Kaan Baltaci
IT430-001
12/13/2023

IT430 Project Report

Introduction

The four exploits I am testing are browser exploitatiation with Aurora, creating and serving standalone payloads with msfvenom, setting a payload manually/reverse shell, and a web attack with SET. The device used for these tests was a laptop. The virtual machines used in these tests were Kali Linux and Windows XP. The browser that was used is Internet Explorer through the Windows XP VM. The tools that were used includes msfvenom, Meterpreter, Metasploit, Aurora Metasploit module, Multi/handler, Apache, and SET. Browser exploitatiation with Aurora is about exploiting a browser by targeting a user. This test is performed to test the vulnerability of the browser. The standalone payloads with msfvenom and web attack using SET are both targeted at the user instead of the system. These tests are performed to help users become aware of the security risks of social engineering. Setting a payload manually/reverse shell is performed to test out if the system is vulnerable to attacks such as taking control over the machine.

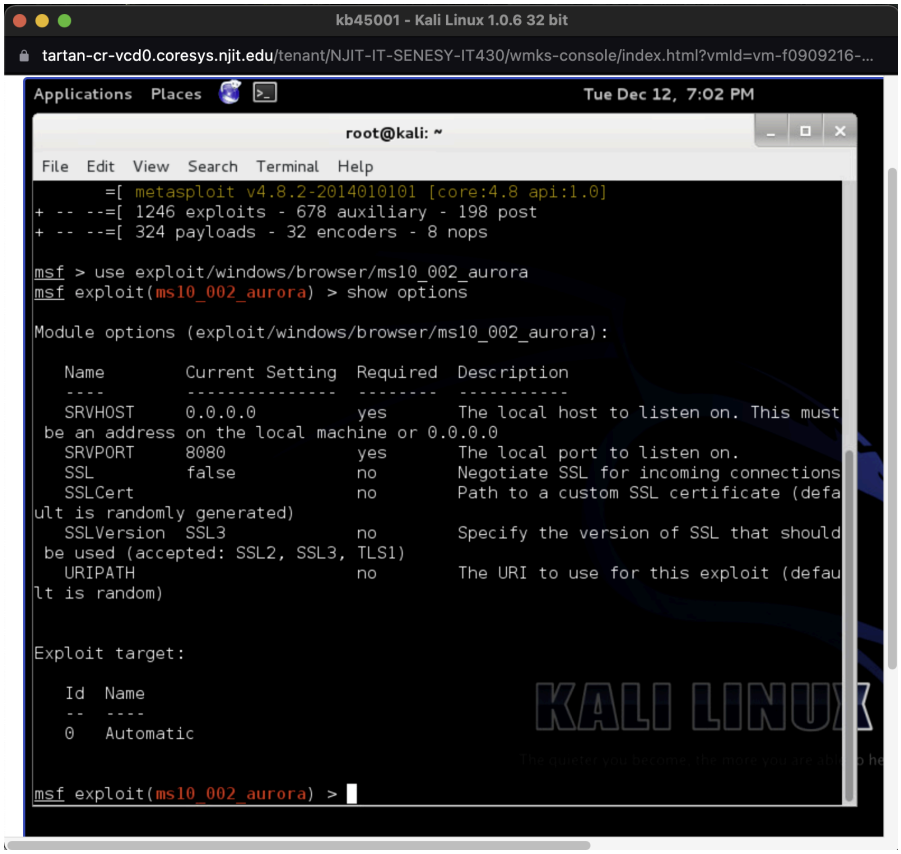
Exploit 1: Browser Exploitation on Aurora

