Keylogging with Metasploit

Yukun Zhang/Yz593

IT3910 Advanced Cyber Security - Fall 2020

University of Missouri

Keylogging with Metasploit

I decided to do my research on keylogging using Metasploit. I have always wondered how attackers were able to capture keystrokes of sensitive information on a target system. While keylogging has been around for a long time, it is still widely used in the real world today. For example, there is a keylogger enabled by default on Microsoft Windows 10 (Brinkmann, 2019). According to Microsoft, "As part of inking and typing on your device, Windows collects unique words—like names you write—in a personal dictionary stored locally on your device, which helps you type and ink more accurately." (Microsoft, n.d.). I chose Metasploit, because it is a powerful tool for penetration testing, and includes keylogging modules. I used Kali Linux, because Metasploit is pre-installed and easily accessible.

A keylogger is a program that records every keystroke made by a user, generally in secret. The keystrokes are recorded as data and can be retrieved by an attacker at a later time. Keyloggers have various uses, such as the example stated above, but are typically known for their malicious use in gaining fraudulent to otherwise confidential information. Due to the nature of keyloggers, they have been mainly used for espionage. An early known use of a keylogger is dated in the 1970s by the Soviet Union. Keylogger programs were installed on IBM typewriters by spies in the US embassy and consulate buildings in Moscow (Crypto Museum, 2015).

Keylogger programs have to be running on the machine in order to record keystrokes, a common use is to retrieve confidential and important information such as passwords, credit card information, or social security numbers. A keylogger program is installed onto a user's program as a trojan; A trojan program is a type of malware that misleads the user of its true intentions (Christensson, 2006). The keylogger precedes to record the user's keystrokes and sends the

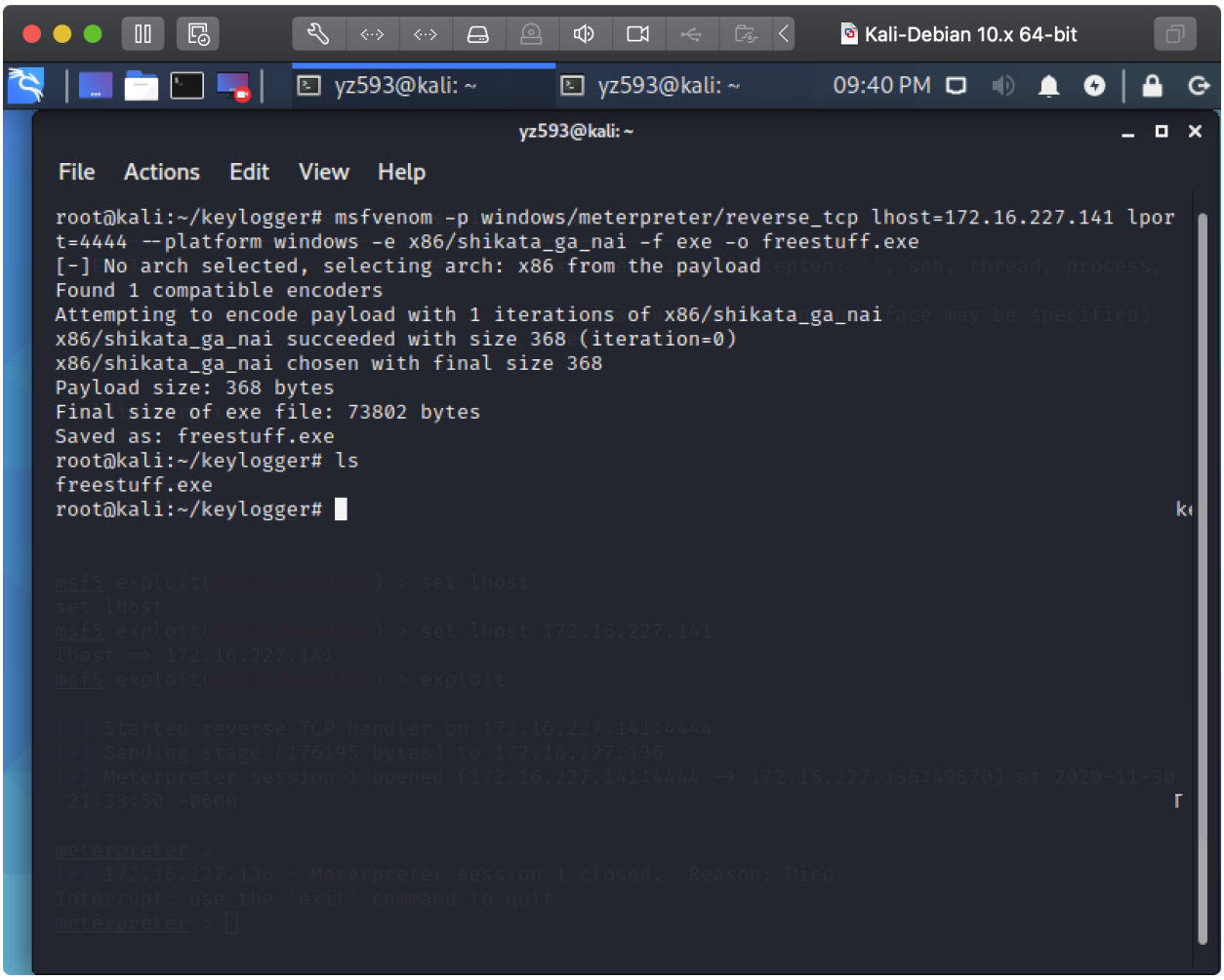
information back to the attacker. The attacker now has access to potential passwords and other information such as credit card numbers and social security numbers. Another use is in law enforcement, warrants can be obtained to install keyloggers for surveillance. In 1999, the FBI broke into and installed a keylogger program on Nicodemo Scarfo, Jr to obtain information to convict him (Center, n.d.).

Preparation

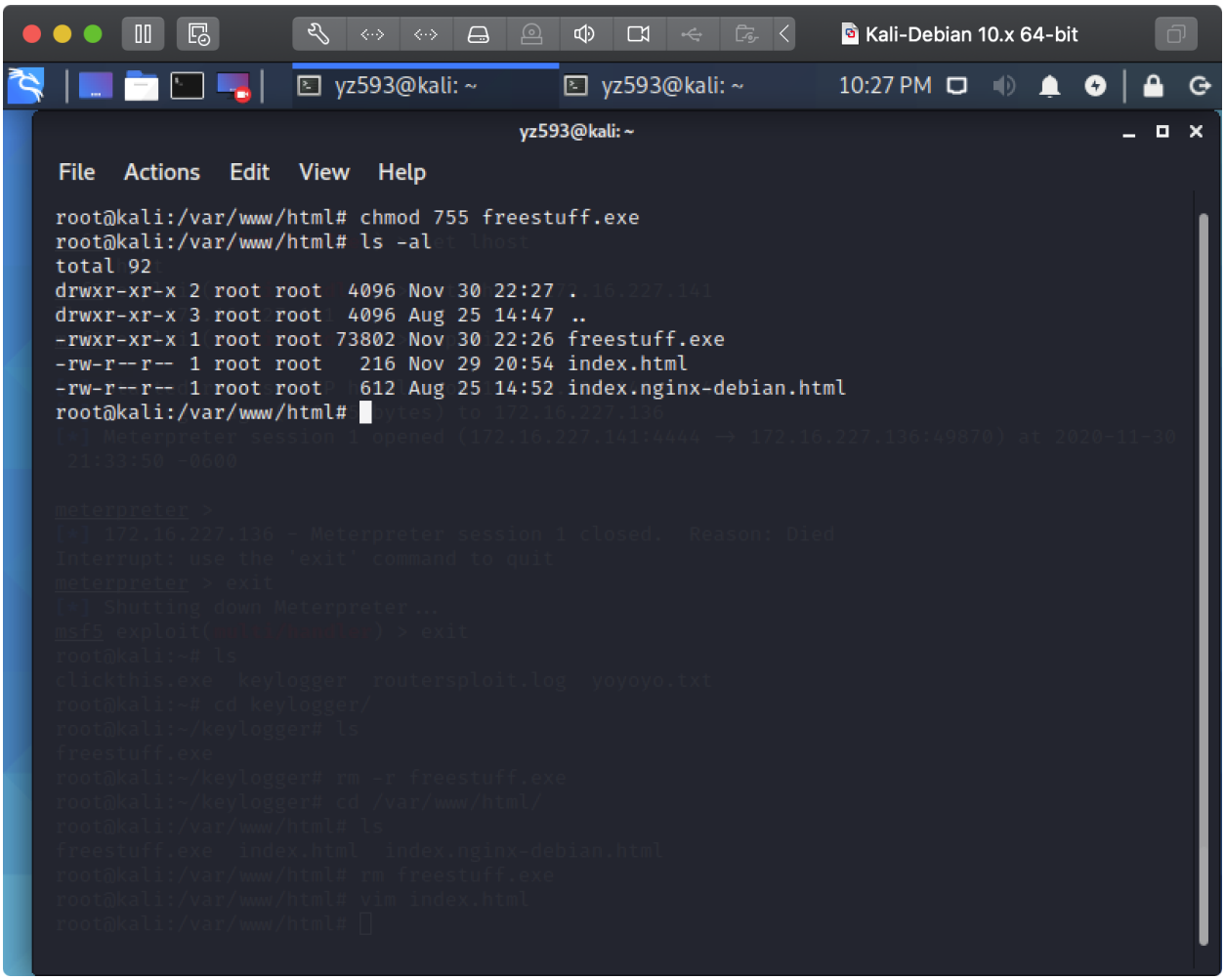
I will be using Msfvenom to create a Windows executable file that contains a Meterpreter reverse shell, which will allow me to gain access to the victim's system once the victim executes the file. Meterpreter is a payload from the Metasploit Framework, a popular tool used for penetration testing. Meterpreter does not write anything to the disk, and lies entirely in memory(Offensive Security, 2019). This allows for attackers to gain access into a target system and perform attacks while leaving very little evidence. Meterpreter can also migrate to other running processes, which makes it even harder for the target system to detect and remove. Msfvenom allows attackers to generate payloads that are often not a part of the Metasploit Framework. Meterpreter provides an interactive shell that allows attackers to control a system and perform many types of attacks.

