ESAME GENNAIO 2024
Crocette giuste:

Domanda 1
- un IPS può permettere di velocizzare ed automatizzare la risposta alle intrusioni rilevate
- un HIDS può verificare che alcuni file non vengano modificati e analizzare quello che riportano i log dei sistemi informativi
- un SOC dovrebbe includere anche personale che si occupa dell'analisi del cybercrime per mantenere aggiornata l'analisi dei rischi

Domanda 2
- I dati relativi allo stato di salute e la razza sono considerati di categoria speciale
- Il Titolare del trattamento dei dati del Politecnico di Torino è il rettore
- Nel GDPR, il principio della privacy by design indica che bisogna usare automaticamente le protezioni più restrittive possibili -> possibile che la invalidi
- Quando una persona accetta il ruolo di DPO diventa responsabile dei danni causati dai data breach
- Un data breach è un incidente informatico che porti alla distruzione, alterazione, diffusione non autorizzata o accesso ai dati personali

Domanda 3
- Per avere una Qualified Electronic Signature la chiave pubblica deve provenire da un Qualified Certificate
- Se un documento è firmato da più persone usando firme parallele, è possibile rimuovere una firma senza che gli altri firmatari se ne accorgano
-Cambiando l'ordine di una delle firme sequenziali può far fallire la verifica di qualche firma digitale
- Il Time Stamp è, in pratica, la firma digitale di una stringa di testo o di un intero che rappresenti un valore temporale e del digest di un documento

Domanda 4
- Il Mandatory Access Control funziona confrontando le etichette (label) delle risorse e degli utenti che ne fanno richiesta e concedono l'accesso secondo modelli formali.
- L'orange book è documento redatto dal DoD il cui titotlo completo è Trusted Computer System Evaluation Criteria.
- I Common Criteria non fanno riferimento ad un processo di valutazione perché questa è trattata dalla Computer Evaluation Methodology.
- Gli standard possono permettere di stimare quando alcuni prodotti di sicurezza possono essere considerati sicuri senza fare test propri

Domanda 5
- S/MIME usa il meccanismo standard di MIME per gestire gli allegati per inserire oggetti crittografici
- HTTP-S è un'implementazione obsoleta che protegge messaggi HTTP usando strutture S/MIME
- la firma digitale di S/MIMEV4 ha sempre valore legale perché dalla versione 4 è uno standard IETF e usa crittografia asimmetrica che permette il non ripudio

Crocette sbagliate:

Domanda 1
- dal punto di vista delle intrusioni, osservare quello che avviene all'esterno della mia organizzazione non è particolarmente rilevante .

- le persone che lavorano in un SOC non dovrebbero occuparsi di vulnerability management e patch management .
- preparare le politiche di risposta agli incidenti è possibile solo se un'azienda ha un Incident Response Team .
- un SIEM (System Information Events Management) combina le funzionalità di analisi degli eventi e per la gestione di un sistema informativo
- un NIDS è uno scanner di rete che identifica vulnerabilità note
- gli honey pot sono strumenti che servono ad attirare gli attaccanti simulando il fatto che le risorse siano più facili da attaccare per aumentare il loro interesse

Domanda 2
- Il GDPR introduce il concetto di minimizzazione, che indica che i dati devono essere collezionati usando il minimo numero di strumenti e resi accessibili al minor numero di operatori
- Il DPO si occupa di riottenere i dati degli utenti quando avvengono dei data breach
-Il principio della Full Functionality del GDPR richiede che i controlli funzionino al massimo livello di sicurezza per garantire la protezione dei dati personali
- I servizi che usano dati personali devono essere pensati per proteggere questi dati durante tutte le fasi di progettazione ma non si può garantire che lo siano anche durante implementazione

Domanda 3
- Un esempio di enveloped signature è quella usata dal PKCS#7
- Un dispositivo di firma sicuro può essere ritenuto sicuro se è tamper proof e usa algoritmi ritenuti sicuri
- Forgiare una firma falsa è più facile se si usano le detached signature
- L'Advanced Electronic Signature può essere usata in tribunale
- Un Qualified Certificate certifica l'identità usando algoritmi qualificati, riconosciuti dalle entità come più efficaci

Domanda 4
- Una strength of mechanisms dichiarata alta indica che il prodotto può ritenersi molto sicuro.
- In Italia non abbiamo un Common Criteria Evalutaion Scheme, perché la certificazione CC funziona solo a livello europeo
- In una valutazione di sicurezza ai fini della standardizzazione, la correttezza della soluzione non deve tener conto del processo di sviluppo.
- Un Protection Profile è un modo per definire in maniera semplificata come verrà gestita la procedura di valutazione per security target specifici
- ITSEC non supporta la ri-valutazione di un precedente processo di standardizzazione

