
  - imprimir dicha información
  - **[no]d2**: imprime información de depuración muy detallada. Precedido de **no**
  - deja de imprimir dicha información
  - **[no]defname**: anexa el nombre del dominio a cada consulta
  - **[no]recurse**: pide una respuesta recursiva a la consulta
  - **[no]search**: usa la lista de búsqueda del dominio
  - **[no]vc**: usa siempre un circuito virtual

- **(Cont)**
  - **domain=NAME**: establece el nombre del dominio predeterminado a NAME
  - **srchlist=N1[/N2/.../N6]** - establece el dominio a N1 y la lista de búsqueda a N1,N2, etc.
  - **root=NAME**: establece el servidor de raíz a NAME
  - **retry=X**: establece el número de reintentos a X
  - **timeout=X**: establece el intervalo de espera inicial a X segundos
  - **type=X**: establece el tipo de consulta (p.e. A, ANY, CNAME, MX, NS, PTR, SOA, SRV)
  - **querytype=X**: igual que type
  - **class=X**: establece la clase de consulta (p.e. IN (Internet), ANY)
  - **[no]msxfr**: usa la transferencia de zona rápida de MS
  - **ixfrver=X**: versión actual que se usa en la solicitud de transferencia IXFR
  - **server NAME**: establece el servidor predeterminado a NAME, usando el servidor predeterminado actual
  - **lserver NAME**: establece el servidor predeterminado a NAME, usando el servidor inicial
  - **finger [USER]**: fija el NAME opcional en el host predeterminado actual
  - **root**: establece el servidor predeterminado actual a la raíz

- (Cont)
  - **ls** [**opt**] **DOMAIN** [**> FILE**]: lista direcciones en DOMAIN (opcional: salida a FILE)
  - **-a**: lista nombres canónicos y alias
  - **-d**: lista todos los registros
  - **-t TYPE**lista registros del tipo dado (p.e. A, CNAME, MX, NS, PTR etc.)
  - **view FILE**:: clasifica un archivo de salida 'ls' y lo ve con pg
  - **exit**: sale del programa.

Herramientas de análisis de red, puertos y servicios y análisis de vulnerabilidades

- Scanning Pentesting
  1. Host Discovery
  2. Port scanning
  3. Banner Grabbing or OS Finger Printing
  4. Scan for vulnerabilities
  5. Draw Network Diagrams
  6. Prepare Proxies
  7. Document all Findings



- No hay que escanear estas redes…….

1. Host Discovery

- El primer paso en un test de penetración en una red es detectar los Hosts activos que hay en la red objetivo
- Puedes intentar detectar estos Host usando herramientas de exploración de redes, aunque es difícil detectar los host activos detrás de un firewall.
- Herramientas:
  - Nmap
  - Angry IP Scanner
  - Netscan

2. Port Scanning

- Realizar escaneo de puertos utilizando herramientas tales como:
  - Nmap
  - Netscan Tools Pro
  - PRTG Network Monitor
  - Net Tools
- Estas herramientas ayudarán a sondear los puertos abiertos de un servidor o un host en la red seleccionada
- Los puertos abiertos son puertas abiertas para los atacantes para instalar malware en un sistema

3. Banner Grabbing or OS Finger Printing

- Banner Grabbing se realiza para obtener información sobre el servidor, es decir, conocer qué infraestructura o sistema se encuentra detrás.
- Otro concepto que está muy ligado es el Finger Printing, que es el proceso de recopilación de información que permite identificar el sistema operativo (activo → nmap o Pasivo→ sniffing)
- Por lo que se puede determinar el Sistema Operativo que se ejecuta en el host de destino y su versión, y así explotar las vulnerabilidades relacionadas.
- Herramientas
  - Telnet
  - Netcraft
  - ID Serve
  - Netcat

4. Scan for vulnerabilities

- Escanear la red en busca de vulnerabilidades utilizando herramientas específicas tipo:
  - Nessus
  - GFI LANGuard
  - SAINT
  - Core Impact Profesional
  - Ratina CS
  - MBSA

5. Draw Network Diagrams

- Dibujar el diagrama de la red de la organización, ayudará a entender la conexión a nivel lógico y la ruta de acceso al host destino en la red.
- El diagrama de la red se puede dibujar utilizando herramientas como:
  - LAN surveyor
  - OpManager
  - LANState
  - FriendlyPinger
- Los diagramas de red proporcionan una valiosa información acerca de la red y su arquitectura

6. Prepare Proxies

- Preparar proxy's utilizando herramientas:
  - Proxifier
  - SocksChain
  - SSL Proxy
  - Proxy+
  - Gproxy
  - ProxyFinder
- Para ocultarse y no ser capturado (detectado)

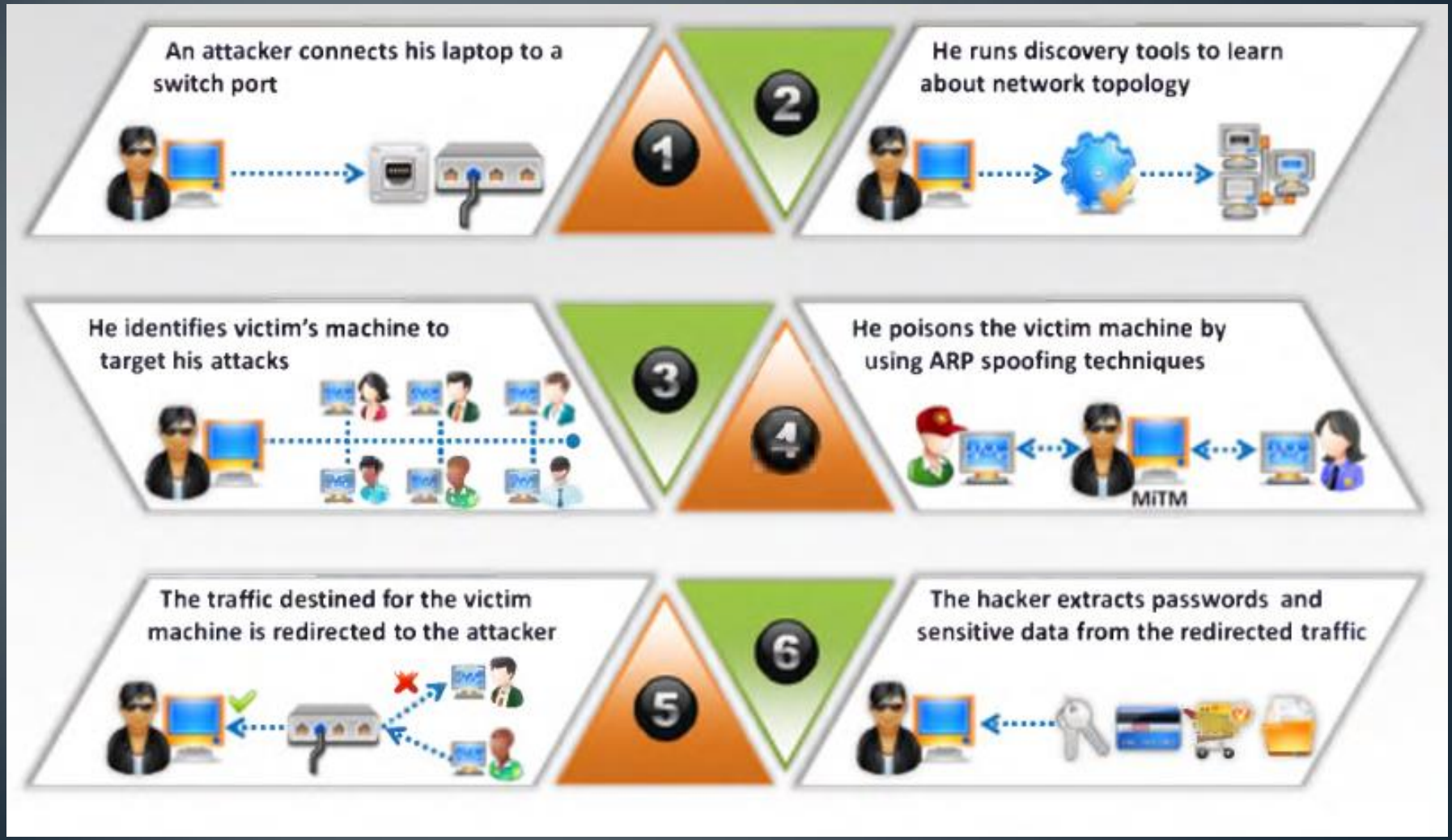
7. Document all Findings

- El último pero el paso más importante en las pruebas de pentesting es preservar todos los resultados de los pasos anteriores en un documento.
- Este documento ayudará a encontrar potenciales vulnerabilidades en la red.
- Una vez que determine las vulnerabilidades potenciales, se puede planificar los contraataques en consecuencia
- Por lo tanto, las pruebas de penetración ayuda en la evaluación de su red antes de introducirse en problemas reales que podrían provocar una pérdida server en términos de costes.

Analizadores de protocolos

- ¿Cómo se puede hackear una red usando Sniffers?
- Protocolos vulnerables al Sniffing
- Protocolos cifrados VS Sniffing
- Analizadores de protocolos HW
- Analizador de Protocolos: WHIRESARK
- Otras herramientas de Sniffing
- ¿Cómo detectar un Sniffer?

¿Cómo se puede hackear una red usando Sniffers?

