TonyTiger_THM

Enumuration

port 80 has only basic stuff and blog

To get tony flag we enumurate this port

as source code and posts doesnt have the flag i downloaded the pictures there and checked them

a picture had the tony flag when i string it

port 8080 is the managing web app so we enumrate that. We see that jboss 3.0.0 is vulnerable to a java seriliaztion rce

Nmap

```
ORT      STATE SERVICE      VERSION
22/tcp   open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d6:97:8c:b9:74:d0:f3:9e:fe:f3:a5:ea:f8:a9:b5:7a (DSA)
|   2048 33:a4:7b:91:38:58:50:30:89:2d:e4:57:bb:07:bb:2f (RSA)
|   256 21:01:8b:37:f5:1e:2b:c5:57:f1:b0:42:b7:32:ab:ea (ECDSA)
|_  256 f6:36:07:3c:3b:3d:71:30:c4:cd:2a:13:00:b5:25:ae (ED25519)
80/tcp   open  http         Apache httpd 2.4.7 ((Ubuntu))
|_http-generator: Hugo 0.66.0
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Tony&#39;s Blog
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
|     xpp5
|     #http://thm-java-deserial.home:8083/q
|     org.jnp.server.NamingServer_Stub
|     java.rmi.server.RemoteStub
|     java.rmi.server.RemoteObject
|     xpwA
|     UnicastRef2
|_    thm-java-deserial.home
3873/tcp open  java-object Java Object Serialization
4446/tcp open  java-object Java Object Serialization
4712/tcp open  msdtc        Microsoft Distributed Transaction Coordinator (error)
4713/tcp open  pulseaudio?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, GenericLines, GetRequest, Help, JavaRMI, Kerberos, LANDesk-RC,
LDAPBindReq, LDAPSearchReq, LPDString, NCP, NULL, NotesRPC, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq,
TLSSessionReq, TerminalServer, TerminalServerCookie, WMSRequest, X11Probe, afp, giop, ms-sql-s, oracle-tns:
|_    126a
5445/tcp open  smbdirect?
5455/tcp open  apc-5455?
5500/tcp open  hotline?
| fingerprint-strings:
|   DNSStatusRequestTCP:
|     CRAM-MD5
|     NTLM
|     GSSAPI
|     DIGEST-MD5
|     thm-java-deserial
```

```
|   GenericLines, NULL:
|     CRAM-MD5
|     NTLM
|     DIGEST-MD5
|     GSSAPI
|     thm-java-deserial
|   GetRequest, SMBProgNeg, TLSSessionReq:
|     GSSAPI
|     DIGEST-MD5
|     NTLM
|     CRAM-MD5
|     thm-java-deserial
|   HTTPOptions:
|     NTLM
|     GSSAPI
|     CRAM-MD5
|     DIGEST-MD5
|     thm-java-deserial
|   Help:
|     DIGEST-MD5
|     GSSAPI
|     NTLM
|     CRAM-MD5
|     thm-java-deserial
|   Kerberos:
|     GSSAPI
|     DIGEST-MD5
|     CRAM-MD5
|     NTLM
|     thm-java-deserial
|   RPCCheck:
|     NTLM
|     CRAM-MD5
|     GSSAPI
|     DIGEST-MD5
|     thm-java-deserial
|   RTSPRequest:
|     DIGEST-MD5
|     CRAM-MD5
