academia madesyp

HONEYPOT III – Servicios emulados con Valhalla Honeypot

Popularidad:	*2*
Simplicidad:	*10*
Impacto:	*9*
Nivel de Riesgo:	***4***

Objetivo:

Usar un honeypot con varios servicios de interacción media

Herramientas necesarias:

Valhala honeypot (http://sourceforge.net/projects/valhalahoneypot/)
Netcat para Windows (http://www.securityfocus.com/tools/139)
Nmap para Windows (http://nmap.org/download.html)
Metaesploit para Windows (http://www.metasploit.com/download/)
John the ripper (http://www.openwall.com/john/)

Montaje del Honeypot:

Una vez descargado *Valhala*, bastará con descomprimir y ejecutar el fichero `honeypot.exe`

A continuación, pulsaremos en el botón "`Options`" y podremos definir dónde enviar las alertas por email, consola remota registro, etc. e incluso la posibilidad de abrir más puertos de los que incluye por defecto.

Haciendo clic en "`Server config`", vamos a definir los servicios de "`Web Server`" (80), "`Finger Server`" (79), "`POP3 Server`" (110), "`SMTP Server`" (25) y "`Daytime Server`" (37) al objeto de continuar con la serie de prácticas sobre los honeypots.

En WEB SERVER, indicaremos las siguientes opciones dejando el resto por defecto:

```
Folder: c:\HoneyBOT\html
Index page: iisstart.asp
```

En FINGER SERVER dejaremos las opciones en inglés o cambiaremos algunas a castellano en función de la localización del honeypot. Igualmente procederemos con el mensaje existente para el servidor POP3. El resto de servicios, los dejaremos conforme se encuentran configurados por defecto.

Aprovechando el directorio proporcionado por *HoneyBOT* en la anterior práctica, crearemos un directorio para alojar varios ficheros de usuarios y contraseñas de las extensiones de *frontpage* para hacer nuestro honeypot más creíble para el atacante.

```
C:\HONEYPOT>md c:\HoneyBOT\html\_vti_pvt
C:\HONEYPOT>cd c:\HoneyBOT\html\_vti_pvt
```

Fichero "service.pwd":

```
# -FrontPage-
johnh:nXbxRcm1Jv7UU
```

Fichero "authors.pwd"

```
# -FrontPage-
s4ur0n:.1jyxcSAFmDkQ
```

Fichero "administrators.pwd":

```
# -FrontPage-
admin:LneM3OJlC.mRw
```

NOTA

A dicho directorio _vti_pvt y puesto que trabajamos con un Windows 7, para que no lo proteja "por defecto", tendremos que asignarle permisos al grupo TODOS de MODIFICACION.

Una vez que tengamos todo correctamente configurado, pulsaremos el botón "Monitoring" para comenzar a registrar las actividades en la consola.

Ataques:

Escaneo con *nmap* para comprobar los que hemos abierto (por razones de tiempo) aunque se debería de escanear la totalidad de los puertos:

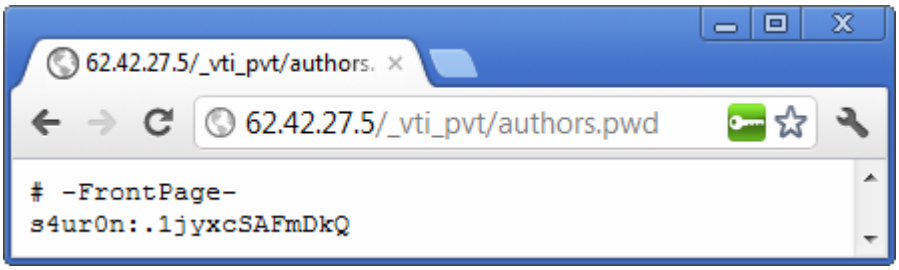
```
C:\HONEYPOT>nmap -p 25,37,79,80,110 -v -sT -sV -S 213.27.5.12 62.42.27.5
```

Observamos que algunos servicios son sobradamente conocidos (como el POP3 que indica que se trata de un *Openwall popa3d*). Sin embargo, no nos muestra cabeceras del resto, por lo que

procedemos con la navaja suiza *netcat* a realizar simples conexiones en búsqueda de posibles patrones.

```
C:\HONEYPOT>nc 62.42.27.5 25
220 Sendmail 8.11.13
QUIT
221 Signing Off
```

Comenzaremos con el servidor de HTTP. En éste caso, vamos a emplear directamente un navegador.



Copiaremos en un fichero de texto las parejas de "`usuario : contraseña_encriptada`" y mediante *John the Ripper* procederemos a intentar descubrir la contraseña que tiene, ya que se trata de las extensiones de *Frontpage* que lo hacen con un simple DES (idéntica a CRYPT de GNU/Linux)

```
C:\HONEYPOT>echo s4ur0n:1jyxcSAFmDkQ > fichero.txt
C:\HONEYPOT>john fichero.txt
...
C:\HONEYPOT>john -show fichero.txt
s4ur0n:n*******
1 password hash cracked, 0 left
```

Luego, ahora desde un *Frontpage* podremos intentar acceder al sitio web empleando el usuario y password que hemos "encontrado".

