FORDHAM UNIVERSITY

THE JESUIT UNIVERSITY OF NEW YORK

PENETRATION TESTING (CISC 7050)

Recon Automation

Name: Gopi Gor

FDIN: A21370441

Recon Automation

In this discussion, we have created a bash script to automate the tasks for Active Reconnaissance. We have used the bash script to automate Nmap and Netcat commands that we used in the Active Information Gathering lab. The script was saved as recon.sh and it has been shown below.

```
#!/bin/bash

# Defining the target IP address
target="10.0.2.5"

# Defining port range
port_range="100-1000"

# Nmap scan
echo "Running Nmap scan on target $target..."
nmap_result=$(nmap "$target") echo "Nmap scan result:"
echo "$nmap_result"

# Netcat scan
echo "Running Netcat on target $target..."
netcat_result=$(nc -v -n -z -w1 "$target" "$port_range")
echo "Netcat result for $target"
echo "$netcat_result"
```

The above script automates the process for the nmap and netcat commands we used previously. The target is pre-defined on this script to scan the metasploitable VM. It can also be altered to take user input. The port range has been predefined in this case too but can be changed in the script as needed. The script first runs an nmap scan on 10.0.2.5 as the target, and then to follow with it, it runs the netcat scan with the command ***nc -v -n -z -w1 10.0.2.5 100-1000*** to specify details and port numbers to be scanned. The nmap runs the command, and echo prints our result according to the nmap_result function. Similarly, the netcat program runs with the command specified and then prints the results obtained. This is very simple code to run automation for nmap and netcat and can be altered as per the commands required and more arguments can be defined as per the need.