

GLOBALTEK SECURITY

COLECCIÓN: SEGURIDAD DE LA INFORMACION

Analisis de vulnerabilidades

Armando Carvajal

Master en seguridad informática Universidad Oberta de catalunia

<http://www.globalteksecurity.com>

armando.carvajal@globalteksecurity.com

Colombia, Junio de 2007

1.0 Problemática de las vulnerabilidades

Grupos de personas y organizaciones algunos de tipo "underground" están en la búsqueda de vulnerabilidades en sistemas operativos y aplicaciones informáticas, las vulnerabilidades son reportadas por estas personas y a diario ellos exponen a grandes riesgos los sistemas afectados por esas amenazas, no importa el segmento de mercado a la que pertenezca la organización afectada.

El análisis de vulnerabilidades se ha convertido en un requisito indispensable dentro del proceso de gestión de riesgos y es clave dentro del sistema de gestión de la seguridad de la información.

1.1 Definición de vulnerabilidad y exploit

En <http://www.cve.mitre.org/about/faq.html#A2>, se define "Vulnerabilidad" como un error de software que puede usar directamente el intruso para ganar acceso a un sistema de información.

Este es el texto original "An information security vulnerability is a mistake in software that can be directly used by a hacker to gain access to a system or network. See the [Terminology](#) page for a complete explanation of how this term is used on the CVE Web site."

Wikipedia en www.wikipedia.org, define el termino "Exploit" (del [inglés](#) *to exploit*, explotar, aprovechar) como el nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa. El fin puede ser la destrucción o inhabilitación del sistema atacado, aunque normalmente se trata de violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.

Los "exploits" se pueden clasificar según las categorías de vulnerabilidades utilizadas:

- Vulnerabilidades de [desbordamiento de buffer](#).
- Vulnerabilidades de [condición de carrera](#) (race condition).
- Vulnerabilidades de [error de formato de cadena](#) (format string bugs).
- Vulnerabilidades de [Cross Site Scripting \(XSS\)](#).
- Vulnerabilidades de [Inyección SQL](#).
- Vulnerabilidades de Inyección de Caracteres ([CRLF](#)).
- Vulnerabilidades de [denegación del servicio](#)
- Vulnerabilidades de Inyección múltiple HTML ([Multiple HTML Injection](#)).
- Vulnerabilidades de ventanas engañosas o mistificación de ventanas ([Window Spoofing](#)).

1.2 Análisis de los términos definidos

Si se revisa nuevamente la anterior definición, una vulnerabilidad representa entonces una falla del sistema informático o programa y el "exploit" se aprovecha de la vulnerabilidad, la vulnerabilidad hace que el riesgo aumente hasta convertirse en una amenaza, la falla del sistema informático o vulnerabilidad puede ser aprovechada por un intruso para obtener el control en forma remota o local de los recursos del sistema.

Un "exploit" que se aprovecha de una vulnerabilidad, fundamentalmente afecta la variable confidencialidad, pero se puede extender a la variable integridad si modifica el recurso informático, ahora si el intruso quiere hacer más daño, puede afectar la variable disponibilidad del sistema, por ejemplo un ataque a una vulnerabilidad de "buffer overflow" impactara las 3 variables del sistema de seguridad:

- Confidencialidad
- Integridad y
- Disponibilidad

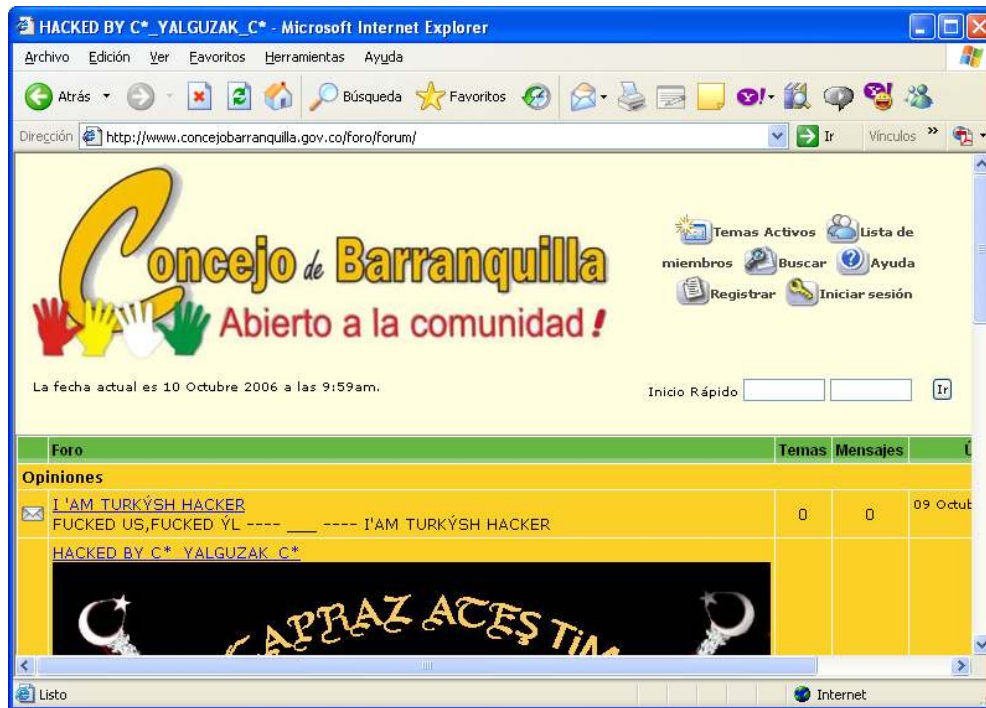
Importante

Cuando no exista una solución "conocida" para una vulnerabilidad, pero si se conoce como explotarla, entonces se le conoce como "vulnerabilidades 0 days".

