Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 2: Vulnerabilidades e intrusión

1- Escanear la red

Un escáner de red es una herramienta que sirve para descubrir qué servicios están activos en máquinas remotas. Para el atacante, es una herramienta fundamental, pues le permite automatizar el proceso de búsqueda de máquinas vulnerables o útiles para sus propósitos.

Los escáneres actuales ya no se limitan a escanear a nivel de puerto TCP o UDP; permiten extraer una mayor cantidad de información útil como cuál es la versión concreta de la aplicación que está corriendo en un determinado puerto, o identificar el sistema operativo que está ejecutando la máquina objetivo.

Va a manejar dos escáneres distintos. Se diferencian en las funcionalidades que proporcionan. Tenga en cuenta que para determinadas opciones puede necesitar permisos de superusuario.

El primero de ellos, *nmap* (http://www.insecure.org/nmap/), es una herramienta muy conocida y que implementa funciones muy avanzadas. Es eminentemente un escáner a nivel de puertos, pero también permite realizar funciones de identificación de sistemas operativos y de aplicaciones.

La sintaxis del nmap es:

nmap [Tipos(s)de escaneo] [Opciones] <servidor o red #1... [#N]>

Donde existen diferentes tipos de escaneo:

- -sT Escaneo TCP connect()
- -sS Escaneo TCP SYN
- -sF -sX –sN Modos Stealth FIN, Xmas Tree o Nul scan
- -sP Escaneo ping
- -sU Escaneo UDP

La aplicación *amap* (http://www.thc.org/releases.php) sirve para averiguar qué aplicación está corriendo en un puerto determinado.

Escaneo

Utilice los equipos PC A y PC B. Dichos equipos ejecutan algunos servicios y lo que se quiere comprobar es como desde uno de los dos equipos puede averiguar información sobre qué servicios están corriendo en el otro, la versión del sistema operativo y la versión de los servicios que corren.

- Configure el equipo PC A y PC B en la misma red
- Realice un escaneo de puertos desde PC A al equipo PC B intentando averiguar:
  - Servicios Activos en PC B y Sistema operativo que está corriendo en PC B
  - Versión de los servicios que están corriendo en PC B.

Checkpoint 2.1: Mostrar al profesor los resultados del escaneo y los comandos ejecutados.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

2- Robustez de las contraseñas de un sistema

Contraseñas en Unix

Las contraseñas son el mecanismo más utilizado para realizar autenticación de usuarios con el fin de permitirles o no el acceso a un sistema. La robustez de las contraseñas escogidas por los usuarios determinará en gran medida la probabilidad de que algún usuario malintencionado pueda obtener acceso a un sistema suplantando a otro usuario.

Los sistemas nunca almacenan las contraseñas en claro (sin cifrar), dado el riesgo que supone esto si algún usuario malintencionado se hace con el fichero o base de datos donde se almacenan. En su lugar, se guarda una palabra cifrada obtenida mediante la aplicación de técnicas criptográficas a la contraseña. Para ello, se escogen técnicas criptográficas sin operación inversa en las cuales es prácticamente imposible deducir la contraseña a partir de la palabra cifrada en un tiempo razonable, para que a un usuario que tenga acceso a las palabras cifradas le resulte muy difícil averiguar las contraseñas.

Los algoritmos de cifrado más habituales hoy en día en sistemas Unix son dos: uno basado en **DES** y otro basado en **MD5**. El basado en **DES** funciona sólo con contraseñas de hasta 8 caracteres y palabras aleatorias de dos caracteres. Si la contraseña tiene más de 8, se trunca. El basado en MD5 admite contraseñas bastante más largas, y las palabras aleatorias tienen hasta 8 caracteres. El sistema basado en **MD5** es más seguro y, por tanto, el preferido actualmente.

