

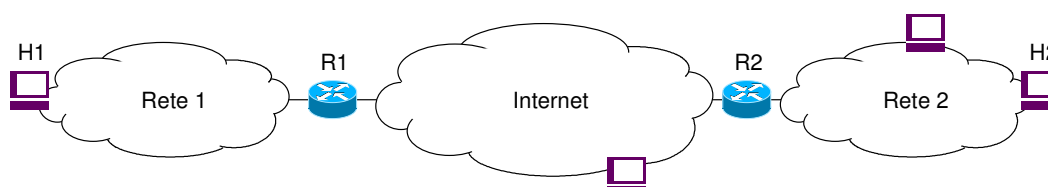
Corso di Sicurezza nelle reti
a.a. 2011/2012

Raccolta di quesiti sulla seconda parte del corso

- 1) Indicare un possibile schema di Key establishment tra due entità A e B di tipo “Symmetric key transport” (schema di Key transport basato su Symmetric key senza utilizzo di server KDC).
- 2) Indicare un possibile schema di Key establishment tra due entità A e B di tipo “Symmetric key transport” (schema di Key transport basato su Symmetric key senza utilizzo di server KDC) con challenge-response.
- 3) Perché il seguente schema di Key distribution tra due entità A e B tramite KDC e basato su crittografia simmetrica non è sicuro?
(si è indicato con K_a e K_b le chiavi segrete condivise rispettivamente tra KDC e A, e KDC e B; con K_s la chiave di sessione).

A	→	KDC:	ID_a, ID_b
KDC	→	A:	$ID_b, \{K_s\}_{K_a}, \{K_s\}_{K_b}$
A	→	B:	$ID_a, \{K_s\}_{K_b}$

- 4) Indicare un possibile schema di Authentication and key distribution tra due entità A e B tramite KDC e basato su crittografia simmetrica (e.g. Needham-Schroeder Protocol).
- 5) Indicare un possibile schema di Key transport tra due entità A e B basato su crittografia a chiave pubblica e senza KDC.
- 6) Si consideri lo schema di rete rappresentato in figura in cui due sottoreti aziendali sono interconnesse tra loro in VPN tramite rete IP pubblica attraverso IPSec.
Nell'ipotesi che la VPN sia instaurata tra i router R1 e R2 utilizzando ESP e AH (con AH che protegge anche il contenuto di ESP), e che si utilizzino i meccanismi di incapsulamento con minor overhead tra quelli possibili (transport/tunnel), si chiede di:
 - i) indicare lo schema dei pacchetti che transitano nel tratto di rete esterna inviati da H1 a H2;
 - ii) per ogni eventuale header IP di tali pacchetti specificare l'indirizzo di sorgente (SA) e di destinazione (DA); come indirizzo usare il nome del nodo.

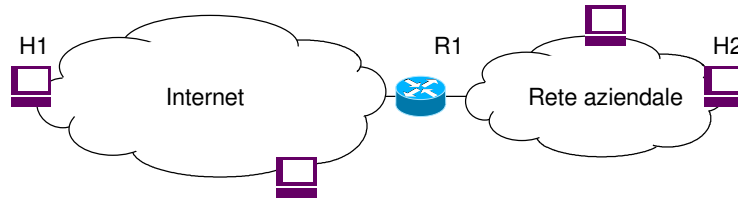


- 7) Si consideri uno scenario tipo road-warrior in cui un nodo H1 si collega tramite IPSec alla sua rete aziendale e comunichi in modo sicuro con un nodo interno H2, come rappresentato in figura.

Nell'ipotesi che H1 si colleghi alla sua rete tramite il router R1 in IPSec/ESP, che H1 protegga la sua comunicazione con il nodo H2 tramite IPSec/ESP, e che si utilizzino i meccanismi di incapsulamento con minor overhead tra quelli possibili, si chiede di:

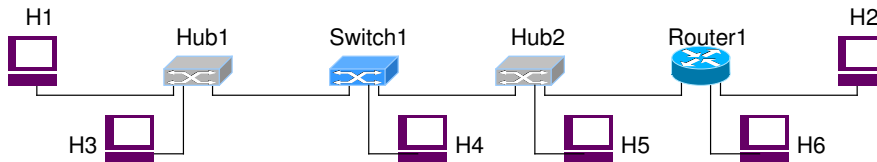
iii) indicare lo schema dei pacchetti che transitano nel tratto di rete esterna inviati da H1 a H2;

iv) per ogni eventuale header IP di tali pacchetti specificare l'indirizzo di sorgente (SA) e di destinazione (DA).

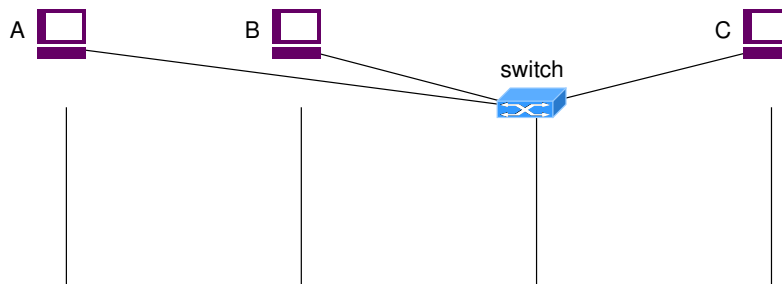


- 8) Nel seguente schema di rete IP su Ethernet quali nodi possono ascoltare (eavesdropping) il traffico scambiato tra H1 e H2?

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



- 9) 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 "spoofo". 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.



- 10) 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).

