DOMANDE VARIE DA TELEGRAM

Domande di teoria prof Basile anno 2020/21

Aggiunte da me

**1) Spiegare i compiti del Data Protection Officer (DPO) ed i suoi doveri in caso di data breach (3-5 punti).**

1) Un DPO è il ruolo aziendale il cui scopo è supervisionare sul trattamento dei dati. Ha il dovere di comunicare un data breach qualora sia presente ed è responsabile dei danni. Deve anche far rispettare le normative in merito alla privacy.

Ha competenze giuridiche, informatiche e di risk management.

**2) Spiegare cosa sono i principi di "accountability" e "reporting" previsti dal GDPR (3-5 punti).**

2) Accountability: Bisogna essere pronti a fornire delle controprove a possibili violazioni del GDRP da parte del responsabile

Reporting: Il reporting dei dati va fatto in modo chiaro e trasparente riguardo tutti i processi che li coinvolgono

**3) Descrivere cosa intende proteggere lo standard PCI DSS, indicando quali sono le categorie di controlli tecnici che vengono necessari ad ottenere una certificazione (5-6 punti).**

3) xd

Slide n. 32 del pacco Standard relativi alla sicurezza informatica

È uno standard richiesto a chi emette carte di credito da usare con transizioni elettroniche via Internet, garantisce sicurezza nell’uso delle carte di credito e uso consapevole nel trattamento dei dati. Tra i requisiti principali troviamo: avere un firewall, non usare password di default, i dati devono essere cifrati e protetti, gestire bene le vulnerabilità, applicare puntualmente le patch, identificare ogni utente e monitorare la rete.

**4) Riguardo allo standard TCSEC, indicare chi lo ha definito e cosa intende proteggere. Spiegare inoltre cosa è la "classificazione basata sui requisiti" e indicare la principale differenza tra la classe C e la classe B (5-6 punti).**

4) TCsec è uno standard americano atto a definire come dovrebbe essere progettato un sistema informatico in merito alla sicurezza. Offre i seguenti livelli di sicurezza: D C1 C2 B1 B2 B3 A1

La grossa differenza fra i livelli C e B sta nella presenza di controlli obbligatori, non presenti nei livelli C (dove sono facoltativi).

**5) Definire i tre principali approcci alla stima dei rischi (es. risk assessment) (3-4 punti).**

5) I principali approcci sono:

Threat-oriented: Il rischio va stimato a partire dai possibili attaccanti e dalle minacce che possono sfruttare.

Asset oriented: Il rischio va valutato a partire dai nostri asset: quali potrebbero risultare più interessanti ad attaccanti.

Vulnerability-oriented: Il rischio va valutato da una fase di vulnerabilty assessment e quindi da un giudizio delle vulnerabilità del nostro sistema.

**6) Definire cosa sono le CVE e le CWE e da chi sono state definite e chi le gestisce. Infine, spiegarne i principali aspetti comuni e le differenze (5-6 punti).**

6) CVE: common vulnerabilty and exposure, una lista di tutte le vulnerabilità ad oggi trovate. Vengono distinte vulnerabilità (sfruttabili direttamente per attaccarci) ed exposure (difetti software che possono portare ad indebolire il nostro sistema).

Ogni vulnerabilità ha un ID, l’anno di scoperta, il numero di attacchi, una descrizione e il software che la introduce.

Sono gestite dal MITRE

CWE: common weakness enumeration, contiene una lista di tutte le debolezze presenti nei software, divise per categorie. Può essere utile per capire errori fatto da altri sviluppatori software per non ripeterli.

**7) Un'azienda ha effettuato un Vulnerability Assessment e identificato molti sistemi (es. server, PC utenti, dispositivi di sicurezza, sistemi legacy) che presentano vulnerabilità che richiedono di essere corrette. Seguendo le direttive del NIST, proponete una strategia per scegliere un ordine di applicazione delle patch che minimizzi l'esposizione ai rischi di sicurezza e riduca i disservizi (5-6 punti).**

7) Per prima cosa andrebbero applicate le patch su dei sistemi non critici e che non richiedano elevato testing. Di conseguenza, escluderei sistemi legacy, dispositivi di sicurezza e server: un difetto in questi sistemi potrebbe compromettere il nostro intero sistema.

Procederei per piccoli gruppi, partendo dai dispositivi che avrebbero teoricamente meno problemi in funzione di tale patch: PC utenti, server, sistemi legacy, dispositivi di sicurezza.

