INITIAL SHELL:

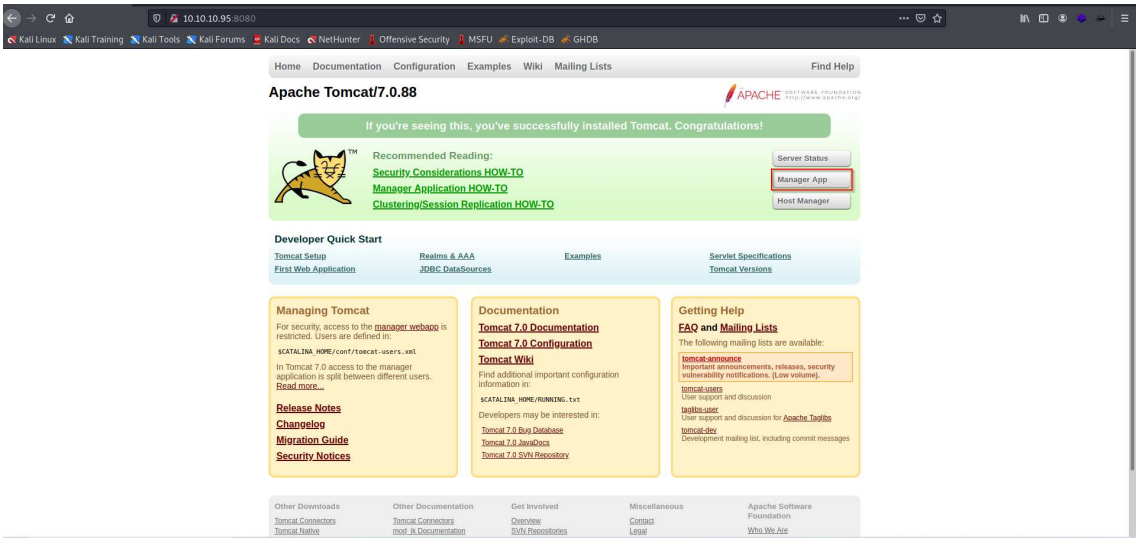
NMAP Scan.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -A -Pn 10.10.10.95
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-05 05:35 EDT
Stats: 0:11:09 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 50.30% done; ETC: 05:57 (0:11:02 remaining)
Stats: 0:11:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 50.51% done; ETC: 05:58 (0:11:19 remaining)
```

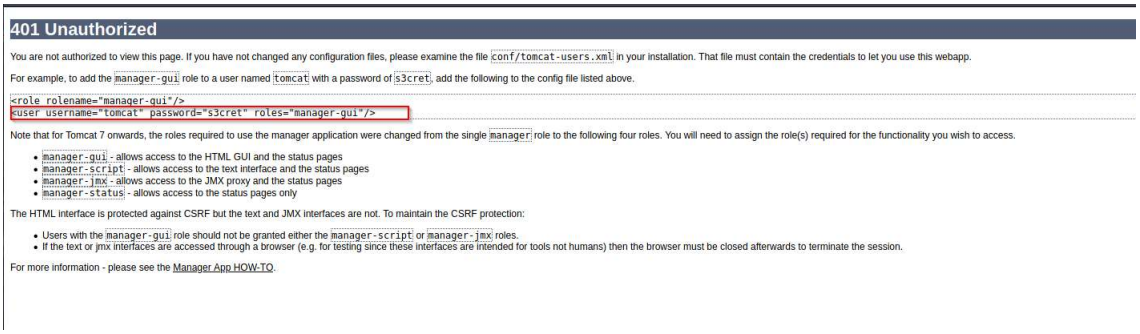
```
Nmap scan report for 10.10.10.95
Host is up (0.27s latency).
Not shown: 65534 filtered ports
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15155.89 seconds