Domanda 5
- il formato PKCS#12 è un metodo ottimizzato per trasportare firme digitali
- il greylisting è uno strumento molto efficace per decidere se rifiutare o accettare mail da un MTA Open Relay
- i messaggi clear-signed sono visibili su qualunque strumento per la gestione delle mail e anche da web perché firmati con firma detached
- il CMS è l'evoluzione del formato PKCS#12 per la rappresentazione di dati crittografici
- il metodo STARTLS è usato per trasmettere in maniera confidenziale messagi di posta elettronica
- un server Open Relay permette di inviare mail senza restrizioni ai soli utenti interni
- il protocollo SMTP permette di autenticare gli utenti prime di inviare mail solo con metodi deboli come LOGIN, PLAIN CRAM-MD5

ESAME FEBBRAIO 2024
Crocette Giuste:

Domanda 4

- abilitando la Data Execution Prevention (DEP) rendo più difficile sfruttare i buffer overflow. [vero, la DEP è stata inventata proprio per quello, perché rendere non-executable lo stack rende impossibile usare shellcode in maniera banale]
- i ROP gadget contengono sempre istruzioni di tipo RET. [vero, per definizione un gadget termina con RET]
- la potency è una misura astratta di quanto è buona una tecnica di protezione del software,
- alcune tecniche di attestazione del codice verificano se i binari sono integri al momento dell'esecuzione o del caricamento in memoria o quando sono salvati su disco. [vero, sono diversi modi di svolgere software attestation verificando l'integrità dei binari (invece di execution correctness)]

Domanda 5

- con l'attacco Heartbleed si possono leggere dati confidenziali e altri segreti, [vero, permette di farsi inviare pezzi della memoria del processo che gestisce TLS]
- le tabelle delle connessione di un server protetto con un SYN interceptor non sono a (elevato) rischio di saturazione, [vero, l'interceptor risponde al posto del server, le tabelle del server non sono quindi troppo a rischio]
- il particolare tipo di attacco usato da Ettercap richiede che siano costantemente inviati messaggi che servono a mantenere le vittime "avvelenate". [vero, le cache si svuotano dopo un certo numero di secondi, quindi bisogna rinfrescare costantemente l'attacco, come visto ad esercitazione con il parametro arp_poison_delay]

Domanda 6

- i problemi matematici che rendono sicuri DH e ECDH sono equivalenti. [il problema dell'inverso su curve ellittiche di EDCH è computazionalmente equivalente al logaritmo discreto di DH, motivo per cui, si dice spesso che ECDH è basato su logaritmo discreto].
- il calcolo della firma digitale di un documento è un'operazione che richiede l'uso di una chiave privata sul digest del documento stesso,
- le Key Derivation Function sono progettate per essere (ragionevolmente) lente ed inefficienti nella gestione della memoria. [vero, le KDF usano le iterazioni per rallentare gli attaccanti che vogliano fare attacchi a forza bruta, le KDF moderne usano molta RAM per rendere inutilizzabili le GPU].
- in RSA, una volta calcolati n e d, non mi servono più p e q per svolgere le operazioni crittografiche.

Domanda 7

- DTLS funziona con UDP ma non con TCP. [vero, per definizione DTLS è la versione per datagram di TLS]
- se il client presenta un session-id, il server potrebbe decidere di saltare (buona parte del) la fase di Handshake e indicare di iniziare a proteggere direttamente i dati di canale a partire dai segreti negoziati in uno dei precedenti Handshake. [vero, uso la master secret del precedente Handshake (unico segreto) e gli algoritmi scelti con l'ultima ciphersuite, i random non sono segreti, ma sono parametri pubblici per la 'freshness']
- la versione più recente di TLS non usa più la compressione. [vero, dalla versione 1.3 la compressione (che era possibile, non era usata da nessuno ma portava vulnerabilità e attacchi) è stata rimossa]
- la ciphersuite TLS_DHE_DSS_WITH_AES_128_CBC_SHA indica la volontà di firmare con DSS i parametri effimeri per lo scambio di chiavi. [vero, DHE_DSS = Diffie-Hellman effimero, parametri effimeri firmati con DSS]

- OpenVPN è un protocollo che può essere usato in alternativa ad IPsec per creare Virtual Private Network.