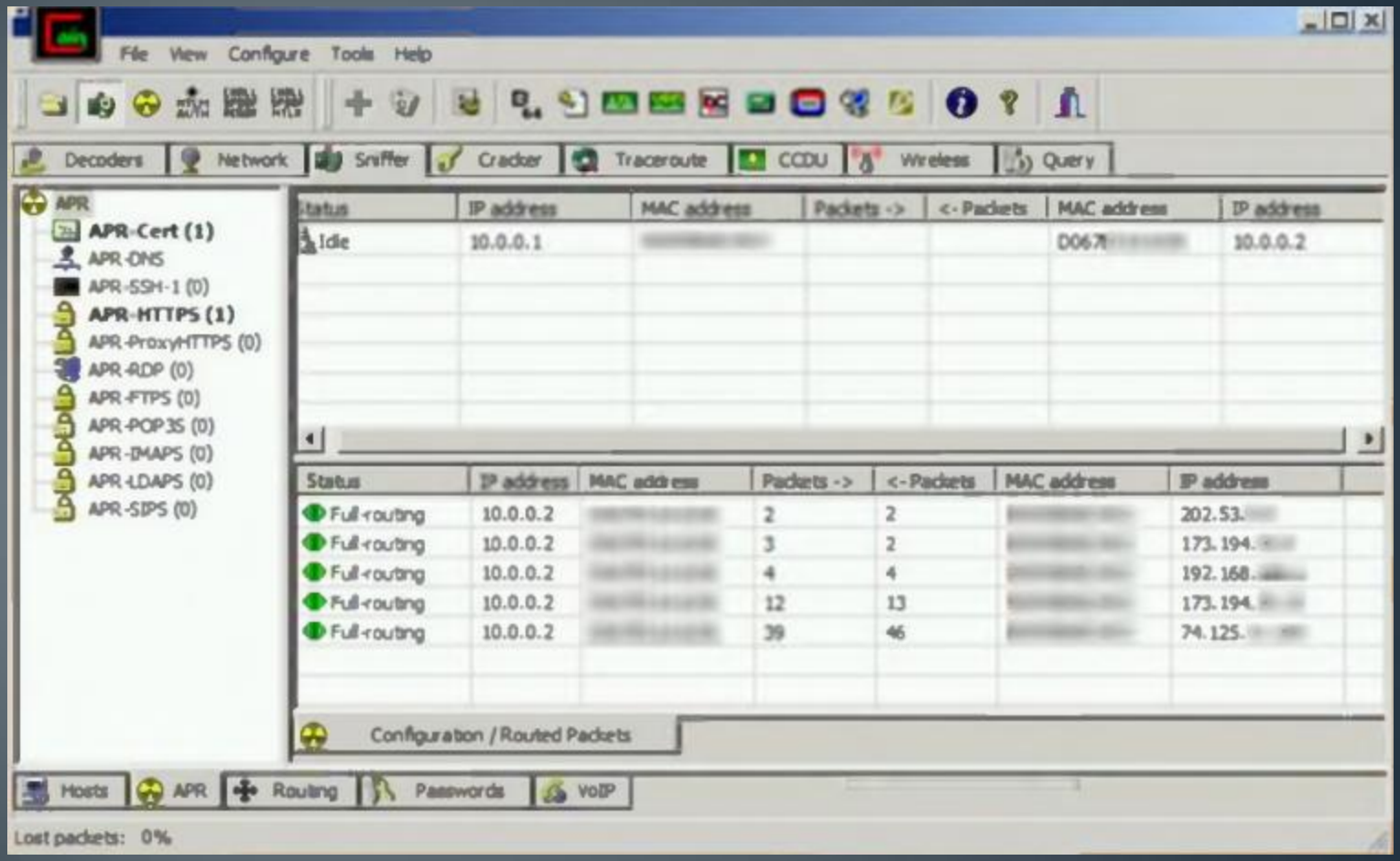


Protocolos vulnerables al Sniffing

- Protocolos que envían la información en texto plano:
  - TELNET
  - HTTP
  - SNMP
  - NNTP
  - POP
  - FTP
  - IMAP
- Estos protocolos se utilizan normalmente para conseguir contraseñas.
- Utilizando el Whiresark

Protocolos cifrados VS Sniffers

- La herramienta Cain & Abel es una herramienta par recuperar Password para Sistemas Operativos de Microsoft.
- Además contiene una función ARP Poison Routing que permite realizar un sniffing en LAN mediante un ataque MITM
- Puede analizar protocolos cifrados como
  - SSH o HTTPS


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert (1)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (1)
APR-ProxyHTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Idle 10.0.0.1 10.0.0.2
Status IP address MAC address Packets -> <- Packets MAC address IP address
Full-routing 10.0.0.2 2 2 202.53.
Full-routing 10.0.0.2 3 2 173.194.
Full-routing 10.0.0.2 4 4 192.168.
Full-routing 10.0.0.2 12 13 173.194.
Full-routing 10.0.0.2 39 46 74.125.
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%

Analizadores de protocolos HW

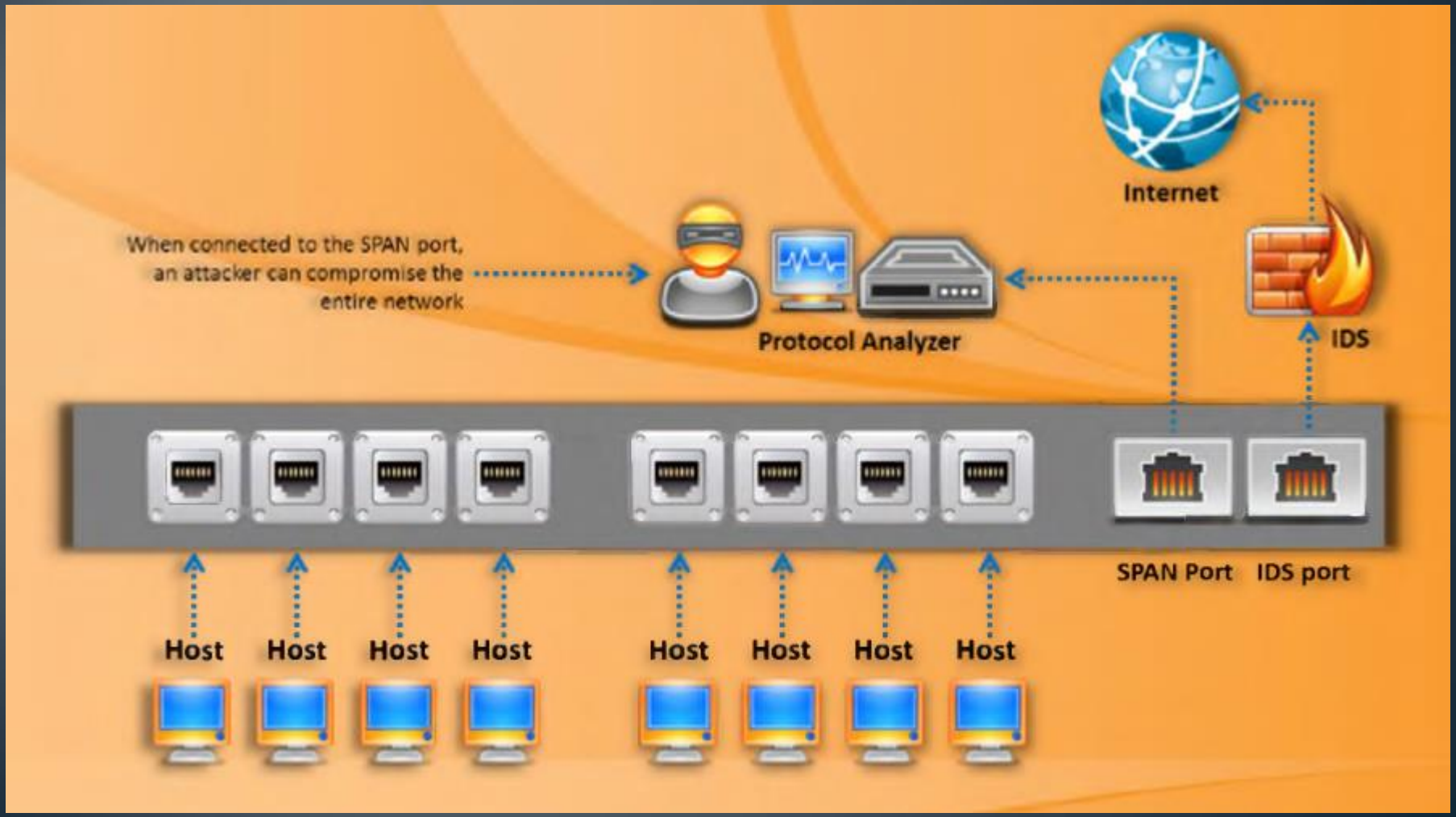
- Un analizador de protocolo de hardware es un dispositivo que interpreta el tráfico que pasa a través de una la red.
- Se utiliza principalmente para capturar las señales sin alterar el segmento de tráfico.
- Puede ser se utilizado para controlar el uso de la red e identificar tráfico malicioso que se podría haber generado por un software malicioso instalado en la red.
- Captura de un paquete de datos y decodifica y analiza su contenido de acuerdo a ciertas reglas predeterminadas.
- Analizadores de hardware son más caros y fuera de su alcance para que los distintos desarrolladores, aficionados, y hackers

