Walkthrough

Foundation: Red

7/18/2016

By: Zachkery Valete Rodriguez

Table of Contents

[Executive Report 3](#_Toc109039169)

[Walkthrough Scenario: 3](#_Toc109039170)

[Tools/Skills Gained: 3](#_Toc109039171)

[Findings: 3](#_Toc109039172)

[Remediation: 3](#_Toc109039173)

[Technical Report 4](#_Toc109039174)

[Actions Taken: 4](#_Toc109039175)

[Lessons Learned 12](#_Toc109039176)

[References 13](#_Toc109039177)

# Executive Report

## Walkthrough Scenario:

Gain the highest privilege on the compromised machine and get admin user NTLM hash by fingerprinting the application using the tools available on the Kali machine and exploit the application using the appropriate Metasploit module. Then, bypass UAC using the UACME tool.

## Tools/Skills Gained:

* Metasploit
* Kali Linux
* UACME

## Findings:

The exploits used with Metasploit and the UACME tool are able to take over the server very quickly. Easily searchable exploit to gain access to low level account with Metasploit and then a slightly difficult for a newbie execution needed by UACME to take over the rest of the system.

## Remediation:

Update the application as soon as possible since these are widely known vulnerabilities that have been patched with newer systems.

# Technical Report

## Actions Taken:

* Start up the lab and locate the IP address for both the Kali Linux machine and target machine
* Enter in the IP for the target machine into Firefox and perform a simple nmap scan of the target machine

Graphical user interface, text

Description automatically generated

* Verify ports open and look to scan for the name and version of the server running on port 80

Text

Description automatically generated

* Naming convention for the server is Http File Server and the version is httpd 2.3
* Use searchsploit to bring up the exploits available

Graphical user interface, text

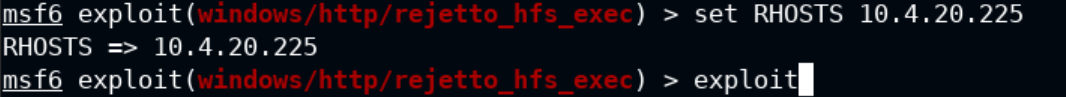
Description automatically generated

* Start up the msfconsole and look for the Rejetto exploit seen available for Metasploit by searching for “Http File Server” with searchspolit
  + As the lab wants us to use a Metasploit exploit, this one seems to match well.

Text

Description automatically generated

* Set the RHOSTS to the target machine. (Thinking RHOSTS is the Receiving Hosts) and run the exploit



Text

Description automatically generated

* Ok, it looks like there’s no issues so far with the exploit
* Now, since I’m new to these tools it’s best to look around to see what commands, flags, and options I can run with help.

Text

Description automatically generated

* A very long list of commands show up that I can choose from.
* I’ll start with dir

Graphical user interface, text

Description automatically generated

* Alright, looks like the general commands work well and now to get back to the task at hand. Using UACME to bypass the UAC and get the NTLM hash of an admin user. (Still pretty cool to see that the exploit is allowing some very decent access of this low level user)
* Next, I’ll look up the user the server is logged in as. While also checking the system information, migrating to a common process (explorer.exe), and seeing if I can elevate my privilege to that of the local system