Application

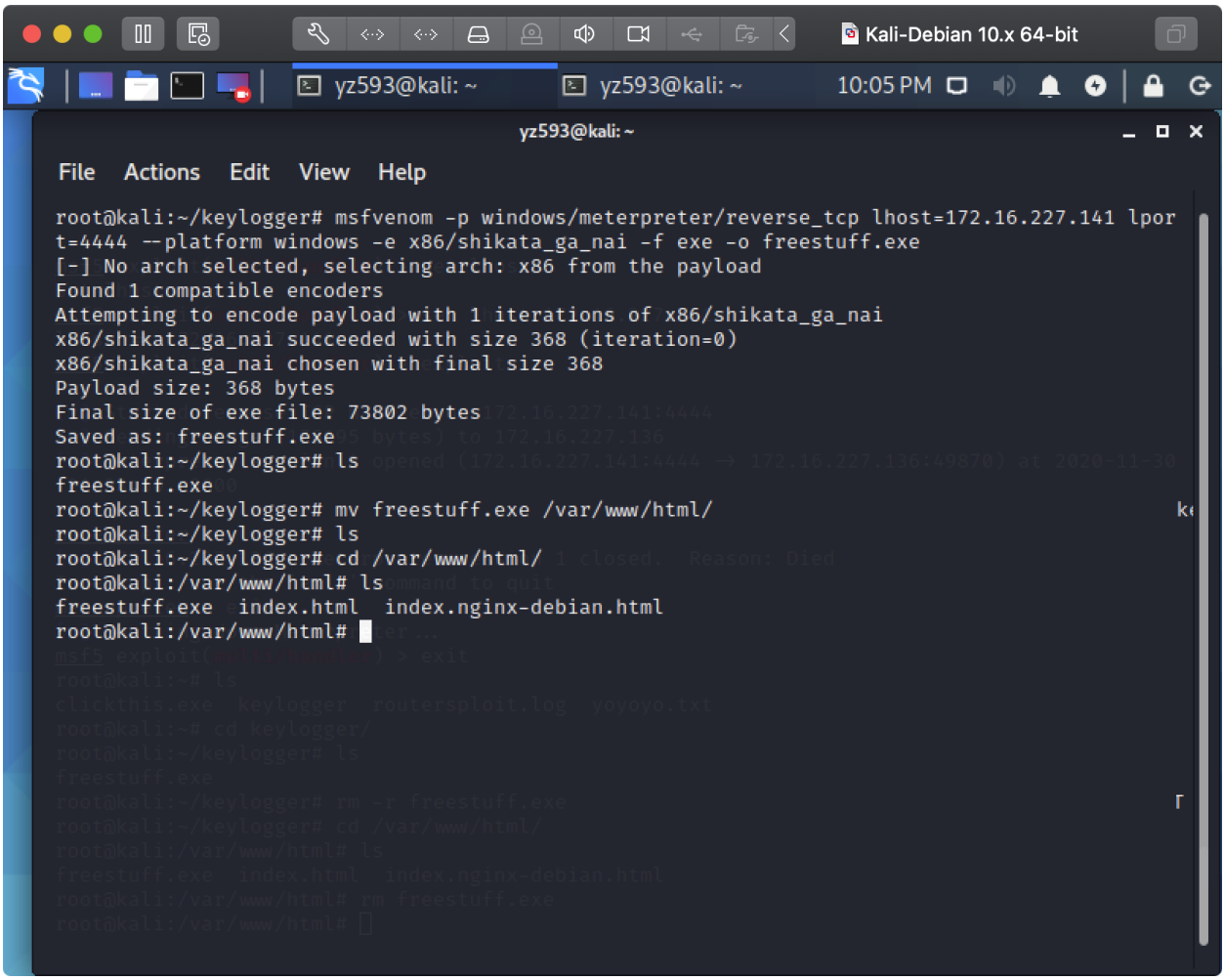
The -p flag is used to specify the payload to be used, in this case, Meterpreter reverse_tcp. The Meterpreter reverse_tcp payload requires a listening host(lhost), and a listening port(lport). The lhost is the address that the target system will connect to, in this case, it is the attacker's IP address, and the lport is the port that the target system will connect to. The --platform flag is used to specify the platform of the payload, in this case it is windows. The -e flag is used to specify the encoder, which will help avoid bad characters in the payload. The -f flag is used to specify the format, in this case it is .exe. Lastly, the -o flag will save the payload to the specified file, in this case the file is named "freestuff.exe."

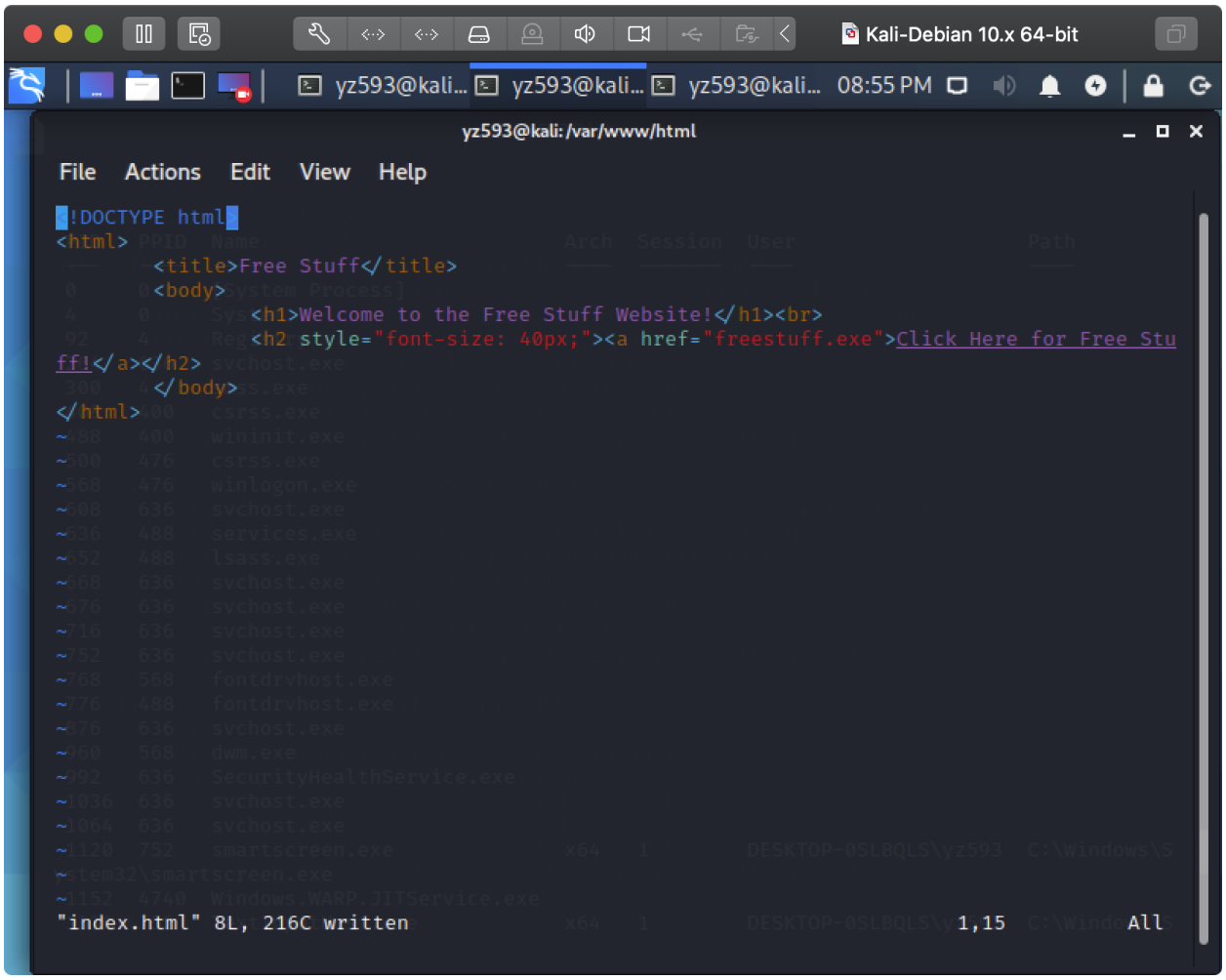


Use “chmod 755” to change the file into an actual executable file. This will allow any user to execute the file, but only allow the owner of the file to make changes.

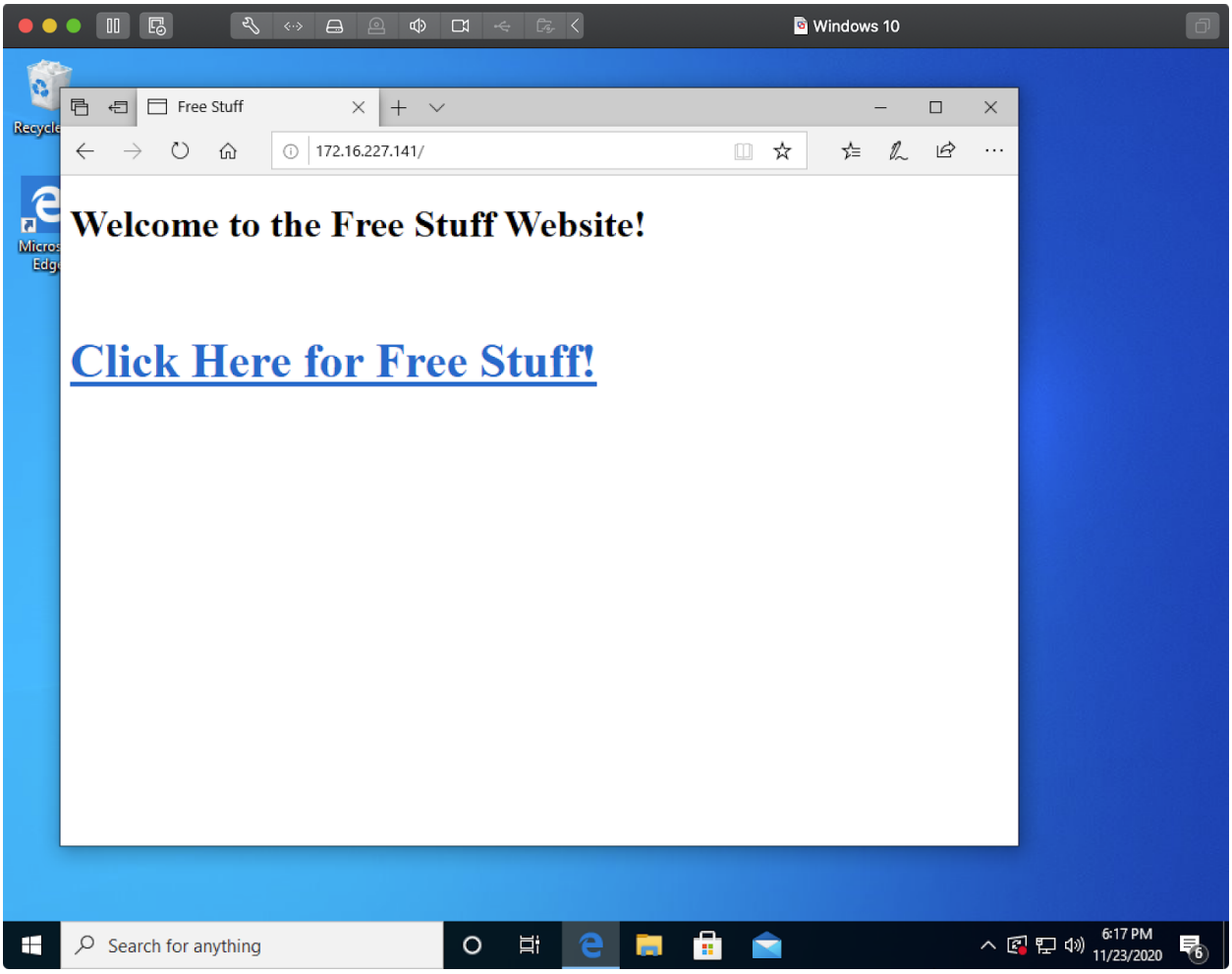


There are many ways to get a target to run a payload on their system. For demonstration purposes, I chose to make a webpage that included a download link to the executable file. I then placed the file in the"/var/www/html" directory for easy access when making the webpage.

