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

Proposta di soluzione della 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* $2^{10} \approx 10^3$.

Soluzione 1

1.1) Charlie conosce la funzione H e ovviamente non conosce la password di Bob. Tutto quello che può fare è generare password in sequenza e spedirle al server, sperando che una delle password P sia in collisione con quella di Bob, il cui hash è memorizzato nel database:

$$H(P) = H(P_{\text{Bob}}).$$

Dato che i valori hash possibili sono 2^{32}, la probabilità di una collisione ad ogni tentativo è 2^{-32}, quindi saranno necessari mediamente $2^{32} \approx 4 \cdot 10^9$ tentativi. Si noti che Charlie può generare password sempre diverse, ma non può sperare che gli hash generati siano tutti diversi.

1.2) La risposta precedente non dipende dalla lunghezza della password di Bob, ma solo dal numero di bit dell'hash e dalla velocità con cui possono essere provati. Infatti, Charlie non ha bisogno di trovare la password di Bob, ma un valore che generi lo stesso hash.

1.3) Anche se Charlie è ora in grado di calcolare 10^9 hash al secondo, non conoscendo $H(P_{\text{Bob}})$ non può farsene molto. In realtà, Charlie può utilizzare la propria capacità di calcolare a priori gli hash delle password prima di inviarle al server, escludendo quelle che collidono con password già provate. In questo modo, i 2^{32} hash possibili sono tentati senza ripetizione, e il numero medio di tentativi necessari si dimezza.

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?

Soluzione 2

Vedere gli appunti di lezione. Si osservi che il fatto che il server invia i certificati corretti non è sufficiente ad assicurare il client della sua identità, perché i ceryificati sono pubblici. L'identità del server viene dimostrata attraverso una sfida basata sul possesso della chiave privata.

Esercizio 3

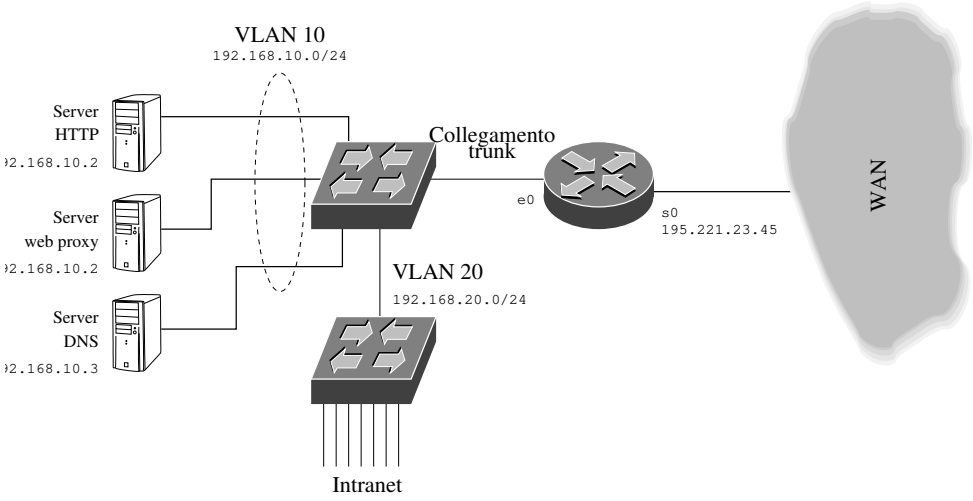
Una rete locale è composta da due intranet:

- 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).

Soluzione 3

Il router ha due sole interfacce, quindi una va dedicata alla connessione esterna e l'altra deve gestire le due intranet, quindi dovrà essere in modalità router-on-a-stick, con uno switch in grado di separare le due VLAN a valle. Una possibile struttura è dunque la seguente:



Per quanto riguarda la connessione con l'ISP, disponiamo di un solo indirizzo IP pubblico, il quale va quindi necessariamente assegnato all'interfaccia `s0` per comunicare con l'esterno. Sappiamo che l'indirizzo pubblico appartiene alla sottorete `195.221.23.40/29`, il cui indirizzo più alto utilizzabile è `195.221.23.46`, che quindi sarà, in base alle specifiche dell'esercizio, il default gateway dell'ISP.
Per quanto riguarda la due intranet, ovviamente le scelte sono arbitrarie; dovremo ovviamente usare indirizzi privati:

- associamo la prima alla VLAN con ID 10, sottorete `192.168.10.0/24` (basterebbe una rete più piccola, ma così è più semplice);
- associamo la seconda alla VLAN con ID 20, sottorete `192.168.20.0/24`.

