MAN IN THE MIDDLE ATTACKS

@shritesh
Tennessee Tech CyberEagles Club

ARP

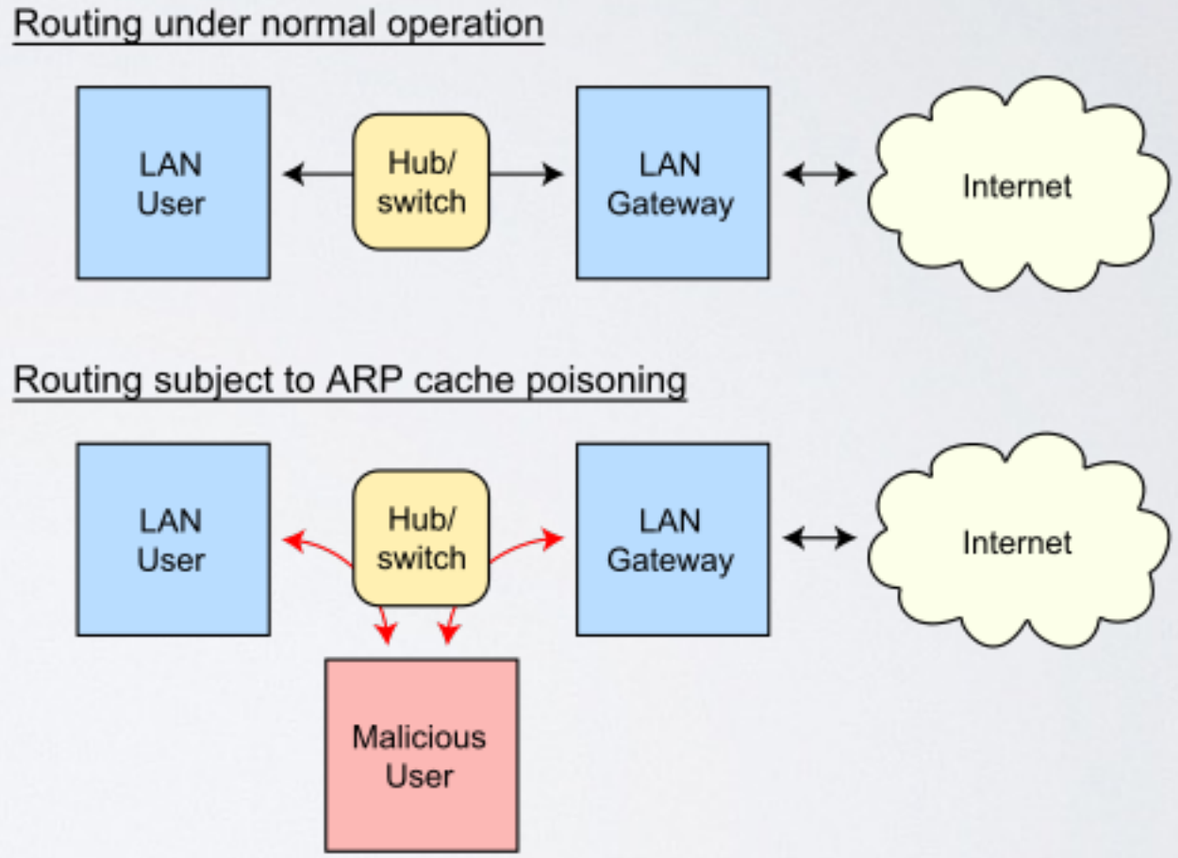
- Address Resolution Protocol
- RFC 826 (1982)
- “IP Address to MAC Address for Ethernet”
- Request <=> Reply
- Response is cached

ARP - PROBLEMS

- Entries are simple mappings
- Stateless
- No authentication
- Ethernet stack depends heavily on ARP

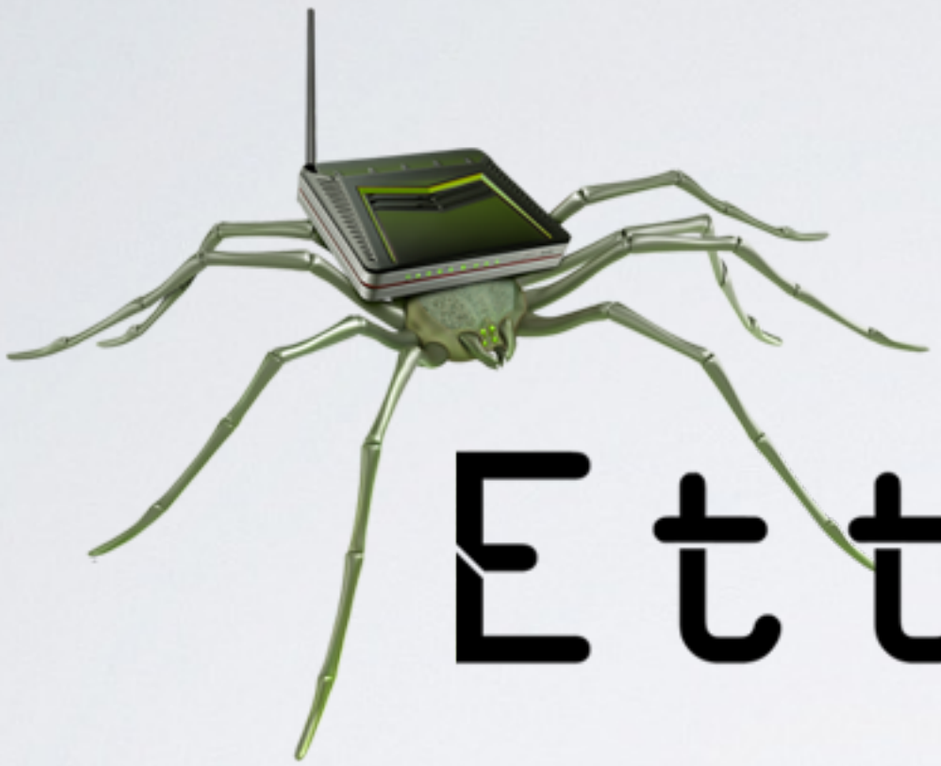
ARP SPOOFING

- Client in a network sends spoofed ARP messages
- Other clients update their ARP mappings
- Traffic is sent to the malicious client



Wikipedia: 0x55534C

April 29



Ettercap

MITM ATTACK WITH ETTERCAP

Tennessee Tech CyberEagles Club


bettercap
A complete, modular, portable and easily extensible MITM framework.

ENTER: BETTERCAP

- Written in Ruby // Opinionated
- Works on *nix
- Easy and intuitive
- Extendible
- Batteries Included
- Actively Developed

BETTERCAP

- Network Discovery
- ARP Poisoning
- Credential Sniffer
- Proxy
- Reset

DEMO TIME

- Simulate ‘casual’ network

- WAN connection with Router

DEFENSES

- Static ARP*
- Physical Security
- ArpON, ARPDefender, …
- Encryption: HTTPS (HSTS), TLS, …

BIGGER PICTURE

- Security is difficult
- Technology adoption is slow
- Humans > Technical Flaws

Thank You!!!

{twitter,github}.com/shritesh