Probemos ahora con el servicio *finger* aprovechando la utilidad cliente que incorpora Windows 7 para poder buscar los usuarios del sistema que tiene.

```
C:\HONEYPOT>finger usuario@62.42.27.5
```

Vemos que no se obtiene respuesta, por lo que vamos a proceder a realizar un pequeño script en el shell para probar con una lista de usuarios para ver si existen en el sistema. Le llamaremos "fingeruser.cmd"

```
@echo off
cls

if "%1"=="" goto noip
if "%2"=="" goto nofile

for /F %%l in (%2) do (
       echo ------------------------------------
       echo Usuario: %%l
       finger %%l@%1 )
goto fin

:noip
echo Uso: %0 IP fichero_usuarios
goto fin

:nofile
echo Uso: %0 %1 fichero_usuarios

:fin
```

Y lo lanzaremos contra el servidor:

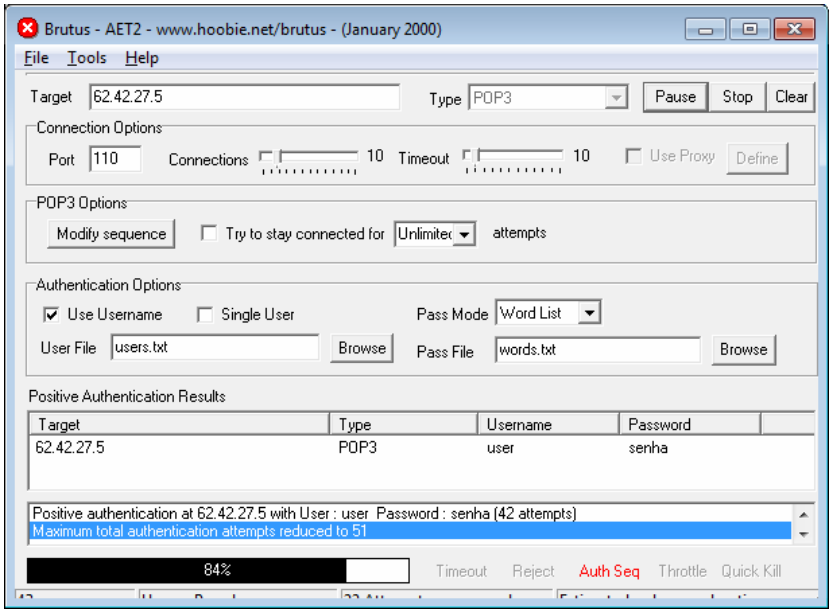
```
C:\HONEYPOT>fingeruser 62.42.27.5 common-users.txt | more
```

Habremos comprobado que existen los usuarios *admin*, *root*, *guest* y *www* que posteriormente probaremos en otros ataques.

Vamos a intentar acceder al servidor POP3 para recuperar el correo de algún usuario por si pusiera algún dato interesante. Lo haremos de nuevo con la herramienta *brutus* con la lista de la práctica anterior.

Es conveniente para un entorno real de pentesting hacer clic en el botón "Modify sequence" para si es necesario, modificar las "palabras clave" que devuelve el servidor y/o las respuestas con los correspondientes códigos para poder ajustarlos a los valores del servidor que tengamos que auditar.

Por defecto, viene instalado con los parámetros de POP3 estándar según la RFC1939



Ya hemos obtenido un usuario y password. Vamos ahora a "leer" su correo online para evitar hacerlo con un gestor que descargue los mensajes a la máquina en la que nos encontramos y los borre del servidor. Para ello, emplearemos la universal herramienta *netcat* otra vez de nuevo.

```
C:\HONEYPOT>nc 62.42.27.5 110
+OK
USER user
+OK Password required
PASS senha
+OK Login OK
LIST
+OK 1 150
.
RETR 1
+OK 200 octects
From: mflavio2k@yahoo.com.br
...
QUIT
+OK Closing communication channel
```

Probemos ahora a ver el servidor de email si admite RELAY, puesto que en nuestros propósitos, entra la "friolera" idea de enviar aproximadamente 3 millones de emails. El problema es que nuestro proveedor no nos deja hacerlo, además requiere que hagamos logon antes de enviar (POP before SMTP) y por supuesto, como somos *spammers* no queremos dejar nuestro verdadero rastro.

```
C:\HONEYPOT>nc 62.42.27.5 25
Heimdall [62.42.27.5] 25 (smtp) open
220 Sendmail 8.11.13
HELO publicidad.miservidordespam.com
250 Hello publicidad.miservidordespam.com
MAIL FROM: noreply@nospam.com
250 noreply@nospam.com Address Okay
RCPT TO: s4ur0n@navajanega.com
250 s4ur0n@madesyp.com Address Okay
DATA
354 Start mail input; end with <CRLF>.<CRLF>
Subject: [publicidad] En Albacete hay invasores los martes
Hola!

¿Sabías que en Albacete los martes ponen un mercado en “la Feria” que le
dicen “los invasores”?

Hay ropa, animales, plantas, calzado, juguetes, fruta... vamos que “hay de
tó”.
.
250 Message Sent
QUIT
221 Signing Off
```

Podremos imaginarnos lo fácil que lo tienen los spammers con muy poco de programación para modificar el campo *RCPT TO:* y enviarlo a los 3 millones de personas generando un fichero y redirigiéndolo a un servidor de relay:

```
C:\HONEYPOT>nc 62.42.27.5 25 < spam.txt
```

Revisión de resultados:

Detendremos el honeypot instalado con el botón de cerrar para poder monitorizar las actividades maliciosas.

NOTA

Para desinstalar completamente Valhala, debido a que no incluye ningún desinstalador, tendremos que editar el registro de Windows y buscar la clave “Valhala”. Normalmente bajo HLKM\...\Software\Valhala. Además, si entramos en la subclave Config\Forms\Honeypot, veremos la configuración de los servicios que hemos configurado, ya que cada vez que finalicemos el programa, guardará los cambios de dichas entradas. Además, si no existiera la clave “Valhala” cuando se inicia el programa, se creará automáticamente la primera vez que cerremos el programa.