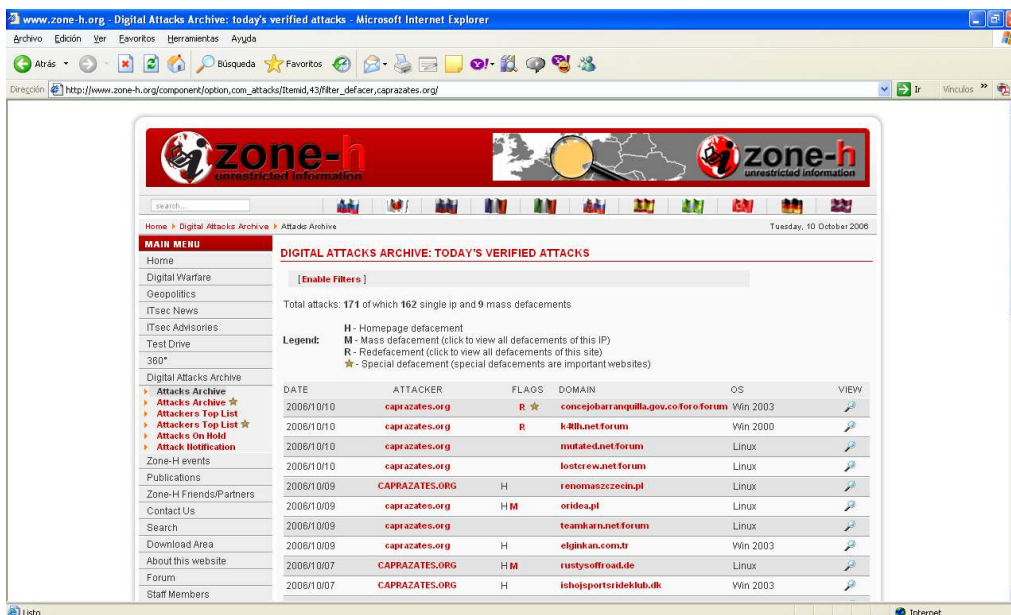
El abogado Carlos Santiago Álvarez Cabrera en su artículo "Honeypots Aspectos penales", Colombia, Diciembre de 2005, <http://cyberlaws.blogspot.com>, concluye respecto de las vulnerabilidades, que: La velocidad de los ataques esta en constante incremento debido a los "0 days vulnerabilities"

1.3 Ejemplos de las vulnerabilidades

El ataque "webdefacement" afecta las variables confidencialidad e integridad, el 10 de octubre de 2006, la página web del concejo de Barraquilla, Colombia lucia así:



Esto fue reportado por el sitio www.zone-h.org, y es un claro ejemplo de webdefacement que ataca alguna vulnerabilidad del servidor web, además el reporte enuncia que el servidor web es un Microsoft Internet Information Server 6.0.



En este portal www.zone-h.org aparecen muchos otros sitios que también fueron atacados y tenían diferentes sistemas operativos como Linux y Unix BSD.

www.zone-h.org - Attackers Special Top List - Mozilla Firefox

http://www.zone-h.org/component?option=com_topatt&Itemid,49

по информационной безопасности

ATTACKERS SPECIAL TOP LIST

This is the list of the first 50 "special" attackers...

NO	ATTACKER	SINGLE DEF.	MASS DEF.	TOTAL DEF.	POLITICALLY MOTIVATED ATTACKS	% OF POLITICALLY MOTIVATED ATTACKS
1	china hacker	715	1223	1938	868	44.79 %
2	Fatal Error	518	468	986	39	3.96 %
3	Iskorpitx	425	360	805	9	1.12 %
4	Red Eye	303	357	660	95	14.39 %
5	DeltahackingSecurityTEAM	297	191	488	0	0.00 %
6	Triad	284	255	539	438	81.26 %
7	Ashlyane Digital Security Team	261	427	688	47	6.83 %
8	B.O.M	252	497	749	3	0.40 %
9	PoisonBlix	251	3	254	0	0.00 %
10	Hi.Tech.Hate	222	6	228	39	17.11 %
11	Prime Suspect2	203	0	203	0	0.00 %
12	core-project	186	284	470	75	15.96 %
13	Silver Lords	184	11	195	2	1.03 %
14	HobobyCoder	179	57	236	229	97.03 %
15	butistuta	175	58	233	0	0.00 %

Esta es una lista muy resumida de los top 50 ataques.

1.4 Problemática específica

1.4.1 Cuando fue su ultimo análisis de vulnerabilidades?

- Con que frecuencia se hacen este análisis en las organizaciones
- Es de conocimiento general que hay mas de 20 nuevas vulnerabilidades diarias

1.4.2 Si se anuncia una nueva vulnerabilidad hoy, cual es su proceso actual para proteger la red?

- Es importante saber si estas vulnerabilidades afectan a su empresa
- Se debe tener un historial de sus vulnerabilidades y su corrección
- Es clave saber cuando y como fueron corregidas

2.0 Antecedentes

Antecedentes

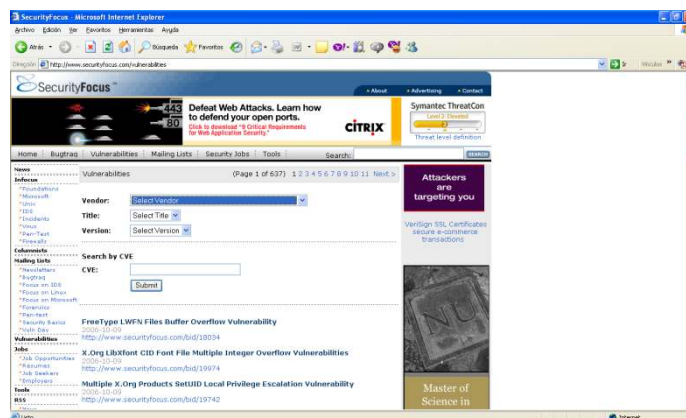
- Generalmente se tienen medidas reactivas contra los ataques, se crean trampas para el momento en que se produce un ataque y además se dispone de herramientas para capturar el tráfico que pasa por un segmento de red

Actualmente las organizaciones tienen medidas reactivas contra los ataques, se crean trampas para el momento en que se produce un ataque y además se dispone de herramientas para capturar el tráfico que pasa por un segmento de red.