|     NTLM
|     GSSAPI
|     thm-java-deserial
|   SSLSessionReq:
|     CRAM-MD5
|     GSSAPI
|     NTLM
|     DIGEST-MD5
|     thm-java-deserial
|   TerminalServerCookie:
|     GSSAPI
|     CRAM-MD5
|     NTLM
|     DIGEST-MD5
|_    thm-java-deserial
5501/tcp open  tcpwrapped
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-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Welcome to JBoss AS
8083/tcp open  http        JBoss service httpd
|_http-title: Site doesn't have a title (text/html).
5 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=7.91%I=7%D=5/2%Time=608F6788%P=x86_64-pc-linux-gnu%r(NUL
```

```
SF:L,17B,"\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\x08objByte
SF:sq\0~\0\x01xpp5\xafFur\0\x02\[B\xac\xf3\x17\xf8\x06\x08T\xe0\x02\0\0xp\
SF:0\0\x004\xac\xed\0\x05t\0#http://thm-java-deserial\.home:8083/q\0~\0\0q
SF:\0~\0\0uq\0~\0\x03\0\0\0\xcd\xac\xed\0\x05sr\0\x20org\.jnp\.server\.Nam
SF:ingServer_Stub\0\0\0\0\0\0\0\x02\x02\0\0xr\0\x1ajava\.rmi\.server\.Remo
SF:teStub\xe9\xfe\xdc\xc9\x8b\xe1e\x1a\x02\0\0xr\0\x1cjava\.rmi\.server\.R
SF:emoteObject\xd3a\xb4\x91\x0ca3\x1e\x03\0\0xpwA\0\x0bUnicastRef2\0\0\x16
SF:thm-java-deserial\.home\0\0\x04J\x92L\xb4T`\xc3\x9d\xbc\x9d\xae9\xcb\0\
SF:0\x01y0&\xd3\xae\x80\x02\0x");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3873-TCP:V=7.91%I=7%D=5/2%Time=608F678E%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4,"\xac\xed\0\x05");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port4446-TCP:V=7.91%I=7%D=5/2%Time=608F678E%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4,"\xac\xed\0\x05");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port4713-TCP:V=7.91%I=7%D=5/2%Time=608F678E%P=x86_64-pc-linux-gnu%r(NUL
SF:L,5,"126a\n")%r(GenericLines,5,"126a\n")%r(GetRequest,5,"126a\n")%r(RTS
SF:PRequest,5,"126a\n")%r(RPCCheck,5,"126a\n")%r(DNSVersionBindReqTCP,5,"1
SF:26a\n")%r(DNSStatusRequestTCP,5,"126a\n")%r(Help,5,"126a\n")%r(SSLSessi
SF:onReq,5,"126a\n")%r(TerminalServerCookie,5,"126a\n")%r(TLSSessionReq,5,
SF:"126a\n")%r(Kerberos,5,"126a\n")%r(SMBProgNeg,5,"126a\n")%r(X11Probe,5,
SF:"126a\n")%r(FourOhFourRequest,5,"126a\n")%r(LPDString,5,"126a\n")%r(LDA
SF:PSearchReq,5,"126a\n")%r(LDAPBindReq,5,"126a\n")%r(SIPOptions,5,"126a\n
SF:")%r(LANDesk-RC,5,"126a\n")%r(TerminalServer,5,"126a\n")%r(NCP,5,"126a\
SF:n")%r(NotesRPC,5,"126a\n")%r(JavaRMI,5,"126a\n")%r(WMSRequest,5,"126a\n
SF:")%r(oracle-tns,5,"126a\n")%r(ms-sql-s,5,"126a\n")%r(afp,5,"126a\n")%r(
SF:giop,5,"126a\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5500-TCP:V=7.91%I=7%D=5/2%Time=608F678E%P=x86_64-pc-linux-gnu%r(NUL