Domanda 8
- durante la fase di risk monitoring potrei dover cambiare tutte le formule che mi permettono di stimare il rischio aziendale,
- secondo il framework RMF del NIST, la fase di framing include l'identificazione degli asset e la valutazione del loro valore,
- l'information gathering è un processo essenziale per la valutazione dell'esposizione delle aziende ai rischi informatici. [vero, l'information gathering serve per il (vulnerability/threat/risk) assessment (e non solo) e senza quelle informazioni non potrei valutare il rischio]
- conoscere il numero di sequenza che un host userà nel corso del prossimo tentativo di connessione TCP è utile agli attaccanti per fare spoofing. [vero, se voglio fare spoofing devo essere in grado di predire il prossimo sequence number che userà un host, come visto ad esercitazione, anche nmap vi dà il parametro di TCP Sequence Prediction]

ESAME FEBBRAIO 2024
CROCETTE SBAGLIATE:

Domanda 4
- nel paradigma Man-at-the-End, gli attaccanti **prendono il controllo** degli endpoint delle vittime. [falso, nel MATE gli attaccanti sono già i proprietari degli endpoint e non sono vittime, lavorano sui loro sistemi per attaccare il software]
- le protezioni del software servono a rendere impossibile violare gli asset presenti nel software. [falso, servono a ritardare gli attacchi]
- uno shellcode è un tipo di gadget; esso rilascia, una volta terminato, il controllo dell'esecuzione alla funzione chiamante e serve quando si attacca un'applicazione mediante Return Oriented Programming (ROP). [falso, shellcode non è un gadget ed il resto sono frasi che non si applicano agli shellcode]
- la white-box cryptography cifra le chiavi nel codice di un'applicazione per proteggerla da attacchi di reverse engineering. [falso, white-box crypto non cifra niente, offusca chiavi e codice]
- un disassembler ottiene in maniera deterministica la rappresentazione in codice assembly del binary machine code di un programma. [falso, i disassembler non sono deterministici, anzi talvolta non funzionano proprio e spesso le protezioni servono a non farli funzionare correttamente]

Domanda 5
- il port scanning è il metodo di information gathering con cui posso identificare con certezza i servizi in base al numero di porta su cui i servizi stessi sono in ascolto, [falso, come visto ad esercitazione, con il port scanning (-sT) so solo il numero di porta aperto, non il servizio che si scopre con la fase di service fingerprinting (-sV) e neanche con certezza]
- dato un keyed-digest calcolato come kd = H(K || M), esiste un attacco che permette di ottenere la chiave K a partire da kd. [falso, posso fare attacchi sulle collisioni ma i dati originali si perdono]
- lo Smurfing attack può essere evitato richiedendo l'autenticazione del target [falso, lo smurfing attack si evita evitando filtrando le richieste in braodcast da reti esterne (Protezione da IP spoofing), in ogni caso, il target è tipicamente esterno e non dovrebbe essere coinvolto nelle difese]
- con il FIN scanning posso distinguere filtri di livello applicativo da packet filter stateful. [falso, il FIN scanning può servire a distinguere stateful vs. stateless, non mi permette di identificare niente a livello

applicativo, del resto il TCP lavora a livello 4]
- l'attacco di Kaminski può essere evitato usando IPsec. [falso, si evita con DNSSEC]

Domanda 6
- il protocollo ESP di IPsec v1 è un esempio concreto di Authenticated Encryption with Associated Data. [falso, la v1 non supportava proprio autenticazione, quindi non può implementare authenticated encryption]
- per ottenere due messaggi che abbiano lo stesso digest usando SHA3-256 (SHA3-256(m1)=SHA3-256(m2)), servono in media gli stessi tentativi di un attacco a forza bruta contro AES-256. [falso, collisioni del secondo tipo (second pre-image attack) dimezzano il numero di bit del digest (paradosso del compleanno), quindi SHA2-256 ha 128bit di sicurezza vs. AES256 invece 256]
- SHA2 è un algoritmo sviluppato quando sono stati individuati i primi potenziali attacchi contro SHA-1.[falso, SHA2 è una famiglia di algoritmi, non un solo algoritmo]
- per fidarmi di una CRL, oltre alla verifica crittografica della firma della CA che l'ha emessa, devo aggiungere la fiducia esplicita al suo contenuto. [falso, mi fido delle CRL solo della verifica crittografica e della CA (o della root CA da cui la CA deriva), come visto anche ad esercitazione, non devo aggiungere la CRL in alcun file per farne una verifica con OpenSSL]
- con l'On-line Certificate Status Protocol posso chiedere ad un server (es. via Internet) se un determinato certificato, identificato da un serial number, è valido al momento della richiesta o in un preciso momento precedente. [falso, OCSP risponde sullo stato di un certificato solo al momento in cui arriva la richiesta]