- Agilent N2X N5540A
  - Es un sistema de test multipuerto que te permite verificar el rendimiento de redes multiservicio y dispositivos
- Agilent E2960B
  - Es una herramienta utilizada para testear y para pruebas. Incluye un analizador de protocolo que soporta de 1 hasta 16 enlaces, con una hoja de cálculo de estilo muy intuitivo

- RADCOM Prism UltraLite Protocol Analyzer
  - Permite supervisar y solucionar problemas de distintas tecnologías de red
  - Se compone por un Prismlite, que es un analizador de porotocolos de LAN/WAN/ATM y el Prism Ultralite, que es un analizador para WAN/FastLAN
  - Estos analizadores se utilizan para testear una amplia gama de protocolos, usando este anilizador se puede controlar TCP/IP de forma remota

- FLUKE Networks OptiView Network Analyzer
  - Permite monitorizar cada parte de HW y todos cada uno de las aplicaciones conectadas a la red.
  - Esta herramientas te permiten diagnosticar y resolver los problemas de rendimiento de aplicaciones de red así como proteger tu red de amenazas internas

- Span Port → Port Mirror (CISCO Switches)



Analizador de Protocolos: WHIRESARK

- Whiresark permite capturar y navegar por el tráfico que genera un ordenador en una red
- Usa Wincap para capturar los paquetes. Wincap soporta:
  - Ethernet
  - IEEE 802.11
  - PPP/HDLC
  - ATM
  - Bluetooth
  - USB
  - Token Ring
  - Frame Relay
  - FDDI
- FOLLOW TCP STREAM para rastrear passwords

- Filtros en Whireshark (http://wiki.whireshark.com)
  - Filtrar por protocolo: arp, http, tcp, udp, dns
  - Filtrar por dirección IP: ip.addr==10.0.0.1
  - Filtrar por múltiples direcciones IP: ip.addr==10.0.0.1 or ip.addr==10.0.0.1
  - Monitorizar puertos específicos: tcp.port==443
  - Múltiples filtros:
    - p.addr==192.168.1.100 machine ip.addr==192.168.1.100 && tcp.port=44
  - GET: http.request
  - Paquetes que tengan la palabra damiansu: tcp contains damiansu

Otras herramientas de Sniffing

- Cascade Pilot
- Windup
- Packet Sniffing tool Capsa Network Analyzer
- Network Packet Analyzer: OmniPeek Network Analyzer
- Network Packet Analyzer: Observer
- Network Packet Analyzer: Sniff-O-Matic
- Network Packet Analyzer: JitBit Network Sniffer
- Chat Message Sniffer: MSN Sniffer 2
- TCP/IP Packet Crafter: Colasoft Packet Builder

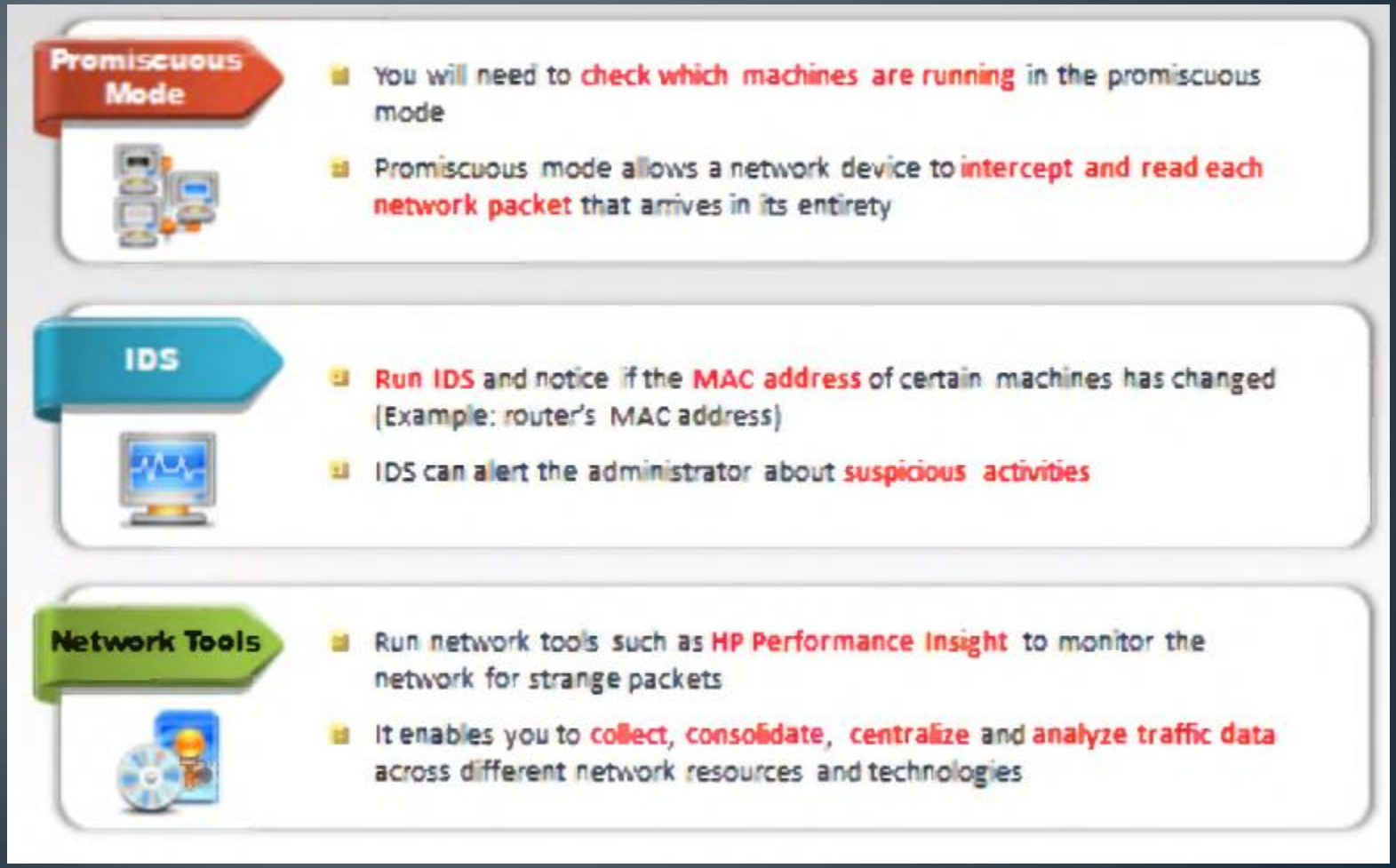
- Ace Password Sniffer available at http://www.effetech.com
- RSA NetWitness Investigator available at http://www.emc.com
- Big-Mother available at http://www.tupsoft.com
- EtherDetect Packet Sniffer available at http://www.etherdetect.com
- dsniff available at http://monkey.org
- EffeTech HTTP Sniffer available at http://www.effetech.com
- Ntop available at http://www.ntop.org
- Ettercap available at http://ettercap.sourceforge.net
- SmartSniff available at http://www.nirsoft.net
- EtherApe available at http://etherape.sourceforge.ne

- Network Probe available at http://www.objectplanet.com
- Snort available at http://www.snort.org
- Sniff'em available at http://www.sniff-em.com
- MaaTec Network Analyzer available at http://www.maatec.com
- Alchemy Network Monitor available at http://www.mishelpers.com
- CommView available at http://www.tamos.com
- NetResident available at http://www.tamos.com
- Kismet available at http://www.kismetwireless.net
- AIM Sniffer available at http://www.effetech.com
- Netstumbler available at http://www.netstumbler.com

- IE HTTP Analyzer available at http://www.ieinspector.com
- MiniStumbler available at http://www.netstumbler.com
- PacketMon available at http://www.analogx.com
- NADetector available at http://www.nsauditor.com
- Microsoft Network Monitor available at http://www.microsoft.com
- NetworkMiner available at http://www.netresec.com
- PRTG Network Monitor available at http://www.paessler.com
- Network Security Toolkit available at http://www.networksecuritytoolkit.org
- Ethereal available at http://www.ethereal.com
- KSniffer available at http://ksniffer.sourceforge.n

- IPgrab available at http://ipgrab.sourceforge.net
- WebSiteSniffer available at http://www.nirsoft.net
- ICQ Sniffer available at http://www.etherboss.com
- URL Helper available at http://www.urlhelper.com
- WebCookiesSniffer available at http://www.nirsoft.net
- York available at http://thesz.diecru.eu
- IP Traffic Spy available at http://www.networkdls.com
- SniffPass available at http://www.nirsoft.net
- Cocoa Packet Analyzer available at http://www.tastycocoabytes.com
- vxSniffer available at http://www.cambridgevx.co

¿Cómo detectar un Sniffer?



Auditoría de Servidores Web

¿Cuál es el servidor web que más se utiliza?

¿Sobre que sistema operativo funciona?

¿Qué tipo de tecnologías hay detrás de un servidor web?

