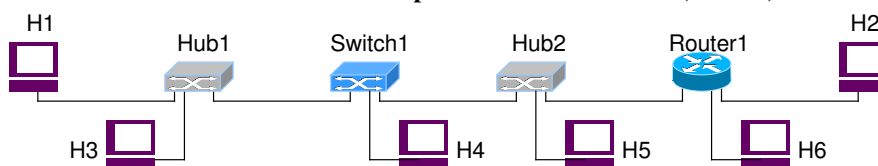


Corso di Sicurezza nelle reti
a.a. 2009/2010

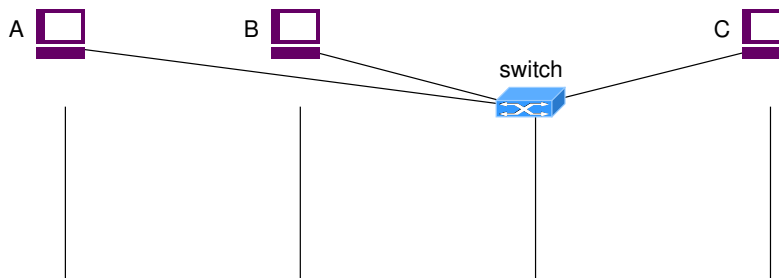
Raccolta di quesiti sulla seconda parte del corso

- 1) Nel seguente schema di rete IP su Ethernet quali nodi possono ascoltare (eavesdropping) il traffico scambiato tra H1 e H2?

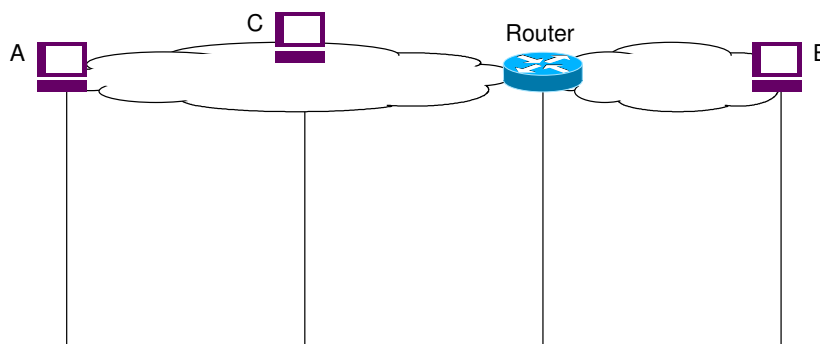
Quali nodi possono effettuare un attacco diretto di tipo Man In The Middle (MITM)?



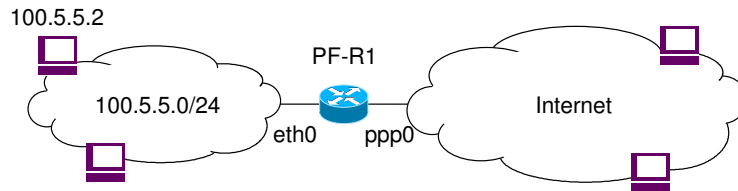
- 2) Nel seguente schema di rete indicare una possibile sequenza di messaggi di un attacco di ARP spoofing (indicato anche come ARP poisoning) da parte del nodo C (attaccante) verso il nodo A (vittima), dove B è il nodo "spoofato". Se ipA, macA, ipB, macB, ipC, macC sono rispettivamente gli indirizzi IP e MAC dei tre nodi, indicare le tabelle ARP di A e C dopo l'attacco.



- 3) Nel seguente schema di rete indicare una possibile sequenza di messaggi di un attacco di ICMP spoofing di tipo ICMP redirect da parte del nodo C (attaccante) che tenta di fare un Man In The Middle tra A (vittima) e B. Si consideri il caso in cui A e B si vogliono scambiare i seguenti 4 pacchetti IP: pkt1:A→B, pkt2:B→A, pkt3:A→B, pkt4:B→A, e l'attacco avvenga sull'invio del primo pacchetto (pkt1).

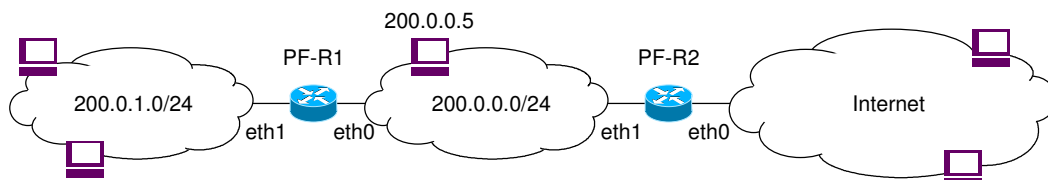


- 4) Si consideri il seguente schema di rete e si supponga che all'indirizzo 100.5.5.2 sia presente un server web HTTP (porta TCP 80) e un server di posta elettronica SMTP (porta TCP 25); si chiede di configurare la tabella di filtering del router R1 in modo che:
- sia possibile accedere dall'esterno al server web interno (100.5.5.2),
 - da tutti in nodi della rete interna sia possibile accedere a qualsiasi server web esterno (limitatamente alla porta TCP 80),
 - sia possibile la comunicazione tra il server SMTP interno de eventuali server SMTP esterni in entrambi i versi (client interno → server esterno porta TCP 25, e server interno porta TCP 25 ← client esterno)