En sistemas Unix, la base de datos suele ser el fichero ***/etc/passwd***. Este fichero almacena información acerca de los usuarios. Dado que debe ser accedido por todos los usuarios, la propia palabra cifrada es también visible. Para incrementar más la seguridad, se desarrolló posteriormente el sistema de ***shadow passwords***. En este caso las palabras cifradas no se almacenan en ***/etc/passwd***, sino en ***/etc/shadow***, accesible en lectura sólo por root.

Aunque resulta prácticamente imposible invertir el algoritmo de cifrado, existen otras técnicas que permiten obtener contraseñas a partir de palabras cifradas, aprovechando que las contraseñas escogidas por los usuarios no tienen suficiente aleatoriedad. Estas técnicas se basan en probar, una tras otra, distintas contraseñas con la esperanza de que alguna de ellas sea correcta. Para ello se emplean **diccionarios de palabras (wordlists)** de distintos idiomas y listas de contraseñas empleadas frecuentemente por los usuarios.

Los administradores de sistemas deben asegurarse de que las contraseñas de los usuarios de sus sistemas sean lo suficientemente robustas como para no caer ante este tipo de ataque. Para ello, es habitual forzar para que utilicen claves complejas (longitud mínima, diferentes tipos de caracteres (mayúscula, minúscula, dígitos e incluso símbolos no alfanumérico) y también pueden atacar periódicamente las claves con estas técnicas para detectar contraseñas débiles (cuando se detecta una, se solicita al usuario que la cambie por otra más robusta).

En este apartado, aprenderá a utilizar la herramienta ***John the Ripper*** para detectar claves débiles en un sistema Unix. Aunque la práctica se centra en contraseñas Unix/Linux, estas técnicas son aplicables a otros tipos de sistemas.

Necesitará el siguiente software, disponible en la página web de la asignatura: (http://www.tlm.unavarra.es):

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

- John the Ripper (john-1.7.0.2.tar.gz)
- Fichero de passwords (passwd.1)
- Listado de palabras en castellano, diccionario (spanish.lst)

Refefencias:

Puede encontrar documentación acerca del sistema de passwords en Unix en las siguientes páginas de manual de Unix: login(1), passwd(1), passwd(5), shadow(5), crypt(3).

El programa John the Ripper (http://www.openwall.com/john/) se distribuye con documentación básica acerca de sus opciones de línea de comandos y funcionamiento.

Crackeo de contraseñas

Nota: Se realizará esta parte de la práctica en el equipo **PC SC**

En este ejercicio debe averiguar las contraseñas de los usuarios de este fichero de contraseñas ficticio (passwd.1). Échele un vistazo y verá que contiene los datos de 13 usuarios.

Utilice el programa John the Ripper para obtener las contraseñas. Aunque sin aplicar una buena estrategia, sólo caerán las contraseñas más débiles. Se propondrá una posible estrategia a seguir para obtener las contraseñas.

Para cada una de las siguientes etapas debe anotar cuánto tarda y qué claves caen. Para cada clave que caiga, piensa dónde reside su debilidad, y por qué no cayó en etapas anteriores.

Paso 0: Instalar el programa John the Ripper

Para instalar el programa debemos seguir los siguientes pasos:

*Descargue el programa en el directorio **HOME** del usuario.* Hecho esto, siga los siguientes pasos:

```
$ tar zxvf john-1.7.0.2.tar.gz
$ cd john-1.7.0.2
```

En el fichero INSTALL (directorio doc) dispone de las instrucciones para realizar la instalación.

Siga las siguientes indicaciones:

```
$ cd src
$ make clean linux-x86-any
$ export JOHN=$HOME/john-1.7.0.2/run
$ cd
```

Comprobemos si se ha instalado bien:

```
$ $JOHN/john --test
```

Paso 1: El primer intento

El primer intento consiste en hacer un ataque sencillo pero rápido, por si hay alguna clave lo suficientemente débil. Ejecute john con la opción -single.

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Para evitar volver a buscar claves que ya ha descubierto en futuras invocaciones, john guarda un fichero con dichas claves.