Text

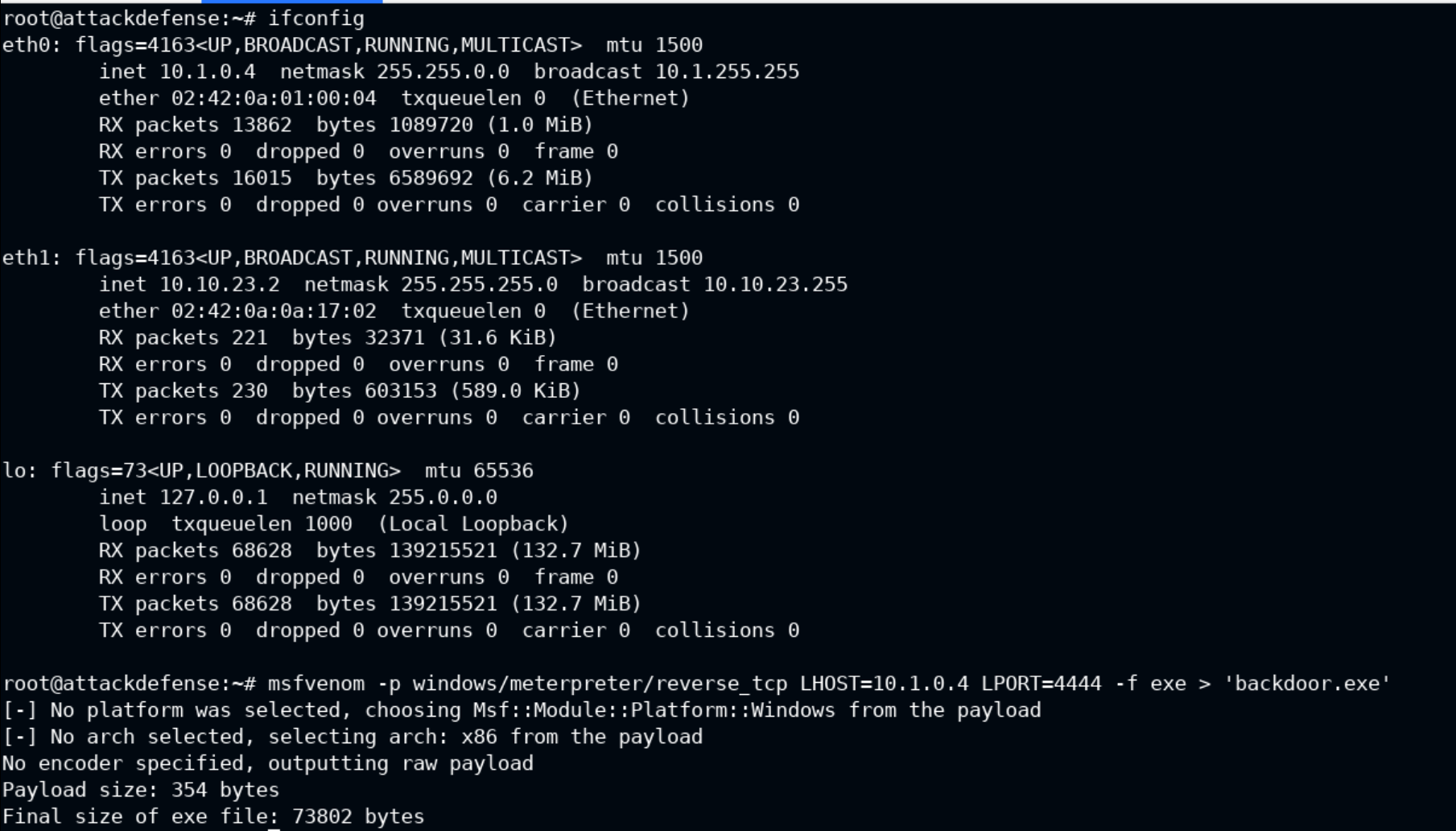
Description automatically generated

* Great, all but the last worked.
* Opening a shell with the shell command and then checking the administrators group

Text

Description automatically generated

* There are two users under this group that I can keep in mind.
* Create a payload with msfvenom called “backdoor.exe”



* Set and run the payload with exploit/multi/handler

Text

Description automatically generated

* Now, I can begin uploading the baddie files (backdoor and UACME)
* Just errr, gotta find them first.

Graphical user interface, text

Description automatically generated

* Great, backdoor is at /root and UACME is in the tools folder under /root/Desktop
* Time to upload the executables

Text

Description automatically generated

* From here I can run the UACME tool with the following

Text

Description automatically generated

* When combined with backdoor.exe, the connection will allow me to be logged in as an elevated user (admin). I’ll make sure to elevate my privilege with getsystem.

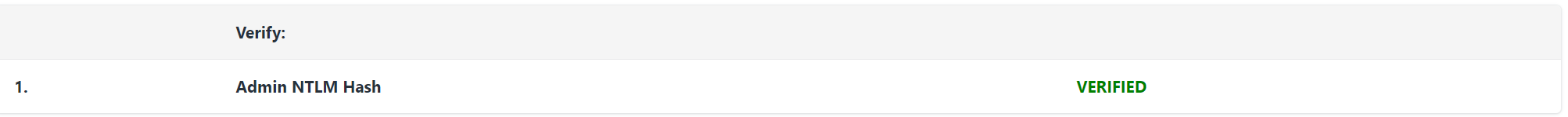
Text

Description automatically generated

Text

Description automatically generated

* Awesome, now I just need to find the NTLM hash for this account with hashdump after migrating to lsass.exe which I’ve found to be the (Local Security Authority Server Service is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system.) when searching it.
* Text

  Description automatically generated
* Wohoooo!
* 

# Lessons Learned

* It is important to poke and test everything such as the naming conventions used with tools.
  + For example, when using searchsploit, I was unable to find exploits listed with HttpFileServer (since this is the name that came up with Nmap). Yet, simply adding in spaces (Http File Server) brought up all the exploits I needed.
* Even though these labs may seem daunting, it seems that even if you need the help of the walkthroughs (I definitely did) the exposure and lessons learned with them are amazingly valuable.
  + Eventually, everything will become second nature since I’ll have seen and worked with the tools in the past, have seen the system structures and capabilities, etc. I LOVE IT!!
* BIGGEST LESSON EVER!
  + GO THROUGH EVERY WALKTHROUGH I CAN AND JUST GET EXPOSURE TO THE POSSIBILITIES OF THIS FIELD AND WORRY ABOUT COMPLETING THESE LABS WITH NO HELP DOWN THE ROAD ONCE MY KNOWLEDGE BASE IS SATURATED. Lol.. uh yeah, I hear it, maybe it’s pride or not wanting to be seen or feel like I don’t know or whatever from the start; but how else are you supposed to learn xD

# References

Pentesteracademy.com: UACME lab under community labs