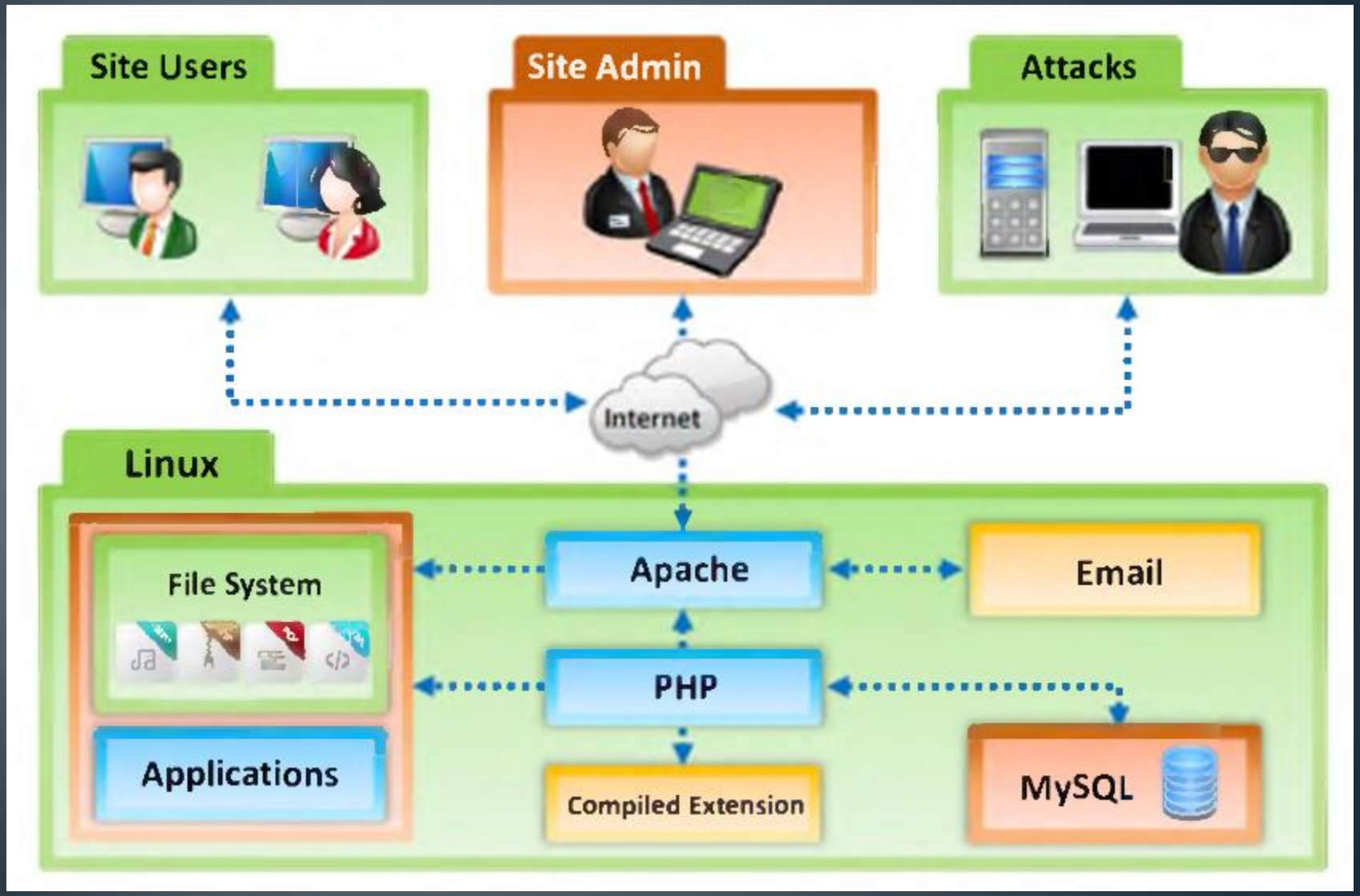
¿Qué tecnologías se ejecutan en el cliente?

¿Qué tecnologías se ejecutan en el servidor?