```

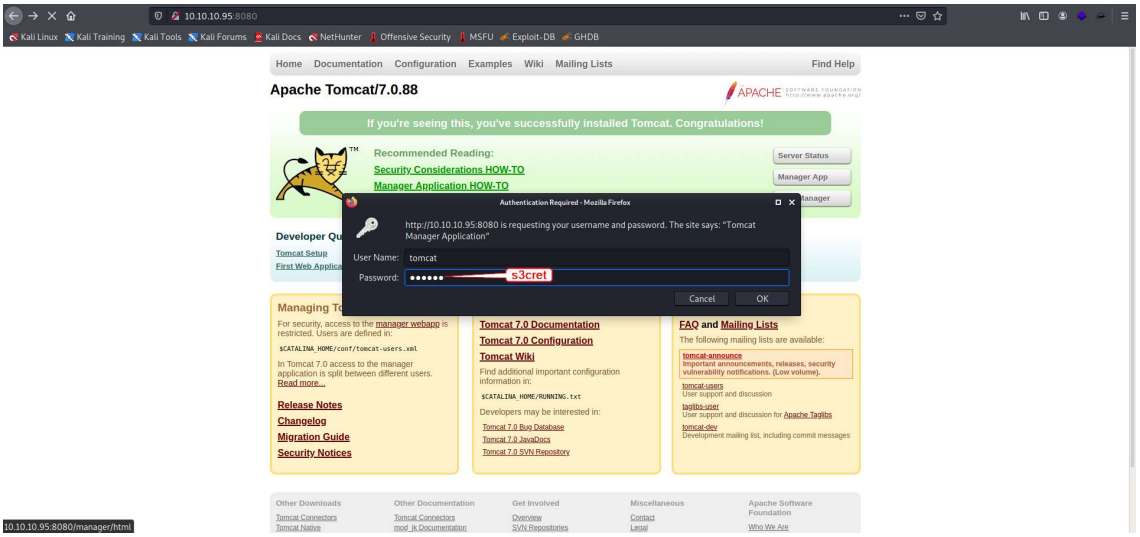
Navigating to port 8080 in a web browser. Apache Tomcat 7.0.88 is running and there is a button to access Manager App.

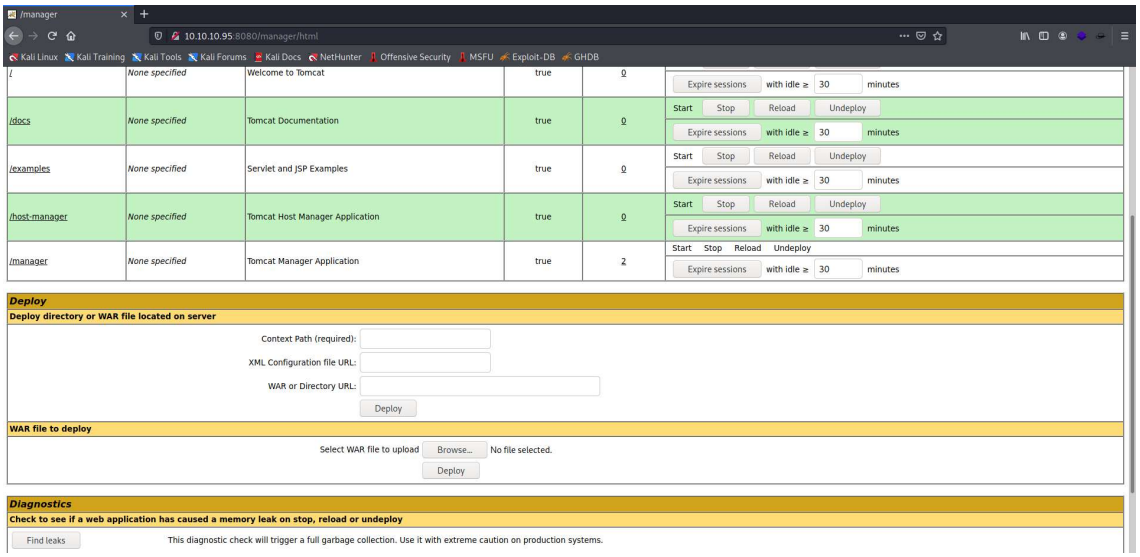


After entering wrong credentials in the popup, there is a “401 Unauthorized” page displayed revealing possible default credentials.

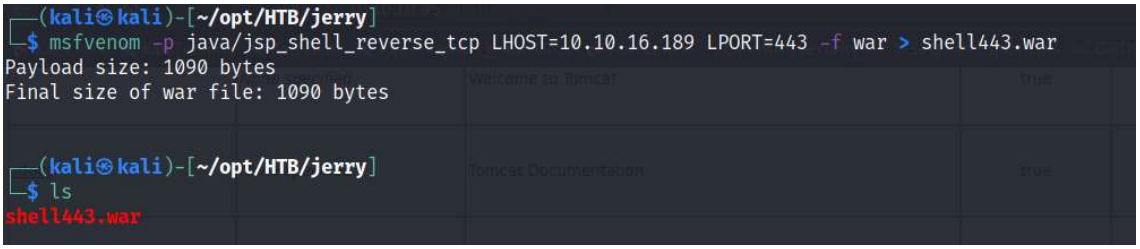


After clicking “Manager App” button and entering the above credentials, the Manager App page is now accessible.

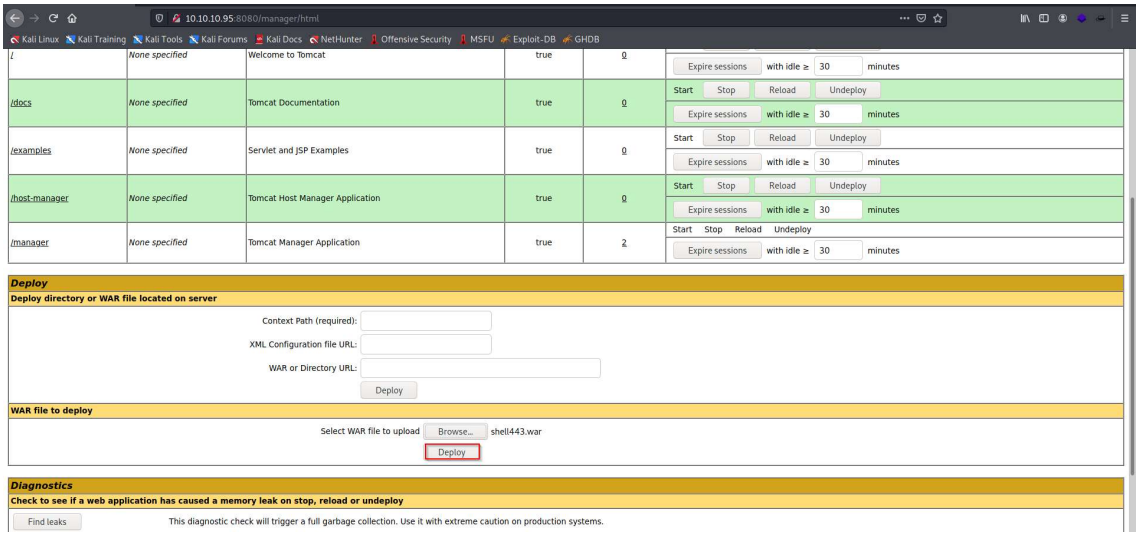




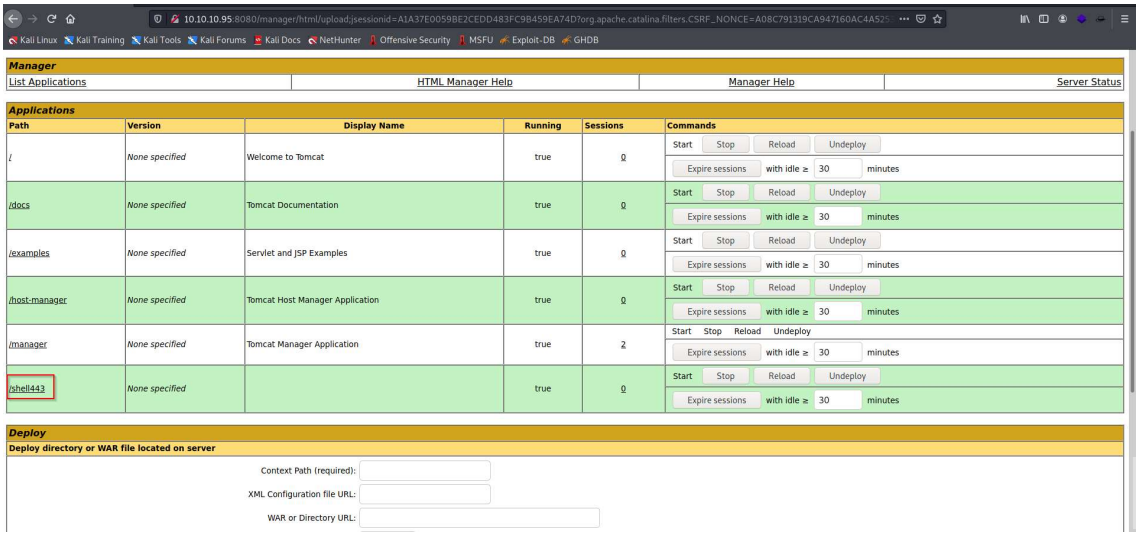
Creating a malicious war file.