Theory

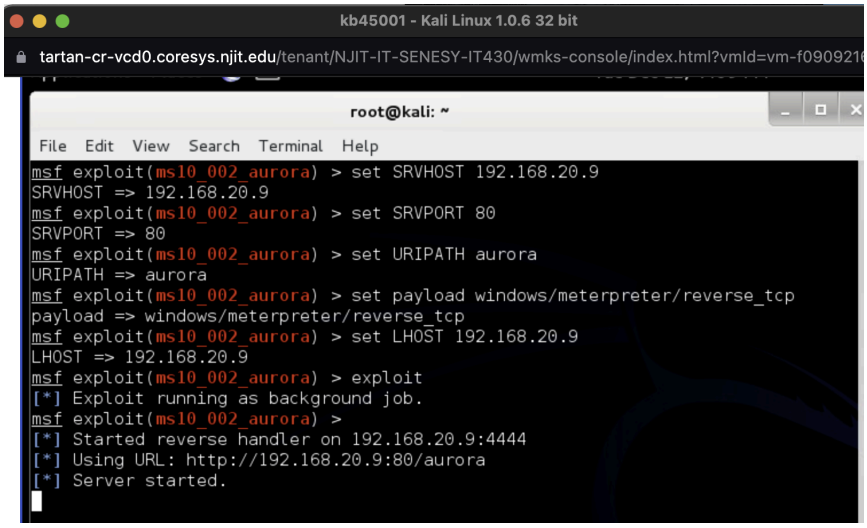
Every browser has codes that are used to load the web pages. Malware can be hidden in these web pages to attack users when they try to access the web page. In this exploit Aurora is used to target vulnerable browsers. A server is set up and waits for access from a browser. This exploit can be used in any version of Windows due to the nature of the exploit taking place inside the browser. There is a downside to this vulnerability due to the exploit ending when the browser crashes or the user quits forcefully. This can be solved by migrating the session and process. An extra tool used for this exploit is the Aurora Metasploit module contained in Metasploit.

Configuration

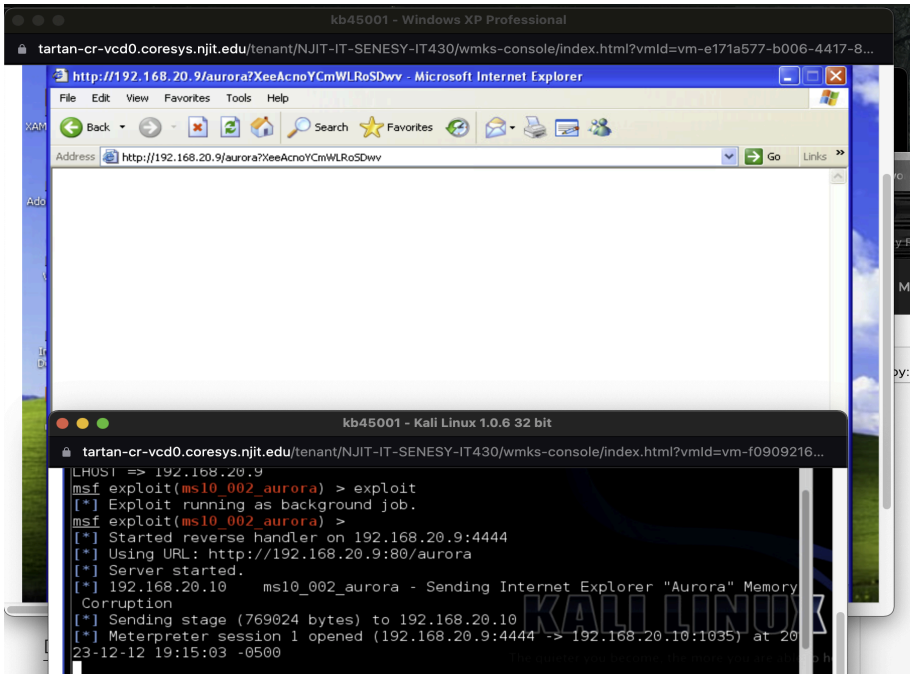
Start of the test: Accessing the Aurora Metasploit through Metasploit and checking the setting to see if they are correct



Configuration of the Setttings, SRVHOST, SRVPORT,URIPATH, payload and LHOST are all set to their correct values.Note make sure apache is not running on port 80. Then the exploit is ran with the command “exploit”.



Exploit is running. Reverse handler is listening for the signal. Signal is received after the user tries to access the web page.



Test Results

Meterpreter session is open after the handler receives the signal.

Mitigation

Keeping browsers up to date is one of the ways this exploit can be mitigated. Secondly the user can also force the browser to close by force quitting.