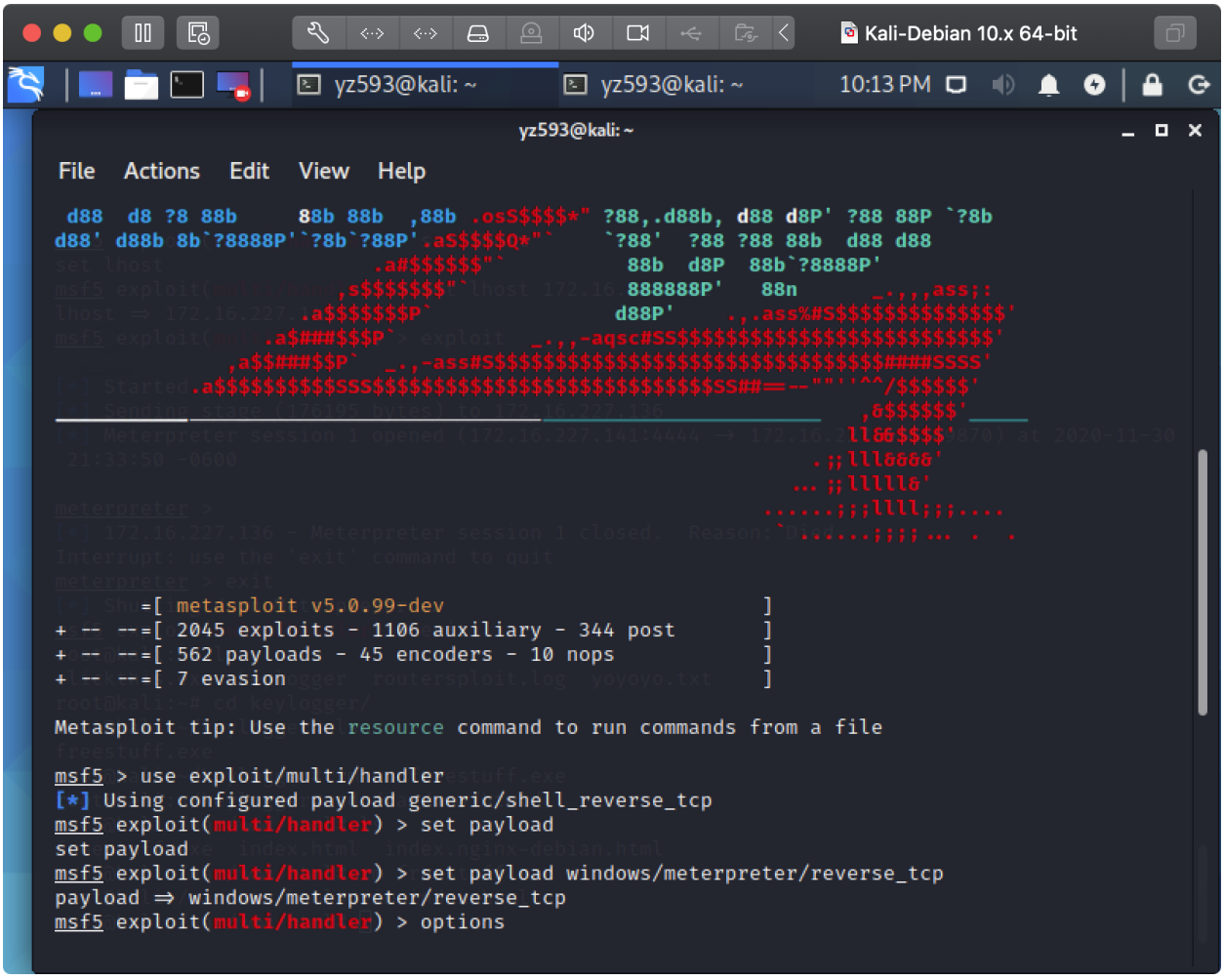



Kali-Debian 10.x 64-bit
yz593@kali...
yz593@kali...
yz593@kali...
08:55 PM
yz593@kali: /var/www/html
File Actions Edit View Help
<!DOCTYPE html>
<html>
<title>Free Stuff</title>
<body>
<h1>Welcome to the Free Stuff Website!</h1>
<h2 style="font-size: 40px;">Click Here for Free Stuff!</h2>
</body>
</html>
"index.html" 8L, 216C written
1,15
All

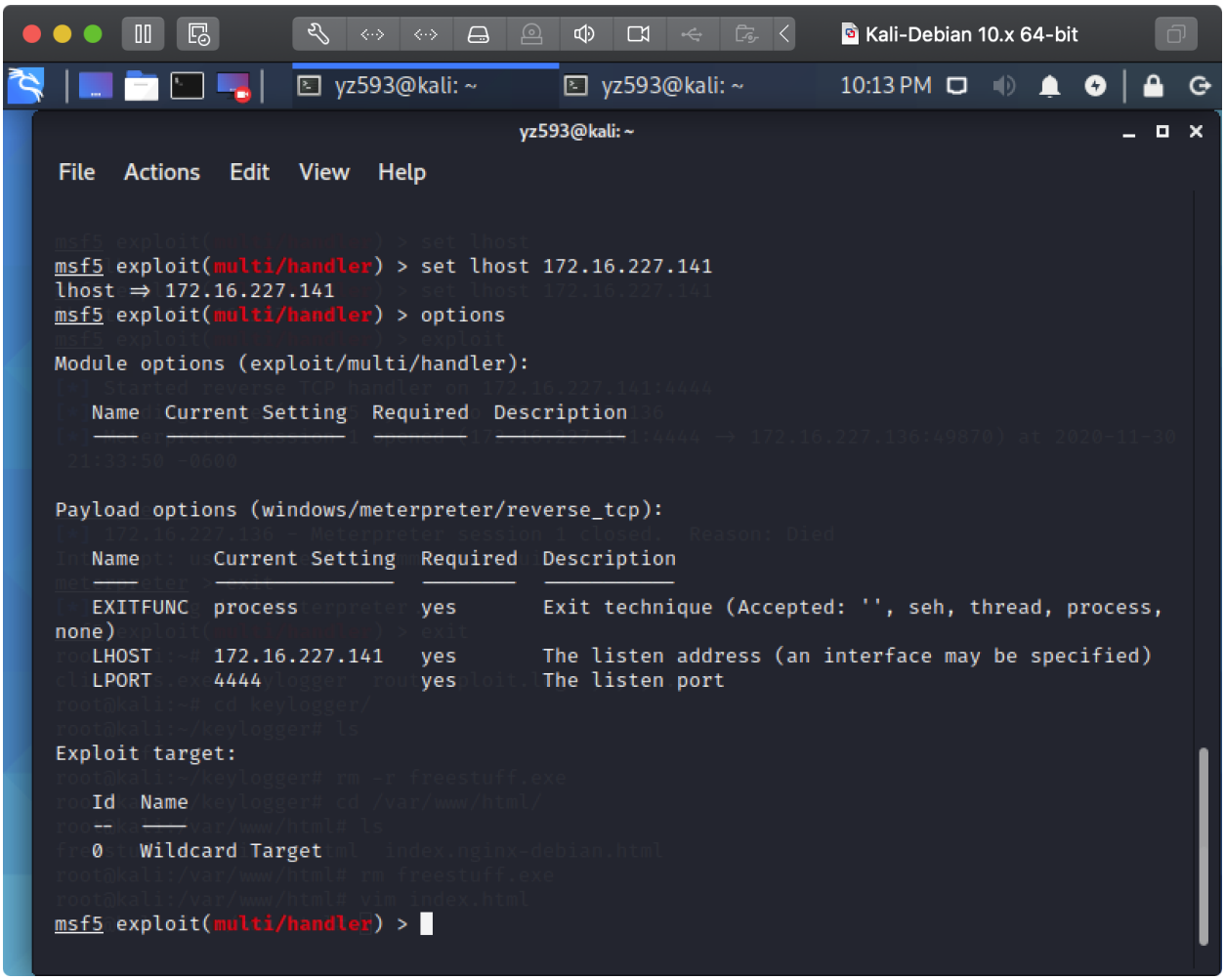
This is how the webpage looks on the target system using the attacker's IP.



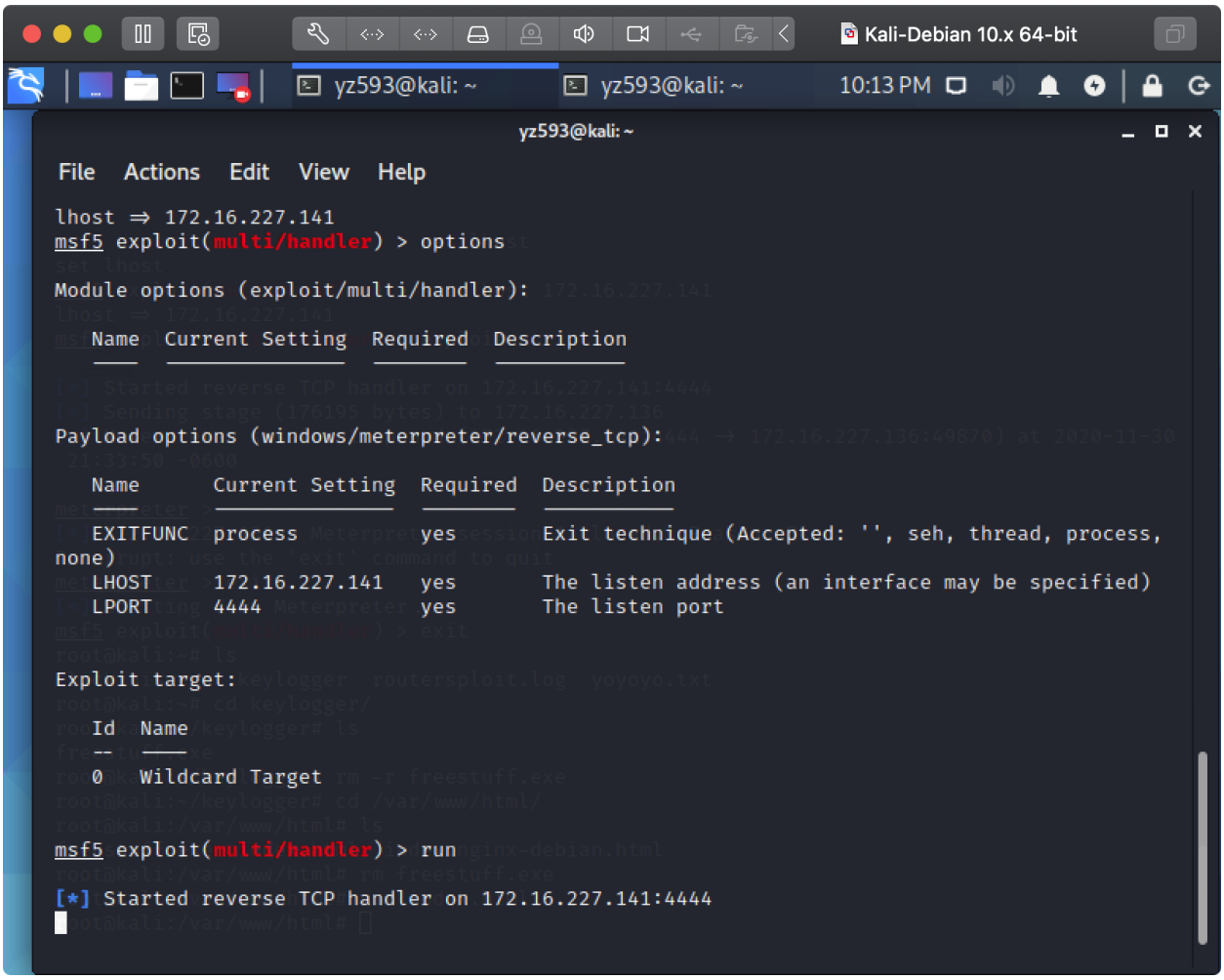
Before the target downloads and runs the payload, we need to set up Meterpreter. Typing "msfconsole" will open the Metasploit and allow access to the framework. The multi/handler exploit will allow attackers to handle exploits outside of the framework, in this case, the executable file with the Meterpreter reverse_tcp payload. We then set the payload to the Meterpreter reverse_tcp payload.