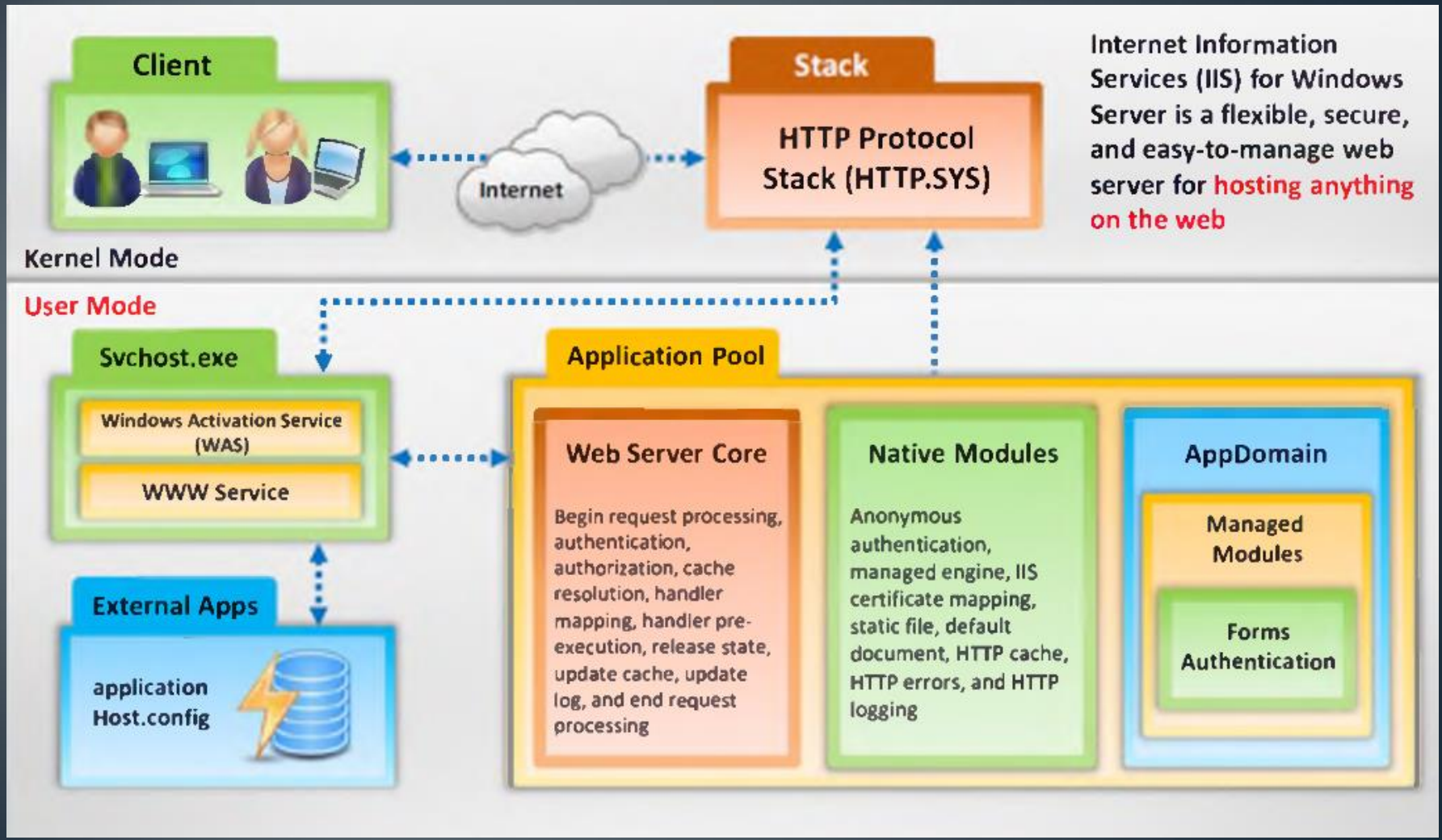
……

http://w3techs.com/

- Arquitectura de un servidor Web de Open Source



- Arquitectura del IIS, Servidor Web de Microsoft

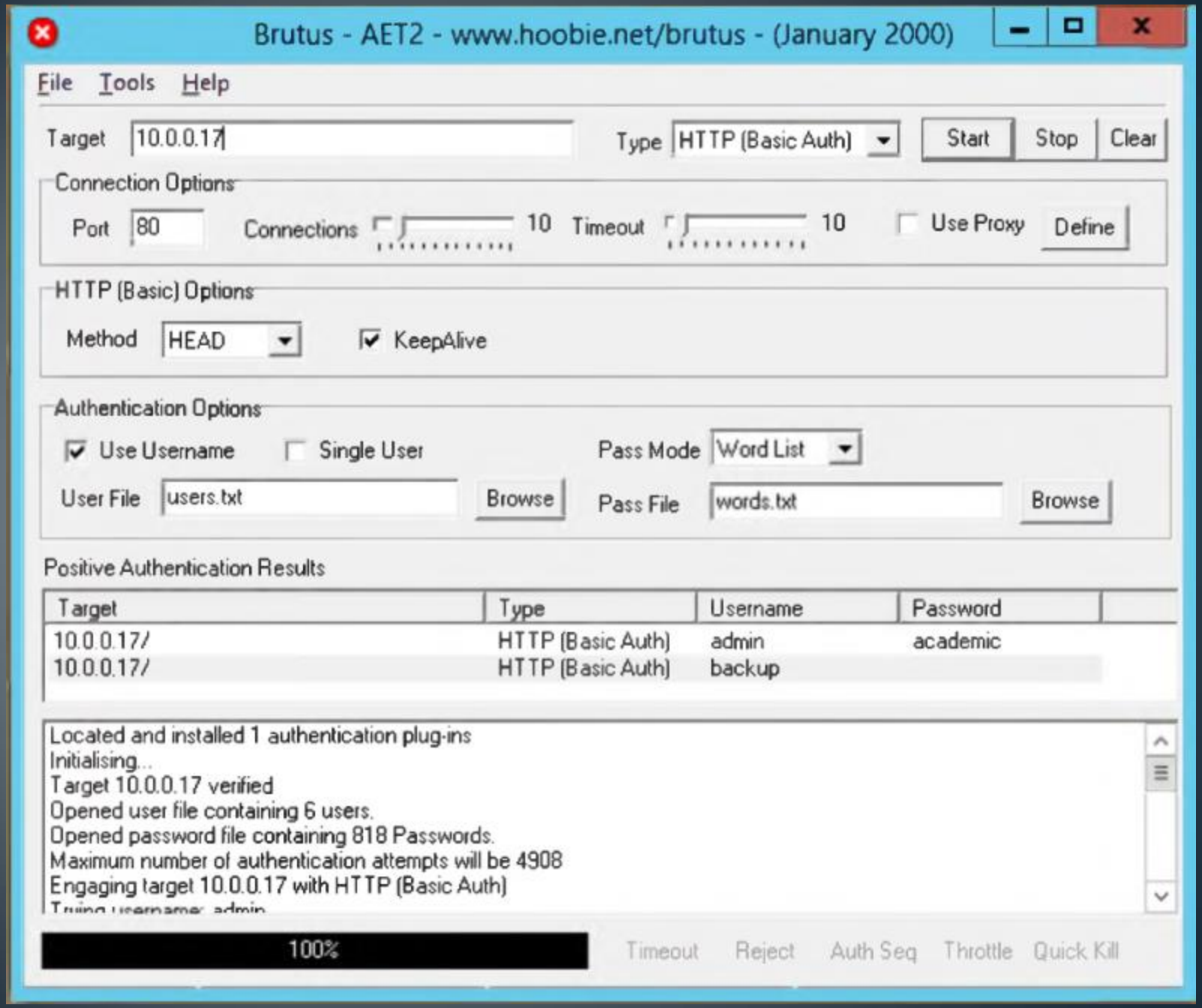


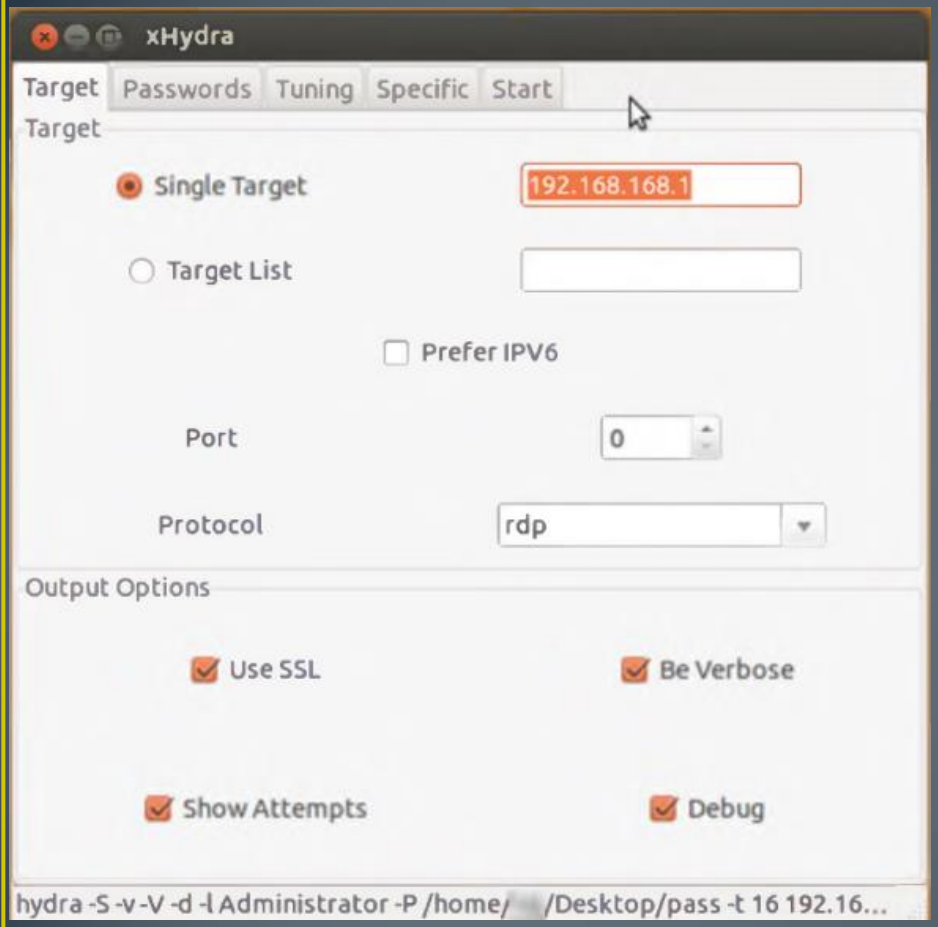
- Impactos de un ataque en un servidor Web
  - Se comprometen las cuentas de usuarios
  - Manipulación de datos
  - Website Defacement
  - Utilizar la web para posteriores ataques
  - Robo de datos
  - Acceso como root a las aplicaciones del servidor
- Ataques a un servidor Web:
  - Directory Transversal
  - Web cache Poisoning
  - HTTP Response Hijacking
  - HTTP Response Splitting
  - Ataque de fuerza bruta sobre SSH
  - Ataque MITM
  - Cracking de password

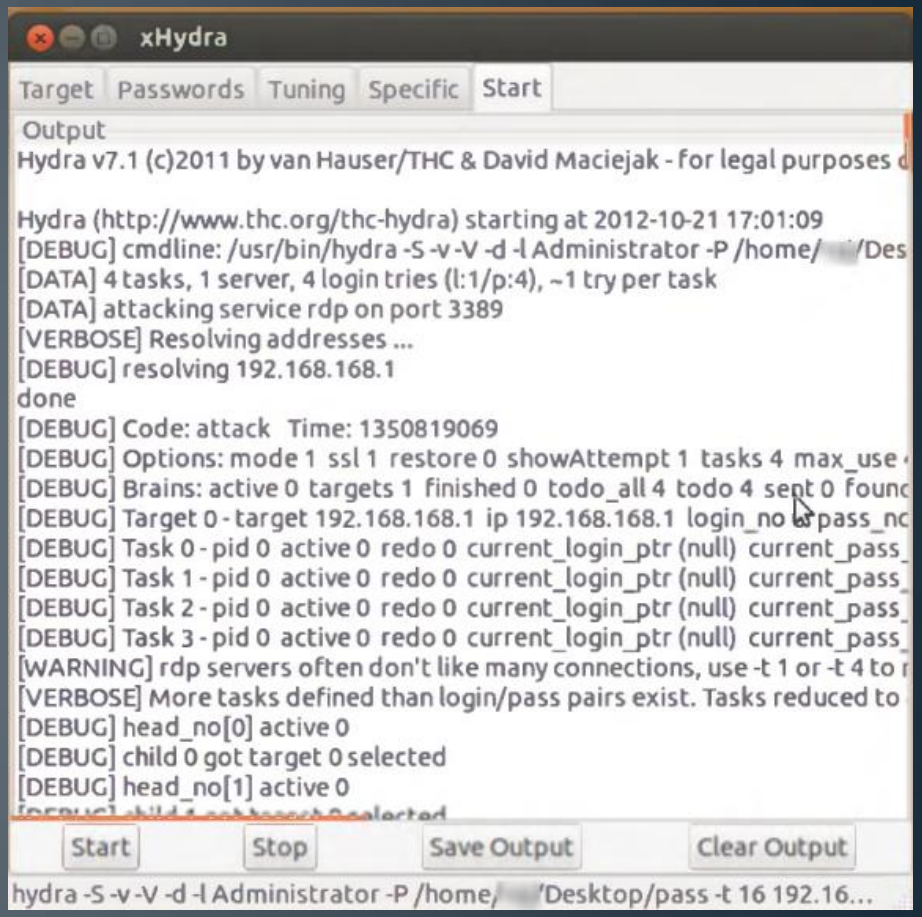
Metodología de ataque de un servidor web

Técnicas Cracking de Passwords de Servidores Web

1. **Adivinación**. Consiste en adivinar la contraseña que ha introducido el usuario: nombre de mascotas, nombres de seres queridos, fecha de nacimiento, QWERTY, password, 12345678… contraseñas que pueden recordar facilmente
2. **Ataque por diccionario**. Se utiliza un diccionario con password típicas o combinación de estas y con caracteres especiales. Tarda menos que la fuerza bruta
3. **Ataque por fuerza bruta**. Se prueban todas las combinaciones posibles A-Z 0-9 a-z. Se puede tardar meses o años en crackear una contraseña
4. **Ataque híbrido**. Se utiliza fuerza bruta con ataque por diccionario, es el mejor método. Así se crackean de forma más fácil las contraseñas


Brutus - AET2 - www.hoobie.net/brutus - (January 2000)
File Tools Help
Target 10.0.0.17
Type HTTP (Basic Auth)
Start Stop Clear
Connection Options
Port 80
Connections 10
Timeout 10
Use Proxy Define
HTTP (Basic) Options
Method HEAD
KeepAlive
Authentication Options
Use Username
Single User
Pass Mode Word List
User File users.txt
Browse
Pass File words.txt
Browse
Positive Authentication Results
Target Type Username Password
10.0.0.17/ HTTP (Basic Auth) admin academic
10.0.0.17/ HTTP (Basic Auth) backup
Located and installed 1 authentication plug-ins
Initialising...
Target 10.0.0.17 verified
Opened user file containing 6 users.
Opened password file containing 818 Passwords.
Maximum number of authentication attempts will be 4908
Engaging target 10.0.0.17 with HTTP (Basic Auth)
100%
Timeout Reject Auth Seq Throttle Quick Kill