El otro lado de la exploración de vulnerabilidades es usarlas como medidas preventivas y para ello, lo que se busca saber es cuán vulnerable son las máquinas de nuestra organización.

Se han hecho grandes esfuerzos en la comunidad informática para crear bases de datos formales donde se encuentra información crítica como: cual es vulnerabilidad, a que sistemas impacta, como se activa la vulnerabilidad, cual es el código que la activa, como se corrige la vulnerabilidad. Algunos portales importantes son:

2.1 <http://www.securityfocus.com/>



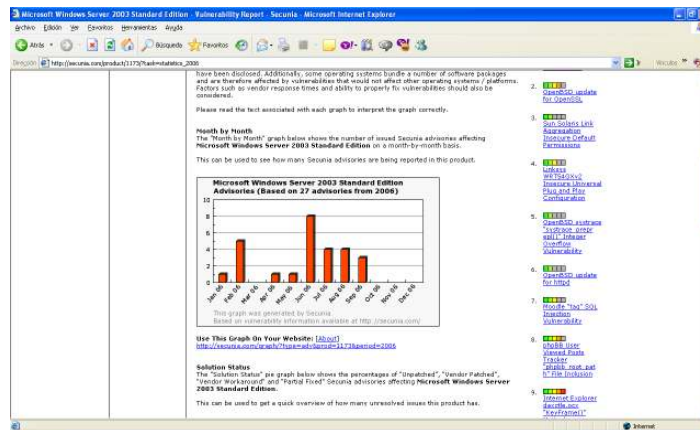
Es una de las bases de datos mas consultadas por los profesionales en seguridad informática por el contexto técnico aportado.

2.2 <http://www.osvdb.org/>



Esta base de datos tiene la mejor información sobre vulnerabilidades en el software open source.

2.3 <http://secunia.com/>



Secunia, tienen las mejores estadísticas de la aparición de vulnerabilidades por sistema operativo.

4.0 Herramientas más conocidas

4.1 Contextualización

Los sistemas operativos cada vez son más especializados y es muy probable encontrar un servidor Linux como servidor web pero es más probable encontrar Windows XP como estación de trabajo cliente en los usuarios finales. Ahora es muy probable encontrar un servidor Windows 2003 como servidor de archivos, impresoras y archivos, pero poco probable encontrar un Unix haciendo esas funciones.

Esto no quiere decir que uno es menor que otro, quiere decir que cada uno tiene características deseables para hacer una tarea específica, cada sistema es especializado para ciertos servicios.

Ahora las vulnerabilidades por errores de programación e implementación son diferentes en cada plataforma, la solución a los desbordamientos de memoria o "buffers Overflows" son diferentes en cada plataforma, y de hecho hay servicios particulares de gestión de bases de datos que son particulares a un sistema operativo, por ejemplo MS SQL Server es específico a Microsoft, es impensable encontrar este motor de gestión en un servidor Unix BSD o Linux.

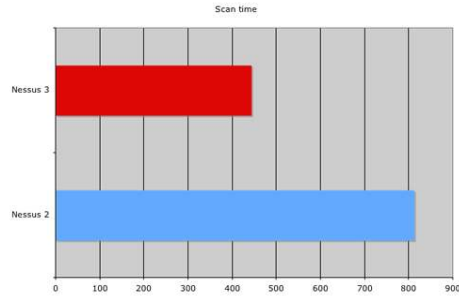
Por lo tanto existen herramientas en el mercado especializadas dependiendo de la plataforma del sistema operativo:

Para hacer este análisis de vulnerabilidades sobre servidores Linux y Unix es de suma utilidad el programa "**Nessus**", en cambio para buscar las vulnerabilidades de los servidores y PC de escritorio MS Windows, se debe usar de preferencia "**Microsoft Baseline Security Analyzer**".

4.2 Nessus presenta una arquitectura modular, cliente-servidor Opensource, dispone de una base de datos de patrones de ataques para lanzar contra una máquina o conjunto de máquinas con el objetivo de localizar sus vulnerabilidades.

Nessus

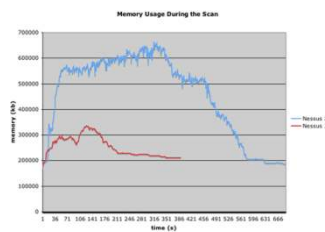
- **Nessus** presenta una arquitectura modular, cliente-servidor Opensource, dispone de una base de datos de patrones de ataques para lanzar contra una máquina o conjunto de máquinas con el objetivo de localizar sus vulnerabilidades.



La versión a la fecha de nessus es la 3 y enfatiza en la eficiencia del lenguaje de ejecución de los scripts de análisis de vulnerabilidades.



Por ejemplo en la grafica anterior se nota que el lenguaje NASL3 el uso de los algoritmos de seguridad ahora es más eficiente en el consumo de ciclos de reloj.



Así mismo se nota que el consumo de memoria RAM es mucho menor que en la anterior versión nessus 2.0

4.3 Limitantes de Nessus

- Es abierto y Opensource, evalúa los sistemas operativos basado en los plugins
- Crece y escala por los plugins
- Hace uso eficiente del ancho de banda
- No hace cumplimiento de políticas
- No hay remediación de vulnerabilidades
- No hay inventario de recursos informáticos
- No hay seguimiento basado en tickets
- No muestra cuanto hace falta para llegar a la norma

4.4 “Microsoft Baseline Security Analyzer”, o MBSA es una herramienta que permite a los usuarios y administradores de sistemas Windows verificar la configuración de seguridad, detectando los posibles problemas de seguridad en el sistema operativo y los diversos componentes instalados.