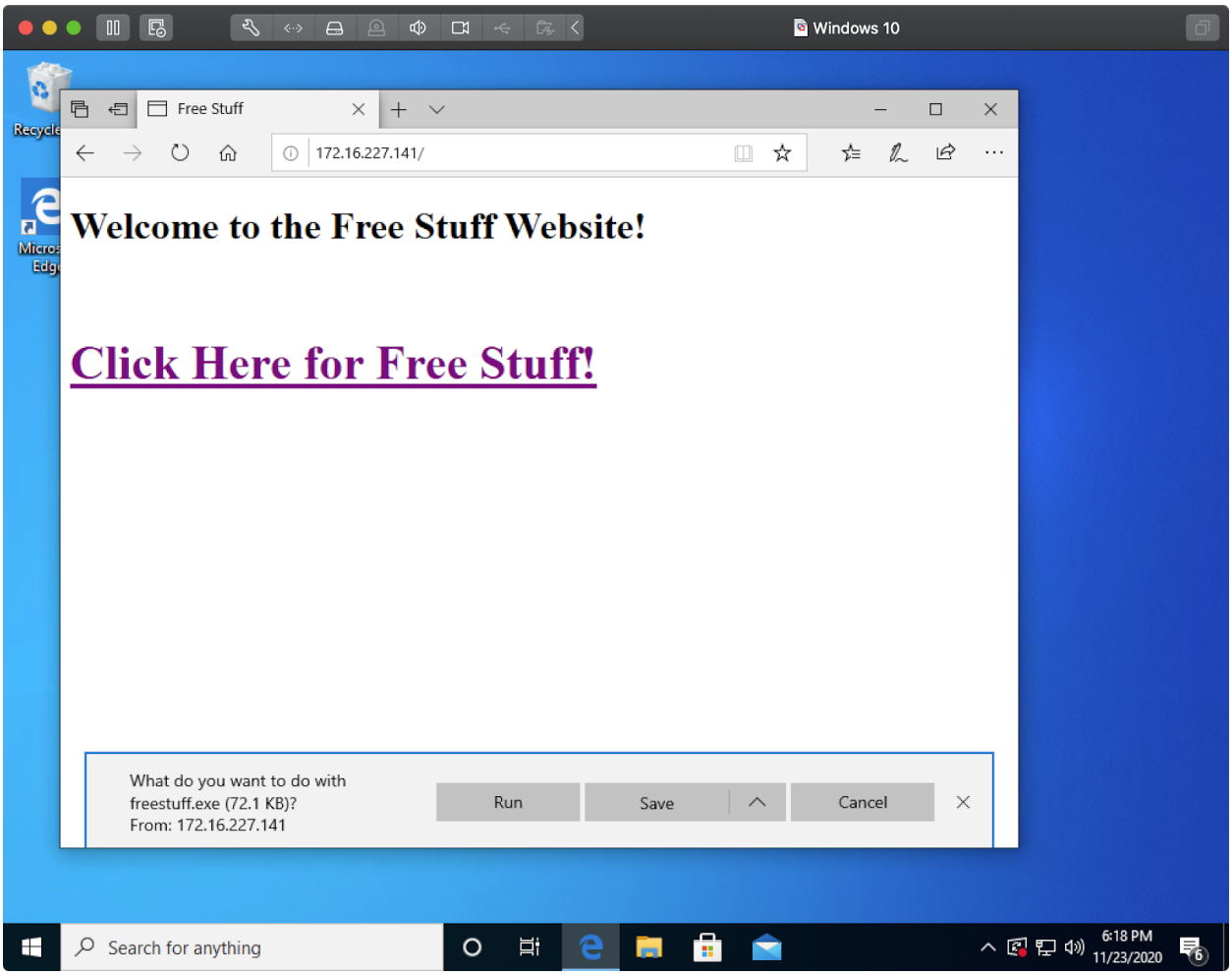
Before running the exploit, we need to set the lhost to the address that the target will connect to, and the lport to the port that the target will connect to. Afterwards, we can run the exploit.



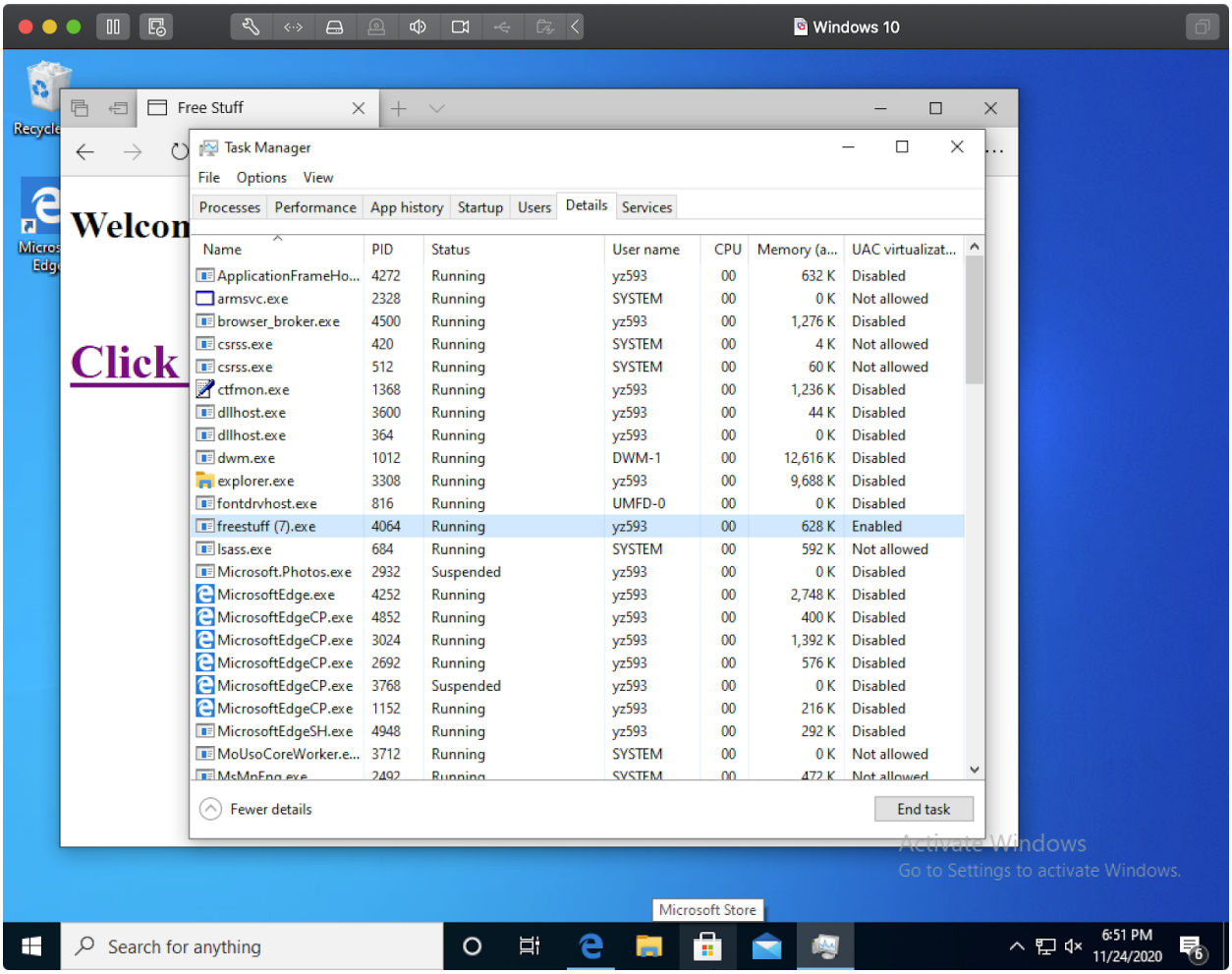
Now we are ready to connect to any system that opens and runs the executable file.



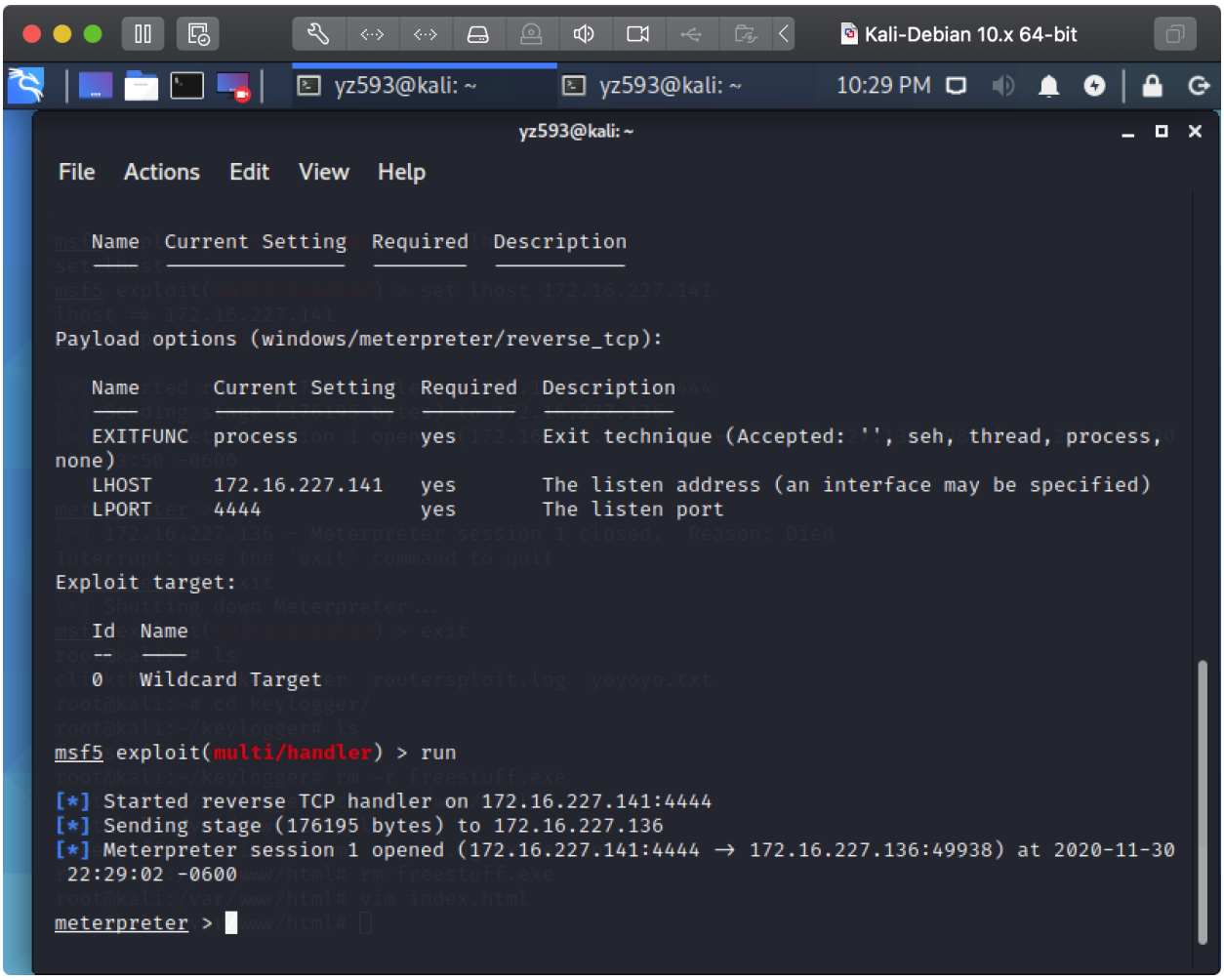
This is an example of a target system downloading and running the executable file. I have disabled the firewall and any antivirus on the target system for the purpose of this demonstration. Under normal circumstances, Windows will not allow this file to be downloaded, or executed, as the payload is basically a trojan. There are ways to work around this, but I wanted to focus more on the actual keylogging aspect.