La ejecución del siguiente comando, le muestra las contraseñas ya obtenidas:

```
$ $JOHN/john -show passwd.1
```

Paso 2: Manos a la obra

Ahora realice un ataque utilizando el pequeño listado de palabras que utiliza john por defecto. Vuelva a ejecutar *john*, pero sin especificar la opción *-single*.

Dado que está en clase y que no dispone de mucho tiempo, puede cortar el ataque tras un tiempo razonable (unos 10 min.)

Paso 3: Buscando palabras en castellano !!

Hasta ahora se utilizaba una lista de palabras pequeña que trae john, pero ya es hora de utilizar una lista más completa. En este caso, pruebe con una de palabras en castellano (fichero spanish.lst).

Ejecute *john* utilizando la lista de palabras que se entrega. Puede tardar varios minutos, pero conviene que lo deje terminar.

Paso 4: Aplicando reglas

En el fichero de configuración *john.conf* se pueden añadir reglas para derivar nuevas palabras a partir del listado. Además de las preestablecidas, haga que genere plurales a partir de las palabras (añadiendo "s" y "es").

Ponga la siguiente regla en el fichero de configuración: *es* al principio de la sección *Wordlist mode rules.*

Ejecute *john* utilizando el diccionario y estableciendo la opción "-rules", que fuerza al programa a ejecutar todas las reglas. Córtelo al cabo de unos minutos, para no perder demasiado tiempo en este apartado.

Paso 5: Modo incremental

Es bastante fácil que las palabras cortas caigan. El modo *incremental* de *john* prueba todas las combinaciones de caracteres, comenzando por las más cortas.

Hay tres tipos de búsqueda incremental:

- alpha: Genera palabras con letras solamente, 26 letras
- digits: Genera palabras con números solamente, desde el 0 hasta el 9
- all: Genera palabras con letras, números y caracteres especiales, en total son 90 caracteres, osea se pueden imaginar lo que tardaría en terminar.

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Suele ser interesante intentar detectar primero las claves con sólo dígitos (*-i:Digits*) y después las de sólo letras (*-i:Alpha*).

Ejecute el modo incremental con las opciones *–i:Digits* y *–i:Alpha* durante unos minutos, y después corta su ejecución

Paso 6: Cuando todo lo demás falla...

Todavía no ha empleado las armas más potentes. Si a estas alturas necesita averiguar más claves, podría recurrir a los siguientes recursos, entre otros:

1. Otros diccionarios: existen muchos diccionarios en la Web que puedes utilizar, algunos de ellos especialmente grandes. También es útil utilizar diccionarios de otros idiomas, sobre todo si sabes qué idiomas habla/conocen los usuarios.
2. Modo incremental: si tienes mucha paciencia, puedes probar con la opción "-i" sin restringir a números ni letras. Las contraseñas cortas caerán.
3. Información acerca de los usuarios: algunos usuarios utilizan como contraseñas nombres de personas cercanas, el nombre de su mascota, su fecha de nacimiento o la de miembros de su familia, su número de teléfono, la matrícula de su coche, etc. Crear una nueva lista de palabras con esta información puede hacer caer este tipo de claves.

Checkpoint 2.2: Muestre al profesor las claves obtenidas e indique en qué pasos de los anteriormente descritos se obtuvieron.

3- Intrusión de equipos remotos

Búsqueda de Vulnerabilidades (Bug Tracking)

Como se vió en la práctica anterior, existen bases de datos de vulnerabilidades donde tanto los posibles atacantes como los administradores pueden comprobar si existen riesgos de seguridad en sus propios sistemas:

- http://www.cert.org
- http://nvd.nist.gov
- http://www.us-cert.gov

Estos registros almacenan información actualizada a cerca de fallos de seguridad en general y posibles amenazas, recogiendo incidencias de productos de distinta índole y procedencia.. Pero también los propios fabricantes de equipos y empresas o colectivos de desarrolladores de software mantienen y actualizan sus propios registros:

- http://www.securityfocus.com
- http://www.debian.org/security
- http://www.ubuntu.com/usn
- http://cve.mitre.org

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Por ello, un responsable de seguridad tiene que estar puesto al día y conocer estos fallos. Saber cuáles son, en qué consisten exactamente, qué consecuencias pueden tener y qué sistemas están afectados. Y lo más importante: cómo proteger los sistemas vulnerables.

