Walkthrough

Foundation: Red

7/7/2016

By: Zachkery Valete Rodriguez

Table of Contents

[Executive Report 3](#_Toc108005764)

[Technical Report 4](#_Toc108005765)

[Conclusion/Remediation/Lessons Learned 5](#_Toc108005766)

[References 6](#_Toc108005767)

# 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:

## Remediation:

# 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

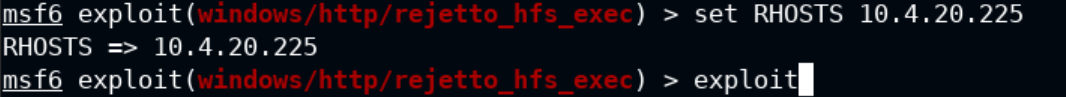
Description automatically generated

* Start up the msfconsole and search for the Rejetto exploit seen available for Metasploit
  + As the lab wants us to use a Metasploit exploit, this one matches perfectly with the server’s name and version.

Text

Description automatically generated

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



* IN PROGRESS

# 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.

# References