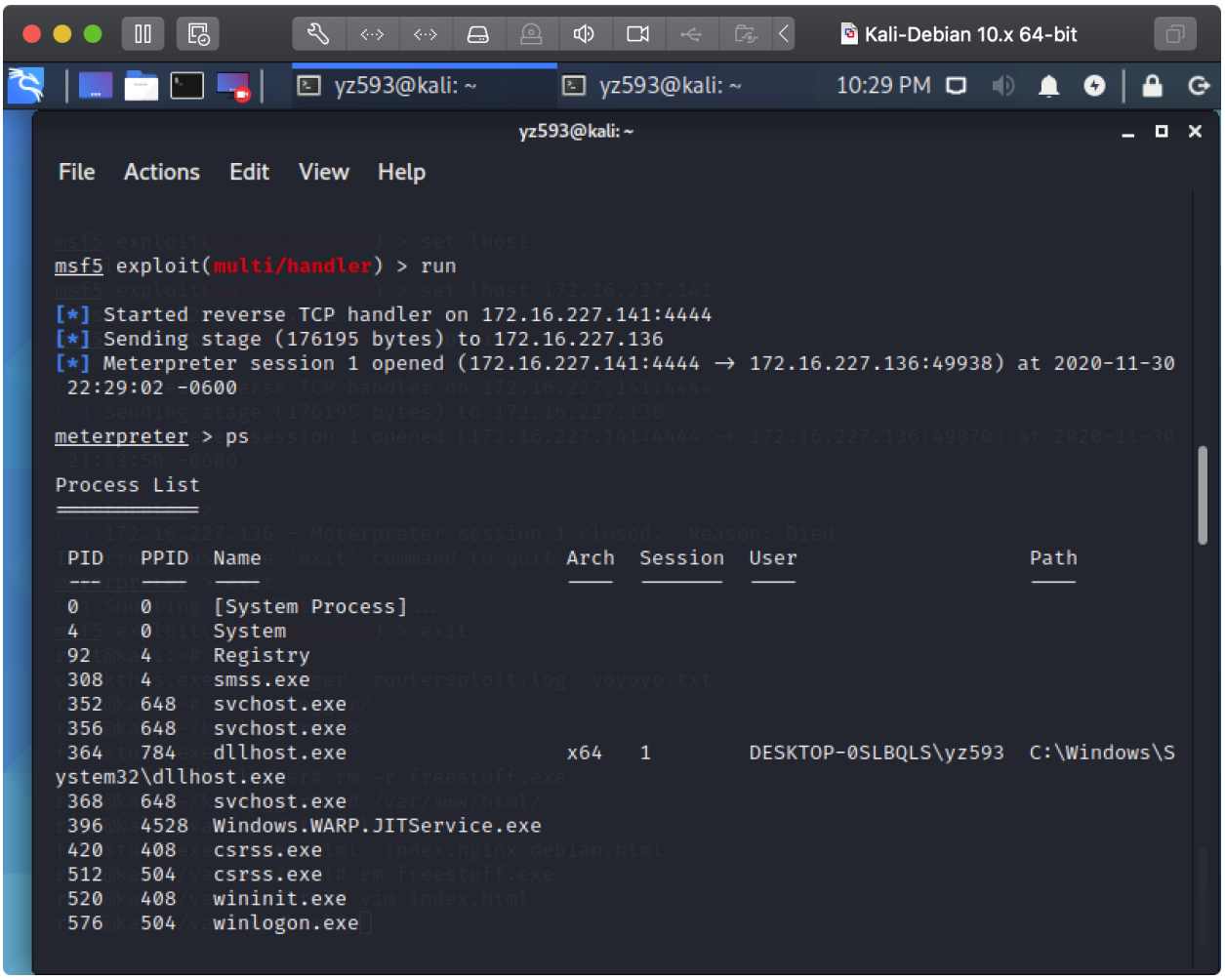
For now, the payload can easily be seen in the task manager, later I will hide the file in another process to make it harder for the target to find and remove.



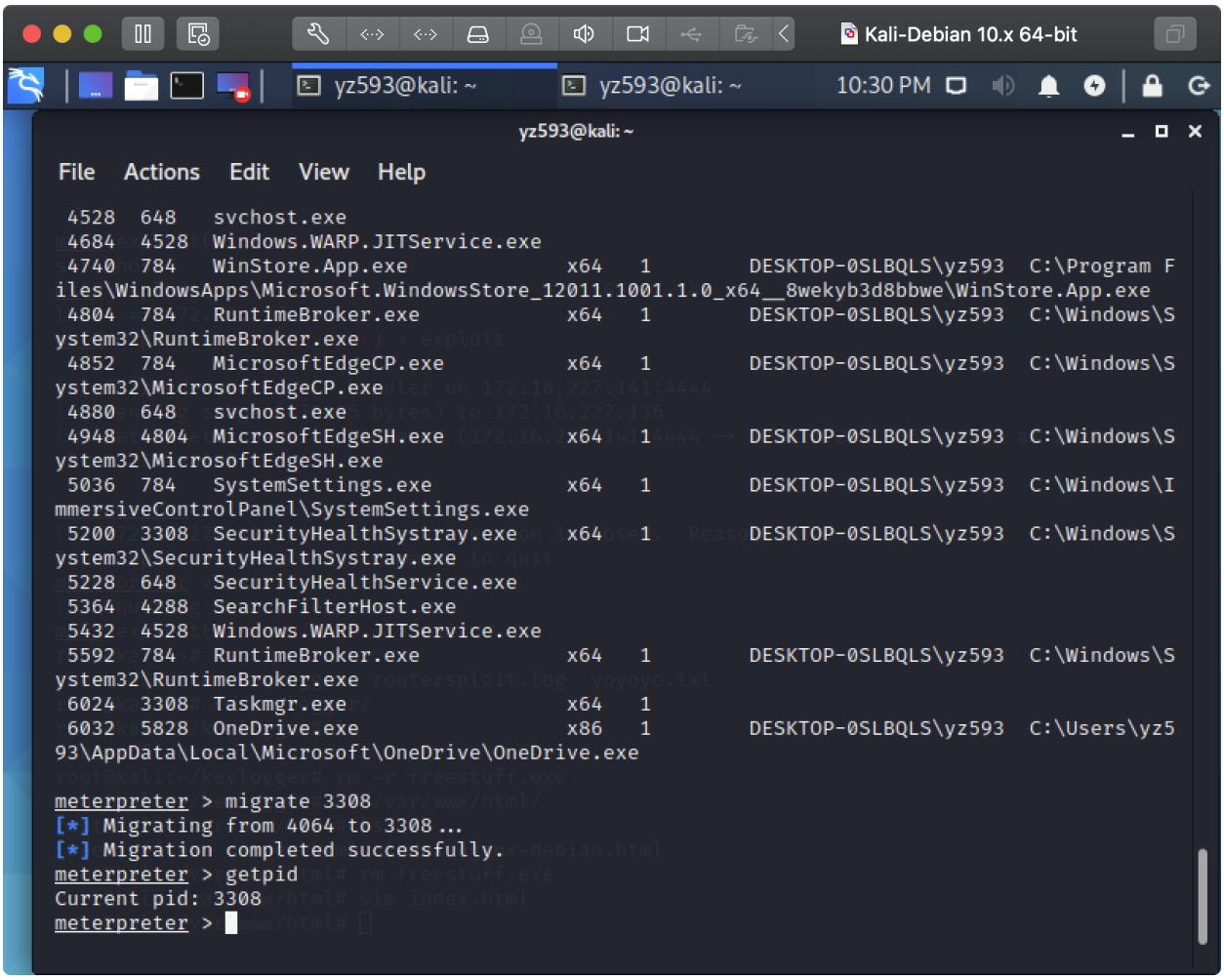
This shows a successful connection once the target runs the file. We are now inside the target's system, and are able to execute the keylogger.



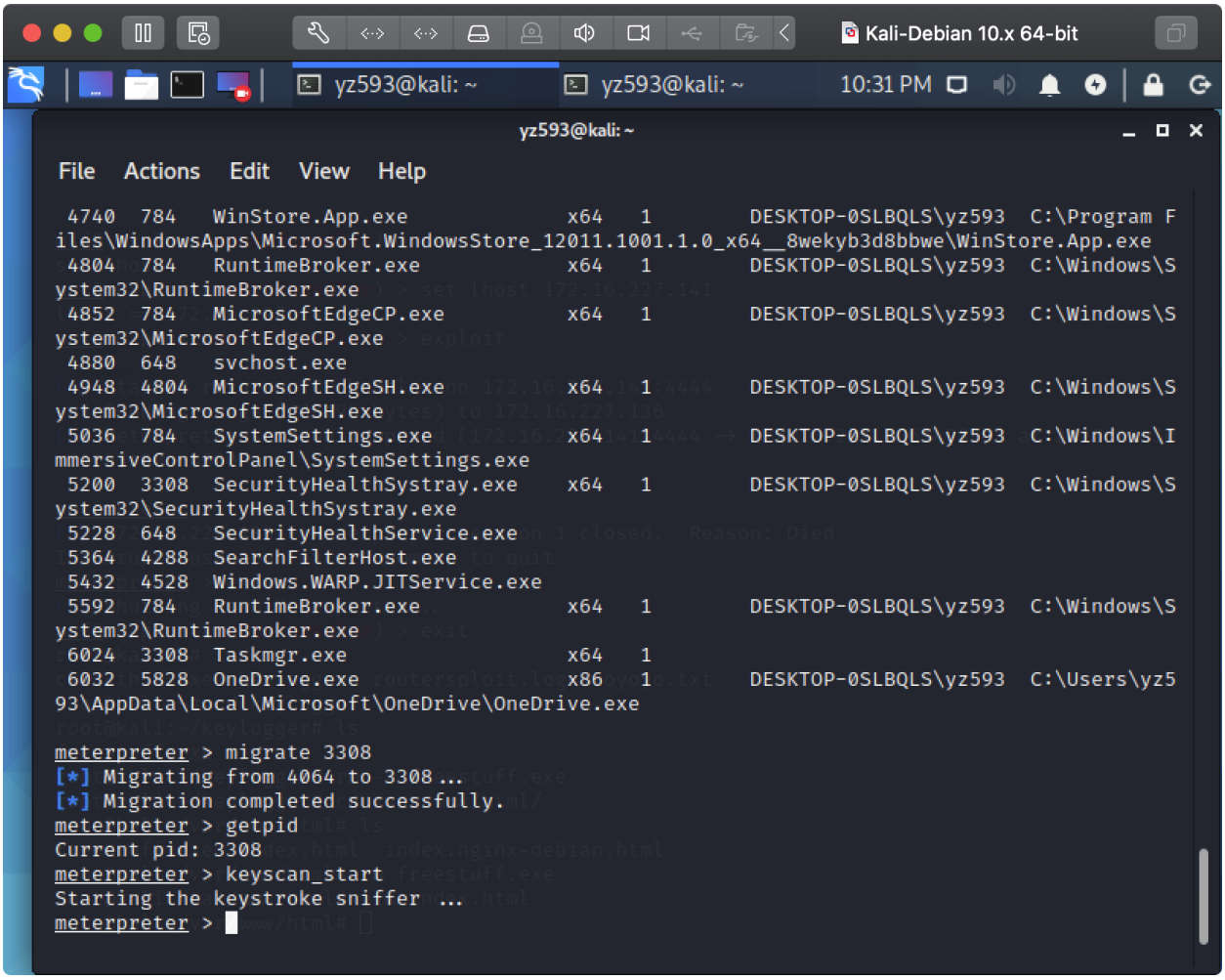
The “ps” command will show all the processes currently running on the target system.