Exploit 2:Creating standalone Payloads with msfvenom/Serving Payloads

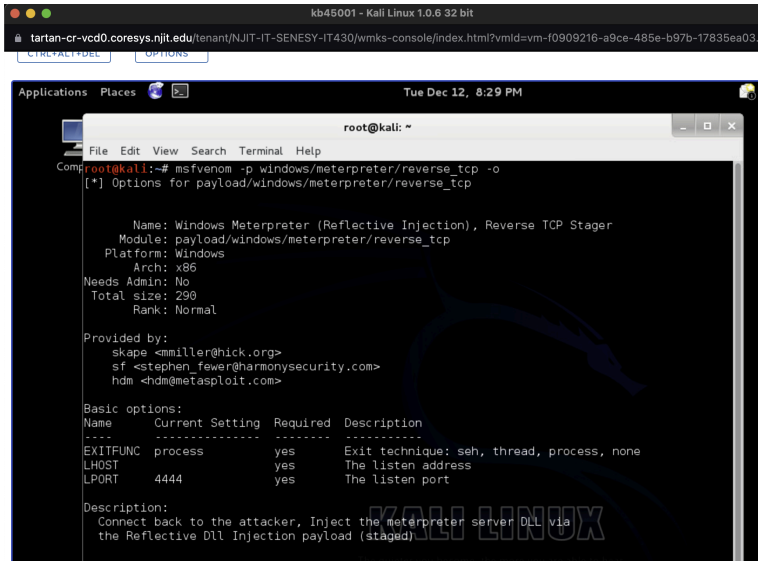
Theory

This exploit targets the users instead of targeting a system and taking control of a machine. This exploit is about creating a standalone payload and to use this payload on a target system through exploiting the user. The user can be exploited through a social engineering attack or a vulnerable server. The payloads can be hidden in web servers and can lure users by appearing harmless. When the user is tricked into downloading it, the handler receives the signal and the attack is successful.

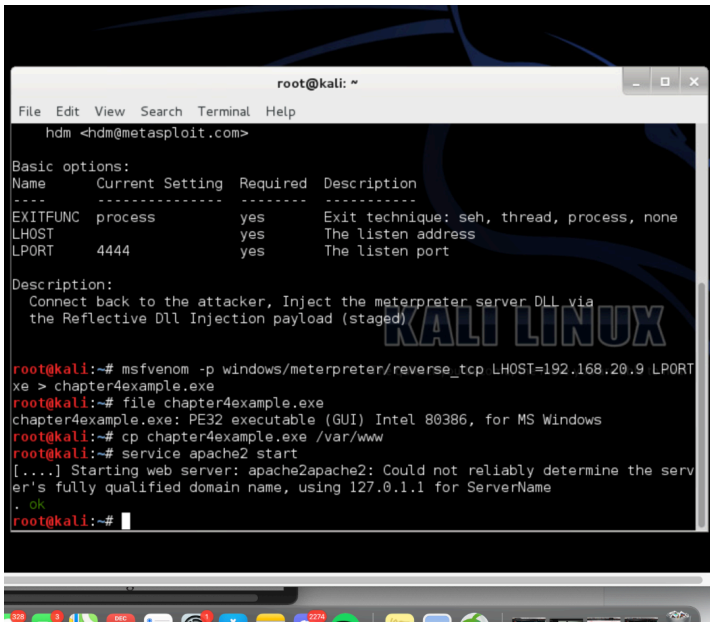
Configuration

The additional tools used for this test is apache which is needed for downloading the executable file and starting the web server. The setting options are checked, the options that are checked