Domanda 7
- SSH usa particolari tipi di certificati X.509 (semplificati) per trasmettere le chiavi RSA tra client e server. [falso, SSH non usa certificati, manda solo chiavi pubbliche e devo accettarle esplicitamente la prima volta che mi connetto]
- TLS usa una sliding window per evitare (parzialmente) attacchi di tipo Replay.[falso, quello è IPsec]
- la ciphersuite TLS_DH_RSA_WITH_AES_128_GCM_SHA256 indica la volontà di usare SHA256 per calcolare il MAC nel Record Protocol.[falso, usando AES_128_GCM si fa authenticated encrpytion quindi il MAC è il TAG del GCM, SHA256 serve solo come pseudo-random function]
- TLS 1.3 è perfettamente interoperabile con TLS 1.2. [falso, non sono mai interoperabili versioni diverse di protocolli, ma per TLS1.3 si poteva essere ancora più sicuri perché cambia completamente l'Handshake protocol]

Domanda 8
- il sistema semi-quantitativo, che usa valori numerici, è più efficace di quello qualitativo per categorizzare i valori delle grandezze usate nel calcolo dei rischi. [falso, sono perfettamente equivalente per la categorizzazione]
- un sistema su cui è presente una vulnerabiltà di tipo patched, nell'analisi dei rischi, deve essere considerato più a rischio rispetto a quando la vulnerabilità non era nota.[falso, una volta 'patchata' la vulnerabilità non influisce più sul rischio, come evidente dal diagramma degli stati delle vulnerabilità]
- OWASP è uno standard che serve (anche) per la valutazione del livello di sicurezza delle applicazioni web. [falso, OWASP non è uno standard, del resto non lo abbiamo visto nella parte degli standard]
- le CVSS definiscono in maniera fissa e assoluta caratteristiche e severità delle vulnerabilità notificate al MITRE. [falso, oltre al valore BASE, includono valori temporali e di contesto che permettono di far variare il valore del punteggio in modo che vulnerabilità vecchie e fuori contesto possano avere score più bassi]
- per minimizzare i rischi e ottimizzare la gestione delle patch, il NIST suggerisce di installare prima possibile le patch sui sistemi legacy perché sono di solito meno sicuri. [falso, standard first, applica le

patch prima ai sistemi che non daranno problemi, i sistemi legacy sono sempre problematici e conviene lasciarli per ultimi]

ESAME ESTIVO 2024

Crocette giuste:

Domanda 4

1) Nel paradigma Man-at-the-End, gli attaccanti **hanno** il controllo completo degli endpoint dove gli attacchi vengono preparati e realizzati
2) i ROP gadget terminano sempre con istruzioni RET
3) Le protezioni del software hanno l'obiettivo di ritardare o rendere meno vantaggiosi gli attacchi contro gli asset presenti nel software

Domanda 5

1) Un IPS può permettere di velocizzare ed automatizzare la risposta a specifiche intrusioni rilevate.
2) Un HIDS può verificare, all'interno di un host specifico, che alcuni file non vengano modificati e analizzare quello che riportano i log dei sistemi informativi.
3) Vulnerability management e patch management, secondo il NIST, sono attività che dovrebbero essere svolte da personale informatico specializzato in cybersecurity.
4) Gli honey pot non espongono asset reali agli attacchi

Domanda 6

1) In una valutazione di sicurezza ai fini della standardizzazione, la correttezza della soluzione deve tener conto anche del processo di sviluppo.
2) Il Mandatory Access Control previsto dalla classe B di TCsec usa modelli formali per stabilire quando garantire l'accesso alle risorse.
3) Anche in Italia abbiamo un Common Criteria Evaluation Scheme, perché questi organismi di valutazione funzionano su base nazionale
4) L'orange book è documento redatto dal DoD il cui titolo completo è Trusted Computer System Evaluation Criteria
5) Common Criteria non includono una metodologia di valutazione, la valutazione è trattata da un ulteriore standard (CEM).

Domanda 7

1) TLS numera i pacchetti per evitare attacchi di tipo Replay.
2) La ciphersuite TLS_DHE_RSA_WITH_AES_128_CBC_SHA indica la volontà di firmare con RSA i parametri effimeri per lo scambio di chiavi.
3) TLS 1.3 usa un Handshake Protocol diverso da quello usato fino al TLS 1.2. → 1.3 ha zero round trip time, quindi è diverso il protocollo
4) OpenVPN è un protocollo che può essere usato in alternativa ad IPsec per creare Virtual Private Network

Domanda 8

1) Per fidarmi di un certificato, oltre alla verifica crittografica della firma della CA che l'ha emesso, devo aggiungere la fiducia esplicita nei confronti della root CA
2) DH e ECDH sono basati su problemi matematici "difficili" diversi ma gli attacchi noti sono (computazionalmente) equivalenti
3) la firma digitale di un documento è il risultato di un'operazione che coinvolge l'uso di un parametro asimmetrico segreto e del digest del documento stesso

ESAME ESTIVO 2024

Crocette sbagliate:

QUESTION 4

1) Uno shellcode serve per svolgere attacchi di tipo Return Oriented Programming (ROP)
2) la Data Execution Prevention (DEP) vieta l'esecuzione di codice dai segmenti in cui ho privilegi di lettura
3) la white-box cryptography cifra le chiavi nel codice di un'applicazione per proteggerla da attacchi di reverse engineering
4) Le tecniche di attestazione del codice impediscono le modifiche al codice garantendo l'integrità
5) Un disassembler genera deterministicamente la rappresentazione in codice assembly del binary machine code di un programma

QUESTION 5

1) Dal punto di vista delle intrusioni, osservare quello che avviene all'esterno della mia organizzazione non è particolarmente rilevante.
2) Un HIDS è un tool che identifica le vulnerabilità presenti su un determinato host prima che vengano sfruttate
3) Un SIEM (Security Incident Events Management) permette di gestire in maniera automatizzata le reazioni ad attacchi e incidenti

QUESTION 6

1) Un Protection Profile dei Common Criteria definisce la procedura di valutazione per security target specifici (es. metodologia di valutazione per smart card, sistemi operativi)
2) ITSEC non supporta la ri-valutazione di un precedente processo di standardizzazione
3) La strenght of mechanism dichiarata permette di distinguere i prodotti sicuri da quelli che lo sono meno

QUESTION 7

1) L'uso della porta 443 per erogare un servizio web implica che la connessione è protetta con TLS →per convenzione ci si aspetta di trovare TLS su quella porta, ma non è detto
2) Se il client presenta un session-id valido, il server deve accettare di eseguire l'Handshake ridotto, computazionalmente molto più leggero e con meno scambi di pacchetti e idoneo a client con poca capacità computazionale (IoT) → il server non "deve" necessariamente accettare l'handshake ridotto. Inoltre, l'Handshake ridotto serve a ridurre il carico sul server, non sul client.
3) Nel caso venga scelta la ciphersuite TLS_DHE_RSA_WITH_AES_128_CBC_SHA, l'uso di algoritmi effimeri impone che SHA1 sia usato solo per generare la Master Secret (e successivamente le 4 chiavi usate per proteggere il canale) → Siccome c'è CBC, SHA serve anche per fare l'HMAC, quindi la risposta è falsa
4) SSH usa certificati X.509 semplificati per trasmettere la chiave del server

QUESTION 8

1) SHA3 è l'algoritmo scelto dopo che SHA-2 è stato deprecato dal NIST
2) Il protocollo ESP di IPsec v2 è un esempio concreto di Authenticated Encryption with Associated Data.
3) in RSA, può essere scelto qualunque esponente pubblico 'e', senza alcun effetto negativo né dal punto di vista della sicurezza né dal punto di vista computazionale
4) con l'On-line Certificate Status Protocol posso chiedere ad un server creato appositamente (es. disponibile via internet) se un determinato certificato, identificato dal suo serial number, è valido in un preciso momento del presento o passato
5) l'uso di Key Derivation Function è tipicamente sconsigliato perché sono funzioni lente ed inefficienti

nella gestione della memoria.

ESAME GENNAIO 2024
DOMANDE APERTE:

Domanda 6

Spiegare come funziona il metodo di autenticazione TOTP, indicando esplicitamente quali dati vengono usati dai client. Quali vengono inviati e quali verifiche vengono svolte dai server.
Indicare i principali tipi di attacco che si possono eseguire lato client, server e nel canale di comunicazione.

Nel modello NIST SP8000-63B, come dovrebbero essere definiti il ruolo del client e server durante l'autenticazione?

Domanda 7

Spiegare cosa è l'algoritmo RSA, quali sono i parametri pubblici e privati, quale è il problema matematico su cui si fonda la sua sicurezza.