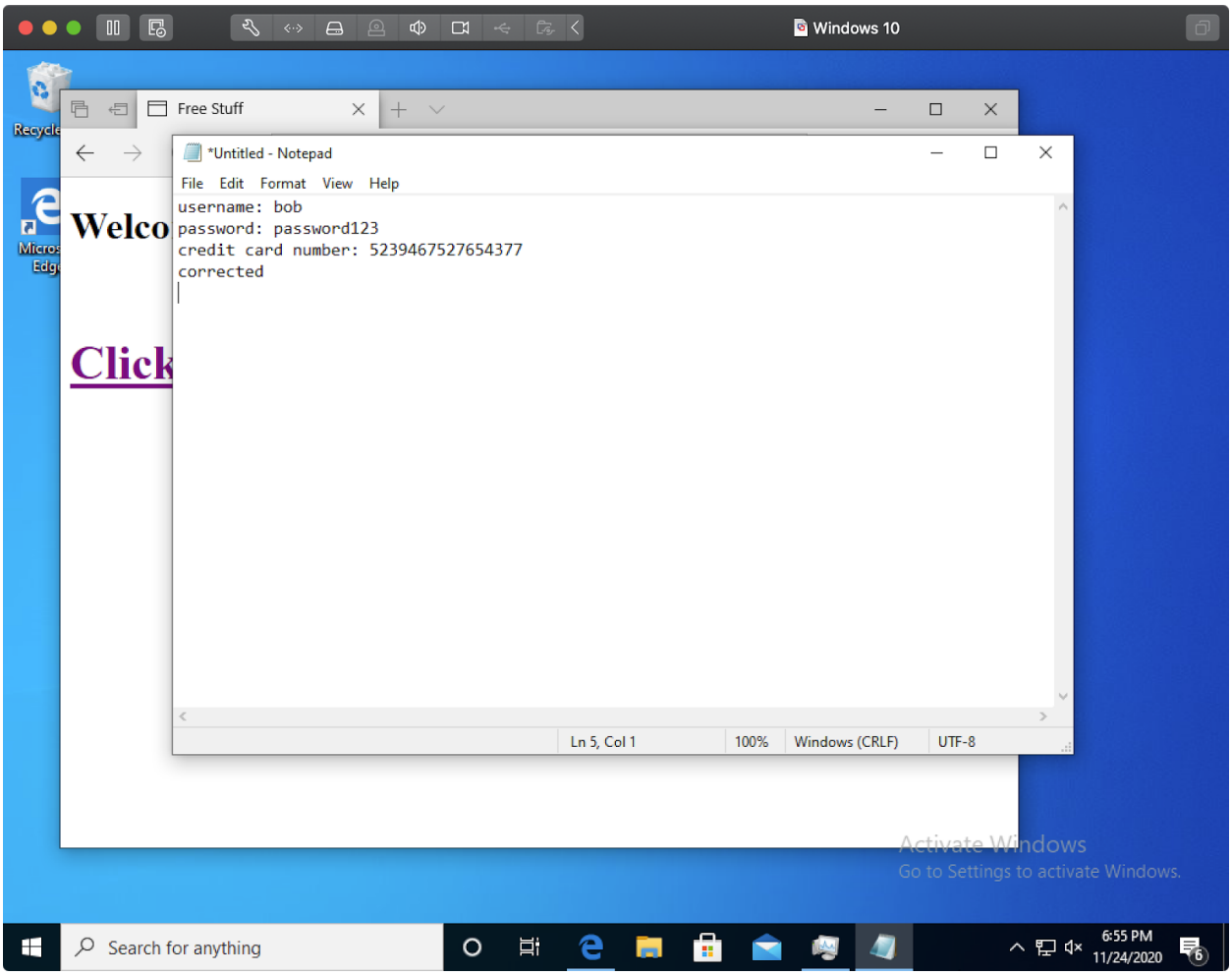
The “migrate” command will move the payload to another process on the target system when give the process ID(PID), in this case, I chose “explorer.exe” with a PID of 3308.



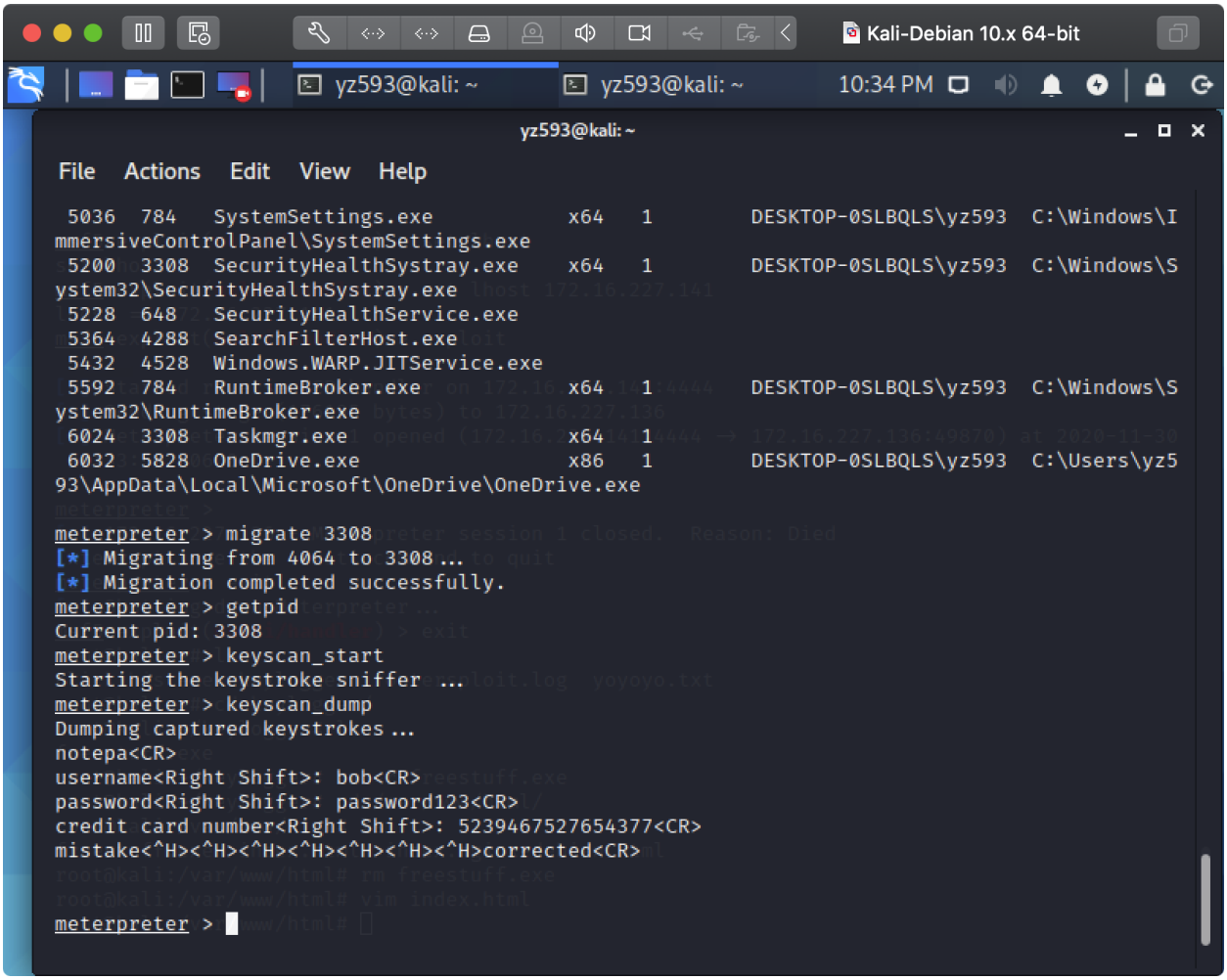
To start keylogging with the keyscan module, I use “keyscan_start” in Meterpreter. This will start the keyscan module and it will begin collecting any keystroke made by the target system.



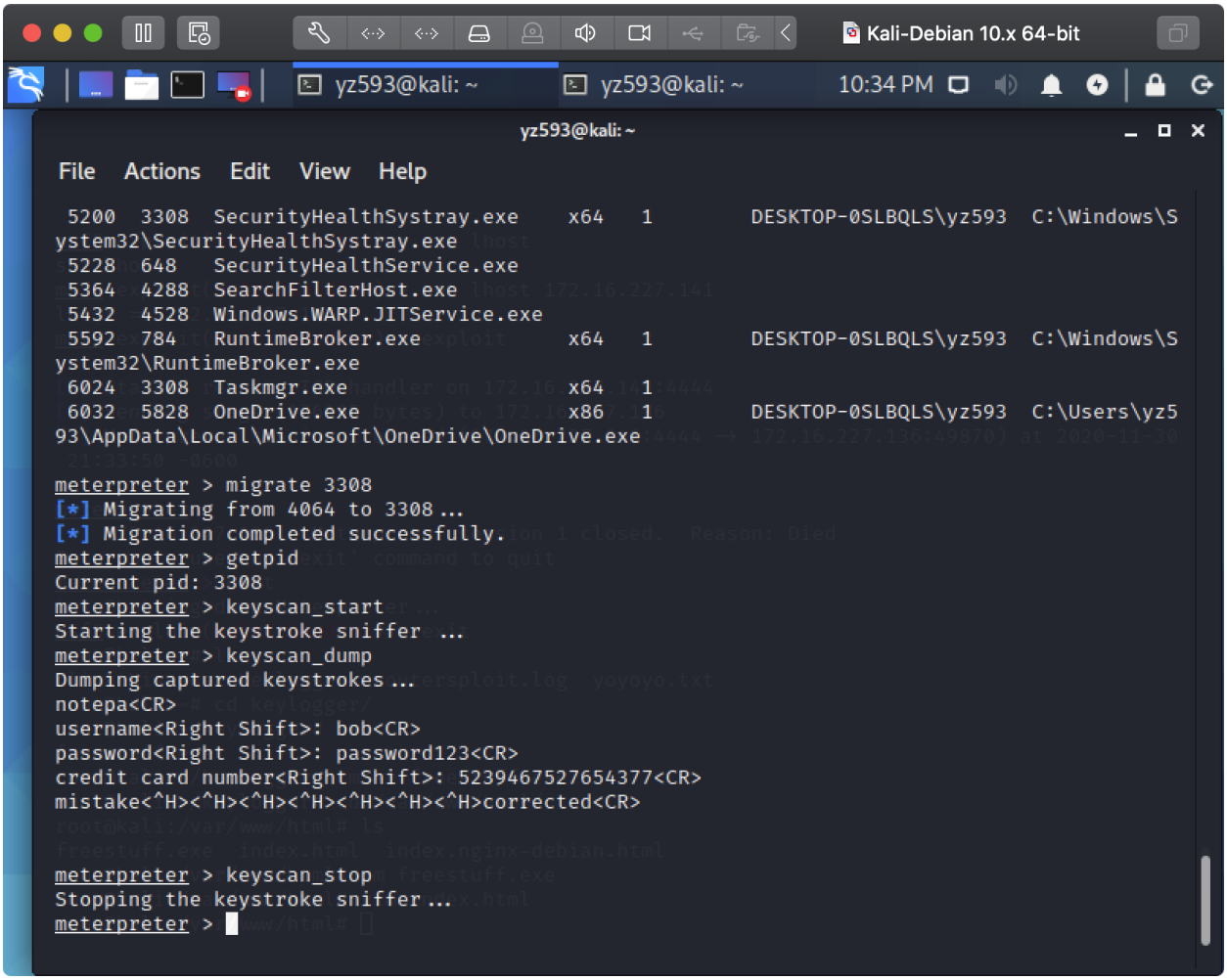
I opened Notepad on the target system and started to type things that a target might type in the real world.



To see what the target has typed, I used “keyscan_dump.” As you can see, the keyscan module captured everything, even the shift button.

