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

Soluzioni dei 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).

SOLUZIONE
$A \rightarrow B$: $E_{Kab}(Ks)$

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.

SOLUZIONE
$B \rightarrow A$: n_B
$A \rightarrow B$: $E_{Kab}(Ks,n_B)$

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 Ka e Kb le chiavi segrete condivise rispettivamente tra KDC e A, e KDC e B; con Ks la chiave di sessione).

A	→	KDC:	ID_a, ID_b
KDC	→	A:	IDb, $\{Ks\}_{Ka}$,$\{Ks\}_{Kb}$
A	→	B:	IDa, $\{Ks\}_{Kb}$

SOLUZIONE
B non ha la prova che la chiave ricevuta è condivisa con A e di parlare proprio con A; ad esempio un intruso C capace di intercettare e modificare la comunicazione tra A e B può ingannare B facendogli credere di dialogare con D (senza però riuscire a decriptate la comunicazione) in questo modo:
$A \rightarrow KDC$: IDa,IDb
$KDC \rightarrow A$: IDb,$\{Ks\}_{Ka}$,$\{Ks\}_{Kb}$
$A \rightarrow C$: IDa, $\{Ks\}_{Kb}$
$C \rightarrow B$: IDd, $\{Ks\}_{Kb}$

Inoltre se l'intruso è utente valido del KDC, che ha precedentemente parlato con B può ottenere dal KDC una chiave Ks1valida per parlare con A (caso 1) o con B (caso 2) e sostituire il messaggio inviato dal KDC ad A con IDb,$\{Ks1\}_{Ka}$,$\{Ks1\}_{Kc}$ (nel caso 1), oppure sostituire con IDb,$\{Ks1\}_{Kc}$,$\{Ks1\}_{Kb}$ (nel caso 2); nel primo caso è in grado di decriptare i messaggi inviati da A a B, mentre nel secondo quelli inviati da B ad A.

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).

SOLUZIONE
$A \rightarrow KDC$: IDa,IDb,Na
$KDC \rightarrow A$: $\{Ks,IDb,Na,\{Ks,IDa\}Kb\}_{Ka}$
$A \rightarrow B$: $\{Ks,IDa\}_{Kb}$
$B \rightarrow A$: $\{Nb\}_{Ks}$
$A \rightarrow B$: $\{Nb-1\}_{Ks}$

5) Indicare un possibile schema di Key transport tra due entità A e B basato su crittografia a chiave pubblica e senza KDC.

SOLUZIONE
$A \rightarrow B$: $\{Ks\}K_B^+$

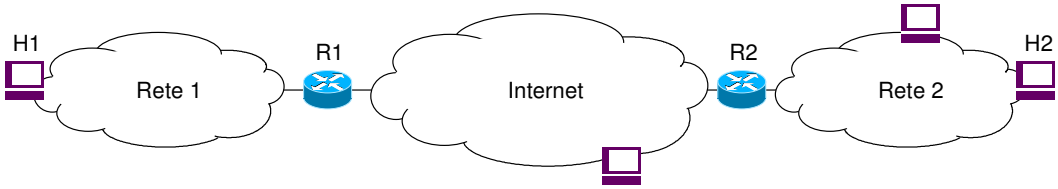
oppure con firma:
$A \rightarrow B$: $\{Ks, sign_A(ID_B,Ks)\}K_B^+$

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.

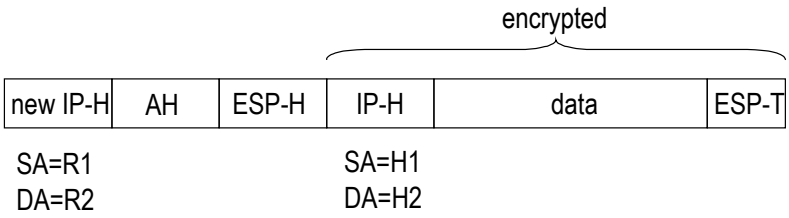
Nell'ipotesi che la VPN sia instaurata tra i router R1 e R2 utilizzando ESP e AH (con AH che protegge anche il contenuto di ESP), e che si utilizzino i meccanismi di incapsulamento con minor overhead tra quelli possibili (transport/tunnel), si chiede di:

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.