Exploits

Wikipedia en www.wikipedia.org, define el término "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.

Una de las herramientas más utilizadas para realizar este tipo de ataques es Metasploit (http://www.metasploit.com), se trata de una suite para el testeo de sistemas utilizando exploits existentes para vulnerabilidades publicadas.

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

- De desbordamiento de buffer (buffer overflow)
- De condición de carrera (race condition).
- De error de formato de cadena (format string bugs).
- De Cross Site Scripting (XSS).
- De Inyección SQL (SQL Injection
- De Inyección de Caracteres (CRLF).
- De denegación del servicio (Denial of Service o DoS)
- De Inyección múltiple HTML (Multiple HTML Injection)

Las propias bases de datos de vulnerabilidades publican los exploits existentes para una vulnerabilidad concreta con el objetivo de que los administradores puedan probar si sus sistemas son vulnerables, por ejemplo Security Focus (http://www.securityfocus.com). Además existen otras páginas de recopilación de exploits como Milw0rm (http://www.milw0rm.com/).

Cuando no existe una solución "conocida" para una vulnerabilidad, pero si se conoce como explotarla, se les conoce como "vulnerabilidades 0 days".

Escalado de privilegios

Nota: Realizará este apartado en los equipos **PC-SC y PC A.** En PC-SC configurará su propia máquina virtual con Windows 2000 Server para ser atacada por otro grupo de prácticas. Desde PC A lanzará el ataque contra una máquina virtual de otro grupo de prácticas. Para ello, lo primero que debe hacer, en su PC A, es configurar una tarjeta de red con la ip 10.3.17.armario/20 y añadir a la tabla de rutas una ruta por defecto al router del laboratorio 10.3.16.1. Si además quiere poder navegar desde PC A, tendrá que configurar su servidor de nombres, para ello:

```
echo nameserver 10.1.1.193 > /etc/resolv.conf.
```

Y no se olvide conectar su PC A a la red del laboratorio.

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

El *ataque remoto* que va a realizar, a un sistema Windows 2000 Server, se vale de una vulnerabilidad conocida,. Se trata de una vulnerabilidad de desbordamiento de buffer detectada y anunciada en el año 2003 (Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability). Esta vulnerabilidad fue utilizada por el virus Blaster para instalar un gusano en el equipo y así propagarse. Para más información sobre el virus Blaster consulte el "eEye Digital Security".

Datos para la realización del ataque:

Disponen de una máquina virtual Windows 2000 Server(sin Service Pack instalado) alojada en /opt3/varios/compartir/Windows2000Server. Descargue la VM(*Windows2000Server*) en su directorio tmp(local) de prácticas (/tmp/**ssi**xy) de su PC-SC.

Para ello teclee la siguiente orden tal y como aparece a continuación:

`$ cp /opt3/varios/compartir/Windows2000Server/*.*  /tmp/$USER`

Espere un par de minutos hasta que se copie su máquina virtual y a continuación láncela mediante:

`$ lanza-vmware.sh /tmp/$USER /Windows2000Server.vmx`

Arranque su VM e inicie sesión como usuario "administrador" y contraseña "administrador". *Cambie su contraseña de "administrador" y asegúrese de que ya no puede entrar con la antigua.*

Configuren su VM con la IP: **`10.1.1.(78+armario)/24`**. A continuación cierren su sesión para dejar la VM bloqueda y disponible para ser atacada por cualquiera de sus compañeros.

Tarea 1. Estudiar la vulnerabilidad

Compruebe si el sistema Windows 2000 Server(sin Service Pack instalado) es vulnerable a la vulnerabilidad DCOM RPC Interface Buffer Overrun Vulnerability (busque la vulnerabilidad en Security Focus)

Tarea 2. Existencia de un exploit para dicha vulnerabilidad

Compruebe si existe un exploit para la vulnerabilidad. Si es así descárguelo y ejecútelo. Habitualmente los exploits se publican en código fuente (lenguaje C) así que será necesario primero realizar la compilación del exploit utilizando un compilador de C (gcc : sintaxis: gcc programa.c -o programa).