SF:L,4B,"\0\0\0G\0\0\x01\0\x03\x04\0\0\0\x03\x03\x04\0\0\0\x02\x01\x08CRAM
SF:-MD5\x01\x04NTLM\x01\nDIGEST-MD5\x01\x06GSSAPI\x02\x11thm-java-deserial
SF:")%r(GenericLines,4B,"\0\0\0G\0\0\x01\0\x03\x04\0\0\0\x03\x03\x04\0\0\0
SF:\x02\x01\x08CRAM-MD5\x01\x04NTLM\x01\nDIGEST-MD5\x01\x06GSSAPI\x02\x11t
SF:hm-java-deserial")%r(GetRequest,4B,"\0\0\0G\0\0\x01\0\x03\x04\0\0\0\x03
SF:\x03\x04\0\0\0\x02\x01\x06GSSAPI\x01\nDIGEST-MD5\x01\x04NTLM\x01\x08CRA
SF:M-MD5\x02\x11thm-java-deserial")%r(HTTPOptions,4B,"\0\0\0G\0\0\x01\0\x0
SF:3\x04\0\0\0\x03\x03\x04\0\0\0\x02\x01\x04NTLM\x01\x06GSSAPI\x01\x08CRAM
SF:-MD5\x01\nDIGEST-MD5\x02\x11thm-java-deserial")%r(RTSPRequest,4B,"\0\0\
SF:0G\0\0\x01\0\x03\x04\0\0\0\x03\x03\x04\0\0\0\x02\x01\nDIGEST-MD5\x01\x0
SF:8CRAM-MD5\x01\x04NTLM\x01\x06GSSAPI\x02\x11thm-java-deserial")%r(RPCChe
SF:ck,4B,"\0\0\0G\0\0\x01\0\x03\x04\0\0\0\x03\x03\x04\0\0\0\x02\x01\x04NTL
SF:M\x01\x08CRAM-MD5\x01\x06GSSAPI\x01\nDIGEST-MD5\x02\x11thm-java-deseria
SF:l")%r(DNSStatusRequestTCP,4B,"\0\0\0G\0\0\x01\0\x03\x04\0\0\0\x03\x03\x
SF:04\0\0\0\x02\x01\x08CRAM-MD5\x01\x04NTLM\x01\x06GSSAPI\x01\nDIGEST-MD5\
SF:x02\x11thm-java-deserial")%r(Help,4B,"\0\0\0G\0\0\x01\0\x03\x04\0\0\0\x
SF:03\x03\x04\0\0\0\x02\x01\nDIGEST-MD5\x01\x06GSSAPI\x01\x04NTLM\x01\x08C
SF:RAM-MD5\x02\x11thm-java-deserial")%r(SSLSessionReq,4B,"\0\0\0G\0\0\x01\
SF:0\x03\x04\0\0\0\x03\x03\x04\0\0\0\x02\x01\x08CRAM-MD5\x01\x06GSSAPI\x01
SF:\x04NTLM\x01\nDIGEST-MD5\x02\x11thm-java-deserial")%r(TerminalServerCoo
SF:kie,4B,"\0\0\0G\0\0\x01\0\x03\x04\0\0\0\x03\x03\x04\0\0\0\x02\x01\x06GS
SF:SAPI\x01\x08CRAM-MD5\x01\x04NTLM\x01\nDIGEST-MD5\x02\x11thm-java-deseri
SF:al")%r(TLSSessionReq,4B,"\0\0\0G\0\0\x01\0\x03\x04\0\0\0\x03\x03\x04\0\
SF:0\0\x02\x01\x06GSSAPI\x01\nDIGEST-MD5\x01\x04NTLM\x01\x08CRAM-MD5\x02\x
SF:11thm-java-deserial")%r(Kerberos,4B,"\0\0\0G\0\0\x01\0\x03\x04\0\0\0\x0
SF:3\x03\x04\0\0\0\x02\x01\x06GSSAPI\x01\nDIGEST-MD5\x01\x08CRAM-MD5\x01\x
SF:04NTLM\x02\x11thm-java-deserial")%r(SMBProgNeg,4B,"\0\0\0G\0\0\x01\0\x0
SF:3\x04\0\0\0\x03\x03\x04\0\0\0\x02\x01\x06GSSAPI\x01\nDIGEST-MD5\x01\x04
SF:NTLM\x01\x08CRAM-MD5\x02\x11thm-java-deserial");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.10 - 3.13 (94%), Linux 5.4 (94%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Linux 3.2 - 3.16 (92%), Linux 3.2 - 3.5 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OSs: Linux, Windows; CPE: cpe:/o:linux:linux_kernel, cpe:/o:microsoft:windows

TRACEROUTE (using port 5445/tcp)
HOP RTT       ADDRESS
1   198.49 ms 10.4.0.1
2   ... 3
```

