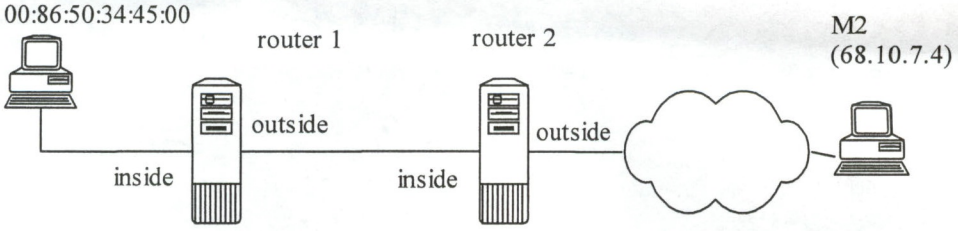
CPRE 530 Exam 1 Fall 2013

NAME: Vivek Sribalusu (vivek@iastate.edu) **SCORE:** 94

1. (15 pts) Given the figure below fill in the table below. An IP packet with 2400 bytes of user data needs to be sent across an Ethernet network from machine M1 to machine M2 and therefore needs to be fragmented. Show the fragments for the network segment **between the two routers** (fill in the table [all parts of the table that are blank], for the data field indicate the length of the data). Assume the first fragment is as large as possible for an Ethernet network.

M1
IP = 129.186.5.4
Enet = 00:86:50:34:45:00



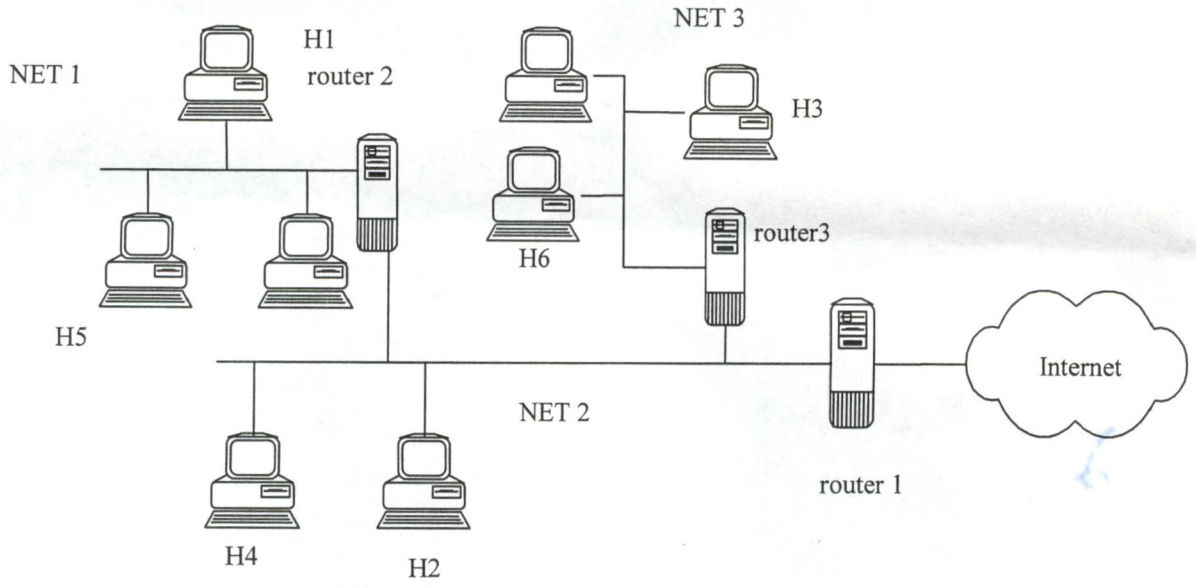
Router 1
outside
IP = 192.34.25.10
Enet = 00:80:08:45:22:FF
inside
IP = 129.186.5.254
Enet = 00:80:08:34:12:45

Router 2
outside
IP = 12.123.34.45
Enet = 00:88:88:38:12:EC
inside
IP = 192.34.25.15
Enet = 00:7C:23:33:19:AA

-6

Layer	Field Name	Original	Fragment 1	Fragment 2
Ethernet	Destination	N/A	~~00:88:88:38:12:EC~~	~~00:88:88:38:12:EC~~
	source	N/A	~~00:86:50:34:45:00~~	00:86:50:34:45:00
	Type field	N/A	N/A	N/A 800
IP	Ver/IHL	4 5	4/5	4/5
	Type	0	0	0
	Len	~~2420~~ 2440	1500 ~~+496~~	~~984~~ 940
	ID	1774	1774	1774
	Flags	0 0 0	0 0 1	0 0 0
	Offset	0	0	182
	TTL	144	~~+47~~	~~147~~ 143
	Protocol	17	17	17
	Checksum	Computed	Computed	Computed
	Source IP	129.186.5.4	129.186.5.4	129.186.5.4
	Destination IP	68.10.7.4	68.10.7.4	68.10.7.4
Data		2400 bytes	~~1456~~ 1480	944 920

2. (20 pts) Using the figure below answer the following questions



Assume the following addresses:

Name	IP
H1	129.186.5.4
H2	129.186.4.10
H3	129.186.10.20
H4	129.186.4.25
H5	129.186.5.34

Name	IP
Router 2	129.186.5.254 (for the network 129.186.5.0)
Router 2	129.186.4.100 (for the main network)
Router 1	129.186.4.254 (for the main network)
Router 1	10.0.0.5 (for the internet side)
Router 3	129.186.4.253 (for NET 2)
Router 3	129.186.10.254 (the NET 3)

Assume DNS is not used

Assume H5 sent a message to H1, H2, H3, H4, H6 and a machine on the Internet (207.14.19.47). How many entries would be in H5's ARP table due to these messages?