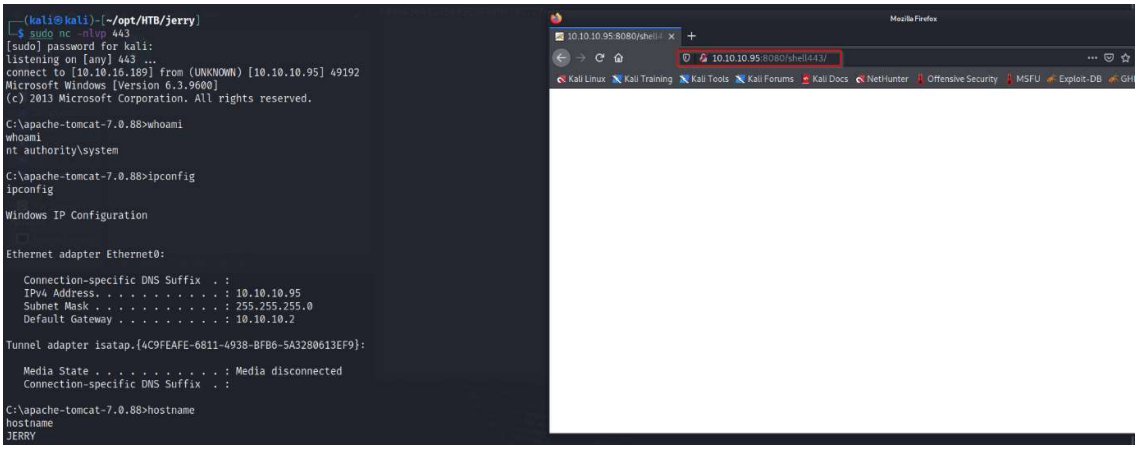
Uploading the malicious war file via Manager App.



War file successfully uploaded.



Navigating to the uploaded war file gives a reverse shell as “nt authority\system”.



User.txt and Root.txt.

```
c:\Users\Administrator\Desktop\flags>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FC2B-E489

 Directory of c:\Users\Administrator\Desktop\flags

06/19/2018  07:09 AM    <DIR>          .
06/19/2018  07:09 AM    <DIR>          ..
06/19/2018  07:11 AM                88 2 for the price of 1.txt
               1 File(s)             88 bytes
               2 Dir(s)  27,523,723,264 bytes free

c:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
type "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00

root.txt
04a8b36e1545a455393d067e772fe90e
c:\Users\Administrator\Desktop\flags>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . : 10.10.10.95
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 10.10.10.2

Tunnel adapter isatap.{4C9FEAFE-6811-4938-BFB6-5A3280613EF9}:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

c:\Users\Administrator\Desktop\flags>hostname
hostname
JERRY

c:\Users\Administrator\Desktop\flags>whoami
whoami
nt authority\system
```