Regole: applicare le patch prima a piccoli gruppi di sistemi (subsets), prima a sistemi che probabilmente non avranno grossi problemi (standard first) e invece quelli che hanno peculiarità e configurazioni speciali, come sistemi legacy e IoT, vanno pachati dopo un’attenta fase di collaudo e test.

**8) Spiegare cosa è un SIEM e quale importante funzionalità di sicurezza aiuta a svolgere. Indicare infine un esempio di azienda che potrebbe aver bisogno di un SIEM (3-5 punti).**

8) *Non ricordavo manco per il cazzo cosa fosse un SIEM,*

ma è un sistema che combina SEM e SIM: analizza log ed eventi non in tempo reale\* (SEM) e produce report su essi (SIM).

Una azienda di medie dimensioni con non troppi dati nei log, altrimenti il monitoring sarebbe troppo lungo.

SIM -> colleziona, analizza e produce report basati sui dati dei log.

\*Quindi un SIEM ci permette di capire se siamo stai attaccati, non se siamo sotto attacco.

ESERCIZIO NUMERI

Il director va messo in un posto qualunque

Riassunto: sugli host metti HIDS, reti NIDS, sui firewall LFM (=Log File Monitor)

1. Sensore per identificare se siamo sotto attacco, se siamo target -> NIDS

2. Sensori che guardino i log da monitorare, come log delle connessioni. Per esempio gli LFM. è importante guardare i log sui Firewall. (Dettaglio non richiesto)

3. DMZ controllo il traffico, ma è utile monitorare se qualcuno sta facendo DoS. (non richiesto sto dettaglio all'esame). NIDS.

5. NIDS, vedere se qualcuno ha superato il FW

6. Stesse cose del firewall 2 con attenzioni su traffici diversi

7. Un altro NIDS

8. Analisi dei log, degli attacchi, dei file, tutto. HIDS, LFM, SIV

9. Scada non è necessario sapere cosa è, ma espone i servizi della rete industriale verso l'esterno. Schiaffiamoci un HIDS e via

10. NIDS

ESERCIZIO (PROTEZIONE SERVIZI) da Esercitazione 2

Intanto mettere un packet filter, che non permette ai pacchetti della sottorete 10.0.1.0/24 di andare verso l'esterno eccetto che verso gli utenti autenticati (politica di whitelisting)

Inoltre, in quanto bisogna tenere conto delle applicazioni e delle differenti porte dei server, è necessario TLS (livello 4) per creare anche protezione di canale.

Tramite TLS è possibile effettuare inoltre integrità e autenticazione obbligatoriamente, riservatezza e autenticazione del server opzionalmente rappresentando quindi una scelta ottimale.

Inoltre, mediante l'uso di VPN tramite TLS è possibile garantire l'accesso ad utenti esterni una volta autenticati. (Soluzione di Mat da Telegram)

SOLUZIONE MAIL PROF SU IPAD

Oppure soluzione foto:

che è giusta ma con whitelisting deny all su s1, S2, s3

Immagine che contiene testo

Descrizione generata automaticamente

**ESAME 1** (Svolto da Mat di Telegram)

**Domanda #1**

Componenti nella soluzione e ruolo:

- Access point wireless: verrà utilizzato come proxy per poi dialogare con il server radius

- Radius server: authentication server

Comunicazioni e protocolli:

L'utente dialogherà con l'access point wireless mediante EAP over wireless, il quale successivamente dialogherà con il RADIUS server mediante EAP over RADIUS. Il pacchetto EAP del cliente verrà incapsulato dall'access point in un pacchetto RADIUS per verificare se l'utente può essere autenticato. Il tutto quindi seguendo lo standard IEEE 802.1x

**O tipo Eduroam???**

**Domanda #3**

Definizione KDF:

Una Key Derivation Function è una funzione del tipo kdf(p,s,i).

Il loro scopo è quindi trasformare una password in una chiave (crittografica, fatta di valori random) utilizzabile ai fini della crittografia.

Data una stringa prevedibile e si ottiene in uscita una stringa random

Problema relativo che permettono di affrontare:

Un esempio di problema che risolvono sono gli attacchi brute force, in quanto le iterazioni rallentano gli attacchi.

Funzioni crittografiche su cui vengono costruite:

Funzioni di hash.

Esempio di algoritmo valido:

Un esempio di algoritmo è PBKDF2.

