Esame 15 Giugno 2016

D: Per quali diversi motivi ci può essere interesse che l'implementazione di un certo algoritmo avvenga su un server a cui accedere mediane un client? (2pt)

La scelta di implementare un algoritmo lato server può comportare i seguenti vantaggi: […]

D: Come funziona, come si crea e a cosa serve un filtro di visualizzazione in WireShark? (2pt)

Il filtro permette di limitare la visione di solo alcuni tipi di PDU. Si può impostare un filtro tramite '`Capture Filter`' -> '`Caputre Options`'. I filtri programmano la scheda di rete al fine di catturare solo determinati pacchetti (PDU). Spesso vengono utilizzati quando ho un sovraccarico della CPU per una grande quantità di pacchetti che passano sulla rete.

D: Quali vantaggi presenta la fibra ottica in un collegamento di rete? (2pt)

La fibra ottica presenta i seguenti vantaggi:
- Può essere utilizzata in ambienti rumorosi (rumore elttromagnetico, es fabbriche)
- Se si ha la necessità di avere un disaccoppiamento magnetico (es ospedali)
- Grandi capacità di trasmissione dei dati (es rispetto al cavo Ethernet)

Il suo funzionamento si basa sulla proprietà della riflessione di una luce LED grazie alla diversa densità degli strati di vetro che la compongono.

D: Si descrivano gli elementi che costituiscono il processo crittografico, e nel caso di crittografia a chiave simmetrica, si mostri un esempio di un semplice sistema crittografico. (4pt)

Un algoritmo crittografico è una funzione che prende come ingresso un messaggio e come parametro una chiave, e produce in uscita un messaggio trasformato (cifrato). Le chiavi tra i due soggetti possono essere uguali o diverse. Da qui si distingue se un algoritmo è simmetrico (chiavi uguali) oppure asimmetrico (chiavi diverse).

Nel caso della crittografia simmetrica, possiamo in caso due entità: *Alice* e *Bob*. Essi si scambiano tramite un canale sicuro la chiave crittografica condivisa, che verrà utilizzata per cifrare e decifrare il messaggio.

Es. *Alice* genera un messaggio `plain_text`, lo codifica con la chiave condivisa e ottiene l'`encoded_text`. *Bob*, trasformerà quindi l'`encoded_text` in `plain_text` sempre tramite la chiave condivisa.

Quindi, con la crittografia simmetrica posso garantire …

D: Si descriva anche attraverso esempi, su quali fattori si basa l'autenticazione degli utenti, indicando gli aspetti positivi e negativi. (4pt)

L'autenticazione è un processo che avviene tra due entità, le quali possono essere utenti o computer. Esistono diverse tipologie di autenticazione:
- Locale : l'utente accede in modo locale
- Diretta: l'utente accede in modo remoto
- Indiretta: l'utente accede tramite un servizio esterno
- Offline: Tramite dei certificati elettronici

Esistono inoltre diversi tipi di autenticazione:
- User/Password (*Qualcosa che si conosce*): semplice, veloce, economico.
- OTP: (*Qualcosa che si possiede*) : più efficace, sicuro, l'utente può utilizzarla come 2FA
- FISICA: (*Qualcosa che si è*) : veloce da impostare, veloce l'uso, sicuro contro attacchi classici

D: Si spieghi cosa si intende come Access Control List, specificando dove sono memorizzate le informazioni e come vengono utilizzate. (4pt)

Le ACL servono a memorizzare una matrice di accesso contenente delle entry per i soggetti e delle entry per gli oggetti contenente in ogni cella i permessi. Questa matrice viene memorizzata per colonne, e ciascuna risorsa memorizza quindi i soggetti che possono interagire con essa. (es. file system unix).

Le ACL sono adatte in un contesto in cui la protezione è orientata ai dati: è semplice gestire gli accessi a un oggetto. Non sono adatte se voglio gestire centralmente i dati e i meccanismi di delega.

Esame 27 Settembre 2016

D: Descrivere il ciclo di vita di un web servicies SOAP. (2pt)

D: Che differenza c'è tra UTP dritto e incrociato? Quando viene usato ciascun tipo?. (2pt)

Il cavo UTP è composto da 4 coppie di cavi arrotolati senza schermatura, e di questi 8 cavi se ne usano solo 4 (due coppie) se si vuole trasmettere alla velocità di 10 o 100 Mb/s; se si usano tutti 8 si può trasmettere fino al gigabit.
Le schede di rete lavorano su due canali (trasmissione e ricezione), e come si può notare il connettore RJ45 ha 2 cavi per la trasmissione e due per la ricezione. Per poter quindi collegare due PC direttamente bisogna utilizzare un cavo *incrociato* perché i pin che trasmettono dovranno essere collegati ai pin che ricevono dall'altra estremità. Quando si collega un PC a un hub o switch il cavo dovrà essere dritto, ovvero la ricezione e la trasmissione non si incrociano.