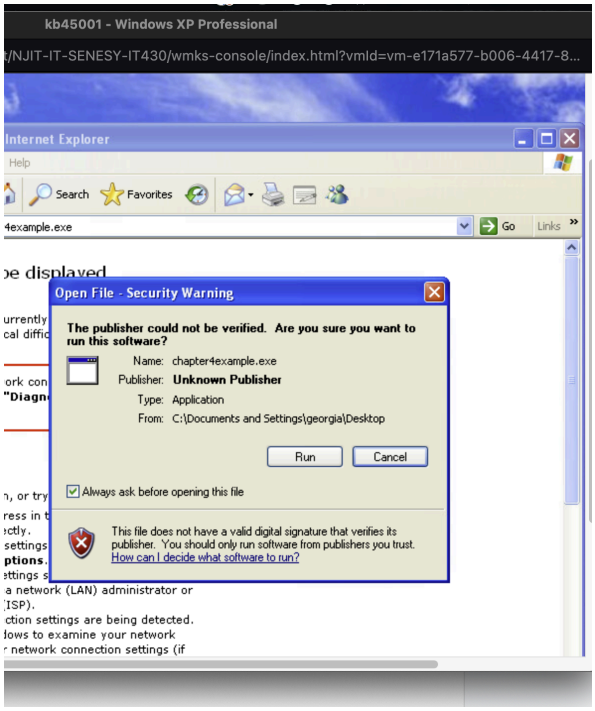
are LHOST and EXITFUNC. It can be seen that both are at their default value which correct.

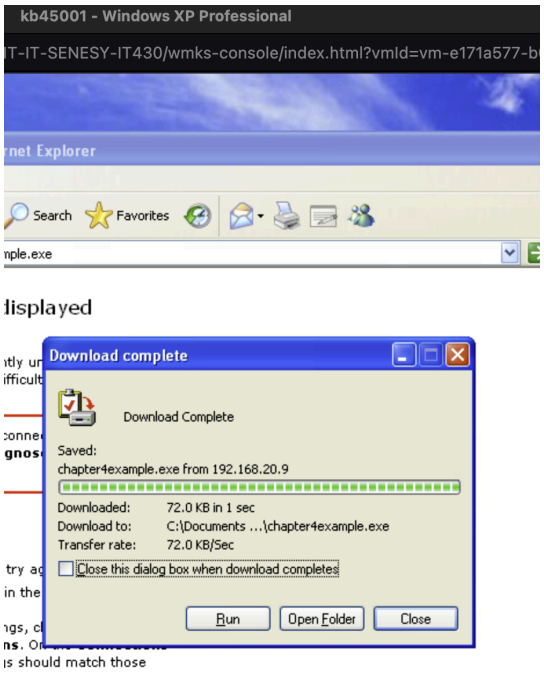


Redirecting the executable file (chapter4example.exe) and running it to see that it is a Windows executable. Copying the the executable file to apache directory and starting apache

