

ARP Poisoning

Andy Ying



ARP Overview

- What is ARP?
- What does it do?
- How does it work?

Structure of an ARP Packet

```
struct arp_hdr
{
    uint16_t htype;
    uint16_t proto;
    uint8_t  hsize;
    uint8_t  psize;
    uint16_t opcode;
    uint8_t  src_mac[6];
    uint8_t  src_ip[4];
    uint8_t  tgt_mac[6];
    uint8_t  tgt_ip[4];
}
```

How ARP Normally Works

- Host A would like to send Host B some data.
- Host A looks in its ARP Cache and determines if an IP->MAC mapping exists.
- For this case assume that they have never communicated before, therefore a mapping does not exist.

How ARP Normally Works (cont)

- Host A sends an ARP Request that says, "Who has the IP of Host B Tell Host A"
- Host B is listening and replies, "IP B is MAC of B".
- Host A updates it's ARP table with the IP->Mac mapping.
- Host A can now communicate freely with Host B having established its location on the network.

Notice any problems?

ARP Flaws

- Stateless Protocol, unlike TCP/IP
- Lacks authentication of any kind
- This means we can have some fun :)

ARP Poisoning, the Fun Part

- Motivations: Why do we want to do this?
- We want to observe the traffic occurring between two machines.

ARP Poisoning

- Assume we have Host A, Host B, and Host M where host M is out machine
- We need A to think B is at M and B to think A is also at M
- How do we do this?

ARP Poisoning

- Host M floods ARP reply packets essentially saying “IP A is at MAC of M” and “IP B is at MAC of M”
- This updates both Host A and Host B's ARP tables
- End result? Host M is the “man in the middle”

ARP Poisoning

- However, there are problems
- Data sent by Host A to Host B will stop at Host M
- Data sent by Host B to Host A will stop at Host M
- We need to route data from Host A to Host B through Host M and vice versa.

Man in the Middle

- Store a table of original MAC addresses and route packets to the appropriate location
- Create an unique MAC address dedicated to spoofing
- Tedious to write the tool yourself

Toolz

- "Ettercap is a suite for man in the middle attacks on LAN. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols (even ciphered ones) and includes many feature for network and host analysis. "

Ettercap

- [root@noone ~]\$ ettercap -T -q -M arp /target ip/ -w output.packets
- -T text mode
- -q don't print raw packet dumps
- -M man in the middle (use arp as opposed to icmp redirection, so we specify a type) /target ip/ of the form /1.2.3.4/ or /1.2.3.0-255/
- -w output.packets write all data to a pcap file

Questions?

Source code at
<http://www.int8h.com/code/arpp>

Citations

- <http://vividmachines.com/download/arpetter.html>