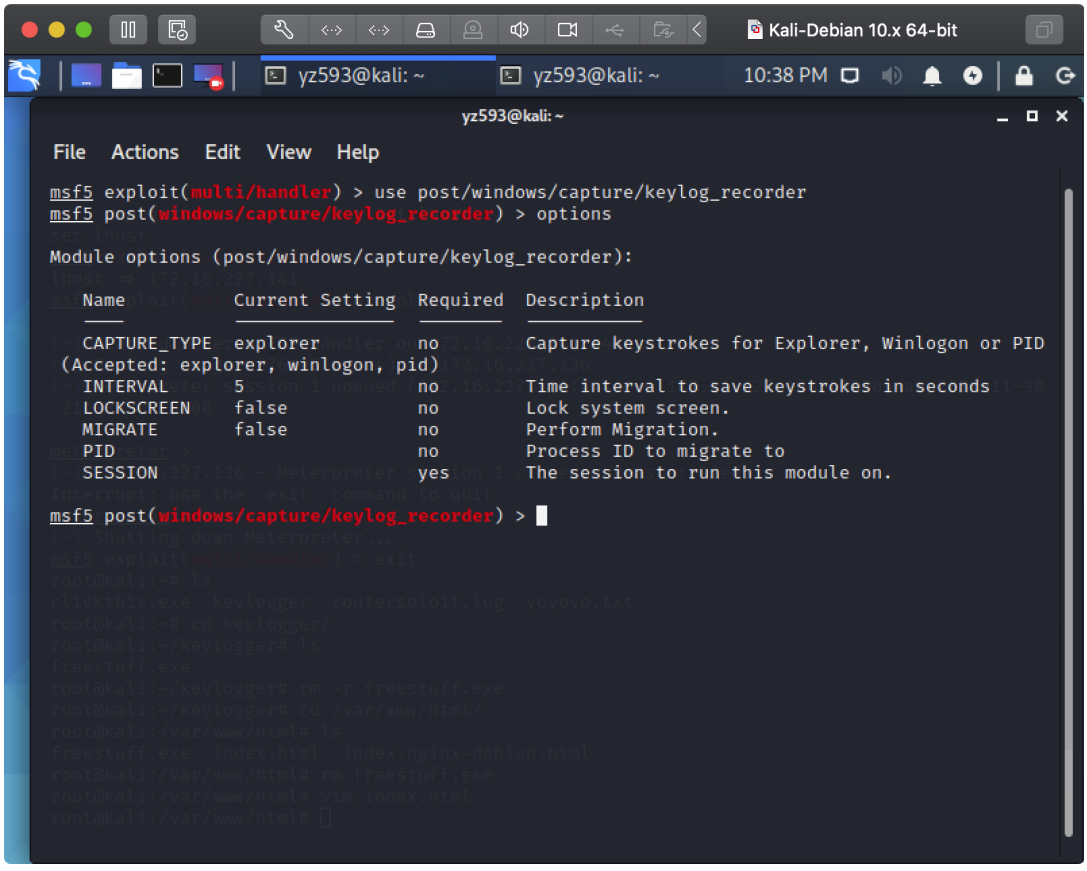


Simply type “keyscan_stop” to stop capturing keystrokes.

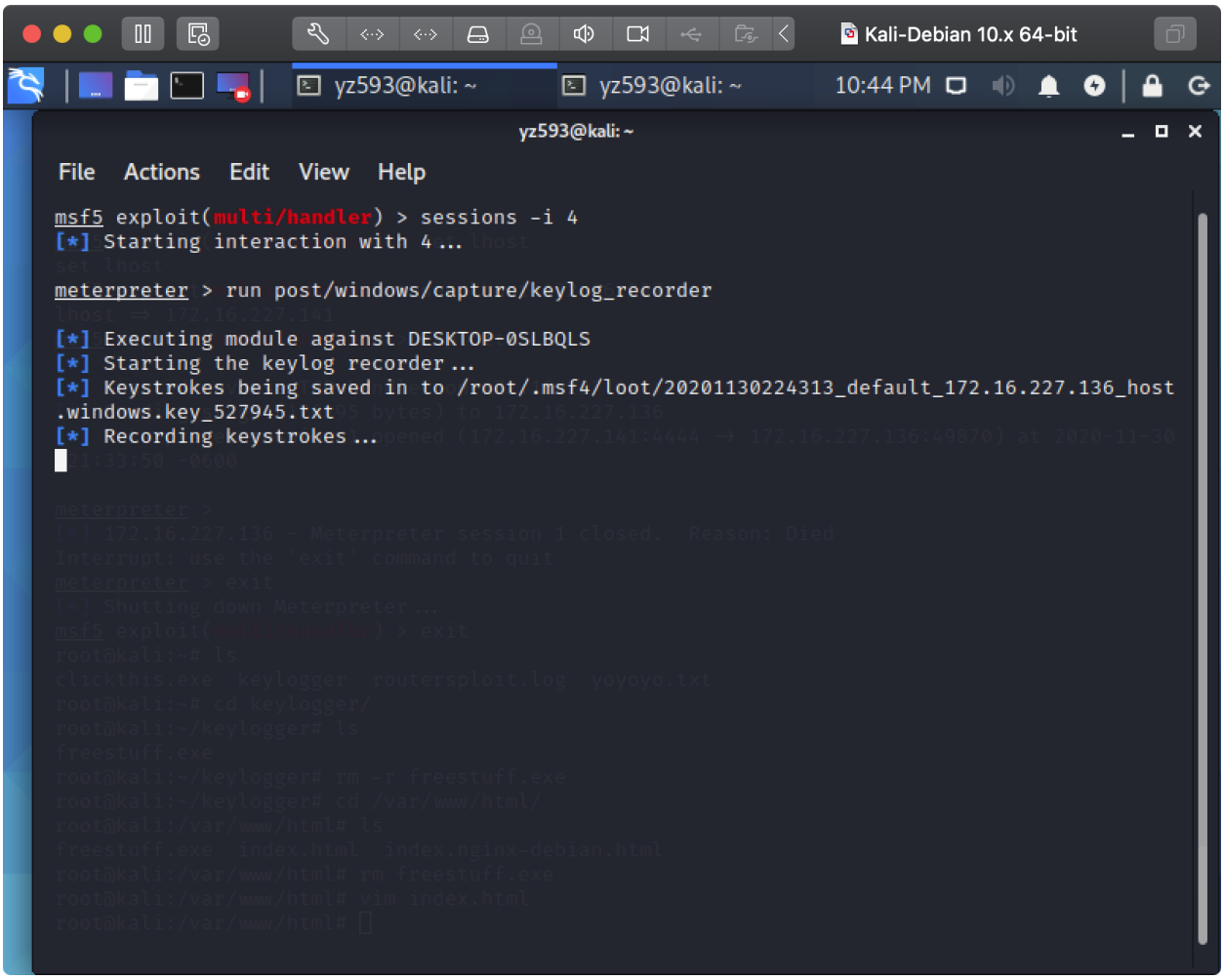


The keyscan module is a great module for keylogging, but “keyscan_dump” only returns keystrokes since the last time you executed “keyscan_dump,” and it is difficult to go back and view previous keystrokes. Another module for keylogging is the keylogrecorder. This is a keylogging module that prints the keystrokes in a log file, so you can access it any time.

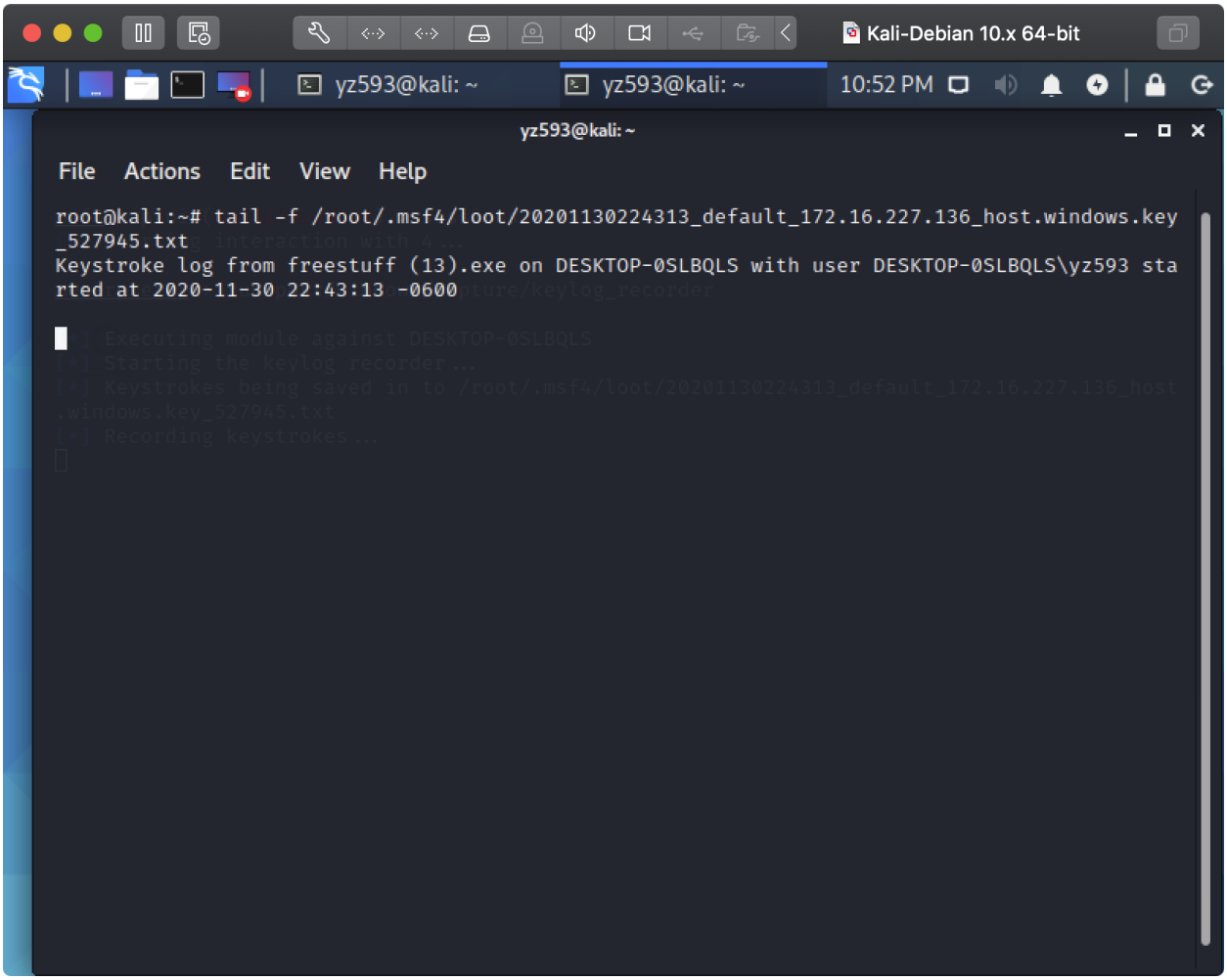
The image below shows how to access the keylogrecorder module. In the options, we can specify which process the keylogger will capture keystrokes. The interval will specify how long the module will wait before printing the keystrokes. A lower interval might result in separating lines of the same string, which might make it confusing to read later. This will be shown later. The lock screen setting will specify if the screen will be locked on load. This is useful when trying to capture windows login details, as it forces the target to enter their credentials before they can use their system again. The migrate setting will specify if the module will move to another process, if true, the PID will be needed to specify which process it will move to.



