

Wall of Sheep

Encrypt,
Or You'll
Regret it in
the End



Tools and Techniques to Succeed at the Wall of Sheep

By: Ming Chow
(ming@wallofsheep.com)



ARIES SECURITY



Our Mission

Security Awareness



ARIES SECURITY



How We Accomplish Our Mission

- Volunteers
- Interactive demonstrations, unconventional methods
- *WoS Sheep Herder* - Capturing and displaying thousands of sheep for security awareness
- (2010 - 2011) *Peek-a-Boo Booth* - Coin operated network sniffer, image display; raised money for the EFF
- (2011) *Juice Jacking* - Power charger security project
- *Capture The Packet (CTP)* - Network forensic skills assessment Challenge, now a DEF CON Black Badge Event
- (2011, 2012) *Wall of Lambs* - 2 talks, 1 workshop at r00tz Asylum (formerly known as DEF CON Kids)
- (2011, 2012) *Kids CTP* - 2 talks, 1 workshop to DEF CON Kids
- *Wi-Fi Sheep Hunt* - hunt mobile wireless devices around DEF CON
- *Speaker Workshops* - 30 minute hands on demos of how to do something real. No theory or vaporware
- *NEW 2013, Packet Detective* - Introduction to network forensics game / training
- *NEW 2013, NFC Scavenger Hunt*



ARIES SECURITY



What is Network Sniffing?

- Look at network traffic
- Also known as analyzing packets
- Most of the traffic on a network is unencrypted, plaintext ("in the clear")

Things That You Can Do...

- Troubleshoot networking issues
- Record communications (e.g., email, voice, chat)
- Record and analyze web traffic
- Catch usernames and passwords, personal information, and other sensitive information

Anatomy of a Network Packet

- **Packet** - unit of data
- A **data stream** (e.g., video, a web page) is comprised of many packets
- In general, a packet contains the following information:
 - Source and destination IP addresses and ports
 - MAC address
 - Time To Live (TTL)
 - Protocol (e.g., TCP, UDP, ICMP)
 - Payload

Getting Started: What You Need

- A computer with wired or wireless networking.
Any platform is acceptable
 - You can also choose a Linux distro live-CD aimed at penetration testing such as BackTrack or Kali to get up-and-running quickly
- Administrative access on computer is required!
- Access to a **span port**, **LAN tap**, or a **network hub**
- For the purpose of this presentation, we will be using Linux.

Span Port

- Also known as port mirroring
- All the packets on one switch port (or an entire virtual LAN) to another port

LAN Tap

- Typically small devices
- Used to monitor Ethernet communications



ARIES SECURITY



Network Hub

- Device for connecting multiple Ethernet devices to a single network segment
- Divides bandwidth across all the ports

Getting Started: First Things First

- Step 1: Put your network card to **promiscuous mode**
 - **Promiscuous mode** - look at all packets regardless of destination address
- Step 2: Disable the use of the Address Resolution Protocol (ARP)
 - For Unix/Linux/Macs: `sudo ifconfig -i <INTERFACE> promisc -arp`
- An interface is the network hardware you want to use for sniffing. To see list of interfaces, run `ifconfig`

A .pcap File

- The common file extension for packet captures and is commonly used in many applications such as Wireshark, ettercap, tcpdump
- A 100 MB pcap file contains tens of thousands of packets
 - We commonly save our network traffic into 100 MB files

tcpdump

- A packet analyzer that runs via command line
- To run: `sudo tcpdump -i <INTERFACE>`
- The manual: `man tcpdump`
- Example: splitting a PCAP file into smaller ones (e.g., 10 MB)
 - `tcpdump -r old_file.pcap -w new_files -C 10`

Wireshark

- Graphical and extensive packet analyzer
- Very similar to tcpdump
- Open source and free
- Features include filtering, reconstructing conversations, reconstructing files based on packets
- <http://www.wireshark.org/>

tshark

- Dumps and analyzes network traffic
- Command-line-based Wireshark
- Installed with Wireshark
- The manual: `man tshark`
- Example, list the hosts in the pcap file
 - `tshark -r file.pcap -q -z hosts,ipv4`

Ettercap

- Graphical and command-line based
- Is not intended for network traffic analysis but has capabilities for:
 - Capturing passwords
 - Conducting man-in-the-middle (eavesdropping) attacks
 - Hijacking sessions
- To run (command line): `sudo ettercap -Tzq`
- The manual: `man ettercap`
- <http://ettercap.github.io/ettercap/>

dsniff

- Suite of networking sniffing tools including
 - dsniff - password sniffer
 - webspy - intercepts URLs entered
 - mailsnarf - intercepts POP or SMTP-based mail
- Written by Dug Song in 2000
- To run: `sudo dsniff -i`
`<INTERFACE>`

ngrep

- Recall `grep`
- Network `grep`
- Currently recognizes IPv4/6, TCP, UDP, ICMPv4/6, IGMP, etc.
- <http://ngrep.sourceforge.net/>
- Example, search for text strings in a PCAP file: `ngrep -q -I file.pcap | grep -i user`

Where Do You Go From Here?

- Sniff and validate passwords
- Reconstruct files (e.g., images, mp3s)
- Volunteer at the Wall of Sheep
- Develop your skills on Packet Detective
<http://www.packetdetective.net>
- Enter Capture The Packet, a DEF CON Black Badge contest

Questions?



ARIES SECURITY



Thank You

References and Cheat Sheets

- <http://www.wallofsheep.com/pages/reference-material>
 - Videos
 - Trainings
 - How-to's
 - Reference material
 - Links to tools that we use