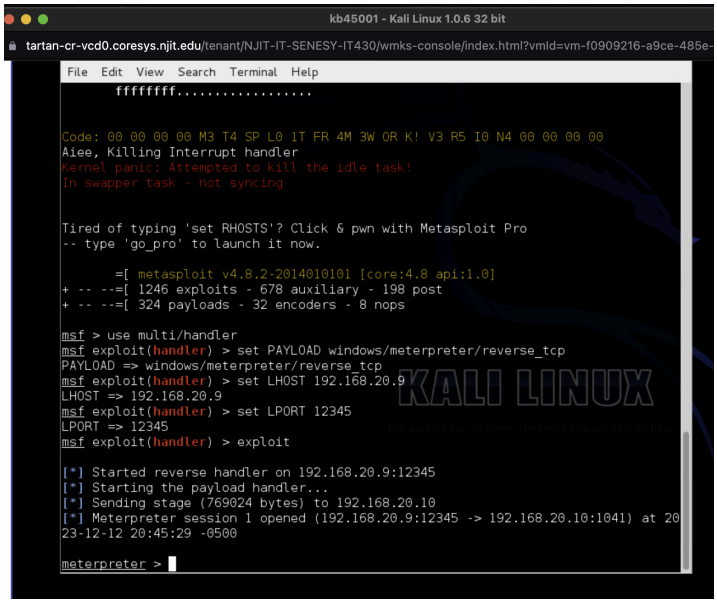


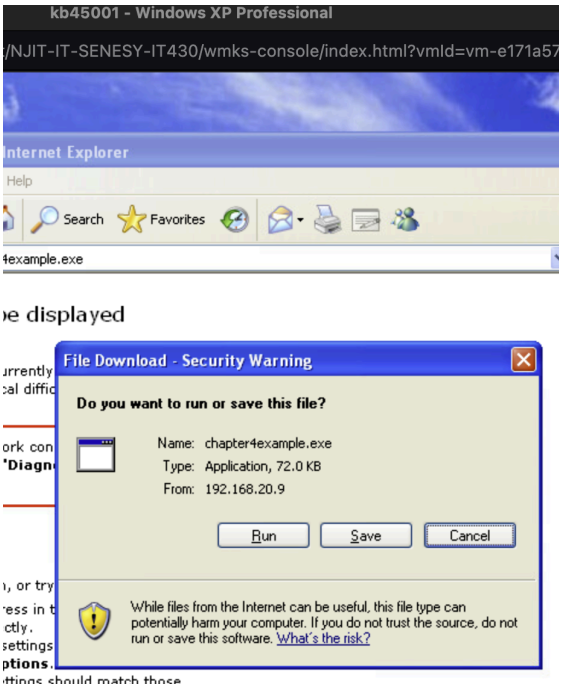
Running and downloading the chapter4example.exe in Windows XP and Internet explorer





Using Metasploit to access the multi/handler and catching the payload. Setting the configuration and starting the reverse handler and payload handler. Running the chapter4example.exe file on Windows XP so that the handler receives the signal of reverse conncention and meterpreter session.



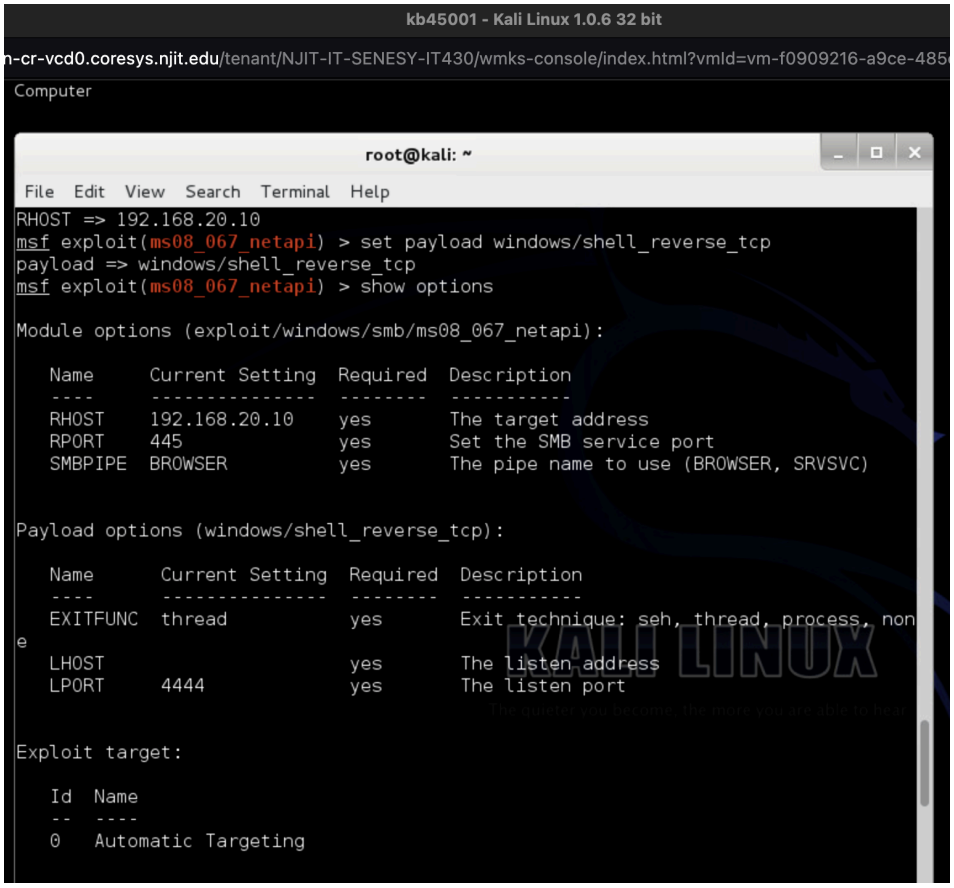


Test Result: The handler listens for the signal from the reverse connection and starts the Meterpreter session when it receives it.
Mitigation: Users should be aware of social engineering attacks. There are antivirus programs that stop these kinds of attacks. Port and Vulnerability scanning are also essential.

