WIRESHARK

Internet Traffic Monitoring and Analysis:

Wireshark Exercises

Dr.S.Geetha

School of Computer Science and Engineering

VIT, Chennai

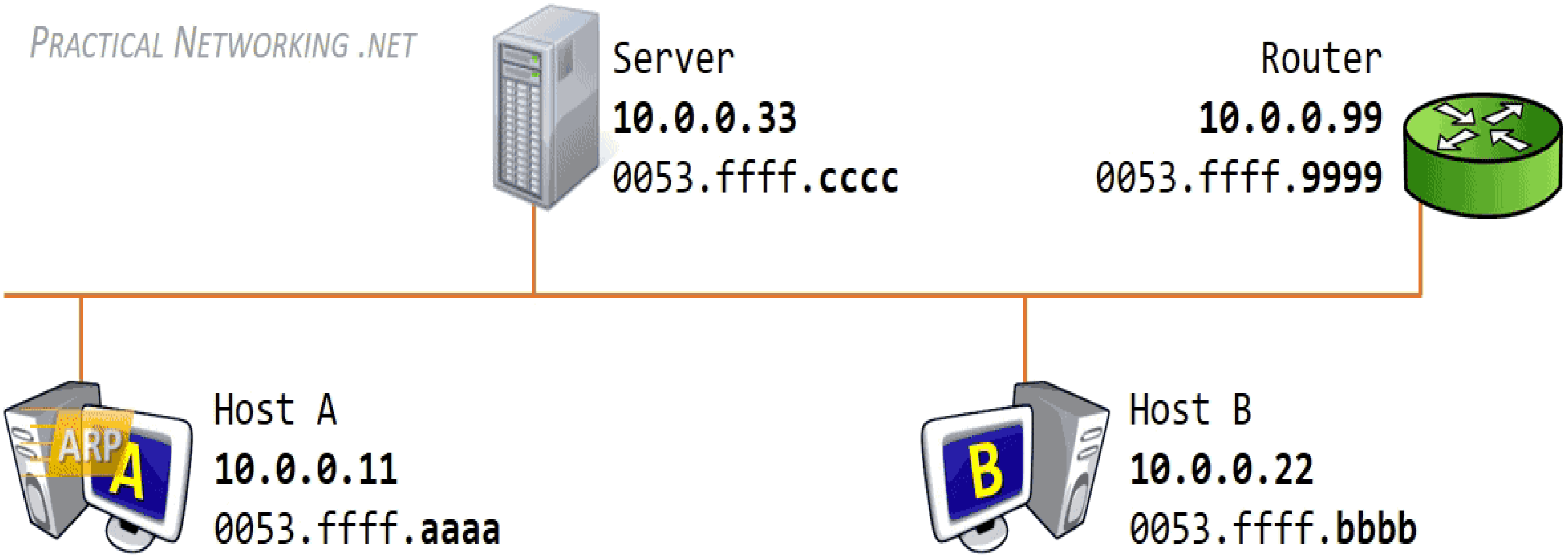
geetha.s@vit.ac.in

WIRESHARK

1. ARP
2. TCP 3 way handshake
3. Packet Sniffing – Password Cracking
4. Packet Analysis
5. Filters - sample

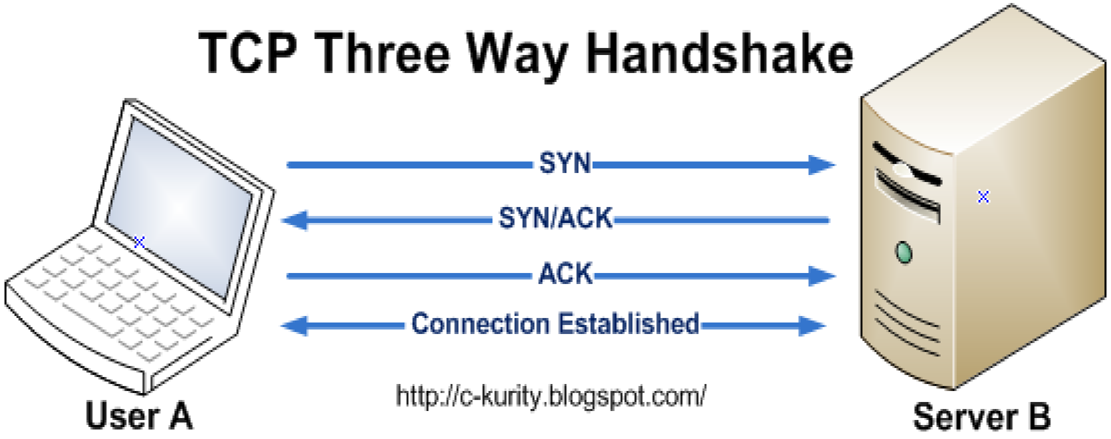
-

