Anch Presents:

The Monkey In the Middle

A pen-testers guide to playing in traffic.

Twitter: @boneheadsanon

A little about me

Over 10 years experience in testing pens (Fountain is my favorite)

Why we play in traffic?

- Traffic is interesting stuff.
  - Gives us insight in to how things work.
  - Allows us to gather information on a target.
  - Allows us to change things as they go by.
  - Most importantly….
    - It allows us to prank our friends.

How to get into traffic…

- Always wear a helmet…
  - It can be dangerous.
    - Really messes with networks.
  - Your host might not be fast enough.
  - Switches alert on some things.
  - IDS usually will catch it.

How to get into traffic…

- A tool discussion
- ARP Spoofing
- DNS Poisoning/Spoofing
- DHCP Snooping
- Transparent Proxies

The most dangerous option

ARP Spoofing/ Poisoning

arpspoof - Provided as part of the dsniff suite of tools.

- EASILY detected on a network.
- If done incorrectly can take down entire segments of the network.
- Need a fairly powerful host to keep up with the traffic.

Another, slightly less dangerous way

DNS Poisoning/ Spoofing

Cain is able to perform this function amongst other tools.

- May still require you to ARP Spoof first.
- Used in conjunction with other tools
- Provides your IP address the answer to DNS queries.

Still a little less dangerous

DHCP Spoofing

The ever famous ettercap provides this function in an excellent way.

- Still need to be able to sniff traffic going to from your target (throwing star works well for this if you have physical access.
- Switches can be configured to check for, deny, and alert on this attack.
- Used in conjunction with other tools.

Actually doing something with traffic once you have it…

Proxies

Multiple tools provide this service:

- Burp
- Mallory
- Squid

Proxies

Burp Suite

Java, runs on almost anything, lots of options in the free version, paid has even more.

- Just Works most of the time.
- Will hold http gets/posts based on configuration.
- Can change cookies, variables, html responses.
- Has powerful SSL options.

Proxies

Mallory!

An excellent tool with very good SSL support, very fast and very configurable.

- Linux/MacOS are easiest to get working.
- Pretty advanced to get setup. Can be very picky.
- Not a lot of pre-built tools for it. (Some firefox extensions)
- Not maintained much.

Proxies

Squid

Fast regular caching proxy. Can be setup to be transparent with iptables/pf

- Good for fast static replacement.
- Lots of modules and support.
- Best to prank your friends with.

Time for a DEMO!

SSH Monkey In the Middle

Lets Talk about Pranks…

The “All Porn Internet” (Redux)

No Demo, but it’s available.

- Adjusts to your taste of pornography.
- Won’t force it on you, you have to ask for it.
- Gender/Preference Neutral

SSID: AllPr0nInternet
WPA: LetMeSeeIt!

"Sometimes questions are more important than answers."

–Nancy Willard