Concordia Institute for Information System Engineering(CIISE)

INSE 6961 – Graduate Seminar in Information and Systems Engineering

Graduate Seminar Report-2

Udemy Course: Learning Ethical Hacking from Scratch

Section Covered: Gaining Access –Server-Side Attacks

Total Time covered for this Segment: 66 Mins

Submitted to:

Professor Ayda Basyouni

Submitted By:

Sai Chandra Sekhar Reddy Dwarampudi - 40189233

Introduction to Gaining Access:

Gaining access to computer devices. Any electronic device is a computer like router, modem, TV, webserver something that has hardware and an operating system associated with it. Most of them are used by the user who uses and configures the electronic device. Let's see how we can gain access to a electronic device and the method used to gain access to every electronic device remains the same. There are two main methods to gain access, one is through client side and the other is through server side. Server side does not require by the user to do anything we all need is just the target IP address. Next, we will start gathering the information, various ports, various services installed. On the other hand, the client side requires user interaction to open a file or a link.

Installing Metasploitable as a Virtual Machine:

First, we need to have a computer that acts as a server to perform the server side attacks. For this purpose, we use a virtual machine called metasploitable which runs on Linux. This OS contains a lot of vulnerabilities which is created for hackers for testing. We will install this virtual machine using a VM ware using an ISO file. While installing make sure to keep the network to NAT and login to the Virtual Machine using the Linux credentials.

Introduction to the Server-Side Attacks:

Sever-side attacks are very simple if the target and the attacker are on the same network. These attacks can be used on webservers and computers. The basic step to perform the server-side attacks is we must know the IP of the target computer and we should be able to ping the target computer. If the target is a personal computer which is accessing the internet through the router, even if we know the IP address of the computer, we will not be able get much information about the target because the target is hiding behind the router. Client-side attacks can be more efficient in this scenario. The server-side attacks can be done only on those computers that you can ping.

Basic Information Gathering and Exploiting:

This is the first step. It will give the operating system, running services and the ports associated with them. We can try various ways to the information by trying the default passwords, some of the services might be misconfigured like giving access to multiple ports, some of the applications will not be coded properly and a backdoor might exist and finally vulnerabilities in the code execution can also be exploited by using Zenmap.

To get the IP address of a website simply run ping on the website and if you Zenmap using the IP address you will get all the services running on the website. The Nmap output gives which services are running in which ports. Here we are performing zenmap on the VM installed metasploitable. In the output of Nmap we observed that on port 21 ftp service is installed and it is misconfigured to allow any anonymous user to login. Now download the ftp client so that you can login without

any credentials. On the 512 tcp port service called netkit-rsh rexecd is running. This is remote execution program which uses rsh rlogin which is like ssh and allows to execute commands remotely. Rsh-client is the package to connect to the service. Now we are installing rsh-client and use rlogin to login as root and give the IP address to which you want to login. This will make you to automatically login as root. So, our observation is rlogin function is not configured properly.

Hacking a Remote Server Using the Basic Metasploit Exploit:

Some programs come with a backdoor embedded in them. Metasploit is a framework which is used here to exploit the backdoor which is made by Rapid7 company. Metasploit is basically an exploit development and execution tool. There are several inbuilt exploits, or we can create one. The following are some of the commands used in Metasploit

- Msfconsole – to launch the console
- Show [something] - to show data about something like exploits, auxiliaries.
- Use [something] - use a certain exploit, payload and auxiliary.
- Set [something] - to set a value to something (option)
- Exploit – to run the task

We are using the already built-in exploit vsftpd_234_backdoor to perform the attack. Then we will show command to show the options available to change using the exploit. Now we will change the option RHOST to the IP we want using the set command and then type exploit. Now you get access to the computer with root privileges.

Exploiting a Code Execution Vulnerability to Hack into a Remote Server:

Now let's see how we can exploit a code execution vulnerability using Metasploit and gain full access to the computer. Now from the Nmap result we will be using the service running on port 139 which is samba 3.x server. The exploit name is username map script which is inbuilt exploit, and the name of the vulnerability is usermap_script. Using this vulnerability try to check various options which can be exploited using the show command. Now change the RHOST to the target IP address by using the set function. You can check it using the show command whether the above set command worked properly or not.

Unlike the previous system which has a backdoor the current system has a buffer overflow or code execution vulnerability. This flaw helps us to run a small piece of code which is called payload on the target computer which helps us to gain access to the target computer. You can display the available payloads using the show payloads command. There are two main types: one is bind payload and the other is reverse payload. The bind payload helps to open a port on the target machine from which we can gain access whereas the reverse payload opens the port in the system we are working and then they connect the target machine to our system using the ports. This will be helpful because the reverse will allow firewalls to be bypassed. The firewalls prevent any

connection coming to the target machine but if the target machine only connects to us and if we don't have a firewall, it is easy to connect.

Now we will be using reverse_netcat to perform the attack and the netcat is a tool used to connect two computers. We will set this netcat payload using the set PAYLOAD command. If you again check the available options, you will get LHOST which is the listening address. Use ifconfig to get our ip address and then set the LHOST to our IP address. We can also set the port using the set LPORT. Set this to port 80 which is generally used by web browsing so the fire walls will generally think that the user is just browsing the web and execute exploit. Then a successful connection is established between the two computers. You will be as root user assessing all the files of the target machine.

Scanning a Target Sever for Vulnerabilities using Nexpose

Nexpose is a framework for vulnerability management which is designed by Rapid7. It. Can discover various open ports, find vulnerabilities, exploits, generate reports and to scan automatically. After successful installation add the details of the target machine you want to scan here Metasploit using create tab. Add details like IP address or range of IP address, add them to a group. In the Authentication tab you can configure how the target machine authenticates the user the various methods and credentials. In the template you can select the scan type like quick scan, full audit, full audit with enhanced login etc. The default one is full audit without web Spider which will be using ICMP, TCP and UDP ports. Schedule is used to schedule the scan whether the scan must run daily, weekly, or monthly and the time at which the scan must run.

In the scan output we can observe that there are 177 exploits and 308 vulnerabilities. Risk analysis is also provided. The services that are running on the application are also provided like HTTP running on port 80 and 8180. If we click the vulnerabilities, we get various exploitable vulnerabilities present like a backdoor. It gives why a particular module can be exploited and how the exploit can be done. You also get various references and a possible solution on how to fix the exploit like to change the administrator password and not to use any default password. It provides various reports like audit reports for technical people, executive overview for higher level non-technical people. It can also be scheduled to generate a report automatically after the scan.

Server-Side Attacks Conclusion

We learned how to perform the server-side attacks both manually and by using a tool like Nexpose. First, we must start by discovering information about the targets which is done by using nmap by identifying the ports that have vulnerabilities. Later try to exploit these vulnerabilities by trying different techniques. Identify a vulnerability, perform an exploit, and verify if it is working or not, if not try to find another exploit on the same vulnerability. Use Nexpose generated reports to map the vulnerabilities that can be exploits. For all the server-side attacks the attack process is same. A bit of research needed to be done to identify the correct vulnerability and the corresponding exploit.

Reference: https://concordia.udemy.com/course/learn-ethical-hacking-from-scratch/learn/lecture/5308842#overview

Course Instructor: Zaid Sahib (Ethical Hacker, Computer Scientist and CEO of zSecurity)