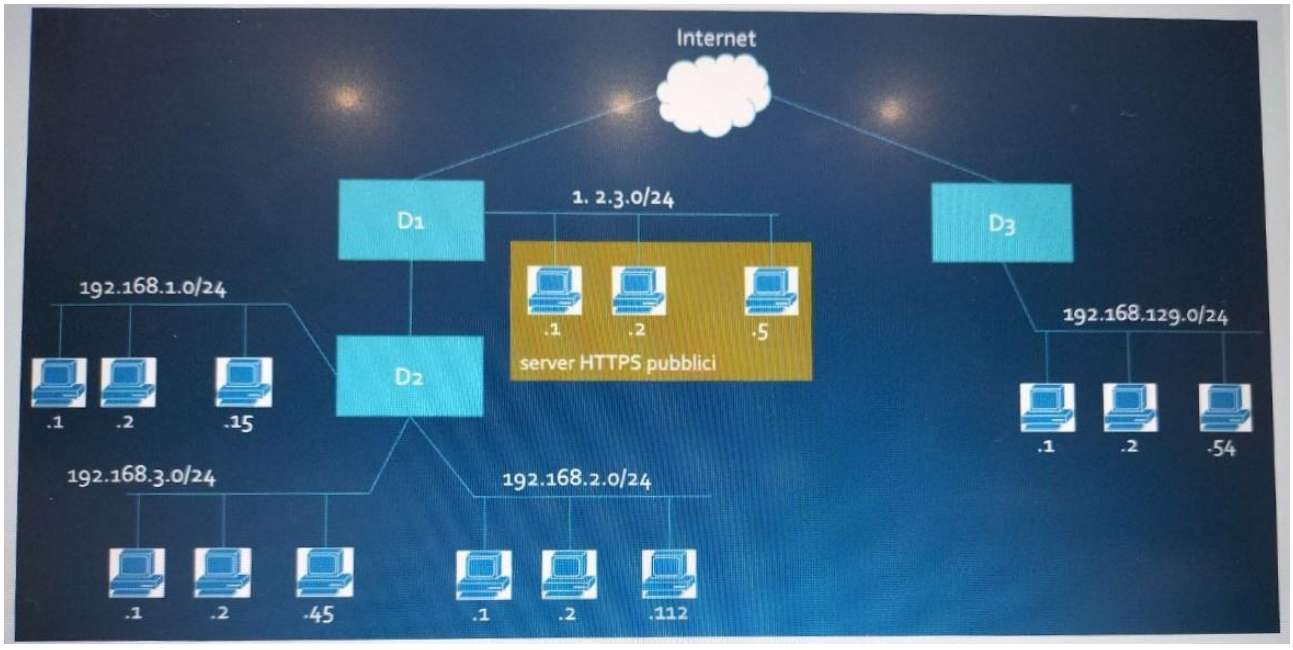
Indicare delle ottimizzazioni computazionali e discutere alcune debolezze note.

Indicare quale è il numero di bit di una chiave RSA che possa essere considerato sicuro nel 2024.

Infine, spiegare in quali fasi del TLS e di IPsec/IKE può essere usato e a quale fine

Domanda 8

Data l'architettura di rete in figura:



Ed i seguenti requisiti:

1. **Nessuna restrizione interna alle sottoreti**

2. **Nessuna rete interna (.1 / .2 / .3 /.129) deve essere raggiungibile dall'esterno**
3. **Gli host della sottorete .1 devono essere raggiungibili dalle sottoreti .2 e .3**
4. **Gli host della sottorete .2 devono essere raggiungibili dalle sottoreti .1 e .3**
5. **Gli host della sottorete .3 devono essere raggiungibili dalla sola sottorete .2**
6. **Tutti gli host interni delle sottoreti .1 .2 .3 .129 possono raggiungere internet solo dopo essersi autenticati**
7. **I server pubblici devono essere raggiungibili da Internet solo su URL fisse note a priori**
8. **Il payload dei pacchetti http che arrivano ai server HTTPs devono essere ispezionati perché non contengano tipi di file potenzialmente pericolosi**
9. **I server pubblici devono essere protetti da attacchi standard**
10. **La sottorete .2 deve comunicare in maniera sicura con la sottorete .129, il traffico deve restare confidenziale rispetto agli utenti esterni**

Indicare quali funzioni di sicurezza si dovrebbero abilitare nei dispositivi D1, D2, D3 per implementare correttamente tutti i requisiti. Notare che non è obbligatorio scegliere almeno una funzione per ognuno dei dispositivi e che in ogni dispositivo possono essere usate più funzioni.

Ogni decisione deve essere motivata e per ogni dispositivo devono essere associati i requisiti che permette di soddisfare.

Infine, scrivere le regole per implementare i requisiti 3) 4) e 5) in uno pseudo linguaggio di configurazione a scelta indicando esplicitamente la politica di default.

Questa è la riposta che ho dato all'esame e mi ha messo 6/6

Dispositivo D1
(replicare lo schema funzione+motivazione+requisiti per ogni funzione che si intende usare per tutti e tre i dispositivi)
funzione: Applicazion level Gateway a tre gambe (server pubblici in DMZ) + WAF sui server + Application level filter
motivazione: serve la DMZ come rete cuscinetto per proteggere la rete interna da eventuali attacchi ai server. Il WAF serve per ispezionare i pacchetti HTTP che arrivano ai server e il filtro per proteggere i server da attacchi standard (serve l'application layer perchè deve lavorare con gli URL dei server).
requisiti soddisfatti: 7 8 9
Dispositivo D2
funzione: Gateway per l'autenticazione + filtro statefull
motivazione: il filtro lo mettiamo per mettere le regole di comunicazione tra le 3 sottoreti (.1, .2, .3) e per verificare che esse non siano raggiungibili da internet. il gateway invece lo mettiamo per fare l'autenticazione delle sottoreti e anche per poter creare una VPN con la sottorete .129 (Basic Vpn con ESP in tunnel mode per autenticazione, integrità e confidenzialità. VPN gateway to gateway per proteggere i dati dagli utenti esterni all'azienda mentre viaggiano su internet)
requisiti soddisfatti: 2 6 10
Dispositivo D3
funzione: Gateway per l'autenticazione + filtro statefull
motivazione: come per D2 mettiamo il gateway per creare la VPN tra la sottorete .2 e la