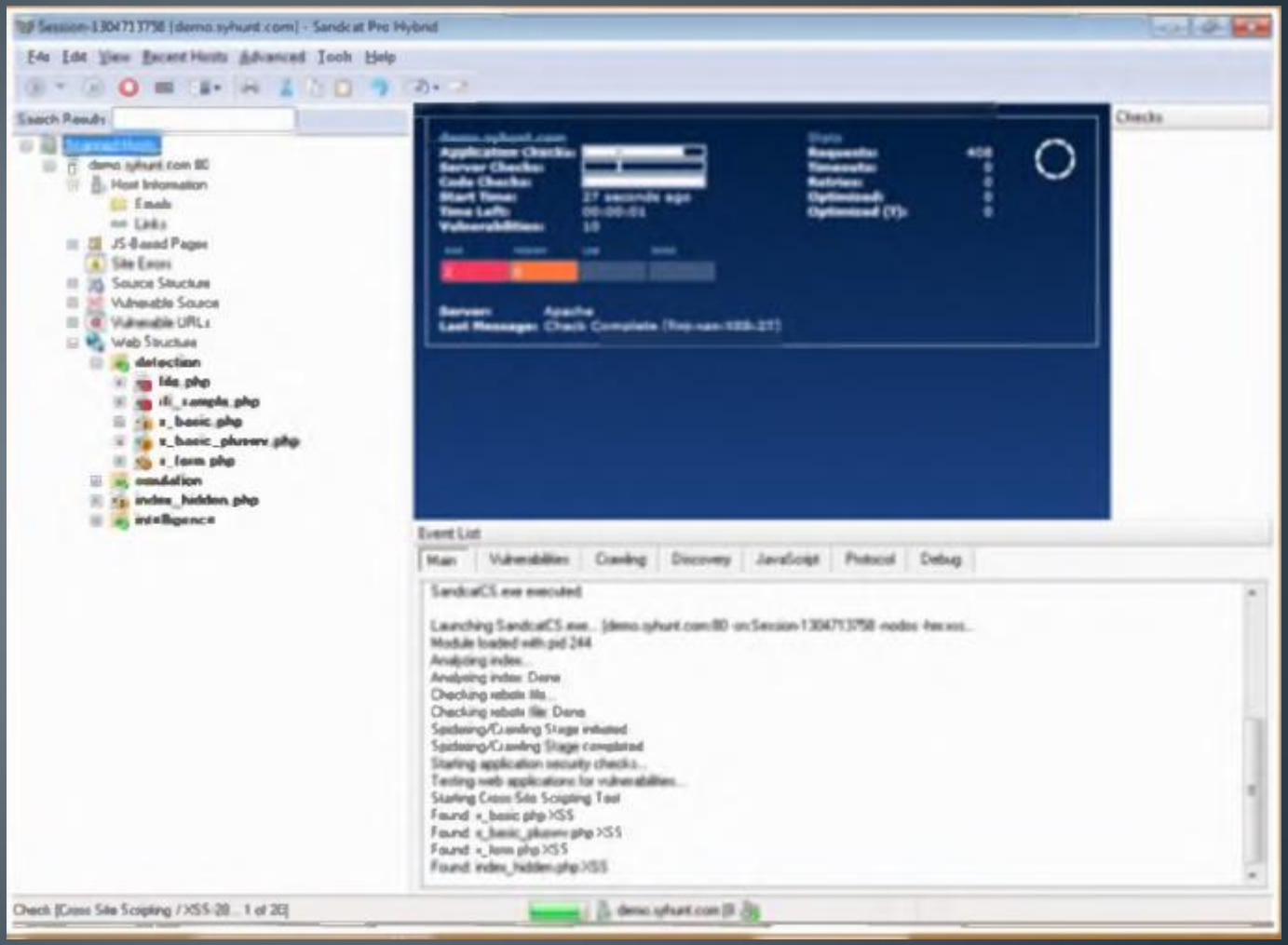

xHydra
Target
Passwords
Tuning
Specific
Start
Target
Single Target
192.168.168.1
Target List
Prefer IPV6
Port
0
Protocol
rdp
Output Options
Use SSL
Be Verbose
Show Attempts
Debug
hydra -S -v -V -d -l Administrator -P /home/ /Desktop/pass -t 16 192.16...

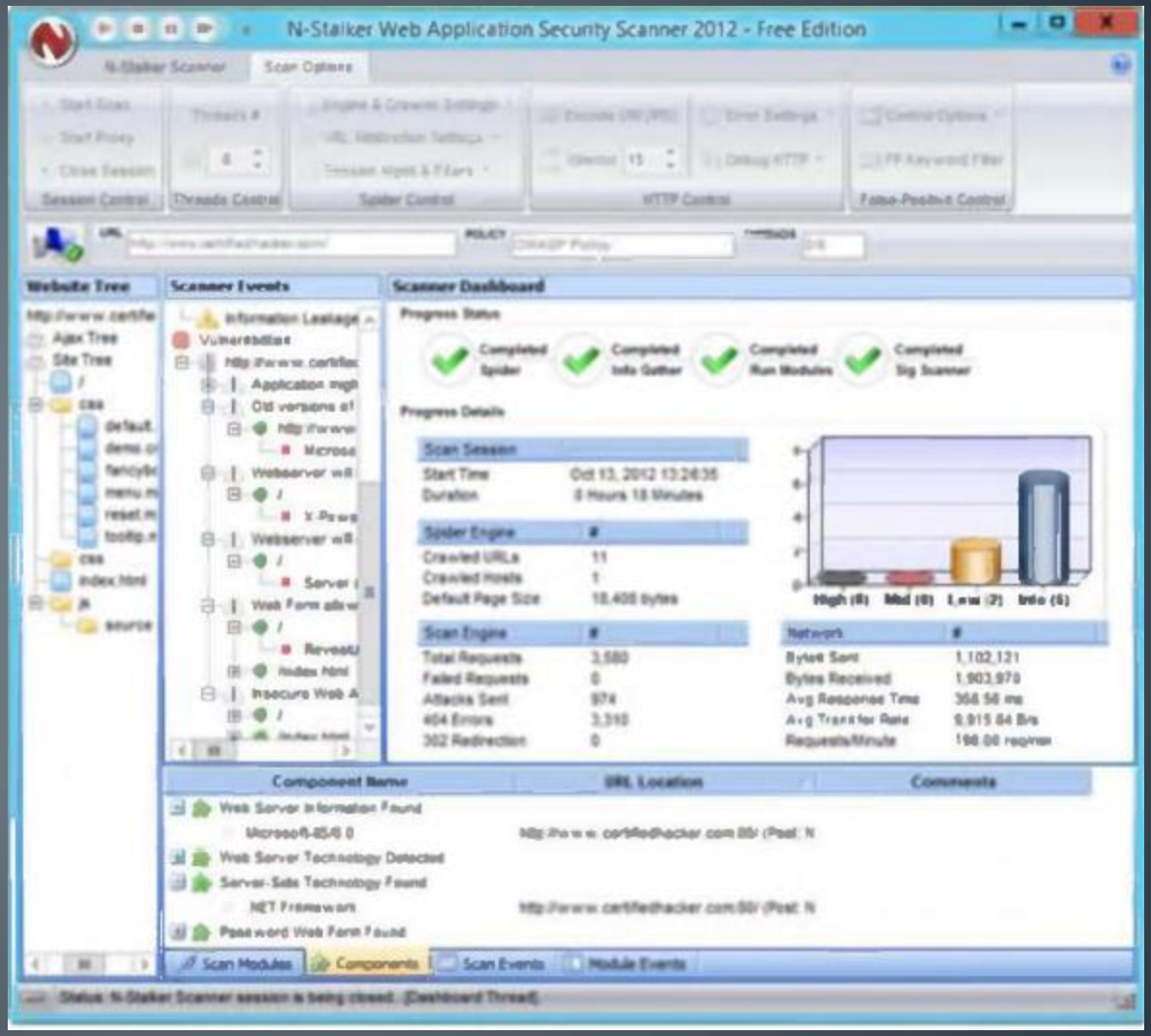

xHydra
Target
Passwords
Tuning
Specific
Start
Output
Hydra v7.1 (c)2011 by van Hauser/THC & David Maciejak - for legal purposes
Hydra (http://www.thc.org/thc-hydra) starting at 2012-10-21 17:01:09
[DEBUG] cmdline: /usr/bin/hydra -S -v -V -d -l Administrator -P /home/ /Des
[DATA] 4 tasks, 1 server, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking service rdp on port 3389
[VERBOSE] Resolving addresses ...
[DEBUG] resolving 192.168.168.1
done
[DEBUG] Code: attack Time: 1350819069
[DEBUG] Options: mode 1 ssl 1 restore 0 showAttempt 1 tasks 4 max_use
[DEBUG] Brains: active 0 targets 1 finished 0 todo_all 4 todo 4 sent 0 found
[DEBUG] Target 0 - target 192.168.168.1 ip 192.168.168.1 login_no
[DEBUG] Task 0 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass
[DEBUG] Task 1 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass
[DEBUG] Task 2 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass
[DEBUG] Task 3 - pid 0 active 0 redo 0 current_login_ptr (null) current_pass
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to
[VERBOSE] More tasks defined than login/pass pairs exist. Tasks reduced to
[DEBUG] head_no[0] active 0
[DEBUG] child 0 got target 0 selected
[DEBUG] head_no[1] active 0
Start
Stop
Save Output
Clear Output
hydra -S -v -V -d -l Administrator -P /home/ 'Desktop/pass -t 16 192.16...

