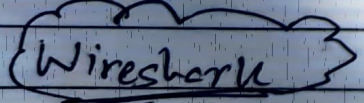

- a network protocol analyser
- logs packets that flow thru selected interfaces
- analyses all packets

Subject :

PAGE NO.:
DATE:

→ designed for network admins to monitor network
→ Open wireshark on kali.
→ go to file → open → {open files that you sniffed} (packets)

☆ Wireshark will capture things flowing thru your iface.
→ It wont capture packets that doesn't go thru your iface | own pc.

→ # run bettercap using caplet spoof
→ go to any website on victim
→ eth0 will capture those packets as you are the MITM
∴ to use wireshark for victim, you need to spoof first.

Sniff & Analyze

↳ Store the packets somewhere permanently, if needed.
↳ Filter information.
  ↳ After capturing all the packets,
  ↳ in the display filter, type http to get filtered packets.
  ↳ Double click any packet to analyze

↳ to discover passwords
  ↳ look for POST requests
  ↳ and open it to look for the data needed

☆ In caplet spoof:
  → before net.sniff on
  → write: set net.sniff.output /root/capture file.cap

☆ This will store all packets in the file, for future analysis.

Subject :

PAGE NO.:
DATE:

Fake Access Point

- access point receives all the requests
- we can replace the access point itself
- we'll create a fake wifi network w/ internet.
- when people connect to it, we'll automatically become MITM since we are router itself.

★ You need:

→ any interface w/ internet across
→ wireless adapture supporting AP Mode

~~★ In settings of kali-VM:~~

★ For our system,

→ eth0 is the internet interface
→ wlan0 is the wireless adapter (not connected)

→ use wifi-hotspot
→ set any ssid
→ open network
→ wifi interface = wlan0
→ internet interface = eth0
→ create hotspot

Detect ARP Poisoning Attack

- run arp -a to list entries of arp table
- ARP poisoning worked because of responses of trust
- when we do arp poisoning, the MAC address of router, in arp -a, changes to the address of attacker
- This is the simplest way to detect it.

→

Subject :

PAGE NO.:
DATE:

☆ There's a tool XARP (xarp) that detects it automatically.
→ it automatically monitors arp tables
→ once arp poisoned, Xarp tells us that there has been an ARP attack.

⇒

☆ Using Wireshark:
↳ go to preferences → protocols → arp → enable detect arp requests storms
⇒ This will detect if someone pings all connected devices on the network.
⇒ Go to analyze → expert information, to get more info.

☆ You can also change address type to static. This won't allow address change.

→ All these detection happens only for ARP Spoofing.
→ Solution is to encrypt our traffic.
↳ use vpn
↳ use only https (plugins available)