.129 e per autenticare per raggiungere internet. il filtro invece per permettere che essa non sia raggiungibile da internet
requisiti soddisfatti: 2 6 10
Configurazione
Policy di default: white list
Regole:
requisito 3
FROM IP 192.168.2.0/24 TO IP 192.168.1.0/24 ALLOW
FROM IP 192.168.3.0/24 TO IP 192.168.2.0/24 ALLOW
requisito 4
FROM 192.168.1.0/24 TO IP 192.168.2.0/24 ALLOW
FROM 192.168.3.0/24 TO IP 192.168.2.0/24 ALLOW
requisito 5
FROM 192.168.2.0/24 TO IP 192.168.3.0/24 ALLOW

ESAME FEBBRAIO 2024
DOMANDE APERTE:

Domanda 1

Spiegare cosa sono i Common Criteria e a cosa servono. Descrivere quali sono le caratteristiche che ereditano dai precedenti standard e le peculiarità che lo rendono più flessibile e funzionale. Infine, discutere in base a cosa si deve svolgere la valutazione e quali sono gli attori in questo processo.

[iniziativa UE per standard che armonizzino i precedenti criteri (USA, EU, Canada), criteri per la valutazione di prodotti di sicurezza, servono per certificare sicurezza, evitare di dover fare assessment locali per valutare il livello di sicurezza di TOE, apertura mercati, ...]
[precedenti: valutazione generici TOE, valutazione a livelli (classi di funzionalità), rivalutazione/upgrade (volendo anche aspetti del CEM: valutazione efficacia dichiarata, valutazione correttezza)
peculiarità: Protection Profile, componenti elementari di correttezza (in classi, estensibili)]
[CEM (+azioni valutatore), Evaluation Scheme Nazionale (OSCI)]

Domanda 2

Spiegare cosa è una DMZ e in che modo può essere creata. Discutere delle implicazioni di sicurezza che portano alla scelta dell'uso di una DMZ spiegando perché la DMZ è una valida soluzione. Supponendo che il traffico da filtrare sia quello diretto verso la seguente URL:

`https://webservice.company.com/showpage.php?cmid=1293`

Commentate quali controlli potrei usare per filtrare tale traffico e fino a che punto possono essere precisi in base al livello nello stack ISO/OSI a cui operano (livello 3/4, livello applicativo, ispezione payload applicativo).

[includere almeno: sottorete a livello di sicurezza intermedio creato mediante un'architettura screened subnet normale o a tre gambe]

[includere almeno: necessità di esporre servizi ad altre reti a livello più basso e allo stesso necessità di proteggere la porzione a livello di sicurezza più alto, valida perché in caso di attacco ai servizi in DMZ la propagazione alla rete interna non è automatica ma richiede superamento di altri filtri]

[livello 3/4: faccio controlli poco precisi, può servire se IP assegnato staticamente alla URL, filtro su porta https=443

livello 7: posso filtrare su tutte le parti della URL, probabilmente non posso fare molto di più perché il traffico è cifrato a livello trasporto da TLS (ad essere precisi ma non richiesto per questo esame, posso anche filtrare in base alla parte in chiaro dell'handshake protocol)

payload: non posso fare niente perché tutto è protetto con TLS

spiegare come funziona in generale in packet filter, l7 filter, WAF, etc. non dava il massimo dei punti]

Domanda 3

Spiegare la differenza tra protezione di canale e protezione di messaggio, indicando in quali contesti è necessario utilizzare l'una o l'altra. Indicare e spiegare il funzionamento di un protocollo che implementi protezione di canale e uno che implementi protezione di messaggio. Per ognuno di essi elencare le proprietà di sicurezza che garantisce e in che modo queste vengono garantite.