Nota: Algunos de los programas publicados crean un ejecutable para Windows y otros para equipos Unix/Linux. Una forma sencilla de comprobarlo es observar si el programa C tiene la entrada siguiente: #include <windows.h>

Tarea 3. Ejecución del exploit

Desde PC A, localice una máquina disponible, que no sea la suya, dentro del rango `10.1.1.(79-92)/24`

Para ello, utilice las herramientas que ha aprendido hasta ahora. Se valorará la detección de la máquina(toda la información que pueda extraer de ella) y su vulnerabilidad.

Ejecute el exploit y observe que obtiene una shell de Windows que muestra el siguiente prompt: C:\WINNT\SYSTEM32> El exploit permitió inyectar una línea de comandos en el servidor, la cual se puede operar directamente. De esta manera, se tiene acceso al disco duro del servidor atacado, para consultar información dentro del mismo o ejecutar comandos con privilegios. Compruébelo ejecutando comandos que muestran información del sistema Windows:

IPCONFIG, HOSTNAME, VER, NET USER, NET USER Administrador

Nota: El usuario con el que está conectado es la cuenta LOCAL SYSTEM, se trata de la cuenta más privilegiada del sistema, más incluso que la cuenta Administrador.

Tarea 4. Aprovechar la vulnerabilidad

Debido a que no conoce un usuario de acceso al sistema va a crear un nuevo usuario en el equipo windows y va a asignarle privilegios de administrador del sistema.

Los comandos para hacerlo son:

NET USER nombre contraseña /ADD

NET LOCALGROUP Administradores nombre_usuario /ADD

Tarea 5. Comprobar el acceso con el nuevo usuario

Realice otra vez una conexión, desde su PC SC(TLMxy), utilizando el programa rdesktop e intente entrar con el usuario anteriormente creado. rdesktop se conecta mediante el protocolo RDP a los equipos Windows 2000 o superior y ofrece el acceso remoto gráfico (Terminal Service de Microsoft Windows). El comando para hacerlo es el siguiente:

$ rdesktop -g 80% <Dirección IP>

Una forma de verificar que realmente es administrador del equipo es comprobar que podemos apagar o reiniciar el equipo (sólo los administradores pueden hacerlo en un equipo Windows 2000 Server). REINICIE el equipo(VM) (*ojo, no lo apague*) y vuelva a entrar con el usuario que creó anteriormente.

Checkpoint 2.3: Muestre al profesor que ha obtenido privilegios administrativos y que ha podido acceder al equipo remoto con un usuario.

¿Sabría explicar en qué consiste la política de seguridad conocida como full disclosure y cuáles son sus ventajas e inconvenientes.¿Cómo se conoce a la política que sigue la filosofía contraria?

Contramedidas

¿Qué puede hacer un administrador para asegurar el sistema? Al igual que se publican las vulnerabilidades y los exploits, así como herramientas para comprobar si nuestros sistemas son vulnerables, también se publican las medidas que tienen que seguir los administradores para proteger sus sistemas ante dichas vulnerabilidades.

Compruebe cómo el sistema deja de ser vulnerable a dicho exploit. Para ello debe instalar el Service Pack 2 de Windows 2000 sobre el sistema, el service pack está descargado en la carpeta C:\GSRO. Aplíquelo en la máquina objeto de su ataque.

Checkpoint 2.4: Instale el Service Pack 2 para Windows 2000 y reinicie el equipo(VM) cuando finalice. Una vez hecho, vuelva a ejecutar el exploit. ¿Funciona ahora? ¿Obtienes esta vez privilegios administrativos?

Fin de la práctica

Conectado con un usuario administrador (el que anteriormente creó) apague la máquina que le corresponde.