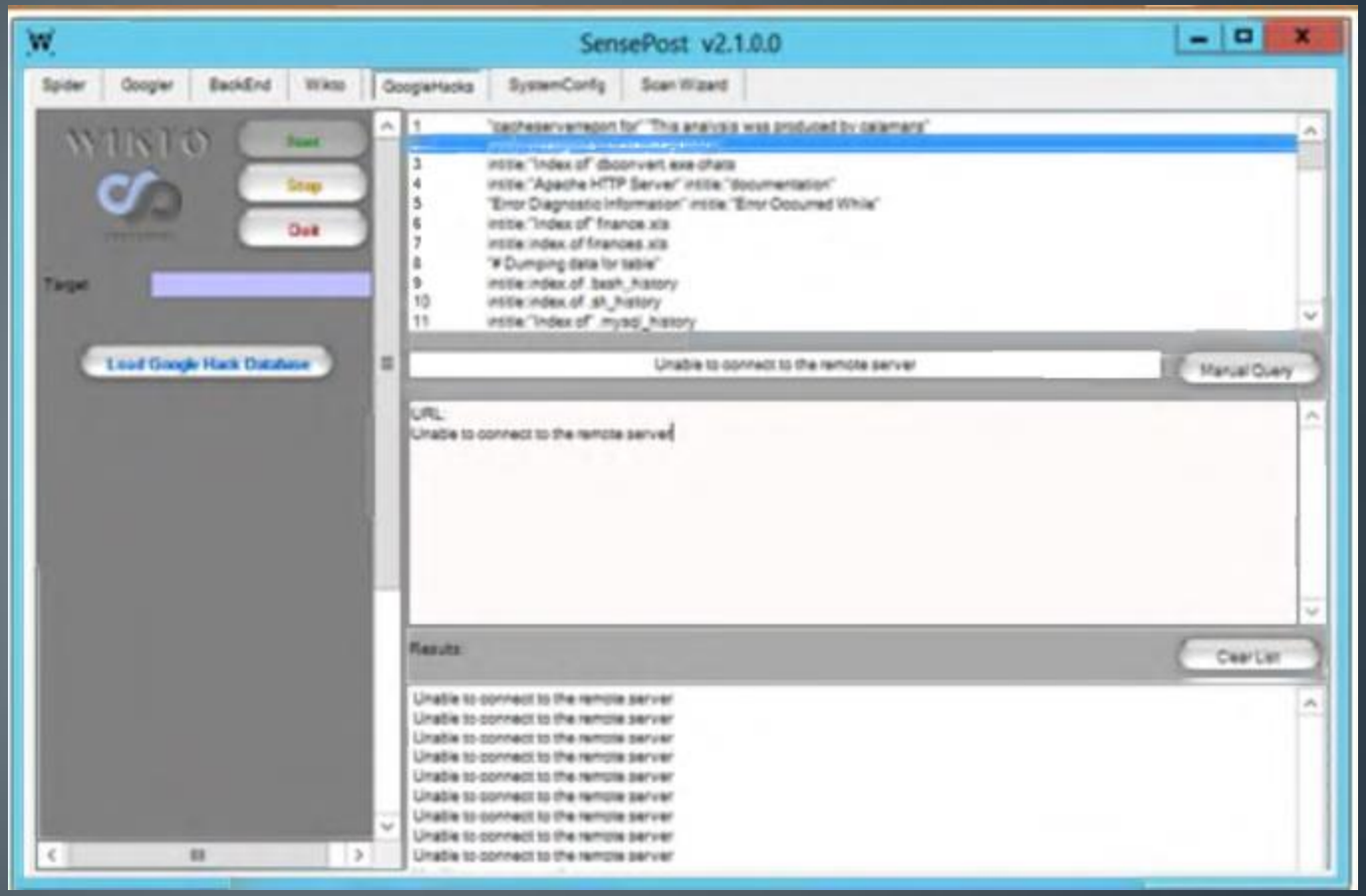

Internet Password Recovery Toolbox
File
Help
Google Chrome Passwords
Site address
Login
Password
http://users.techtarget.com/
@yahoo.com
<evaluation copy>
Ready

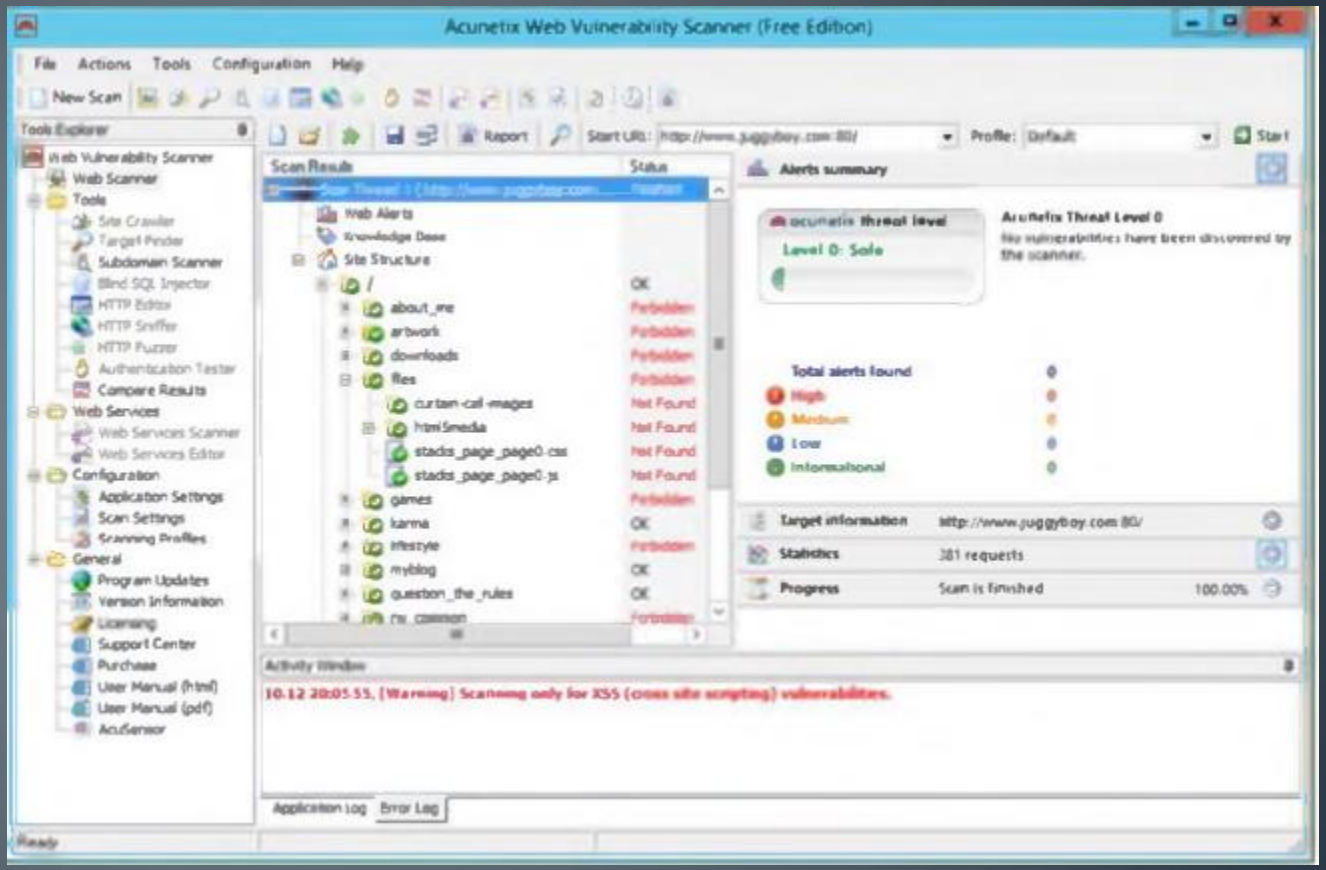
Web Application Security Scanner

- Syhunt Dynamic
- N-Stalker Web Application Security Scanner
- Wikto
- Acunetix


Session-1304713758 [demo.syhunt.com] - Sandcat Pro Hybrid
File Edit View Recent Hosts Advanced Tools Help
Search Results
Scanned Hosts
demo.syhunt.com:80
Host Information
Emails
Links
JS-Based Pages
Site Errors
Source Structure
Vulnerable Source
Vulnerable URLs
Web Structure
detection
Checks
Event List
Main
Vulnerabilities
Crawling
Discovery
JavaScript
Protocol
Debug
SandcatCS.exe executed
Module loaded with pid 244
Analyzing index...
Analyzing index: Done
Checking robots.txt...
Checking robots.txt file: Done
Spidering/Crawling Stage initiated
Spidering/Crawling Stage completed
Starting application security checks...
Testing web applications for vulnerabilities...
Starting Cross Site Scripting Test
Found: x_basic.php XSS
Found: x_basic_plusenv.php XSS
Found: x_form.php XSS
Found: index_hidden.php XSS