In entrambi i casi, il router avrà l'indirizzo più alto fra quelli utilizzabili. La configurazione del router è dunque

Interfaccia fisica	Interfaccia virtuale	IP	Netmask	
`s0`	—	`195.221.23.45`	`255.255.255.248`	Indirizzo assegnato dall'ISP
`e0`	`e0.10`	`192.168.10.254`	`255.255.255.0`	Indirizzo più alto VLAN 10
	`e0.20`	`192.168.20.254`	`255.255.255.0`	Indirizzo più alto VLAN 20

L'interfaccia `e0` del router sarà ovviamente collegata a una porta switch in modalità trunk, e sarà responsabilità dello switch separare correttamente il traffico delle due VLAN configurando opportunamente le modalità delle porte. Ad esempio, in figura lo switch ha tre porte in modalità access sulla VLAN 10 per i tre server, e una porta in modalità access sulla VLAN 20 collegata a uno switch non gestito.
Data la configurazione delle porte, ecco la corrispondente tabella di instradamento:

Destinazione	Interfaccia	Gateway	
`192.168.10.0/24`	`e0.10`	—	Connessione diretta alla VLAN 10
`192.168.20.0/24`	`e0.20`	—	Connessione diretta alla VLAN 20
`195.221.23.40/29`	`s0`	—	Connessione diretta alla rete ISP
`0.0.0.0/0`	`s0`	`195.221.23.46`	Default

Occupiamoci ora della raggiungibilità dei server dall'esterno. Il servizio NAT offerto dal server dovrà avere le seguenti caratteristiche:

- interfaccia interna: `e0.10` (l'intranet 20 non deve poter comunicare con l'esterno, quindi se non si attiva il NAT su `e0.20` si risparmiano regole ACL), sugli indirizzi da `192.168.10.1` a `192.168.10.3`;
- interfaccia esterna: `s0`, sull'unico indirizzo disponibile;
- mentre le connessioni del proxy web vengono sempre iniziate dall'interno, e quindi sono gestite automaticamente dal NAT, per il server web e il server DNS è necessario impostare la tabella del port forwarding in modo che il server inoltri connessioni iniziate dall'esterno:

Protocollo	Porta router	Porta locale	IP locale	
TCP	`80`	`80`	`192.168.10.1`	Server web
UDP	`53`	`53`	`192.168.10.3`	Server DNS

Per quanto riguarda la sicurezza, dobbiamo bloccare le connessioni del server web verso l'esterno, e consentire le connessioni dall'intranet ai server. Assumiamo che la porta del proxy sia la 3128, e che la ACL sia applicata dal lato interno della traduzione NAT.

Prot.	Provenienza	Destinazione	Flag	Esito	
TCP	`192.168.10.1/32:80`	`0.0.0.0/0`	ESTABLISHED	PASS	Risposte server web
UDP	`0.0.0.0/0`	`192.168.10.2/32:53`	*	PASS	Richieste al DNS
UDP	`192.168.10.2/32:53`	`0.0.0.0/0`	*	PASS	Risposte del DNS
TCP	`192.168.10.2/32`	`0.0.0.0/0:80`	*	PASS	Richieste del proxy
TCP	`0.0.0.0/0:80`	`192.168.10.2/32`	ESTABLISHED	PASS	Risposte al proxy
TCP	`192.168.20.0/32`	`192.168.10.2/32:3128`	*	PASS	Intranet a proxy
TCP	`192.168.10.2/32:3128`	`192.168.20.0/32`	ESTABLISHED	PASS	Proxy a intranet
*	*	*	*	DROP	Tutto il resto non passa