Parametri in input e scopo di loro utilizzo:

key = kdf (pass, salt, iteration)

S = sale (numero pubblico random) i = iterazioni(solitamente è un numero elevato)

Essa prende in input una password, un sale crittografico da aggiungere ad essa al fine di aumentarne l'entropia, un numero di iterazioni al fine di aumentare l'entropia e per rallentare la funzione per un attaccante. In output fornisce una chiave generata a partire tra questi dati in input.

**Domanda #4**

Spiegare cosa è e a cosa serve il vulnerability assessment:

Il vulnerability assessment è un processo che permette di identificare le vulnerabilità del nostro sistema e i problemi a cui esso è esposto dal punto di vista della rete

4 fasi: planning, information gathering, scanning, report

Indicare quali categorie di informazioni colleziona:

Le informazioni ottenute mediante il vulnerability assessment sono relative a:

- Informazioni se un host è acceso o no

- Informazioni sull'attività delle porte relative ad un host

- Informazioni sul sistema operativo

Oltre a ciò, è importante identificare quali software sono installati sui nostri dispositivi

Spiegare quali approcci e strumenti esistono per collezionare le informazioni:

Un esempio di approccio è il SYN scan, il quale permette di capire se un host è in ascolto su una determinata porta in base alla risposta fornita rispetto al pacchetto TCP inviato. In base ai tempi di risposta è possibile anche intuire qual è il sistema operativo dell' host scansionato.

2 tecniche di scansione: host discovery (ping, ARP, TCP SYN o UDP) e port scanning

Riportare le principali fonti di informazione (almeno due):

Alcune delle fonti che possono fornirci più dettagli in tale ambito sono il CVSS (è giusto??), che permette di valutare il livello di sicurezza basandosi su delle metriche relative alla vulnerabilità e il CWE, che contiene una lista di vulnerabilità per ogni software divise per categoria. …e CVE

Slide 23 di analisi del rischio (?) -> NIST propone di creare e mantenere un DB con info su tutto il software/firmware/codice che potrebbe contenere vulnerabilità

**Domanda #5**

Common Criteria:

I Common Criteria sono uno standard di sicurezza nato all'interno dell'UE il quale permette di catalogare determinate funzionalità.

Sono semplici criteri/regole che definiscono quanto il nostro sistema è sicuro

Protection Profile:

Richiesta di analisi dei requisiti di sicurezza di una specifica funzionalità, per esempio soltanto l'autenticazione.

Ciò permette di attribuire livelli di sicurezza diversi a parti diverse del nostro sistema.

Sono l’interpretazione dei principi generali di una classe declinata per un prodotto specifico.

Componenti Funzionali:

I componenti funzionali sono dei componenti mediante i quali è possibile catalogare la sicurezza del nostro sistema. In base alle specifiche del nostro sistema viene quindi associata alla funzionalità in esame un determinato livello di sicurezza, i quali vanno da EAL0 a EAL7.

**Domanda #6 (1.5 punti)**

Cosa è un VPN Concentrator?

Sono dei router ottimizzati per l'uso di IPsec

Come viene utilizzato?

Essi vengono usati come terminatori di tunnel IPsec, in quanto presentano prestazioni ottimali in ambito crittografico.

**Domanda #7** **(1.5 punti)**

Orange book:

L'orange book rappresenta uno dei primi standard di sicurezza definiti, ormai obsoleto. Esso si rifà allo standard americano TCSEC.

Esso veniva utilizzato per assegnare un determinato livello di sicurezza al nostro sistema fra i seguenti livelli, in ordine di sicurezza crescente: D, C1, C2, B1, B2, B3, A1.

Ciascun livello fornisce delle linee guida da rispettare al fine di poter raggiungere quel determinato livello di sicurezza.

**ESAME 2**

**DOMANDA #1**

Analisi di sicurezza

Immagine che contiene testo

Descrizione generata automaticamente

Asset (secondari):

Chiave privata della CA

Chiave privata del server

Chiave privata di ogni utente

Punti di attacco principali:

Attacco di tipo MITM durante la trasmissione della security bag PKCS#12

Tentativi di accesso al segreto utente o ad informazioni sensibili (spoofing richiesta server)

Tentativi di accesso al segreto lato server (manomissione SW, Dump RAM)

Tentativi di compromissione della CA Aziendale

Problema 1:

Il primo problema è l'ottenimento, in seguito alla registrazione della security bag PKCS#12 da parte dell'utente. Infatti, se questa viene trasmessa, è possibile utilizzare TLS ma senza autenticazione del client (in quanto ancora non possiede un certificato). Di conseguenza se qualcuno entra in possesso del file PKCS#12 che è semplicemente protetto da passphrase, potrà con un attacco a dizionario entrare in possesso dell'identità di un utente. Ad esempio ci potrebbe essere un MITM che si interpone tra noi ed il server nella fase di registrazione e negozia un canale TLS client-MITM e uno server-MITM facendo spoofing. Tutto ciò è possibile se la rete aziendale non è sicura.