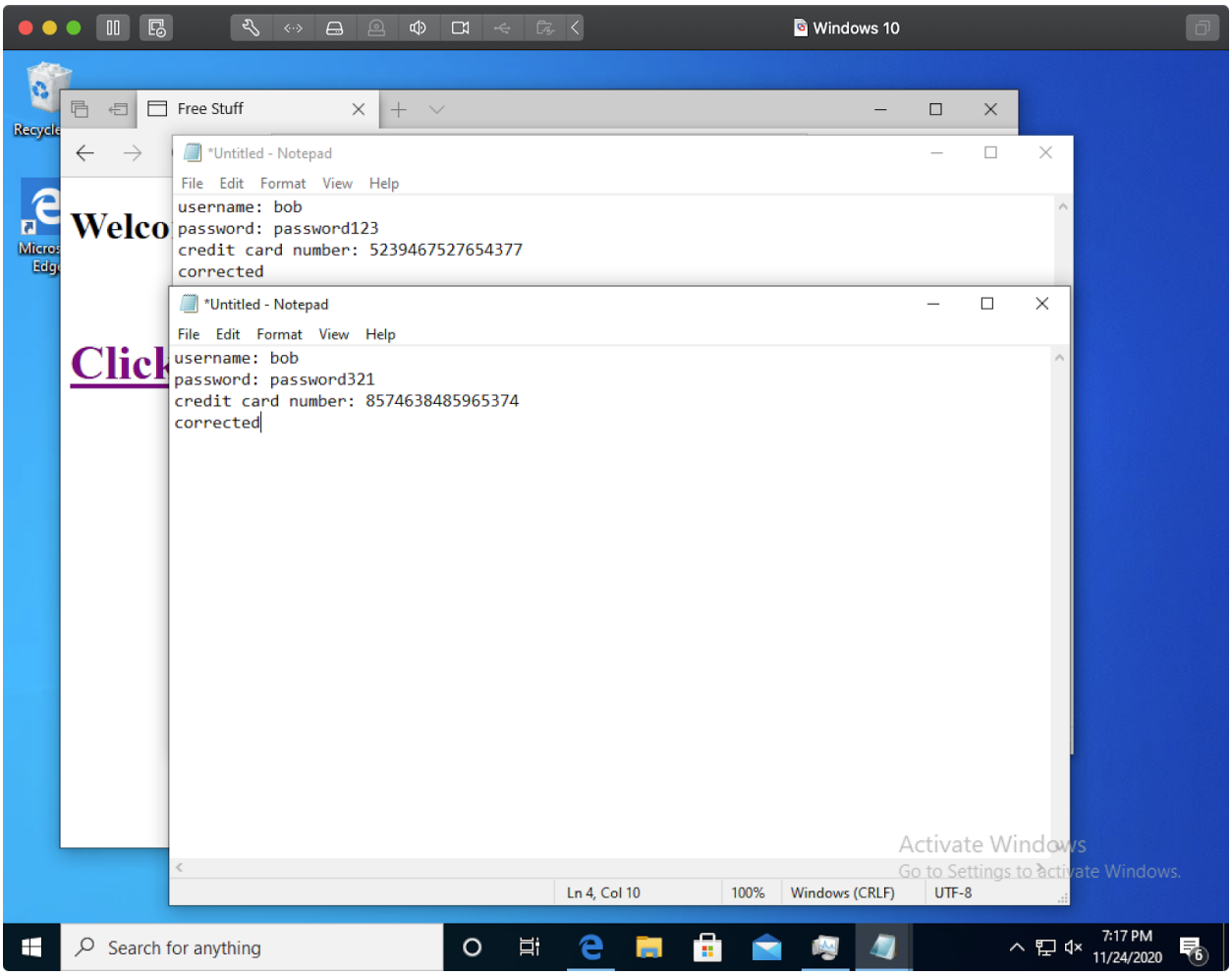
Once the module starts, any keystrokes made by the target system will be saved to the log file specified, and can be accessed any time.



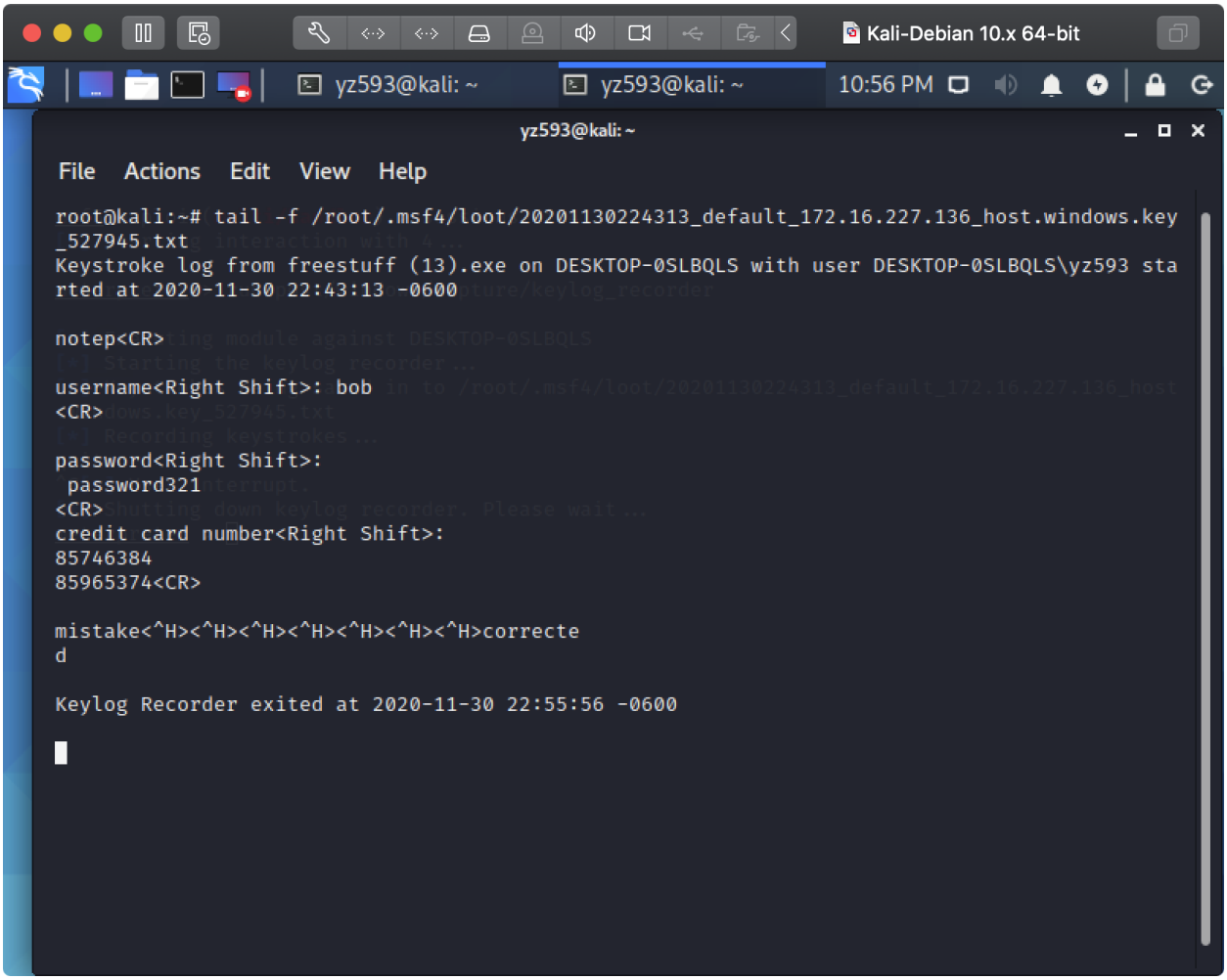
To see a continuous output of keystrokes, we can use the tail command with the -f flag. This will allow us to see the logs in real-time as new keystrokes are registered. This will all be saved in the log file.



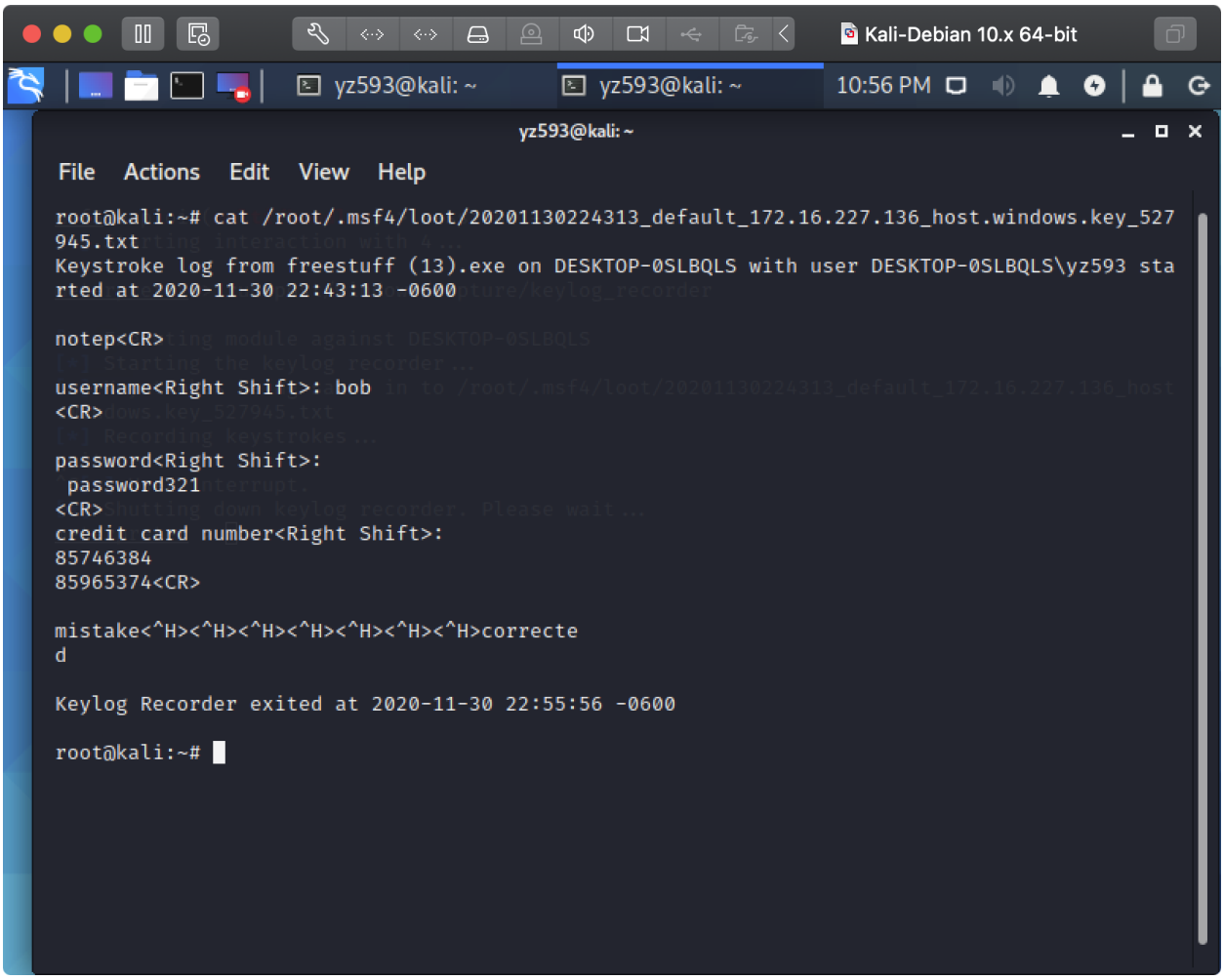
I opened up another Notepad to allow keylogrecorder to capture new keystrokes.



This shows the real time capturing of keystrokes using keylogrecorder.



This shows the output of the log file after it has captured the keystrokes.



References

Brinkmann, M. (2019, March 28). *Windows 10 "keylogger" setting moved in Windows 10 Spring Creators Update*. GHacks Technology News. https://www.ghacks.net/2018/03/26/windows-10-keylogger-setting-moved-in-windows-10-spring-creators-update/

Center, E. P. I. (n.d.). EPIC - United States v. Scarfo, Criminal No. 00-404 (D.N.J.). Epic.Org. https://www.epic.org/crypto/scarfo.html

Christensson, P. (2006). *Trojan Horse Definition*. TechTerms. https://techterms.com/definition/trojanhorse

Crypto Museum. (2015, October 14). *Selectric bug*. https://www.cryptomuseum.com/covert/bugs/selectric/index.htm

Microsoft. (n.d.). *Speech, voice activation, inking, typing, and privacy*. Microsoft.Com. https://support.microsoft.com/en-us/windows/speech-voice-activation-inking-typing-and-privacy-149e0e60-7c93-dedd-a0d8-5731b71a4fef

Offensive Security. (2019, November 2). *About the Metasploit Meterpreter*. https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/