MBSA ha sido diseñado para analizar las máquinas que utilizan los sistemas operativos Microsoft Windows NT 4, Windows 2000, 2003, Windows XP (Professional y Home Edition) para determinar la presencia de los últimos parches de seguridad publicados y, adicionalmente, verificar la configuración de los diversos componentes para determinar la posible presencia de configuraciones erróneas que pueden provocar brechas en la seguridad.

4.5 Limitantes de MBSA

- Es propietario, solo sirve para evaluar vulnerabilidades en Microsoft
- Hace uso eficiente del ancho de banda
- No hace cumplimiento de políticas
- No hay remediación de vulnerabilidades
- No hay inventario de recursos informáticos
- No hay seguimiento basado en tickets
- No muestra cuanto hace falta para llegar a la norma

5.0 Que tipo de precauciones deben tomarse con las herramientas de exploración de vulnerabilidades

- Se recomienda poner banners que informen al intruso sobre las políticas de no hacer scanner a nuestros servicios
- Si ya hay logs que nos indiquen que se están haciendo scanners a nuestros servicios se podría poner un detector de scanners como portsentry, courtney, icmpinfo y scan-detector por ejemplo

6.0 Quien debe ejecutar las herramientas de exploración de vulnerabilidades

- El Administrador de la red
- Los asesores externos en seguridad informática que estén autorizados por la organización
- El grupo de investigación forense encargado de los honeypots de la organización
- Es recomendable automatizar la ejecución de estas herramientas así como el envío de los reportes generados

7.0 Como ayudan los resultados obtenidos por las herramientas de exploración de vulnerabilidades

- Los reportes que generan las herramientas son tan detallados que nos indican exactamente como arreglar las vulnerabilidades de nuestros sistemas críticos del negocio
- Según las necesidades se debería ejecutar con frecuencia en nuestra red por lo

menos cada semana para buscar vulnerabilidades y detectarlas antes de que los intrusos lo hagan por nosotros

8.0 Quien debe leer esos reportes dentro de la organización

- La dirección de informática, la dirección de riesgos, auditoria: La alta gerencia debe estar informada para generarles conciencia sobre el hecho de que los recursos informáticos si impactan al negocio al ser accionados los “exploits” respectivos que ya son de conocimiento publico

Quien debe leer los reportes?

- ⌚ La dirección de informática: La alta gerencia debe estar informada para generarles conciencia sobre el hecho de que los recursos informáticos si impactan al negocio al ser accionados los “exploits” respectivos que ya son de conocimiento publico

9.0 Productos Comerciales

Existe la tendencia de usar el motor de análisis de vulnerabilidades “nessus” por su riqueza en características y bajo costo, además del soporte a la extensibilidad y escalabilidad por medio de plugins o componentes que amplían las características de nessus.

Los productos más importantes que usan este motor para el análisis de vulnerabilidades son Catbird (c) (www.catbird.com):

9.1 Catbird (c) es muy fuerte pues usa un portal para la gestión centralizada de las vulnerabilidades, analiza externamente e internamente la red teniendo en cuenta los accesos inalámbricos. Además hace monitoreo de servicios de red como el DNS y la disponibilidad de los portales web de las organizaciones.



- Análisis de tendencias de Seguridad
- Resumen de alto nivel:
 - Gerencia
 - Directoria
- Exámenes
 - Auditores
 - Examinadores

9.2 Tenable Network Security (c) (www.tenablesecurity.com):



Su fortaleza es la gestión de los eventos de seguridad y el cumplimiento de las políticas de parches o suplementos a la infraestructura de servidores y PCs de usuarios. Es vital el análisis de vulnerabilidades para saber que suplementos debe instalar.

10.0 Laboratorios

10.1 Laboratorio: Nessus

Se recomienda usar una maquina virtual para emular los diferentes sistemas operativos, es recomendable el Linux Auditor, Remote-exploit o el Linux knoppix-std.

Antes de empezar con cualquier prueba es importante remarcar que la actividad de la herramienta nessus para exploración de vulnerabilidades se considera un ataque contra la máquina objetivo, y como tal nunca debe hacerse sin previo permiso del administrador del sistema implicado.

Nos planteamos ahora ver cuál es el estado de la seguridad de nuestra máquina virtual linux.



Para disponer de más datos, vamos a hacer que el sistema Linux de pruebas se comporte como un servidor de muchos servicios.

Prerrequisitos:

Debe utilizarse el sistema Linux orientado a las auditorias en seguridad informatica recomendado que ya tenga instalado el software nessus, ahora si tiene otro Linux como Fedora Core V, siga los siguientes pasos:

1. Posicionese en el directorio /tmp

```
# cd /tmp
```

2. Baje e instale la ultima version del sitio www.nessus.org, a la fecha de este documento existe la version 3.0.5

```
# rpm -Uhv Nessus-3.0.5-fcs.i386.rpm
```

3. Adicione el usuario administrador llamado "admin" con la clave "sistemas" para gestionar la herramienta

```
# /opt/nessus/sbin/nessus-add-first-user
```

4. Suba el servicio con el comando

```
# /sbin/service nessusd start
```

5. Instale el software de tipo cliente para interactuar con el servidor

```
# rpm -Uhv NessusClient-1.0.2-fc5.i386.rpm
```

6. Ejecute el cliente y pruebe un analisis de vulnerabilidades

```
# /usr/X11R6/bin/NessusClient &
```

A continuación, ejecutaremos nessus para ver las vulnerabilidades que detecta en el servidor Linux de pruebas.

