Reti Avanzate e Sicurezza dei Dati, A.A. 2017–2018

Prova scritta

Martedì 4 settembre 2018

Esercizio 1

Un server è accessibile mediante username e password; per comodità, si supponga che le password siano stringhe casuali di 64 bit.
Il server applica alle password degli utenti una funzione hash crittografica H che genera un valore a 32 bit, e memorizza nel proprio database solamente questo valore hash. Il valore hash viene utilizzato per verificare la correttezza della password inserita al momento del login.
Bob possiede un account sul server; il suo nome utente è noto a tutti, ma non la sua password.
Charlie vuole impersonare Bob, quindi realizza uno script che tenta ripetutamente il login utilizzando password generate casualmente. Il server web non ha difese contro il DoS e risponde a ogni tentativo di login.

1.1) Supponiamo che Charlie non conosca la funzione di hash H, ma che sappia che Bob utilizza una password di 64 bit. Quanti tentativi deve fare Charlie in media per riuscire ad accedere come Bob?

1.2) Supponiamo che Bob raddoppi la lunghezza della propria password, portandola a 128 bit casuali.
La risposta alla domanda 1.1 cambia? Se sì, come?

1.3) Supponiamo che Charlie conosca la funzione di hash H.
Le risposte alle domande 1.1 e 1.2 cambiano? Se sì, come?

Suggerimento — *Motivare le risposte fornite!! È consentito arrotondare le risposte. Considerare la consueta approssimazione* $2^{10} \approx 10^3$.

Esercizio 2

Descrivere a grandi linee l'handshake iniziale del protocollo TLS nel caso in cui al server sia richiesta l'autenticazione tramite certificato, mentre non è richiesta l'autenticazione del client. In particolare, come fa il client ad accertarsi dell'identità del server? Come viene stabilita la chiave di sessione?

Esercizio 3

Una rete locale è composta da due intranet:

- la prima contiene un server HTTP (porta TCP 80), un server DNS (porta UDP 53) e un proxy web (porta TCP 3128).
  - i tre server devono essere accessibili da tutte le macchine della rete locale;
  - il server HTTP dev'essere accessibile anche dall'esterno, ma non può iniziare comunicazioni verso l'esterno;
  - Il server DNS seve poter ricevere ed effettuare richieste DNS anche all'esterno;
  - il proxy web deve avere i permessi minimi necessari per servire l'altra intranet, descritta qui sotto;
- una seconda intranet da 200 host;
  - l'intranet può accedere ai server HTTP e DNS;
  - l'intranet non può accedere all'esterno, ma può utilizzare il proxy web.

La rete ha a disposizione il solo indirizzo IP pubblico `195.221.23.45` con netmask `255.255.255.248`; il default gateway messo a disposizione dall'ISP ha l'indirizzo più alto utilizzabile della stessa sottorete.
Si ha a disposizione un router con due interfacce (una seriale verso l'ISP e una Ethernet verso le reti locali), capace di NAT e di incapsulamento 802.1Q, e di tutti gli switch gestiti di cui si ha bisogno.
Descrivere l'architettura fisica e logica della rete, attribuire indirizzi e sottoreti IP ale varie parti; descrivere la configurazione dei tre server (HTTP, DNS, proxy) e del router (porte fisiche e virtuali, tabelle di instradamento, tabelle di port forwarding, ACL).