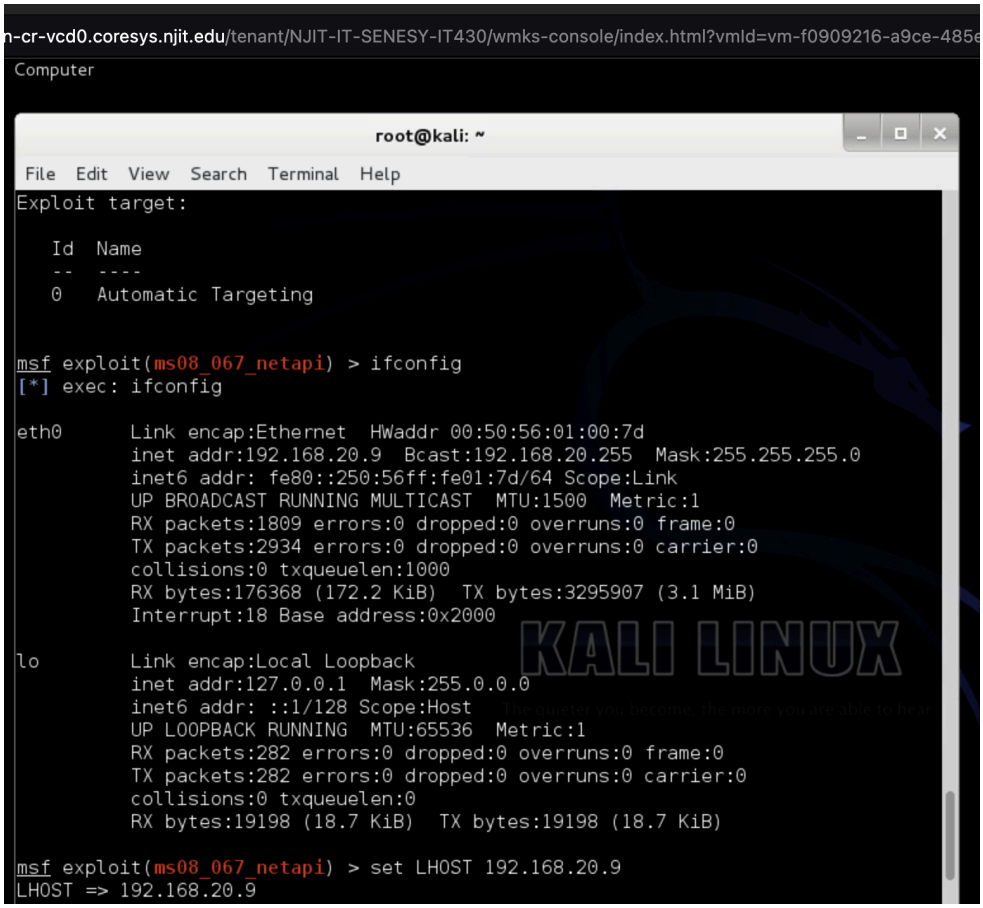
Exploit 3: Setting a Payload Manually/ Windows Reverse Shell

Theory
This test uses a payload thay has a Windows reverse shell. For the reverse shell to work, an IP address and the port of the attack machine needs to be located. Then this information is used to tell the target where to send the shell. For this expoit the ms08_067_netapi Metasploit module is used. A listener is opened by Metasploit to receive the reverse shell to take control of the target machine. The additional tools needed for this exploit is the ifconfig command and a Windows Reverse shell.

Windows reverse shell selected for the payload. Payload options are checked.



Ifconfig is used to find the IP address of the target machine. LHOST is set after finding the ip address.



Test Result:

Exploit is entered and is successfully completed. Metasploit has control of the machine after finding the right exploit to access the machine and sending the exploit string to execute the payload.

Mitigation

Ways to Mitigate a reverse shell are performing vulnerability scans and updating the patch hosts. Solid password security and configure the firewall to check traffic for odd activity.