SOLUZIONE

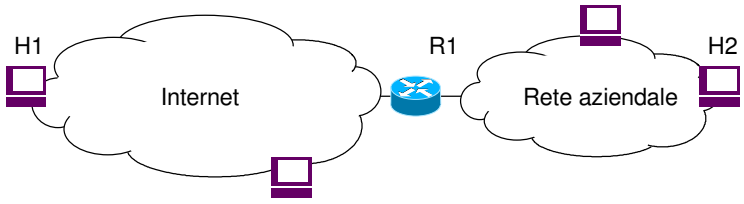


7) Si consideri uno scenario tipo road-warrior in cui un nodo H1 si collega tramite IPSec alla sua rete aziendale e comunichi in modo sicuro con un nodo interno H2, come rappresentato in figura.

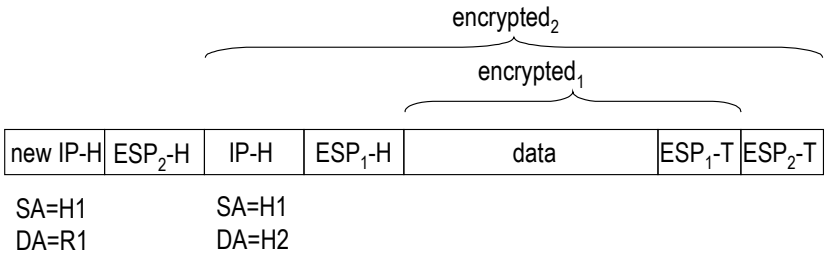
Nell'ipotesi che H1 si colleghi alla sua rete tramite il router R1 in IPSec/ESP, che H1 protegga la sua comunicazione con il nodo H2 tramite IPSec/ESP, e che si utilizzino i meccanismi di incapsulamento con minor overhead tra quelli possibili, si chiede di:

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

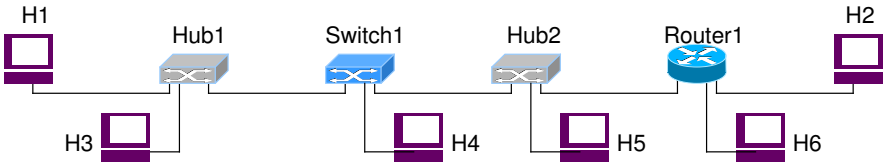
iv) per ogni eventuale header IP di tali pacchetti specificare l'indirizzo di sorgente (SA) e di destinazione (DA).



SOLUZIONE



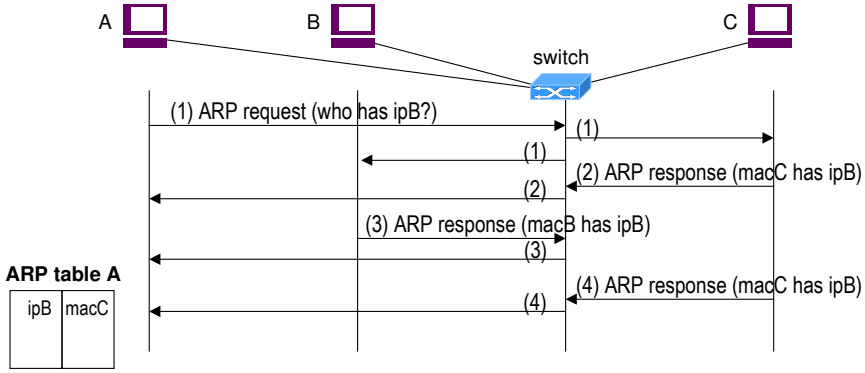
8) Nel seguente schema di rete IP su Ethernet quali nodi possono ascoltare (eavesdropping) il traffico scambiato tra H1 e H2?
Quali nodi possono effettuare un attacco diretto di tipo Man In The Middle (MITM)?