D: Perché in laboratorio è stata utilizzata una VM per l'esercitazione "UDP vs TCP"?. (2pt)

Nell'esercitazione è stata utilizzata la VM per poter utilizzare Wireshark per catturare i pacchetti perché bisogna eseguirlo in modalità root. E' stata inoltre necessaria per configurare l'iptables

D: Tra i primi sistemi di crittografia a chiave simmetrica vi è la cifratura monoalfabetica: si spieghi come funziona tale schema e si indichi la dimensione dello spazio delle chiavi (4pt)

La cifratura monoalfabetica si basa sulla permutazione (sostituzione) dell'alfabeto che costutiuisce la chiave:
i.e.

plain A B C D E F G
key D R G H Z Y O

Quindi si può notare che ad esempio la parola 'FEDA', viene codificata in 'YZHD'.
Lo spazio delle chiavi di questa cifratura è 21! (circa 10^{19}). Questa tecnica è però debole contro gli attacchi delle analisi delle frequenze

D: Si descriva il funzionamento del Message Authentication Code (MAC) per l'autenticazione di un messaggio (non è necessario garantire la confidenzialità dei dati). (4pt)

L'autenticità di un messaggio viene garantita con il MAC. La chiave utilizzata è associata a un utente ed è privata. Per scambiarsi la chiave è necessario utilizzare un canale sicuro. E' possibile garantire l'autenticità tramite la firma digitale sfruttando RSA in modo inverso:

- L'algoritmo di cifratura diventa l'algoritmo di verifica
- L'algoritmo di decifratura diventa l'algoritmo di firma

D: Un sistema di rilevamento delle intrusioni IDS si può basare su diversi modelli: rilevamento della anomalia, oppure rilevamento di uso malevole, oppure rilevamento in base alle specifiche. Si spieghi il principio di funzionamento di uno tra questi modelli, anche attraverso esempi. (4pt)

L'IDS è uno strumento hw o sw che automatizza il processo di monitoraggio impiegato pr individuare eventi che rappresentano un'intrusione non autorizzata.

Nel caso specifico della *detection delle anomalie* si analizzano insiemi di caratteristiche del sistema confrontando i valori con quelli attesi segnalando quando non sono uguali utilizzando:

- Metriche a soglia
- Momenti statici
- Modelli di makarov

Le metriche a soglia: conta le occorrenze di un evento, e se sono diverse vuol dire che c'è un'anomalia (nel caso del login di windows può non essere accurato, i.e. un francese che usa una tastiera americana)

I momenti statici: il calcolatore calcola i due momenti dai diversi momenti e se sono fuori di un certo intervallo vuol dire che è possibile ci sia un'anomalia

Nel modello di makarov: la storia passata influenza il prossimo evento: le anomalie sono riconosciute dalle sequenze di eventi e non dalla loro occorrenza. Il sistema deve essere addestrato per rilevare queste sequenze anomale.

Esame 14 Giugno 2017

D: Che cosa si può osservare in Wireshark nella prima fase di scambio di messaggi TCP per l'apertura di una connessione? Perché? (2pt)

Tramite lo strumento di Wireshark si può osservare che nell'instaurazione di una connessione TCP ci sono i tipici messaggi di 3-Way Handshake di TCP per instaurare la connessione. Dopodichè il messaggio successivo sarà la richiesta del client verso il server a cui si è connesso.

D: Per cosa è servito chiamare il comando IPTABLES durante l'esercitazione? (2pt)

IPTABLES è un firewall di linux che consente di specificare regole per il traffico di rete. E' stata utilizzata nelle esercitazioni per simulare delle reti non funzionanti.

D: Come è strutturato un cavo UTP per ethernet? (2pt)

Il cavo UTP è composto da 4 coppie di cavi arrotolati senza schermatura, e di questi 8 cavi se ne usano solo 4 (due coppie) se si vuole trasmettere alla velocità di 10 o 100 Mb/s; se si usano tutti 8 si può trasmettere fino al gigabit. Il cavo ethernet utilizza il connettore RJ45.