Exploit 4:SET Toolkit/ Web Attacks

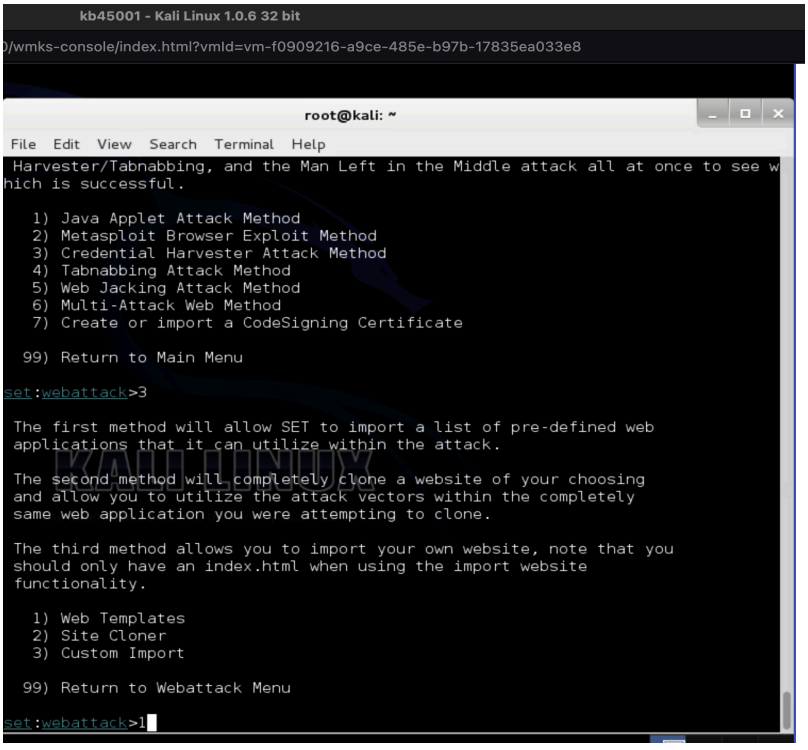
Theory

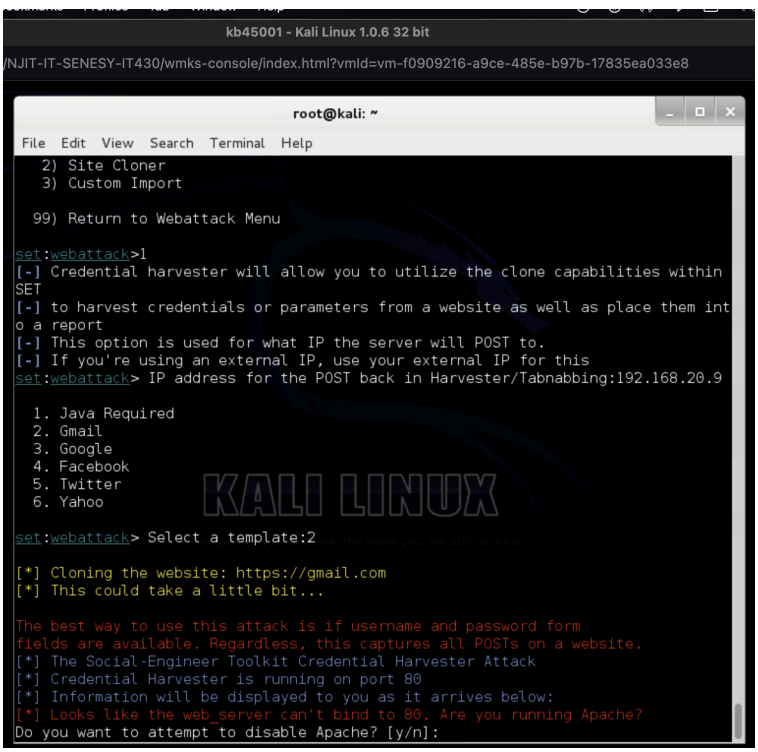
This test is conducted to pentest the social engineering side due to the numerous social engineering attacks. This can also be conducted to check the security awareness of the targeted user. Social engineering attacks are attacks targeted at users instead of the system. It is usually conducted by deceiving the user by tricking them into giving out private information. This test is on web attacks and Credential Harvester Attack Method. The Credential Harvester Attack Method is used to create fake websites that look real to deceive users to steal their private information. One example of this is the login information of an account.

Configuration

The additional tools include the Internet-facing IP address and choosing a web template in this case is Gmail.

