Metasploit v5.0.52-dev ]

+ -- --=[ 1929 exploits - 1079 auxiliary - 332 post ]

+ -- --=[ 556 payloads - 45 encoders - 10 nops ]

+ -- --=[ 7 evasion

Comenzamos haciendo un escaneo con nmap a un Windows server 2003, para detectar si tiene abierto el puerto TCP 3389 y el puerto UDP 3389 por defecto que viene de forma predeterminada, en el servidor escucha en Microsoft el cual se refiere actualmente a su software de cliente RDP oficial como Remote Desktop Connection, El protocolo es una extensión ITU-T T.128.del protocolo para compartir aplicaciones.

En este video vamos a demostrar cómo utilizar un módulo auxiliar desde metasploit, para hacer un ataque DOS, al servidor, en Windows server 2003,

Comenzamos escaneando la ip.

Nmap 192.168.52.222

root@computaxion:~# nmap 192.168.52.222

Starting Nmap 7.80 ( https://nmap.org )

Nmap scan report for 192.168.52.222

Host is up (0.00059s latency).

Not shown: 975 closed ports

PORT STATE SERVICE

21/tcp open ftp

25/tcp open smtp

53/tcp open domain

80/tcp open http

88/tcp open kerberos-sec

135/tcp open msrpc

139/tcp open netbios-ssn

389/tcp open ldap

443/tcp open https

445/tcp open microsoft-ds

464/tcp open kpasswd5

593/tcp open http-rpc-epmap

636/tcp open ldapssl

1025/tcp open NFS-or-IIS

1027/tcp open IIS

1037/tcp open ams

1038/tcp open mtqp

1040/tcp open netsaint

1050/tcp open java-or-OTGfileshare

1059/tcp open nimreg

1433/tcp open ms-sql-s

3268/tcp open globalcatLDAP

3269/tcp open globalcatLDAPssl

3306/tcp open mysql

3389/tcp open ms-wbt-server

MAC Address: 00:0C:29:EF:CD:60 (VMware)

Una vez encontrado el puerto abierto invocamos la herramienta metasploit con el comando msfconsole, recuerden antes de activar la base de datos. El servicio postgresql

Luego vamos a buscar el modulo auxiliar con el id ms12\_020