D: Si descriva lo schema di crittografia a chiave asimmetrica e come esso viene utilizzato nella comunicazione tra due entità. (4pt)

Nella crittografia asimmetrica ogni utente ha una chiave pubblica e una privata: la chiave pubblica viene resa nota, mentre quella privata deve rimanere segreta.
La risorsa viene cifrata con la chiave pubblica del destinatario, il quale dovrà usare la propria chiave privata per decifrare il messaggio.

Il vantaggio è quello di non dover più scambiarsi la chiave (come nel caso della crittografia simmetrica), e che la stessa chiave pubblica può essere utilizzata da più utenti. Però comporta dei requisiti (…)

D: Si descriva il funzionamento del Message Authentication Code MAC per l'autenticazione di un messaggio (4pt)

- [Vedi Sopra]

D: Si illustri attraverso esempi cosa si intende per la politica di tipo "default deny" adottata da un Firewall. (4pt)

I firewall sono apparecchiature o sistemi che controllano il flusso del traffico tra due reti con diversi livelli di sicurezza. Esistono due filosofie di ragionamento: *default deny* e *default permitt*.
Nel caso del default deny Tutto quello che non è espressamente ammesso è proibito:

- I servizi sono abilitati solo caso per caso dopo un'analisi accurata
- Gli utenti quindi sono molto ristretti

Tipicamente i firewall adottano la filosofia *default deny* poiché garantisce maggiore sicurezza

Esame 8 Febbraio 2017

D: Per quali diversi motivi ci può essere interesse che l'implementazione di un certo algoritmo avvenga su un server a cui accedere mediante un client? (2pt)

La scelta comporta dei vantaggi tecnologici e di comodità:
- Si protegge la proprietà intellettuale dell'algoritmo
- Si aumenta la potenza di calcolo
- E' comodo da distribuire agli utenti
- Semplice da installare e da utilizzare (si appoggia ai protocolli già noti)
- Si può utiilizzare uno standard e Interoperabilità

D: In quale modo Wireshark capisce come (cioè con quali formati di protocollo) interpretare i byte che vengono catturati dall'interfaccia di rete? Si risponda per i diversi livelli di ISO/OSI. (2pt)

Wireshark riesce a scomporre i diversi livelli di rete poiché conosce la propria struttura, quindi è in grado di visualizzare i pacchetti, incapsulamenti e i singoli campi ed interpretare il loro significato

D: Che differenza c'è tra UTP dritto e incrociato? Quando viene usato ciascun tipo?. (2pt)
- [Vedi Sopra]

D: Si dia una breve spiegazione di ciascuno dei tre principali obiettivi della sicurezza (confidenzialità, integrità, disponibilità) anche con l'aiuto di esempi che mostrino come tali proprietà possono essere compromesse. (4pt)

Confidenzialità: nessun utente deve poter ottenere o dedurre dal sistema informazioni che non è tenuto a conoscere. Attacco ?.

Integrità: Bisogna impedire l'alterazione diretta (o indiretta) delle informazioni, sia dalla parte egli utenti sia dalla parte di processi non autorizzati. Attacco MITM.

Disponibilità: Rendere disponibile a ciascun utente le informazioni alle quali ha solo diritto di accedere, nei tempi e nei modi previsti. Attacco DDOS.

D: Si descriva il funzionamento del Message Authentication Code MAC per l'autenticazione di un messaggio (4pt)

- [Vedi Sopra]

D: Si illustri attraverso esempi cosa si intende per la politica di tipo "default deny" adottata da un Firewall. (4pt)

- [Vedi Sopra]

Esame 12 Luglio 2016

D: Descrivere motivazioni e funzionamento dello Spanning Tree. (2pt)

Spanning Tree è un algoritmo per rimuovere cicli nei collegamenti tra gli switch disattivando momentaneamente i link rindondanti e riattivandoli in caso di guasti.
Ogni porta dello switch ha un peso e uno stato (blocked, listening, forward, learning).

D: In quale modo Wireshark capisce come (cioè con quali formati di protocollo) interpretare i byte che vengono catturati dall'interfaccia di rete? Si risponda per i diversi livelli di ISO/OSI. (2pt)

- [Vedi Sopra]

D: In uno Switch, l'associazione MAC/porta è uno-a-una o molti-a-una? Perché? (2pt)

Lo switch possiede l'algoritmo di backward learning: ossia impara quali indirizzi MAC hanno le stazioni attaccate su una cera porta guardando il campo source MAC dei frame che arrivano su quella porta.
Quindi, l'associazione MAC-porta è molti-uno perché si possono raggiungere più MAC da una porta. (Caso banale: uno switch ha come porta un altro switch ad albero al quale ci sono collegati più host. Sulla porta del primo switch posso raggiungere tutti i MAC del secondo switch)

