“TBA” TO BE ANNOUNCED IS THE NEW SSLSTRIP

Virgil Vaduva

Man in the middle with sslstrip

- HTTPS stripping attack using homographs
- http://www.thoughtcrime.org/software/sslstrip/
- Written in Python
- Version 0.9
- Multiple attacks involved:
  - Arp spoofing/poisoning
  - Mis-direction and plaintext interception

ARP

- Address Resolution Protocol (ARP) is a telecommunications protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks.
- ARP was defined by RFC 826 in 1982.
- It is Internet Standard STD 37.

SSLSTRIP

- Transparently hijack HTTP traffic on a network, watch for HTTPS links and redirects, then map those links into either look-alike HTTP links or homograph-similar HTTPS links.
- It also supports modes for supplying a favicon which looks like a lock icon, selective logging, and session denial
- Requirement: Attacker and Victim must be on the same subnet

Step 1

- Enable forwarding:
- echo 1 > /proc/sys/net/ipv4/ip_forward

Step 2

- Poison ARP cache on victim machine using "arpspoof"
- arpspoof -i eth0 -t VICTIM_IP GATEWAY_IP
- arpspoof is part of the dsniff package with dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy
- http://monkey.org/~dugsong/dsniff/

ARP cache timeouts

- Windows 2000 – 10 minutes
- Windows XP – 2 minutes
- Windows 2008 - ?
- Fedora – 60 seconds
- OSX?

Step 3

- Use iptables to accept and forward interesting traffic
- iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-ports 10000
- Tables: filter, nat, mangle and raw
- Prerouting: alter packets before routing them
- Redirect: redirect packets to primary interface

Step 4

- python sslstrip.py -w logfile.txt

Defense?

- Replace ARP?
- Static entries
- Smarter browsers and users
- Anything else?