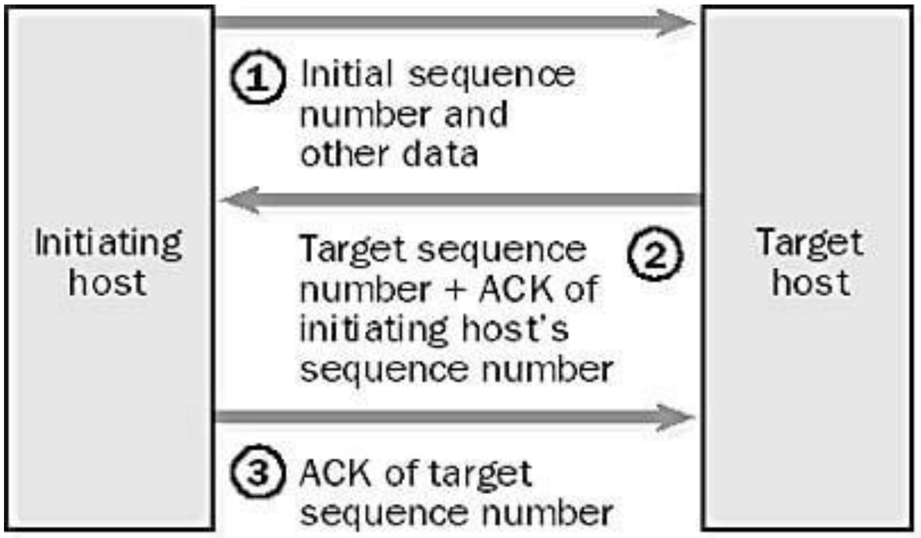
Address Resolution Protocol

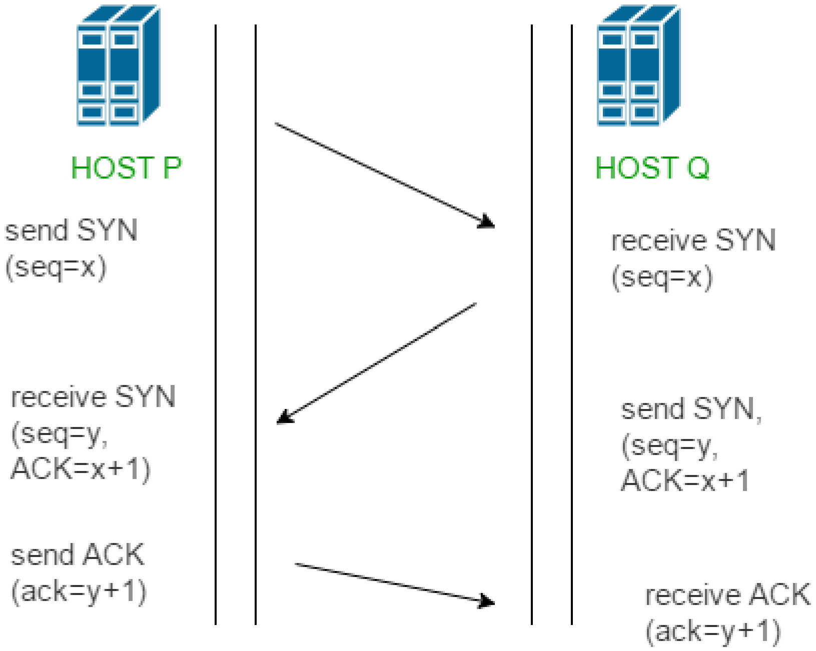


https://www.practicalnetworking.net/series/arp/traditional-arp/

TCP 3 Way Handshake




Initiating host
1 Initial sequence number and other data
2 Target sequence number + ACK of initiating host's sequence number
3 ACK of target sequence number
Target host



