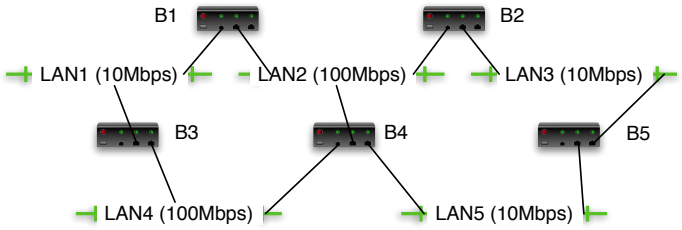
Esame di Reti di Calcolatori e Sicurezza

Soluzione

4 dicembre 2006

1. Si consideri la seguente rete locale:



	Identifier	Pri
B1	08:00:2B:34:4A:21	32768
B2	08:00:2B:14:40:2F	32768
B3	08:00:2B:2A:85:20	32768
B4	08:00:2B:24:5A:21	32768
B5	08:00:2B:99:10:A1	32768

   (a) Si determini il root bridge

   (b) Si determini il root path cost di ogni LAN.

   (c) Si determini la designed port di ogni LAN.

   Risposta:

   (a) (2pt) Il root bridge è B2, perché ha l'ID minore e la priorità è uguale per tutti.

   (b) (2pt) LAN2=LAN3=0; LAN1=1000/100=10; LAN4=1000/100=10; LAN5=1000/100=10

   (c) (2pt) LAN1: da B1; LAN2: da B2; LAN3: da B2; LAN4: da B4; LAN5: da B4. Quindi i collegamenti da B5 a LAN5 e da B3 a LAN1 sono inattivi, e quindi anche i bridge B3 e B5 si disattivano.

2. (a) Si descrivano le caratteristiche fondamentali di RC4: modalità di utilizzo, principio di funzionamento.

   (b) In quali situazioni viene usato, e perché?

   (c) Quale tipo di attacco può essere condotto su questo tipo di cifrario?

   Risposta:

   (a) (2pt) RC4 è un algoritmo di cifratura a flusso, ossia genera uno flusso di byte pseudocasuali (keystream) da mettere in XOR con i byte in chiaro; il flusso cifrato così ottenuto può essere decifrato rimettendolo in XOR con lo stesso keystream. In RC4, il keystream è generato in base alla chiave privata (di 40 o 128 bit) con una serie di permutazioni di un vettore inizializzato con uno stato noto.

   (b) (2pt) I cifrari a stream si usano dove si vuole cifrare un carattere alla volta, e non a blocchi di 8-16 byte (come in DES o AES). Ad esempio, comunicazioni seriali (TLS), ssh, https, WEP...

   (c) (3pt) Il problema è quando la stessa chiave viene usata in congiunzione con lo stesso vettore di inizializzazione. In tal caso, si ottiene lo stesso identico keystream M. Se questo viene usato su due diversi stream P_1, P_2, facendo lo XOR dei due stream cifrati $P_1 \oplus M$ e $P_2 \oplus M$ si ottiene lo XOR dei stream in chiaro $P_1 \oplus P_2$, perché i due keystream si annullano a vicenda. A questo punto si possono applicare tecniche analitiche per risalire ai due testi in chiaro.

3. Relativamente al protocollo IPSec:

   (a) Si descrivano i servizi di sicurezza offerti dal protocollo AH.

(b) Si descrivano i servizi di sicurezza offerti dal protocollo ESP.

(c) Quali sono le principali differenze tra il modo "trasporto" e il modo "tunnel"?

Risposta:

(a) (2pt) AH (Authentication Header) garantisce integrità dei dati ed autenticazione dei pacchetti IP, ma non cifratura del payload. Inoltre offre una difesa contro gli attacchi replay.

(b) (2pt) ESP (Encapsulating Security Payload) offre principalmente la segretezza del payload (che viene cifrato), difesa dall'attacco replay, ed opzionalmente anche l'autenticazione del mittente.

(c) (3pt) Nella modalità trasporto, l'autenticazione (e la cifratura) avvengono end-to-end; è necessaria una SA ed una autenticazione per ogni connessione. Nella modalità tunnel, invece, le connessioni utilizzano normali pacchetti IP che vengono incapsulati all'interno di un tunnel IPSec tra i due host, o più spesso tra due firewall/router tra le due LAN dei due host. In questo modo, solo i due firewall devono autenticarsi tra di loro, ed una volta sola, in modo trasparente per gli utenti. Il tunnel mode viene spesso usato per creare VPN.

4. (a) Come funziona un firewall a filtro di pacchetti (packet filter)?

(b) Come funziona un firewall a livello applicazione?

(c) Si dica almeno un vantaggio ed uno svantaggio per ognuna di queste soluzioni.

Risposta:

(a) (2pt) Un packet filter è un algoritmo che opera a livello di rete, analizzando ogni pacchetto IP entrante o uscente dalla rete. In base a delle regole configurabili, ogni pacchetto può essere lasciato passare, rigettato o cancellato, in base agli indirizzi IP del mittente e del destinatario, tipo di protocollo, e (talvolta) porta TCP (nonostante questa sia una informazione di trasporto).

(b) (2pt) Un application firewall è un programma che si interpone nel protocollo applicativo tra client e server. Come tale, può analizzare il traffico che intercorre tra client e server in dettaglio, e prendere le decisioni in base alle informazioni specifiche del protocollo in oggetto.

(c) (3pt) Un packet filter è solitamente più efficiente (se le regole non sono troppo complicate), e trasparente all'utente. Tuttavia le decisioni che possono essere prese a questo livello sono abbastanza generali, e non si basano sull'effettivo uso della connessione; ad esempio, non è possibile impedire l'uso di FTP su una porta non standard. Può essere difficile impostare correttamente le regole per cogliere tutti i casi in cui una interazione tra client e server possono avvenire.

D'altra parte, un application firewall è meno efficiente (in pratica ci sono due connessioni in piedi, e i dati devono attraversare completamente lo stack TCP/IP due volte), ma può fare un controllo più accurato. Inoltre si può decidere quali protocolli supportare, uno per uno.

5. [Da sviluppare su foglio a parte]

Si descriva la tipologia di attacchi "Denial of Service" (DoS), fornendo anche una spiegazione dettagliata di un attacco di questo tipo (es. Ping Of Death). L'utilizzo di una botnet può aumentare l'efficacia degli attacchi DoS? Se sì, come?