Mitigazione al problema 1:

E' possibile (se l'azienda è di piccole dimensioni) distribuire in modo offline le chiavi. Per un'azienda di grandi dimensioni è possibile fare monitoring sulla rete interna rendendola sicura ed evitando intrusioni di MITM

Problema 2:

Se il server presenta delle vulnerabilità, una manomissione del server potrebbe permettere di arrivare a manomettere/scoprire la chiave privata della CA. Anche scoprire la chiave privata del server avrebbe conseguenze importanti.

Se si manomettesse la CA sarebbe possibile emettere un qualsiasi certificato e quindi garantire l'accesso a chiunque, oppure negare l'accesso ad utenti legittimi.

Manomettendo il server, sarebbe ovviamente possibile si potrebbe allo stesso modo autenticare/ respingere chiunque

Mitigazione al problema 2:

Separare server e CA, mettendo la CA su una rete a maggior sicurezza e protetta da firewall. Inoltre utilizzare un HSM per salvare la chiave privata del server ed un HSM per il salvataggio della chiave privata della CA

2 soluzione:

“Qualcuno ha fatto questo esercizio? A me vengono in mente alcune cose, però mi sembrano un po' "banali"

Tipo che in fase di registrazione se non si hanno le credenziali il canale non è sicuro, ma il server ha il certificato quindi il tunnel TLS puo' essere instaurato con DH senza paura di MITM

Le chiavi sono salvate sul PC e sono esposte ad attacchi MATE, però si puo' risolvere cifrandoli

La CRA asimettrica potrebbe essere oggetto di known plaintext o signature trap, però basterebbe accettare solo richieste firmate dalla CA del server

Non lo so nessuno di questi tre problemi mi sembra quello che si aspetterebbe, idee?”

3 soluzione: 2 problemi di sicurezza per autenticazione con x.509 (da telegram)

1. L’autenticazione non è forte perché basata su certificati. Deve avere un basso rischio associato e, tra le altre cose, deve essere multifattore: la soluzione proposta non lo è.

2. La CA aziendale non serve a niente, anzi la sua presenza all’interno del sistema la rende sensibile ad attacchi: invalidare una CA significa invalidare tutti i certificati da essa generati con grossi problemi di sicurezza, senza dimenticare che la CA da sola non garantisce autenticazione se non attraverso la catena di CA esterne comunque necessaria.

3. PKCS#12 deve contenere solo la chiave privata: la chiave pubblica è già contenuta all’interno del certificato X.509 in transito nel pacchetto.

4. Le credenziali salvate in un solo PC aziendale costituiscono un single point of failure: converrebbe memorizzare tali informazioni in un HW apposito (HSM) e realizzare backup frequenti conservati con estrema cautela.

**DOMANDA #2**

Es protezione servizi dell’esercitazione 2

**DOMANDA #3**

**Quali proprietà di sicurezza possono essere applicate al traffico usando IPsec (v2) ESP in transport mode, per ognuna dire se è obbligatoria o opzionale e a quale parte del pacchetto Ip si applicano.**

Autenticazione e integrità mediante keyed digest OPPURE encryption con cifratura simmetrica, una delle due obbligatoria

Protezione parziale da attacchi replay mediante sequence number.

Tutte le protezioni sono relative solo al payload, in quanto transport mode.

**DOMANDA #4**

**Vulnerability assessment (già fatta)**

Il vulnerability è una fase fondamentale al fine di identificare le vulnerabilità del nostro sistema.

Si divide in 4 fasi: planning, information gathering (topologia della rete, software installati, quanti device), scanning, report.