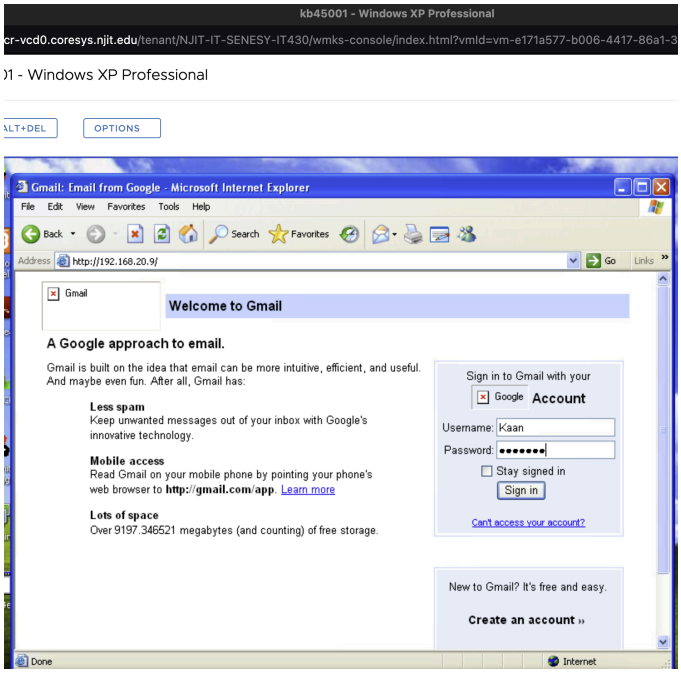
SET is used in this test which is already installed in Kali Linux. To access the SET the command setoolkit is entered. Then to perform the web attack, the first step is to enter 1 which is “social-engineering attacks” then enter 3 to a select “Credential Harvester Attack Method” then to pick the format of the website, enter 1 again for “Web Templates”. Final steps is entering the IP address, which is where the information will be sent to and choosing the intended web template which is Gmail. After selecting the template, the cloning process of the Gmail page begins. It is important to know that the Credential Harvester is running at port 80.

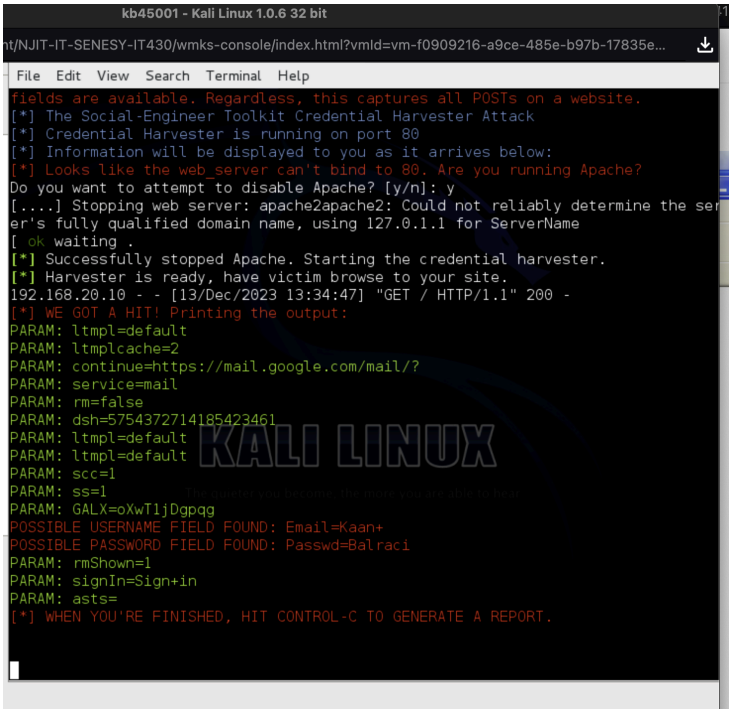




Test Results

When the user clicks the fake website and enters their private information such as account credentials, the entered information will be sent back to the SET. SET highlights the information that it deems useful. In this instance it is the user's google account information.





Mitigation

Mitigation against web attacks include security assessments and vulnerability scans. It is important to have input validation and sanitization. Processing external entities can be disabled, validating file and directory path also add an extra layer of security.