4 491.41 ms 10.10.47.16

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 218.30 seconds

SSH:22

HTTP:80

gobuster

/.hta (Status: 403) [Size: 282]
/.htaccess (Status: 403) [Size: 287]
/.htpasswd (Status: 403) [Size: 287]
/categories (Status: 301) [Size: 314] [--> http://10.10.47.16/categories/]
/css (Status: 301) [Size: 307] [--> http://10.10.47.16/css/]
/fonts (Status: 301) [Size: 309] [--> http://10.10.47.16/fonts/]
/images (Status: 301) [Size: 310] [--> http://10.10.47.16/images/]
/index.html (Status: 200) [Size: 16608]
/js (Status: 301) [Size: 306] [--> http://10.10.47.16/js/]
/page (Status: 301) [Size: 308] [--> http://10.10.47.16/page/]
/posts (Status: 301) [Size: 309] [--> http://10.10.47.16/posts/]
/server-status (Status: 403) [Size: 291]
/sitemap.xml (Status: 200) [Size: 661]
/tags (Status: 301) [Size: 308] [--> http://10.10.47.16/tags/]

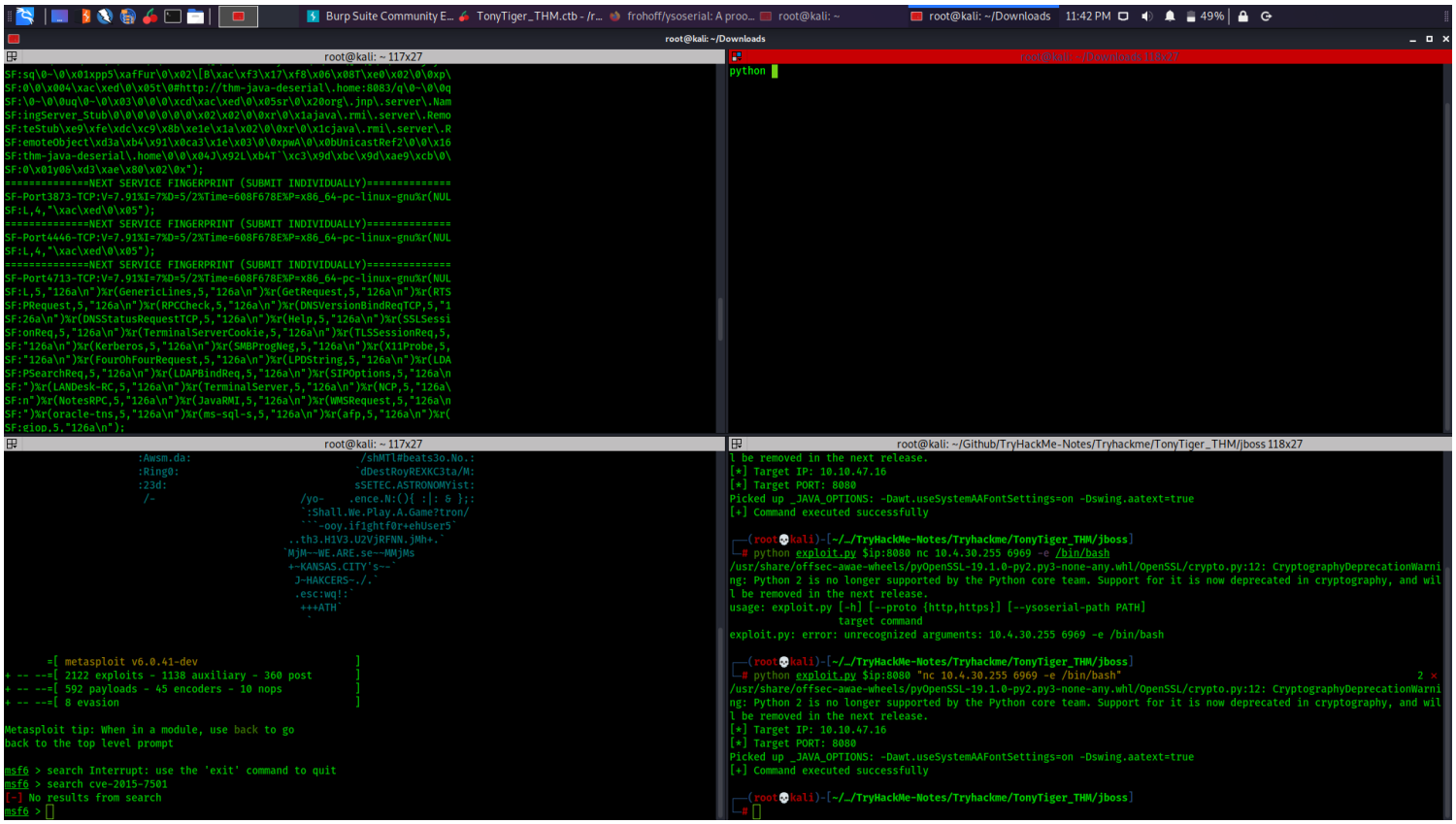
HTTP:8080

THis is the maanaging web app and is uisng jboss web manager

jboss 3.0.0 is vulnerable to a java seriliazation rce attack

we download its exploit and a ysoserial.jar file which is required for proper serialization and execution of our payload

Nowwe get a reverse shell with this rce



#

Exploitation

we download its exploit and a ysoserial jar file alongside it to properly deserilaize the code