Pasos:

7. Poner en funcionamiento los servidores de correo, web y SSH si no estan activaados
8. Crear el certificado de seguridad con el comando nessus-mkcert si no ha sido creado
9. Crear un usuario nessus con el comando nessus-adduser si este no se ha creado
10. Iniciar el servidor con el comando nessusd si este no se ha lanzado
11. Ejecutar el cliente "nessus" desde el modo grafico con el comando nessus si tiene un Linux de auditoria
12. Hacer inicio de sesión como usuario nessus o admin., dependiendo del usuario creado en el paso respectivo
13. Indicar como Target el objetivo de nuestro análisis. En concreto será el host local 127.0.0.1. Notar que podríamos indicar una red entera.
14. Revisar el conjunto de 'plugins' que tiene la herramienta. en nuestro caso le diremos que realice todos los ataques excepto los peligrosos. ('Enable all but dangerous plugins').
15. Una vez hecho esto, iniciar el scanning de puertos (Start scan).
16. Finalmente, comprobar el informe de resultados de vulnerabilidades.

Resultado: Se describen las más importantes:

Puerto	Severidad	Descripción	Factor de riesgo
Web(80)	Hueco de seguridad	Problema: El cgi perl puede ser lanzado por un usuario malintencionado y quedaria con los permisos del usuario que lanzo el servidor apache. Solucion: Se debe remover el programa perl del directorio /cgi-bin	Alto
Web(80)	Warning	Problema: El directorio /doc es explorable Solucion: Restringir el acceso con el comando Directory.	Alto

Puerto	Severidad	Descripción	Factor de riesgo
Ssh(22)	Hueco de seguridad	Problema: Una version del servidor ssh anterior a la version 3.2.1 esta instalada y se cree que existe una vulnerabilidad en la administracion de buffers que permite al atacante ejecutar comandos en forma arbitraria. Solucion: Se debe actualizar a una version mas reciente o parchar la actual	Alto
Netbios-ssn(139)	Hueco de seguridad	Problema: Una sesion NULL puede tener accso al recurso IPC\$ con permisos de lectura y escritura Solucion: En el explorador de windowsNTelija boton derecho en cada carpeta y elija permisos para denegarlos.	Alto

Este es una parte del archivo del reporte para leer en nessus:

```

timestamps||scan_start|Fri Jan 27 12:05:31 2006|
timestamps||127.0.0.1|host_start|Fri Jan 27 12:05:31 2006|
results|127.0.0|127.0.0.1|sunrpc (111/tcp)|10223|Security Note|\n
The RPC portmapper is running on this port.\n\n
An attacker may use it to enumerate your list\n
of RPC services. We recommend you filter traffic\n
going to this port.\n\n
Risk factor : Low\n
CVE : CAN-1999-0632, CVE-1999-0189\n
BID : 205\n
results|127.0.0|127.0.0.1|microsoft-ds (445/tcp)|11011|Security Note|A CIFS server
is running on this port\n
results|127.0.0|127.0.0.1|netbios-ssn (139/tcp)|11011|Security Note|An SMB server
is running on this port\n
...

```

Fin del laboratorio

10.2 Laboratorio: Microsoft Baseline Security Analyzer

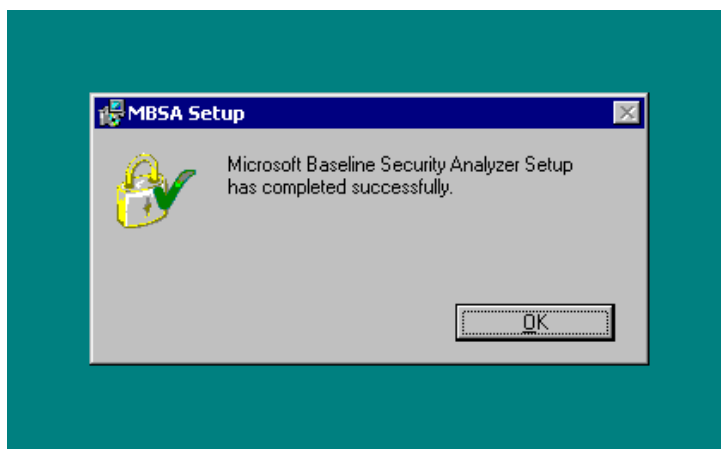
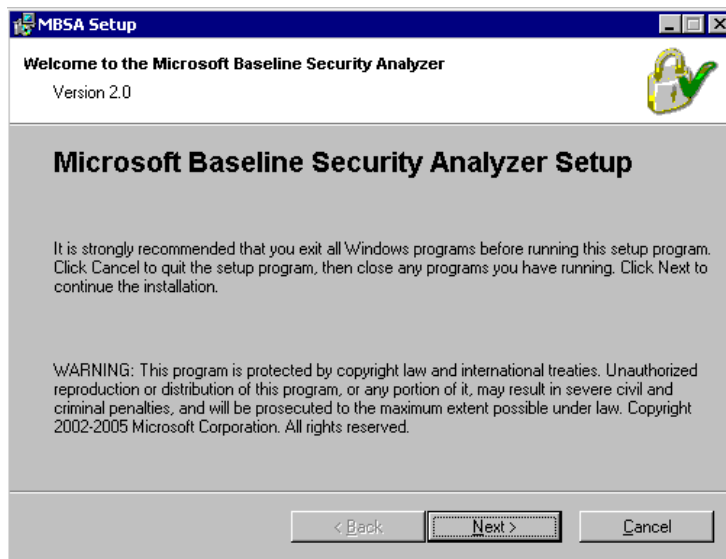
Se debe hacer exploración de vulnerabilidades a un servidor Windows 2000 como mínimo y es deseable que el Windows 2000 este con suplementos a la fecha.

Se recomienda usar una maquina virtual para emular los diferentes sistemas operativos.

Prerrequisitos: Instalar la herramienta MBSA 2.0 (**Microsoft Baseline Security Analyzer 2.0**) en la máquina virtual Windows.