SOLUZIONE
Nodi in grado di effettuare eavesdropping (tramite network sniffing): H3, H5, R1
Nodi in grado di effettuare MITM: R1

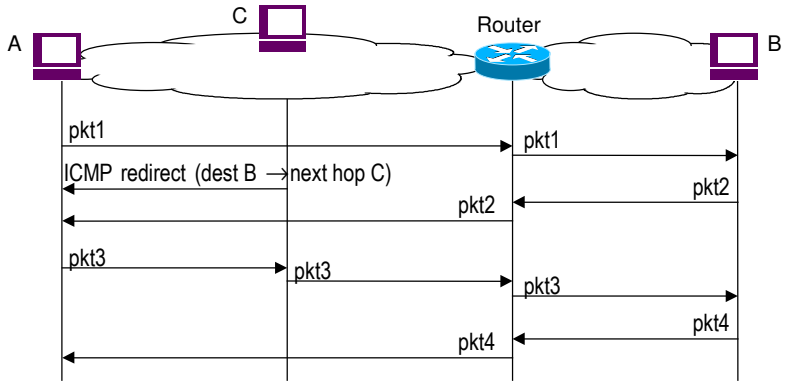
9) Nel seguente schema di rete indicare una possibile sequenza di messaggi di un attacco di ARP spoofing (indicato anche come ARP poisoning) da parte del nodo C (attaccante) verso il nodo A (vittima), dove B è il nodo "spoofato". Se ipA, macA, ipB, macB, ipC, macC sono rispettivamente gli indirizzi IP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

SOLUZIONE

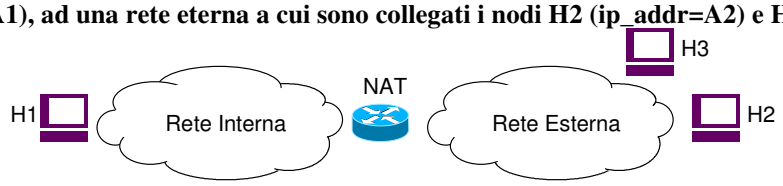


10) Nel seguente schema di rete indicare una possibile sequenza di messaggi di un attacco di ICMP spoofing di tipo ICMP redirect da parte del nodo C (attaccante) che tenta di fare un Man In The Middle tra A (vittima) e B.
Si consideri il caso in cui A e B si vogliano scambiare i seguenti 4 pacchetti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

SOLUZIONE



11) 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: pkt1=A1:p1→A2:p2, e se tale datagramma viene modificato dal NAT in pkt1':A10:p10→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"?

SOLUZIONE

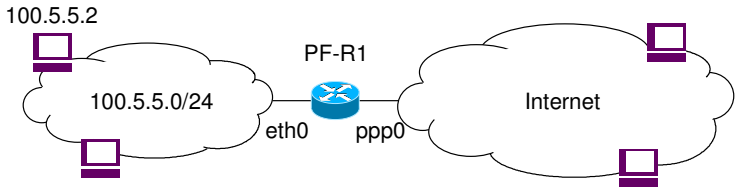
pkt2=A2:p2→A1:p1	**NO**
pkt3=A2:p4→A1:p1	**NO**
pkt4=A3:p3→A1:p1	**NO**
pkt5=A2:p2→A10:p10	**Sì**
pkt6=A2:p4→A10:p10	**Sì**
pkt7=A3:p3→A10:p10	**NO**

12) 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:

i) sia possibile accedere dall'esterno al server web interno (100.5.5.2),

ii) da tutti in nodi della rete interna sia possible accedere a qualsiasi server web esterno (limitatamente alla porta TCP 80),

iii) 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)



SOLUZIONE

FORWARD								
Matching								action
in_int	out_int	s_addr	d_addr	Proto	s_port	d_port	altro	ACCEPT/ DROP
*	*	*	*	*	*	*	state= ESTABLISHED	ACCEPT
ppp0	eth0	*	100.5.5.2	TCP	*	80	state=NEW	ACCEPT
eth0	ppp0	100.5.5.0/24	*	TCP	*	80	state=NEW	ACCEPT
ppp0	eth0	*	100.5.5.2	TCP	*	25	state=NEW	ACCEPT
eth0	ppp0	100.5.5.2	*	TCP	*	25	state=NEW	ACCEPT
*	*	*	*	*	*	*	*	DROP