H5's ARP table would contain 2 entries :-
message from H5 to H1 -> ARP for H5
message from H5 to H2, H3, H4, H6, 129.186.5.254 for -> ARP for Router 2

For the next three parts assume all caches are cleared before machine H5 sends a single ICMP ECHO request to machine H3

How many packets are transmitted on the network segment NET 1 (including the ECHO request and reply)?

4 packets are transmitted

How many packets are transmitted on the network segment NET 3 (including the ECHO request and reply)?

4 packets are transmitted

How many packets are transmitted on the network segment NET 2 (including the ECHO request and reply)?

4 packets are transmitted.

3. (10 pts) Describe ARP cache poisoning and what damage an attacker could cause by poisoning the ARP cache.

ARP cache poisoning or spoofing is a technique whereby an attacker sends fake Address Resolution Protocol (ARP) message onto a Local Area Network. The aim is to associate the attackers MAC address with the IP address of another host causing any traffic meant for that IP Address to be sent to the attacker instead.
ARP cache poisoning allows an attacker to intercept data frames on a LAN, modify or stop the traffic altogether. Often the attack is used for opening of other attacks such as denial of service, man in the middle or session hijacking.

4. (15 pts) Which category or categories in the taxonomy does each of the following mitigate?

a) VLAN

- Traffic - Based Vulnerabilities and Attacks

b) WPA/WEP

- Authentication Based Vulnerabilities and Attacks
- Traffic Based Vulnerabilities and Attacks.

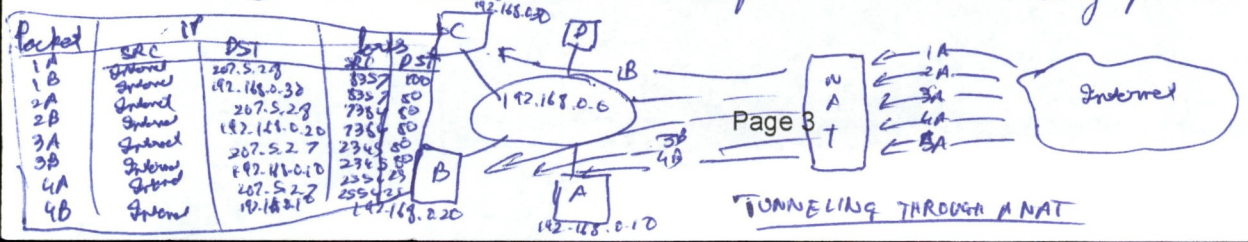
c) VPN/IPSEC

- Authentication Based Vulnerabilities and Attacks.
- Traffic Based Vulnerabilities and Attacks.

5. (10 pts) Describe how a tunnel is used to allow remote users to access a web server that has a private address behind a NAT.

The idea behind the tunnel is to map a public IP address and port number to a private IP address and port number. When a packet arrives at the NAT on a port that has been tunneled, the NAT takes the inbound packet and re-writes the IP address and port numbers and sends the packet to the computer in the private network based on the values in the tunnel table. The tunnel table indicates that the packet should be sent to the device with the private IP address. NAT rewrites destination IP address and destination port. The following figure shows packets 2 and 3 from a device on the Internet connecting to a web server that are on private network using port 80 on public Internet.

Packet	IP SRC	IP DST	ports SRC	ports DST
1A	Internet	207.5.2.8	3357	100
1B	Internet	192.168.0.30	3357	80
2A	Internet	207.5.2.8	7364	80
2B	Internet	192.168.0.20	7364	80
3A	Internet	207.5.2.7	2345	80
3B	Internet	192.168.0.10	2345	80
4A	Internet	207.5.2.7	2557	25
4B	Internet	192.168.0.20	2557	25



TUNNELING THROUGH A NAT

Public IP	Public Port	Private IP	Private Port
207.5.2.7	25	192.168.0.10	25
207.5.2.7	80	192.168.0.10	80
207.5.2.8	100	192.168.0.20	80

6. (30 pts) Describe each of the following and what impact it will have on security:

a. Rogue wireless access point

An access point that is installed inside a network without the knowledge of the organization.

Impact:

Rogue access points pose a security threat to large organizations with many employees, as anyone with access to premises can install a router that can potentially allow access to secure network to unauthorized parties.

b. Rogue DHCP server

A Rogue DHCP server is a DHCP server on a network which is not under the administrative control of the network staff.

Impact:

It can be used to cause network attacks like man in the middle attack.

c. Network Sniffing

network sniffing is the process in which as data stream flow across the network, sniffer captures each packet and if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content

Impact:

The impact of network sniffing is loss of confidential data like unencrypted username, passwords. It can also impact the bandwidth and computing power utilization.

d. Denial of service

Denial of service attack is an attempt to make a machine or network resource unavailable to its intended users. It generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the internet.

Impact:

DoS attack temporarily or indefinitely interrupt or suspend services of a host connected to the ~~so~~ internet.

e. IP Address Spoofing

IP Address spoofing is the creation of Internet Protocol packets with a forged source IP address, with the purpose of concealing the identity of sender or impersonating another computing system.

Impact:

IP spoofing is most frequently used in Denial of Service attack. IP spoofing can also be a method of attack used by network intruders to defeat network security measures.

f. Fake wireless access point

Fake wireless access point is an access point set up by an attacker to mimic the access points installed within an organization.

Impact:

The attacker can obtain the access to the network of the organization with the access to its confidential data.