Se puede descargar desde la siguiente URL:

<http://www.microsoft.com/technet/security/tools/mbsa2/default.aspx>



Paso 1: Ejecute MBSA localmente y comente tanto el funcionamiento de la herramienta como el resultado obtenido. Note que la herramienta indica los posibles errores y agujeros de seguridad del servidor y en la mayoría de los casos indica cómo solucionarlos. Observe que no se limita a la seguridad del sistema operativo, sino que

además busca vulnerabilidades en otras aplicaciones servidor de Microsoft como IIS o SQL.

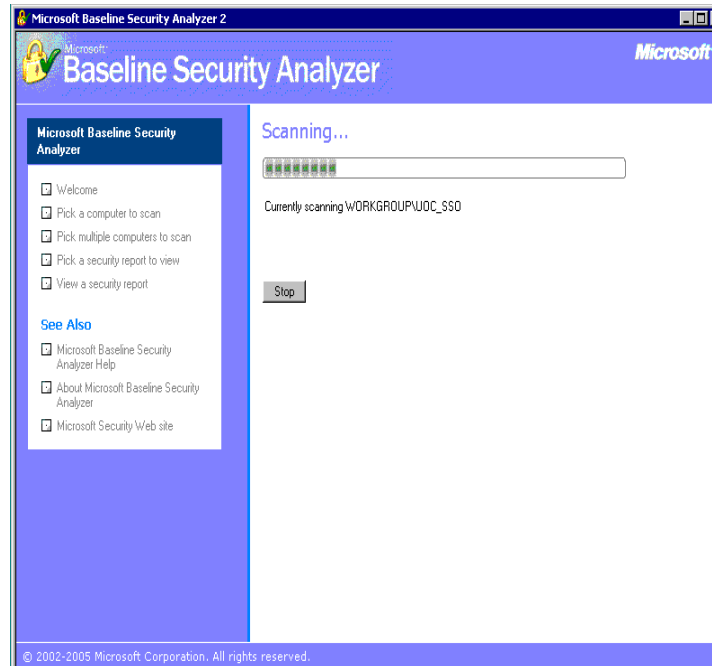
Se inicia el programa MBSA:



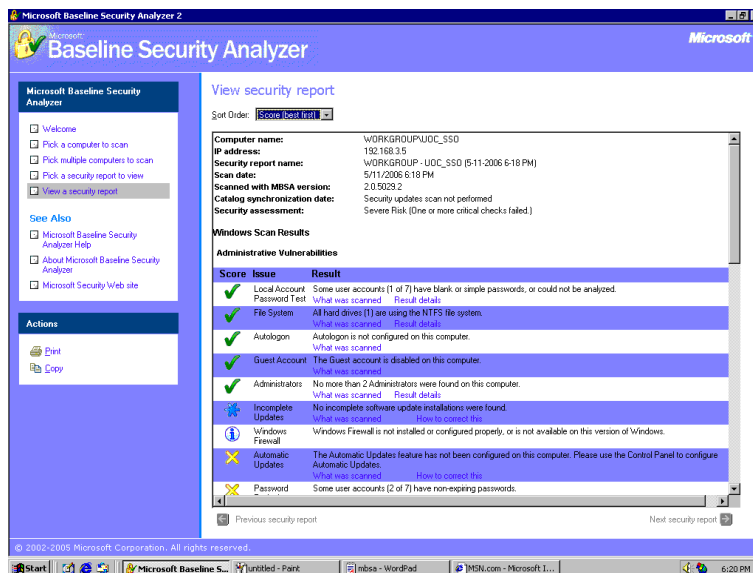
Se diligencian los datos requeridos para escanear la maquina que para este caso es la maquina local:




Ahora se da inicio a la exploración de vulnerabilidades haciendo click en la opción Start scan:




Al terminar genera un reporte que se muestra en pantalla así:



Revisemos los estados de las diferentes alertas o avisos que genera el reporte:

 : Este símbolo significa que paso la revisión

 : Este símbolo significa que se recomienda implementar



: Este símbolo significa que es información adicional



: Este símbolo significa que es una falla no crítica



: Este símbolo significa que es una falla crítica.

Bien ahora pasemos a comentar el resultado obtenido en el escaneo:

Computer name: WORKGROUP\UOC_SSO
IP address: 192.168.3.5
Security report name: WORKGROUP - UOC_SSO (5-11-2006 6-18 PM)
Scan date: 5/11/2006 6:18 PM
Catalog synchronization date: Security updates scan not performed
Security assessment: Severe Risk

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Restrict Anonymous	Computer is running with RestrictAnonymous = 0. This level allows basic enumeration of user accounts policies, and system information. Set RestrictAnonymous = 2 to ensure maximum security.

En esta parte de vulnerabilidades administrativas en nuestro primer dato nos indica que hay una falla crítica referente a restringir anónimos, nos indica que Windows esta corriendo en un nivel cero (0) y que lo correcto debería ser un nivel dos (2).

	Password Expiration	Some user accounts (2 of 7) have non-expiring passwords. User Administrator Guest IUSR_PRACTICAUOC IWAM_PRACTICAUOC TsInternetUser
--	---------------------	---

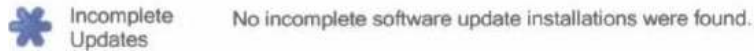
En esta parte de expiración de claves nos indica que existen de 2 a 7 claves que no tienen configurado tiempo de expiración y nos lista los usuarios que en nuestro caso son cinco, y es una falla no crítica.

	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please use the Control Panel to configure Automatic Updates.
--	-------------------	--

Aquí nos indica que Windows no tiene configurado la parte de actualizaciones automáticas y nos indica que por panel de control podemos habilitarlo, y es una falla no crítica.



En esta parte nos indica que Windows no tiene un firewall instalado o que tiene una versión que no soporta, y recomienda implementar un firewall dentro del servidor.

