Montana State University

Hint, BlackBox, RedTeam

CSCI-476 Final Practicum

Author:
Gunnar Holwerda

May 5, 2015
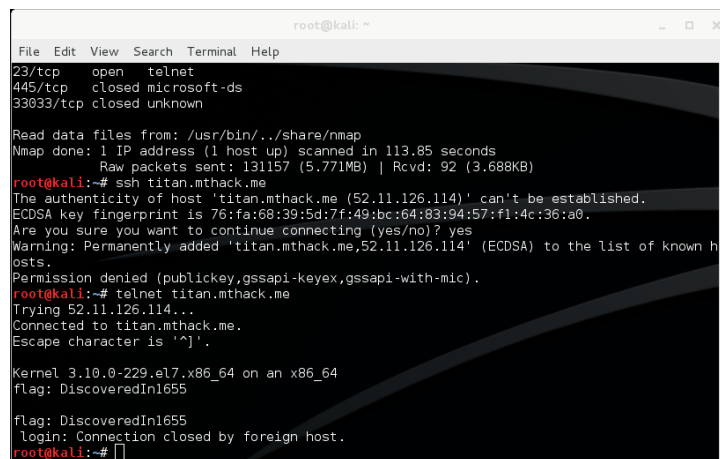
Table of Contents

Executive Summary

Round 1

1.1 DiscoveredIn1655

When starting out I was given the information that the members of mhk 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".
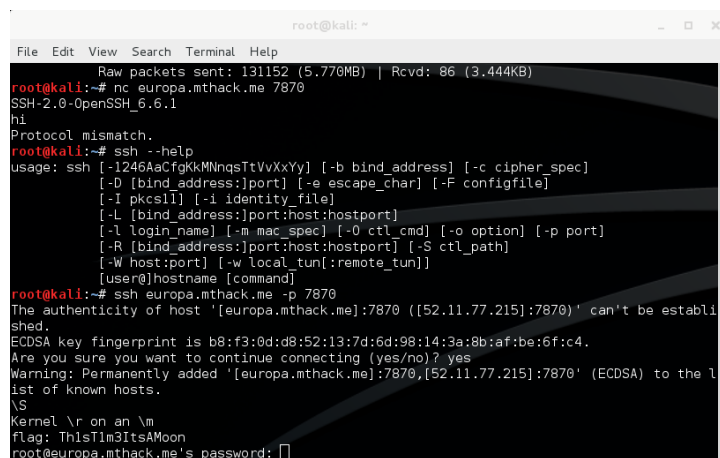
1.2 Th1sT1m3ItsAMoon

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".

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 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".

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 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".
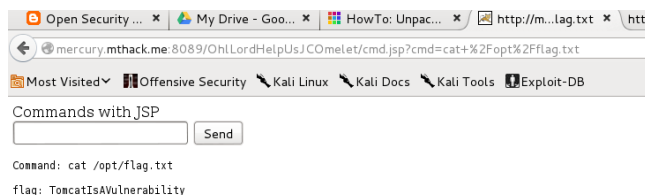
Round 3

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 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".
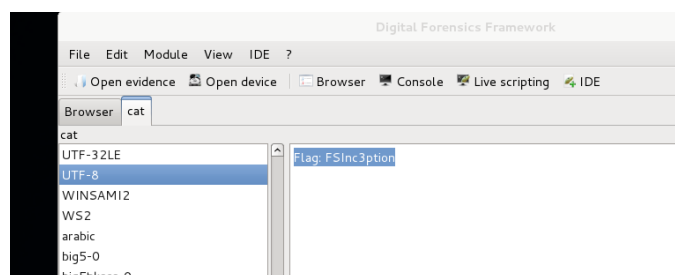
4.2   deaddrop

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 fcrack tool which is used to brute force passworded zip files.

```
$ fcrack -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".
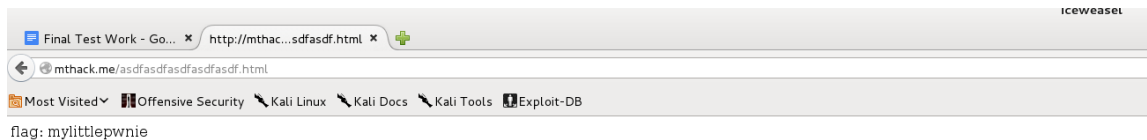
Round 5

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".

Summary

Bibliography