D: Si descriva lo schema di crittografia a chiave asimmetrica e come esso viene utilizzato nella comunicazione tra due entità. (4pt)

- [Vedi Sopra]

D: Si illustrino le caratteristiche che le funzioni hash devono possedere per poter essere utilizzate in ambito crittografico. (4pt)

Una funzione hash trasforma un qualsiasi messaggio in una lunghezza predefinita (digest)
Per stabilire la sicurezza, le condizioni degli algoritmi che eseguono hashing devono essere:

- Coerenti: gli input uguali devono corrispondere ad output uguali
- Casuali: bisogna impedire l'interpretazione del messaggio originale
- Univoci: due messaggi non dovrebbero generare lo stesso digest
- Non invertibili: non deve essere possibile risalire al messaggio originale

Gli HASH non invertibili vengono di solito utilizzati per assegnare un'impronta digitale alle risorse. Le funzioni hash più comuni sono MD5 e SHA.

Esame 12 Luglio 2017

D: A cosa serve e come funziona l'algoritmo/protocollo spanning tree? Esiste uno standard IEEE che lo regola? (2pt)

Spanning Tree è un protocollo utilizzato nelle reti complesse a livello fisico con percorsi rindondanti utilizzati a livello datalink. Lo spanning tree viene eseguito dagli switch per mantenere inattive alcune interfaccie di rete per rimuovere eventuali loop e per garantire che la rete rimanga sempre connessa. Lo standard IEEE è 802.1D.

D: Che differenza c'è tra un connettore RJ11 e un connettore RJ45? Quale dei due è usato per Ethernet? In che modo può essere configurato? (2pt)

Sia Il connettore RJ45 che RJ11 utilizzano un cavo UDP. Nel caso del RJ45 ho 4 coppie di cavi, mentre nel caso dell'RJ11 ne ho 2. Ethernet utilizza il connettore RJ45 ma utilizza solo due coppie di cavi per il Megabit mentre ne utilizza 4 per il PoE oppure per raggiungiere il Gigabit se disponibile.
Il cavo ethernet può essere utilizzato dritto o incrociato.

D: Perché Wireshark ha bisogno di essere eseguito con l'utente Root per fare un'acquisizione live? (2pt)

Per poter configurare e catturare i pacchetti dalla scheda di rete bisogna configurare appunto la scheda di rete in modalità promiscua permettendo al sistema di poter disattivare il "filtro hardware" basato su MAC per poter mettersi in ascolto di tutto il traffico passante sul cavo.

D: Si descriva lo schema di crittografia a chiave simmetrica e come esso viene utilizzato nella comunicazione tra due entità? (4pt)

- [Vedi Sopra]

D: Si mostri uno schema di firma digitale attraverso l'utilizzo della crittografia asimmetrica? (4pt)

La firma digitale è un'equivalente informatico di una firma convenzionale, genericamente non repidiabile. Nella crittografia asimmetrica non si può garantire l'autenticità, per essere sicuri che il mittente sia quello pensato bisogna utilizzare la firma digitale:

Si utilizza la cifratura assimetrica nel modo inverso:
- L'algoritmo di cifratura diventa l'algoritmo di verifica
- L'algoritmo di decrifratura diventa l'algoritmo di firma

Però firmare l'intero documento può diventare oneroso, si firma quindi solo l'HASH del documento. Anche in questo modo non è garantito che se un utente si dichiara che è Bob vuol dire che sia Bob. Per ovviare a ciò esistono i certificati digitali rilasciati da una CA.

D: Si spieghi cosa si intende per Access Control List, specificando dove sono memorizzate le informazioni e come vengono utilizzate. (4pt)
Le ACL sono un servizio per il controllo degli accessi, esse mantengono una matrice di controllo (precedentemente salvata con righe x soggetti e colonne x oggetti e il contenuto sono i permessi), viene salvata per colonne e ciascuna risorsa viene memorizzata con la lista dei soggetti che possono interagire conessa (ad esempio il file system di unix).
Le ACL sono adatte in un contesto in cui la protezione è rivolta ai dati, perché è semplice per gestire gli accessi di un oggetto.
Invece, le ACL, non sono adatte se voglio gestire centralmente i dati e introdurre anche meccanismi di delega.

Esame 26 Settembre 2017

D: Spiegare come funziona un bridge/switch (2pt)

Lo switch/bridge permettono la comunicazione tra le loro porte (tramite store&forward). Eliminano le PDU errate e in collisione e utilizzano degli algoritmi (come selecvite flooding e learning) per gestire e salvare come indirizzare le PDU tra le loro porte.
Lo switch spezza il dominio di collisione ma non di broadcast/multicast.