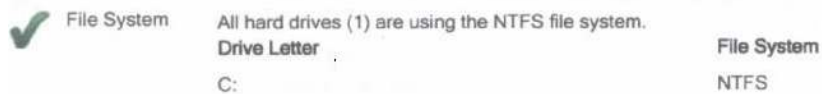


Aquí en actualizaciones incompletas nos indica que no encontró ninguna instalación de actualizaciones incompleta.

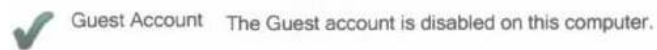
Local Account Password Test Some user accounts (1 of 7) have blank or simple passwords, or could not be analyzed.

User	Weak Password	Locked Out	Disabled
Guest	Weak	-	Disabled
Administrator	-	-	-
IUSR_PRACTICAUOC	-	-	-
IWAM_PRACTICAUOC	-	-	-
JParra	-	-	-
TsinternetUser	-	-	-
csso	-	-	-

En esta prueba de cuentas locales, las 7 cuentas pasaron la prueba y muestran la señal que paso la revisión.



Aquí nos indica en la parte de File System que los discos están usando NTFS y que esto es correcto.



En esta parte de cuentas de invitados me indica que esta opción esta deshabilitada en Windows y que esto es correcto.



Aquí me indica que la parte de autologon en Windows no esta configurada y que esto es correcto.



A green checkmark icon is followed by the text: "Administrators No more than 2 Administrators were found on this computer. User Administrator".

En la parte de administradores me indica que no hay más de 2 cuentas administradoras y por consiguiente es correcto.



The section is titled "Additional System Information". It contains a table with the following content:

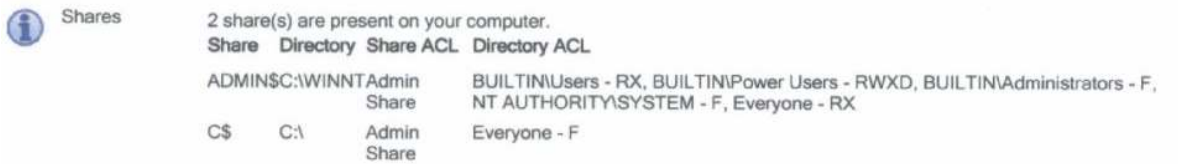
Score	Issue	Result
	Windows Version	Computer is running Windows 2000 or greater.

En esta sección de Información adicional del sistema, el primer ítem nos indica a modo de información que el sistema operativo es Windows 2000 o superior.



A blue gear icon is followed by the text: "Auditing Enable auditing for specific events like logon/logoff. Be sure to monitor your event log to watch for unauthorized access."

En esta parte de auditoria recomiendan habilitarla, para verificar los logs que se generen mediante el monitor de eventos y así poder controlar accesos indebidos.



An information icon is followed by the text: "Shares 2 share(s) are present on your computer." Below this is a table:

Share	Directory	Share ACL	Directory ACL
ADMIN\$C:\WINNT	Admin Share		BUILTIN\Users - RX, BUILTIN\Power Users - RWXD, BUILTIN\Administrators - F, NT AUTHORITY\SYSTEM - F, Everyone - RX
C\$	C:\	Admin Share	Everyone - F

En este ítem de compartir, ha manera de información nos indica que hay dos directorios que Windows esta compartiendo.



A blue gear icon is followed by the text: "Services Some potentially unnecessary services are installed." Below this is a table:

Service	State
FTP Publishing Service	Running
Simple Mail Transport Protocol (SMTP)	Running
Telnet	Stopped
World Wide Web Publishing Service	Running

En la parte de servicios recomienda que los cuatro servicios que lista son innecesarios y por consiguiente seria bueno deshabilitarlos.

Internet Information Services (IIS) Scan Results


Administrative Vulnerabilities

Score	Issue	Result
	Sample Applications	Some IIS sample applications are installed. Web Site Administration Web Site Default Web Site Default Web Site Default Web Site Virtual Directory IISHelp IISHelp IISSamples MSADC


En esta sección de administración de vulnerabilidades, el ítem de ejemplos de aplicaciones, nos dice que algunos ejemplos de aplicaciones de IIS se encuentran instalados y toma esto como una falla crítica.

	Parent Paths	Parent paths are enabled in some web sites and/or virtual directories. Web Site Administration Web Site Administration Web Site Default Web Site Default Web Site Default Web Site Default Web Site Default Web Site Default Web Site Default Web Site Default Web Site Default Web Site Default Web Site Virtual Directory - IISAdmin - Scripts IISAdmin IISSamples MSADC _vti_bin PBServer PBSDData Rpc
---	--------------	--

Aquí nos indica que algunas rutas de alta jerarquía están habilitadas en algunos sitios web o directorios virtuales, y nos muestra un listado de dichos sitios. Por consiguiente esto lo toma como una falla crítica.

	IIS Lockdown Tool	The IIS Lockdown tool has not been run on the machine.
---	-------------------	--

En este ítem de IIS Lockdown Tool, nos dice que esta aplicación no está corriendo en la máquina y por consiguiente lo cataloga como falla crítica.


	MSADC and Scripts Virtual Directories	MSADC virtual directory was found under one or more web sites. Scripts virtual directory was found under one or more web sites.
---	---------------------------------------	---

Aquí nos indica que el directorio virtual MSADC fue encontrado en al menos uno o más sitios Web y esto lo cataloga como una falla no crítica.


	IISAdmin Virtual Directory	IISADMPWD virtual directory is not present.
---	----------------------------	---

En este ítem de Administración de directorios virtuales de IIS, nos indica que el directorio virtual IISADMPWD no está presente y cataloga esto como correcto.

Additional System Information

Score	Issue	Result
	Domain Controller Test	IIS is not running on a domain controller.