FORWARD								
matching								action
in_int	out_int	s_addr	d_addr	proto	s_port	d_port	altro	ACCEPT/ DROP

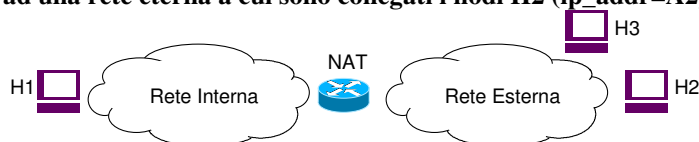
- 5) Si consideri il seguente schema di rete aziendale composta da una rete interna e da una DMZ separate dal screening router R1 e collegate alla rete esterna (pubblica) tramite il screening router R2. Si chiede di configurare la tabella di filtraggio (ACL) di R2 in modo che:
- sia possibile instaurare comunicazioni a livello applicativo client-server (con qualsiasi protocollo di trasporto) da qualsiasi nodo della DMZ verso qualsiasi nodo della rete esterna;
 - sia bloccata qualsiasi comunicazione client/server da rete esterna a DMZ;
 - sia bloccata qualsiasi comunicazione tra rete interna e rete esterna;
 - sia possibile instaurare connessioni TCP da rete esterna al nodo 200.0.0.5, porta 80 (HTTP).



- 6) Considerando lo schema di rete dell'esercizio precedente si configuri la tabella di filtraggio (ACL) di R1 in modo che:
- e) sia possibile instaurare comunicazioni a livello applicativo client-server (con qualsiasi protocollo di trasporto) da qualsiasi nodo della rete interna (200.0.1.0/24) verso la DMZ;
 - f) sia bloccata qualsiasi comunicazione client/server da rete DMZ alla rete interna;
 - g) sia bloccata qualsiasi comunicazione tra rete interna e rete esterna.

FORWARD								
matching								action
in_int	out_int	s_addr	d_addr	proto	s_port	d_port	altro	ACCEPT/ DROP

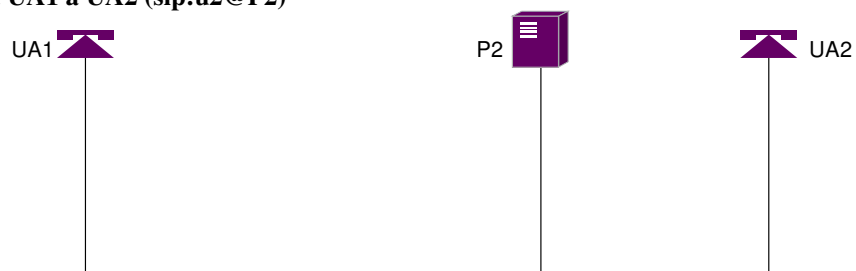
- 7) si consideri il seguente schema di rete in cui un nodo NAT che interconnette una rete interna, a cui è attaccato l'host H1 (ip_addr=A1), ad una rete eterna a cui sono collegati i nodi H2 (ip_addr=A2) e H3 (ip_addr=A3).



Se il nodo H1 invia il seguente datagramma UDP al nodo H2: $\text{pkt1}=\text{A1:p1} \rightarrow \text{A2:p2}$, e se tale datagramma viene modificato dal NAT in $\text{pkt1}'=\text{A10:p10} \rightarrow \text{A2:p2}$, quali dei seguenti pacchetti inviati da H2 e H3 a H1 arriveranno effettivamente ad H1 nell'ipotesi che il NAT sia di tipo "restricted cone NAT"?

- $\text{pkt2}=\text{A2:p2} \rightarrow \text{A1:p1}$
- $\text{pkt3}=\text{A2:p4} \rightarrow \text{A1:p1}$
- $\text{pkt4}=\text{A3:p3} \rightarrow \text{A1:p1}$
- $\text{pkt5}=\text{A2:p2} \rightarrow \text{A10:p10}$
- $\text{pkt6}=\text{A2:p4} \rightarrow \text{A10:p10}$
- $\text{pkt7}=\text{A3:p3} \rightarrow \text{A10:p10}$

- 8) Indicare una possibile successione di messaggi relativi alla registrazione di un UA2 (sip:u2@P2) su un proxy P2 e della chiamata da UA1 a UA2 (sip:u2@P2)



- 9) Nello stesso scenario del quesito precedente, indicare un possibile attacco di call hijacking (dirottamento di chiamata) da parte di un attaccante UA3