D: Che cos'è e come funziona e a cosa serve una Virtual LAN? (2pt)

Gli switch/bridge separano i domini di collisione ma non di broadcast e multicast e servizi come ARP possono generare traffico di rete saturando la banda. Inoltre si possono avere problemi di attacchi di tipo poisoning e flooding.
Una soluzione a ciò è suddividere la lan in tante lan collegate a un router IP.
Posso avere diverse lan collegate allo stesso switch, poiché l'admin di rete può assegnare ogni lan alla porta dello switch e l'assegnazione è facile e veloce via sw.
Per poter suddividere le lan è necessario scrivere un lan-id nella trama ethernet (chiamato tag)

D: Perché in laboratorio è stata usata una VM per l'esercitazione UDP VS TCP? (2pt)

- [Vedi Sopra]

D: Si dia una breve spiegazione di ciascuno dei tre principali obiettivi della sicurezza (confidenzialità, integrità, disponibilità) anche con l'aiuto di esempi che mostrino come tali proprietà possono essere compromesse. (4pt)

- [Vedi Sopra]

D: Si illustrino le caratteristiche che le funzioni hash devono possedere per poter essere utilizzate in ambito crittografico. (4pt)

- [Vedi Sopra]

D: Un sistema di rilevamento delle intrusioni IDS si può basare su diversi modelli: rilevamento della anomalia, oppure rilevamento di uso malevole, oppure rilevamento in base alle specifiche. Si spieghi il principio di funzionamento di uno tra questi modelli, anche attraverso esempi. (4pt)

- [Vedi Sopra]

Esame 21 Febbraio 2018

D: Che cosa si può osservare in Wireshark nella prima fase di scambio di messaggi TCP per l'apertura di una connessione? Perché? (2pt)

- [Vedi Sopra]

D: Per cosa è servito chiamare il comando IPTABLES durante l'esercitazione? (2pt)

IPTABLES è un firewall di linux che consente di specificare delle regole per la configurazione della scheda di rete. E' stato utilizzato nelle nostre esercitazioni per simulare dei guasti di rete durante le simulazioni dei programmi con le socket TCP / UDP.

D: Come è strutturato un cavo UTP per ethernet? (2pt)

- [Vedi Sopra]

D: Tra i primi sistemi di crittografia a chiave simmetrica vi è la cifratura monoalfabetica: si spieghi come funziona tale schema e si indichi la dimensione dello spazio delle chiavi (4pt)

- [Vedi Sopra]

D: Si descriva, anche attraverso esempi, su quali fattori si basa l'autenticazione degli utenti, indicando aspetti positivi e negativi di ciascun fattore (4pt)

Esistono quattro tipologie di autenticazione: locale, diretta, indiretta e offline. I fattori di autenticazione sono:

- Qualcosa che si conosce (PIN, PSW) [1]
- Qualcosa che si possiede (Carta, Tessera) [2]
- Qualcosa che si è (Impronta, iride..) [3]

[1]
Vantaggi: E' semplice, economico e non richiede di salvare i dati (client)
Svantaggi: spesso utilizzano password semplici, vengono dimenticate, e i metodi di autenticazione sono deboli

[2]
Vantaggi: La password generata a 2fa è più sicura, servono due metodi di autenticazione, si possono combinare
Svantaggi: spesso si perde la carta / tessera

[3]
Vantaggi: è veloce, è sicuro (univoco)
Svantaggi: spesso le misure sono imprecise e si possono usare dei template; C'è la possibilità di usare dei falsi positivi o negativi

D: Relativamente al certiicato digitale, si descriva come viene creato, da chi viene creato, cosa contiene e il suo utilizzo. (4pt)

Un certificato digitale associa l'identità di una determinata persona a una chiave pubblica. Il certificato è quindi elettronico e rilasciato da una CA (firmato dalla chiave privata della CA)

Il certificato viene creato da una CA: l'utente genera una coppia di chiavi, le invia alla -CA con la richiesta di certificato; la CA autentica l'utente chiedendoli di recarsi a uno sportello per validare il certificato; quando viene verificata il certificato viene inviato tramite posta elettronica e salvato nel registro delle chiavi pubbliche.

Per utilizzare il certificato Bob invia ad alice il suo certificato firmato dalla CA. Alice controlla la firma ed estrapola la chiave pubblica di bob. Alice ha la chiave pubblica di bob garantita dalla CA