Oppure, considerando separatamente le regole anti-spoofing legate alle interfacce:

ppp0	eth0	100.5.5.0/24	*	*	*	*	*	DROP
*	*	*	*	*	*	*	state= ESTABLISHED	ACCEPT
*	*	*	100.5.5.2	TCP	*	80	state=NEW	ACCEPT
*	*	100.5.5.0/24	*	TCP	*	80	state=NEW	ACCEPT
*	*	*	100.5.5.2	TCP	*	25	state=NEW	ACCEPT
*	*	100.5.5.2	*	TCP	*	25	state=NEW	ACCEPT
*	*	*	*	*	*	*	*	DROP

Oppure, senza mantenimento dello stato e utilizzando info sui flag TCP:

ppp0	eth0	*	100.5.5.2	TCP	*	80	*	ACCEPT
eth0	ppp0	100.5.5.2	*	TCP	80	*	tcp-flags!= {SYN=1,ACK=0,FIN= 0,RST=0}	ACCEPT
eth0	ppp0	100.5.5.0/24	*	TCP	*	80	*	ACCEPT
ppp0	eth0	*	100.5.5.0/24	TCP	80	*	tcp-flags!= {SYN=1,ACK=0,FIN= 0,RST=0}	ACCEPT
ppp0	eth0	*	100.5.5.2	TCP	*	25	*	ACCEPT
eth0	ppp0	100.5.5.2	*	TCP	25	*	tcp-flags!= {SYN=1,ACK=0,FIN= 0,RST=0}	ACCEPT
eth0	ppp0	100.5.5.2	*	TCP	*	25	*	ACCEPT
ppp0	eth0	*	100.5.5.2	TCP	25	*	tcp-flags!= {SYN=1,ACK=0,FIN= 0,RST=0}	ACCEPT
*	*	*	*	*	*	*	*	DROP

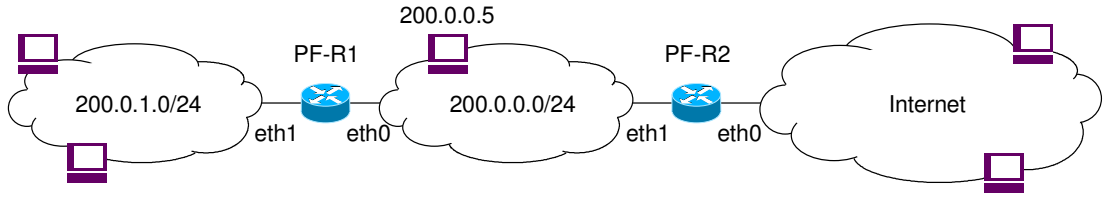
13) Si consideri il seguente schema di rete aziendale composta da una rete interna e da una DMZ separate dal screening router R1 e collegate alla rete esterna (pubblica) tramite il screening router R2.
Si chiede di configurare la tabella di filtraggio (ACL) di R2 in modo che:

a) 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;

b) sia bloccata qualsiasi comunicazione client/server da rete esterna a DMZ;

c) sia bloccata qualsiasi comunicazione tra rete interna e rete esterna;

d) sia possibile instaurare connessioni TCP da rete esterna al nodo 200.0.0.5, porta 80 (HTTP).



SOLUZIONE

FORWARD								
Matching								action
in_int	out_int	s_addr	d_addr	Proto	s_port	d_port	altro	ACCEPT/ DROP
*	*	*	*	*	*	*	state= ESTABLISHED	ACCEPT
eth1	eth0	200.0.0.0/24	*	*	*	*	state=NEW	ACCEPT
eth0	eth1	*	200.0.0.5	TCP	*	80	state=NEW	ACCEPT
*	*	*	*	*	*	*	*	DROP

14) 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.

SOLUZIONE

FORWARD								
Matching								action
in_int	out_int	s_addr	d_addr	Proto	s_port	d_port	altro	ACCEPT/ DROP
*	*	*	*	*	*	*	state= ESTABLISHED	ACCEPT
eth1	eth0	200.0.1.0/24	200.0.0.0/24	*	*	*	state=NEW	ACCEPT
*	*	*	*	*	*	*	*	DROP