En esta sección de información adicional del sistema, este ítem nos indica que ISS no esta corriendo en un controlador de dominio y recomienda que sea así.

	IIS Logging Enabled	Some web or FTP sites are not using the recommended logging options.
	Name	Protocol
	Administration Web Site	HTTP
	Default FTP Site	FTP
	Default Web Site	HTTP


Aquí en este ítem de IIS Logging Enable, nos indica que hay dos sitios Web y un ftp que no están usando las opciones recomendadas para claves, y recomienda en tal caso que se implementen dichas opciones.

SQL Server Scan Results

Score	Issue	Result
	SQL Server/MSDE Status	SQL Server and/or MSDE is not installed on this computer.

Desktop Application Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	IE Zones	Internet Explorer zones do not have secure settings for some users.
	User	Zone Level Recommended Level
	UOC_SSO\Administrator	Restricted sites Custom High
	Setting	Current Recommended
	Script ActiveX controls marked safe for scripting	Enable Disable
	Macro Security	No Microsoft Office products are installed

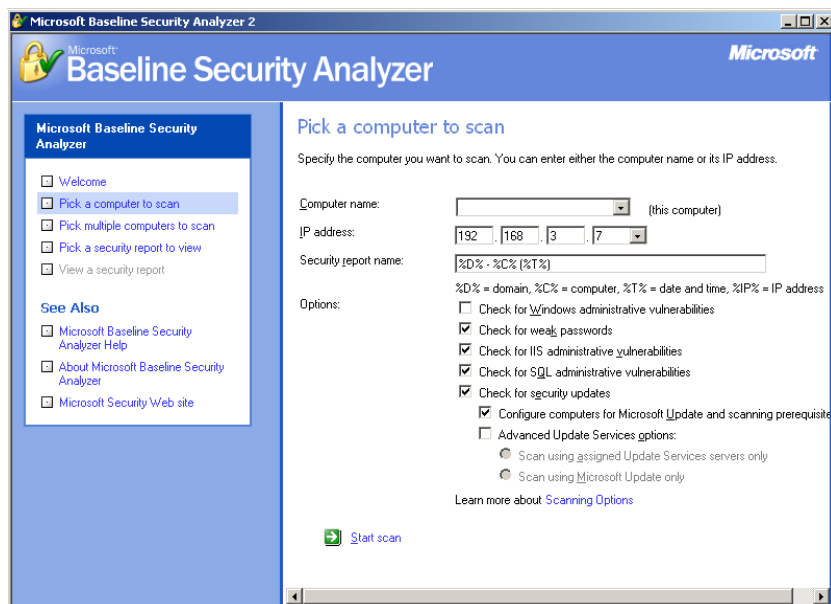
En esta ultima parte nos indica que SQL Server no esta instalado por consiguiente no se realizo ninguna revisión.

Ahora en la parte de Vulnerabilidades administrativas, en el ítem de Zonas de Internet nos indica que hay una falla critica ya que el usuario administrador no tiene el nivel de seguridad apropiado ya que esta en Custom y debería estar en High, además la opción de Scripts ActiveX controls marked safe for scripting esta enable y debería estar en Disable.

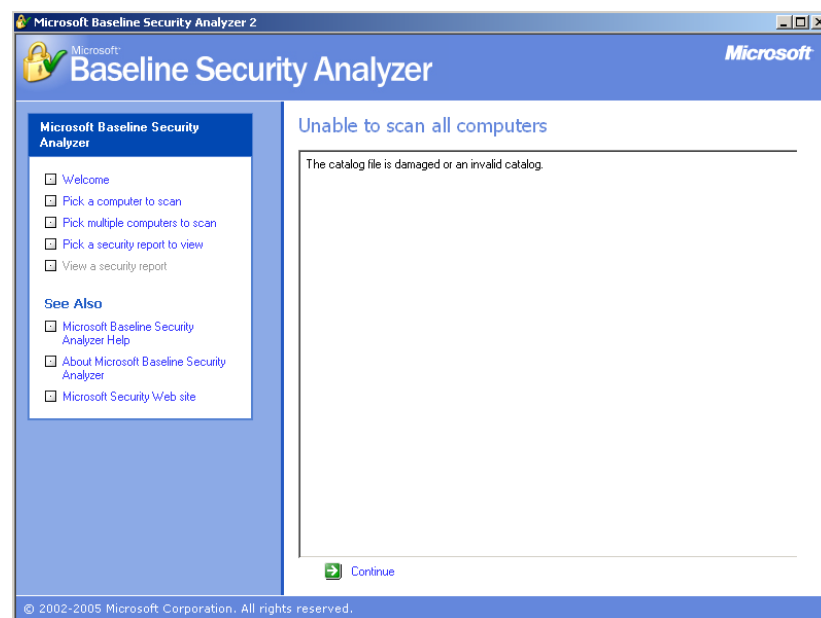
Por ultimo nos dice que no existen productos de Office Instalados.

Paso 2: Ejecutar la aplicación contra la máquina virtual Linux o cualquier otra máquina Linux y comentar el resultado.

Pasamos a ejecutar la aplicación a nuestro servidor Linux 192.168.3.7



Se genera el siguiente error:



Si se prueba varias veces realizando la exploración a la maquina virtual Linux se notara que esta no funciona para sistemas diferentes a Microsoft.

Fin del laboratorio

11.0 Evaluación del Modulo

11.1 ¿Cuál es la diferencia entre vulnerabilidad y exploit?

11.2 ¿Qué es una vulnerabilidad 0 days?

11.3 ¿Defina exploit?

12. Bibliografía Relacionada

Open Source penetration testing and security professional double CD, Syngress Publishing, Jay Beale, 2006



Nessus, snort and ethereal power tools, Neil Archibald, Gilbert Ramirez, Noam Rathaus, and Josh Burke, 2005