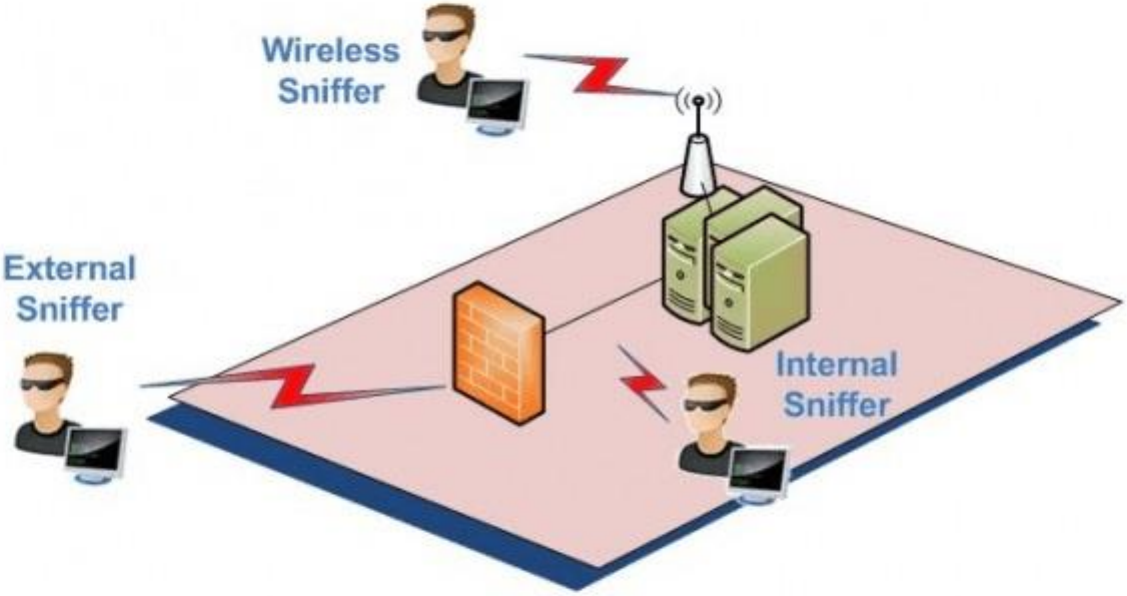
Network Sniffing

- Computers communicate by broadcasting messages on a network using IP addresses. Once a message has been sent on a network, the recipient computer with the matching IP address responds with its MAC address.
- **Network sniffing is the process of intercepting data packets sent over a network.**
- Capture sensitive data such as login credentials
- Eavesdrop on chat messages
- Capture files have been transmitted over a network