Vengono ottenute informazioni differenti con tecniche di scan differenti. Le due macrocategorie di scanning sono host discovery e port scanning: le prime permettono di dire se un host è attivo o no, le seconde scendono più nel dettaglio e permettono di dire su che porta è in ascolto un host. Inoltre, mediante euristiche sui tempi di risposta dei vari device, è possibile carpire anche qual è il sistema operativo in uso. Alcune metodologie di scanning sono SYN scan (mediante invio di un pacchetto con SYN a 1 su una porta. Non completa la creazione della connessione con l'ack finale), TCP connect (Come syn scan ma completa la connessione, UDP scan (scannerizza più porte insieme).

Le principali fonti di informazioni al riguardo sono:

- il CVE, common vulnerability and exposure, che elenca tutte le vulnerabilità ed exposure fino ad ora. Le exposure sono errori che possono causare vulnerabilità.

- Il CWE, common weakness and enumeration, che elenca le vulnerabilità dei software catalogando anche il tipo di vulnerabilità presente

**DOMANDA #5**

**6 aspetti uso algoritmo di cifratura simmetrica per cifrare dati at rest per avere confidenzialità mentre l’integrità non è necessaria**

- cifra bene ed è safe da attacchi vari di known-plain text

- se usi una kdf la chiave non la trovi con i dictionary attack

- la chiave deve essere lunga almeno 128 bit e devi cambiarla spesso per mantenere il tutto sicuro

- l'algoritmo pure devi cambiarlo spesso. Se cifri 10 TB di storage con un algoritmo e il giorno dopo ti trovano una vulnerabilità in quell'algoritmo sei fottuto

- Devi cambiare pure l'IV perché altrimenti hai un altro fattore di vulnerabilità

- la generazione della chiave è semplice

- nel caso di CBC per esempio, si garantisce un alto livello di protezione e si rende la cifratura più robusta verso attacchi di tipo plain-text

- Per essere robusto ad attacchi di tipo plain text va cambiato spesso l'IV, quindi anche questo fattore influisce sulla sicurezza

- La distribuzione della chiave rappresenta uno dei problemi della cifratura simmetrica ma vi sono diversi metodi per ovviare a ciò

- Qualora si entrasse in possesso della chiave, si potrebbe decifrare tutto ciò che è stato cifrato con quella chiave. Nella cifratura asimmetrica, possono decifrare quello che mandano a te ma non quello che tu mandi agli altri

-Un altro fattore cruciale è la lunghezza della chiave. Essa dovrebbe essere almeno 128 bit per garantire un buon livello di sicurezza

**DOMANDA #6 (1.5 punti)**

**Perché versioni “doppie” degli algoritmi di cifratura simmetrici non vengono mai usate**

Le versioni sono soggette ad attacchi know plaintext e aumentano il tempo di computazione senza aumentare notevolmente la sicurezza. Un esempio è 2DES, che è ormai obsoleto in quanto viene usato 3DES.

**DOMANDA #7 (1.5 punti)**

**Cos’è il fraggle attack e come viene sfruttato dagli attaccanti?**

è un attacco simile allo smurfing attack, il quale viene effettuato mediante ICMP echo request. Il fraggle attack viene utilizzato mediante UDP echo request, mandata in una sottorete in broadcast con destinazione un particolare host della sottorete. Ciò causerà l'invio di moltissimi pacchetti di risposta dagli host della sottorete verso l'host destinazione, ed essendo UDP il tempo di elaborazione dei pacchetti è ancora maggiore (va analizzato l'UDP e l'IP)

Si può prevenire come lo smurfing, ossia proibendo l'invio di messaggi in broadcast da host esterni alla rete.

é più potente dello smurfing, ma più complesso computazionalmente.

**ESERCIZIO 1 OTP** (da telegram)

La OTP non viene più erogata da un autenticatore hardware ma da un applicazione, motivo per cui è fondamentale verificare che sia l’app che il dispositivo su cui è installata siano aggiornati all’ultima versione disponibile in modo da assicurare l’installazione di eventuali patch correttive.

Inoltre, come nel caso dell'HSM è necessaria un’autenticazione multifattore. In questo caso però si può sostituire il pin con un dato biometrico utilizzando FIDO: l’utente inserisce username e password e si autentica mediante l’uso di un fattore biometrico. La flessibilità di FIDO è dovuta anche al fatto che tutto questo processo viene gestito automaticamente dal backend di FIDO e il nostro sistema non dovrà occuparsene direttamente.

TLS usato per autenticazione

Lato server direi che non deve più mantenere segreti dell'utente, si mettono d'accordo sul metodo di generazione OTP e via.