No we have rce and we get a reverse shell

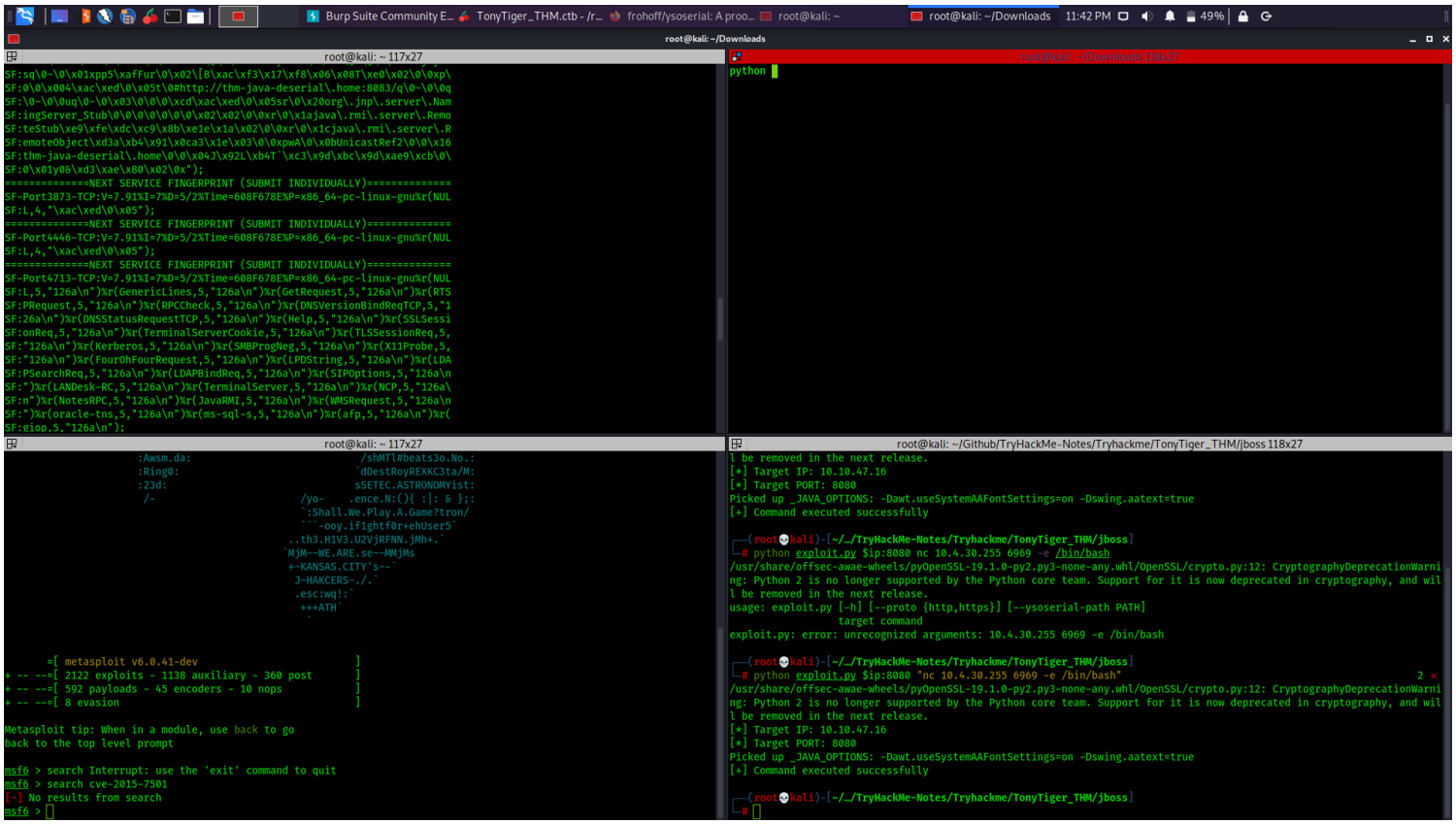
Java Sereliazation

THis is the maanaging web app and is uisng jboss web manager

jboss 3.0.0 is vulnerable to a java seriliazation rce attack

we download its exploit and a ysoserial.jar file which is required for proper serialization and execution of our payload

Nowwe get a reverse shell with this rce



#

PostExploitation

we see a note in jboss home directory and we ge jboss ssh password which is likeaboss

Then we sudo -l as jboss and we can use find with sudo privelege so we spawn a root by escaping shell sequence

we get a root file and a base64 encoded value

we decode it and get a BC77AC072EE30E3760806864E234C7CF

the flag is **zxcvbnm123456789**

Loot

Credentials

User creds

jboss:likeaboss

Flags

tony flag

THM{Tony_Sure_Loves_Frosted_Flakes}

jboss flag

THM{50c10ad46b5793704601ecdad865eb06}

root flag

zxcvbnm123456789