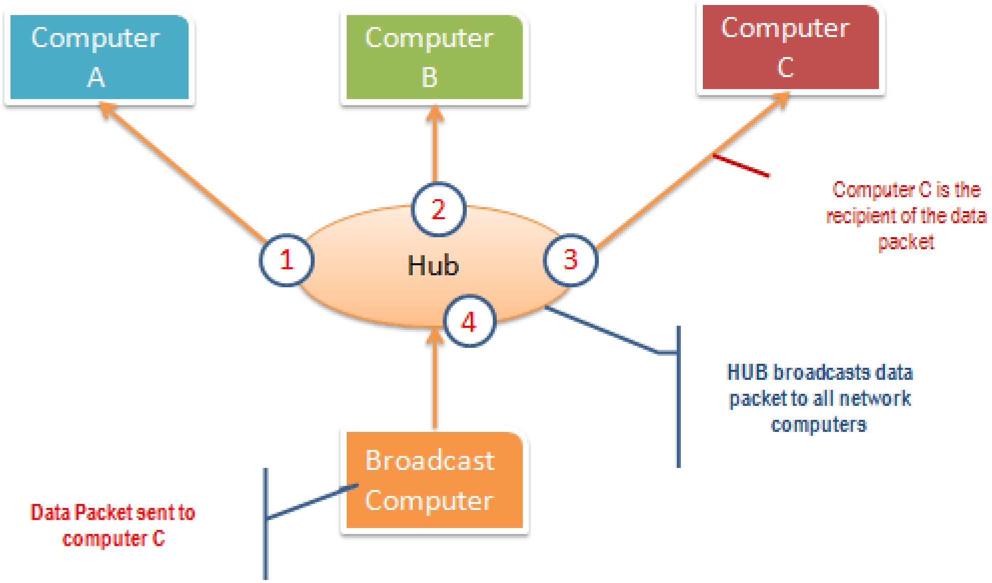
Network Sniffing

Vulnerable Protocols (if login details are sent in plain text)

- Telnet
- Rlogin
- HTTP
- SMTP
- NNTP
- POP
- FTP
- IMAP



Active & Passive Sniffing



Computer A

Computer B

Computer C

Hub

1

2

3

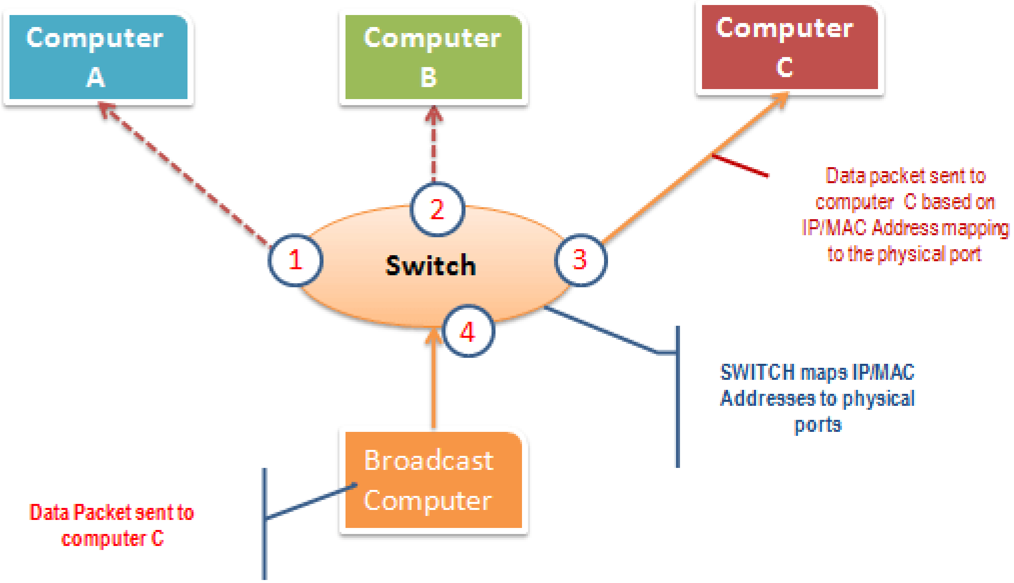
4

Broadcast Computer

Computer C is the recipient of the data packet

HUB broadcasts data packet to all network computers

Data Packet sent to computer C



Computer A

Computer B

Computer C

Switch

1

2

3

4

Broadcast Computer

Data packet sent to computer C based on IP/MAC Address mapping to the physical port

SWITCH maps IP/MAC Addresses to physical ports

Data Packet sent to computer C

Password Cracking

- weevil.info
- http://testing-ground.scraping.pro/login?mode=login
- You can try this on any of your personal ftp, application software (PUTTY)
- What about on https sites?
- Multiple ways
  - Edit→ Filter packets → string and then search
  - Filters →

Password Cracking

Ping packets (ICMP)

www.1112.net/lastpage.html - TCPStream

TCP Congestion Control testmy.net (Upload huge data) Statistics --> TCP Stream Graph

- 6. TCP Filters
- ip.addr == 10.0.0.1
- tcp or dns
- tcp.port == 443
- tcp.analysis.flags
- !(arp or icmp or dns)
- follow tcp stream
- tcp contains facebook
- http.response.code == 200
- http.request
- tcp.flags.syn == 1