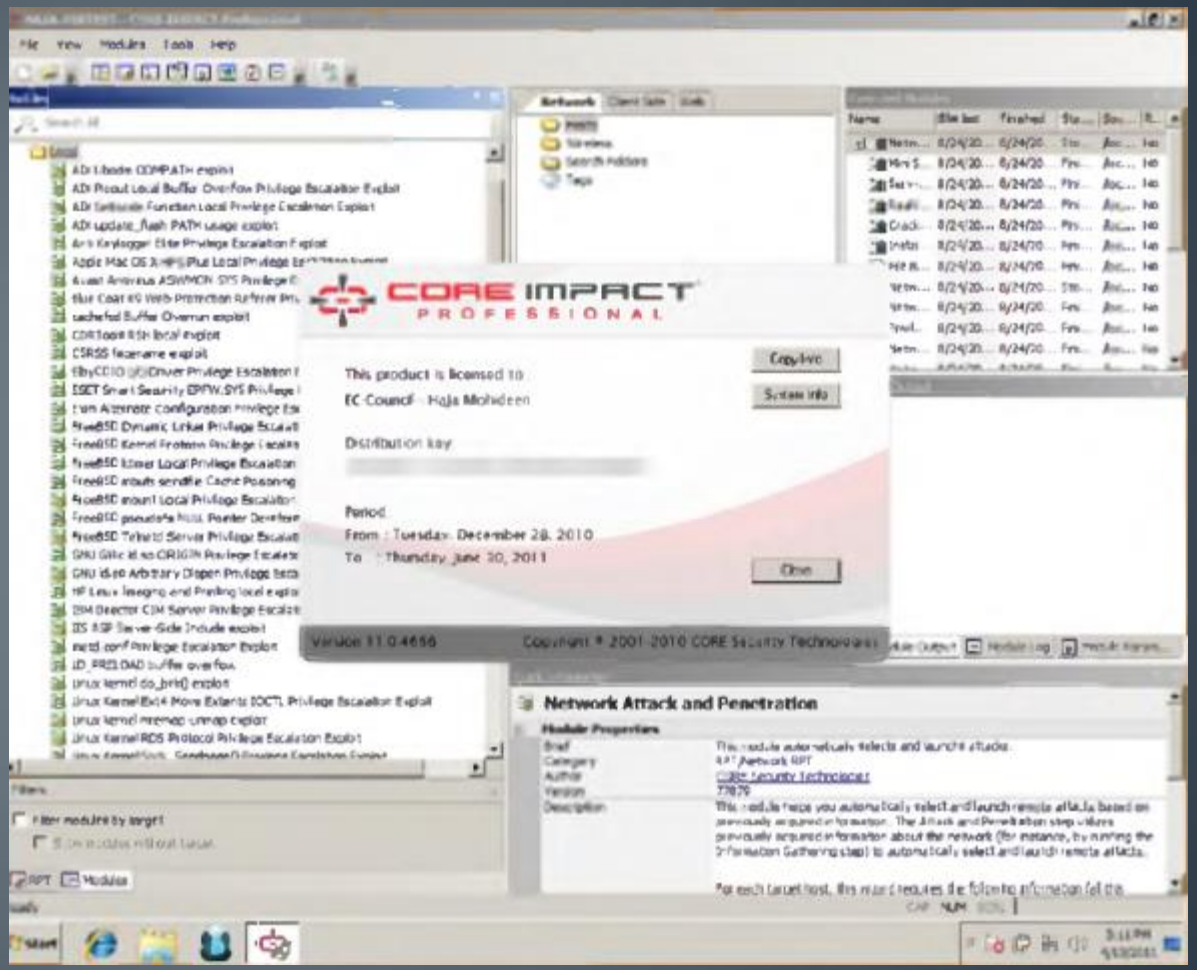

N-Stalker Web Application Security Scanner 2012 - Free Edition
N-Stalker Scanner
Scan Options
Website Tree
Scanner Events
Scanner Dashboard
Progress Status
Completed Spider
Completed Info Gather
Completed Run Modules
Completed Sig Scanner
Progress Details
Scan Session
Start Time Oct 13, 2012 13:24:35
Duration 8 Hours 18 Minutes
Spider Engine #
Crawled URLs 11
Crawled Hosts 1
Default Page Size 18,408 bytes
Scan Engine #
Total Requests 3,580
Failed Requests 0
Attacks Sent 974
404 Errors 3,310
302 Redirection 0
Network #
Bytes Sent 1,102,121
Bytes Received 1,903,979
Avg Response Time 356.56 ms
Requests/Minute 198.00 req/min
High (0) Med (0) Low (2) Info (6)
Component Name
URL Location
Comments
Web Server Information Found
Web Server Technology Detected
Server-Side Technology Found
Password Web Form Found
Scan Modules
Components
Scan Events
Module Events

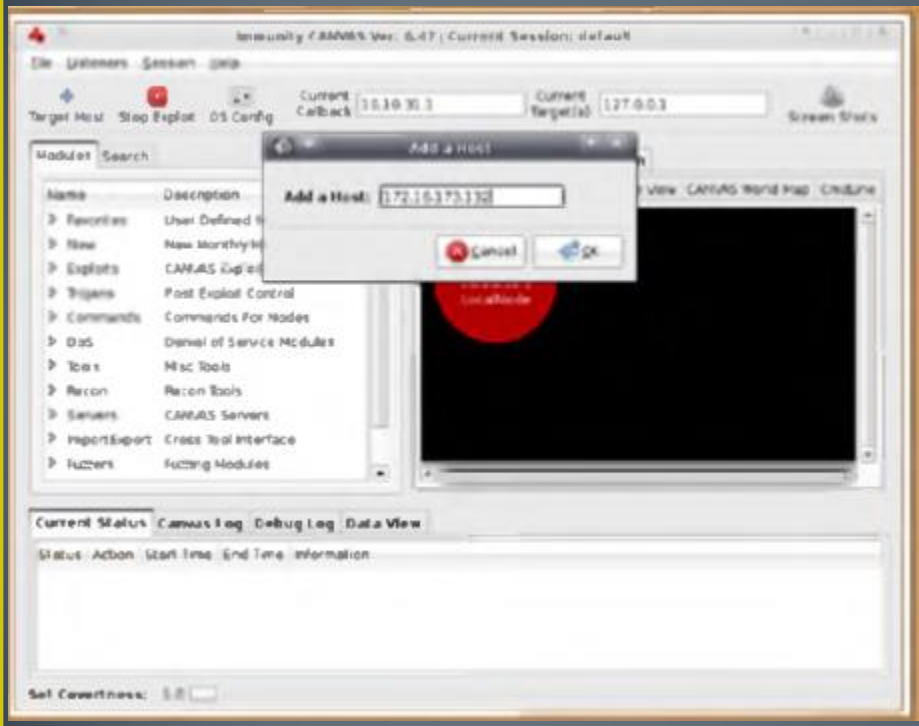

SensePost v2.1.0.0
Spider
Googler
BackEnd
Wikto
GoogleHacks
SystemConfig
Scan Wizard
WIKTO
Start
Stop
Quit
Target
Load Google Hack Database
1 "cacheserverreport for" "This analysis was produced by calamaris"
3 intitle:"Index of" dbconvert.exe chats
4 intitle:"Apache HTTP Server" intitle:"documentation"
5 "Error Diagnostic Information" intitle:"Error Occurred While"
6 intitle:"Index of" finance.xls
7 intitle:index.of finances.xls
8 "# Dumping data for table"
9 intitle:index.of .bash_history
10 intitle:index.of .sh_history
11 intitle:"Index of" .mysql_history
Unable to connect to the remote server
Manual Query
URL:
Unable to connect to the remote server
Results:
Clear List
Unable to connect to the remote server
Unable to connect to the remote server
Unable to connect to the remote server
Unable to connect to the remote server
Unable to connect to the remote server
Unable to connect to the remote server
Unable to connect to the remote server
Unable to connect to the remote server
Unable to connect to the remote server


Acunetix Web Vulnerability Scanner (Free Edition)
File
Actions
Tools
Configuration
Help
New Scan
Report
Start URL:
Profile:
Default
Start
Tools Explorer
Web Vulnerability Scanner
Web Scanner
Tools
Site Crawler
Target Finder
Subdomain Scanner
Blind SQL Injector
HTTP Editor
HTTP Sniffer
HTTP Fuzzer
Authentication Tester
Compare Results
Web Services
Web Services Scanner
Web Services Editor
Configuration
Application Settings
Scan Settings
Scanning Profiles
General
Program Updates
Version Information
Licensing
Support Center
Purchase
User Manual (html)
User Manual (pdf)
AcuSensor
Scan Results
Status
Web Alerts
Knowledge Base
Site Structure
/
about_me
artwork
downloads
files
curtain-call-images
htmlmedia
stadis_page_page0.css
stadis_page_page0.js
games
karma
lifestyle
myblog
question_the_rules
Alerts summary
Acunetix threat level
Level 0: Safe
Acunetix Threat Level 0
Total alerts found
High
Medium
Low
Informational
Target information
http://www.juggyboy.com:80/
Statistics
381 requests
Progress
Scan is finished
100.00%
Activity Window
Application Log
Error Log
Ready

Herramientas para Pentesting

- Core Impact
- Immunity CANVAS


CORE IMPACT
PROFESSIONAL
This product is licensed to
EC-Council - Hoja Mohideen
Distribution key
Period
From : Tuesday, December 28, 2010
To : Thursday, June 30, 2011
Copy key
System Info
Close
Version 11.0.4656
Network Attack and Penetration


Add a Host
Add a Host:
172.16.173.132
Cancel
OK