[canale = endpoint fidati, protezione da MITM
messaggio= mi fido solo dell'originator, protezione aggiunta al messaggio
canale = protocolli interattivi
messaggio = store&forward]
[*canale: TLS, SSH, IPsec
es. TLS
- spiegare come funziona almeno handshake protocol per scambio di ciphersuite, segreti, autenticazione peer
- autenticazione server obbligatori, client opzionale con CRA asimmetrico con credenziali su certificati X.509
autenticazione dati e integrità: MAC o TAG di AE
confidenzialità opzionale: crittografia simmetrica, con scambio di chiavi durante handshake con DH/RSA
anti-replay: pacchetti TLS numerati
messaggio: S/MIME, DNSSEC

es. S/MIME
spiegare almeno messaggio inbustato in strutture CMS inviate come normali allegati MIME
- autenticazione originator + authc messagio e integrità: firma digitale in strutture SignedData + certificati
- confidenzialità: crittografia simmetrica in strutture Enveloped Data]

ESAME ESTIVO 2024
DOMANDE APERTE:

Domanda 1
Spiegare cosa sono il phishing (e alcune delle sue varianti) e il pretexting, indicare quali debolezze sfruttano e tramite quali canali raggiungono le vittime.
indicare un attacco famoso che ha sfruttato anche debolezze riconducibili agli esseri umani e spiegare quale debolezza ha sfruttato.

Domanda 2
Spiegare cosa sono i CRA asimmetrici, a cosa servono e come funzionano.
Fare un confronto con le TOTP indicando esplicitamente dove i CRA asimmetrici sono migliori e peggiori delle OTP

Domanda 3
Un'azienda dotata della sua rete privata aziendale vuole esporre all'esterno due servizi (HTML e posta elettronica) da due server aziendali (fisici, di proprietà dell'azienda, collocati nella rete aziendale).

Approfittando delle modifiche, hanno deciso di dividere la rete aziendale in due parti a diversi livelli di sicurezza. La parte rete della rete aziendale a livello di sicurezza più basso potrà accedere direttamente ad internet, la parte a livello di sicurezza più elevato è separata da internet dalla rete a livello di sicurezza più basso.

Progettate una soluzione che permetta di implementare una politica di autorizzazione di rete che consenta di:
- dividere la rete nei due livelli di sicurezza,
- rendere raggiungibili da internet i due servizi esposti dai server aziendali.

Indicate quali architetture e quali security control usare e come questi dovrebbero essere collegati alle varie reti e ai due server.

ESAME SETTEMBRE 2024

Solo domande:

Spiegare cosa si intende quando si parla di protezione di canale e in quali contesti viene utilizzato.

Indicare e spiegare in dettaglio il funzionamento del TLS indicando quali proprietà di sicurezza garantisce e quali tecniche vengono usate per garantirle.

Protezione di canale:

TLS:

Proprietà e modo per garantirla:

Spiegare cosa è il Risk Management Framework del NIST e quali sono gli obiettivi di tale framework.

Elencare e descrivere le fasi e alcune delle operazioni potrebbero essere svolte in ognuna di esse.

RMF: descrizione e obiettivi :

Fasi e relativa descrizione:

Spiegare cosa sono i Common Criteria e a cosa servono. All'interno di questo contesto, spiegare cosa sono i Protection Profile e perché sono utili.

Infine discutere cosa è il CEM e come si integra con i Common Criteria.

Common Criteria:

Protection Profile:

CEM:

CROCETTE:

a. se viene effettuato un port scanning contro un server posso identificare tutte le porte aperte, quelle chiuse e quelle filtrate

b. l'attacco di Kaminski permette di forgiare richieste DNS false ma può essere evitato con DNSSEC

c. dato un keyed-digest calcolato come kd = H(k || M), è possibile ottenere la chiave K a partire da kd e da M indipendentemente da H perché esiste il length extension attack

d. lo Smurfing attack può essere evitato cifrando i pacchetti in uscita dalla rete

e. il FIN scanning permette di riconoscere i packet filter stateful da quelli stateless

f. un SYN interceptor evita che le tabelle delle connessioni dei server che scherma si saturino con attacchi di flooding

g. ettercap avvelena la cache del protocollo ARP per lanciare attacchi di tipo MitM

h. il padding calcolato con Optimal Asymmetric Encryption Padding (RSA-OAEP) evita gli attacchi contro le firme digitali calcolate con RSA

i. l'attacco Heartbleed permette di ottenere le chiavi private del server TLS attaccato

---

a. Il DPO è un soggetto indipendente che deve garantire la corretta applicazione della normativa in materia di privacy

b. Il principio della Full Functionality del GDPR richiede siano abilitati di default i controlli al massimo livello di sicurezza

c. Il GDPR introduce il concetto di minimizzazione, che indica che i dati devono essere collezionati usando il minimo numero di strumenti e resi accessibili al minor numero di operatori

d. Un data breach è un incidente informatico che porta alla distruzione, alterazione, diffusione non autorizzata o accesso ai dati personali

e. I dati relativi allo stato di salute e la razza sono considerati di categoria speciale e potrebbero richiedere protezioni aggiuntive

f. Nel GDPR, il principio della privacy by design indica che i dati devono essere protetti preventivamente e obbligatoriamente

g. In un'azienda, chiunque abbia accesso a dati relativi alla privacy devono essere noti e autorizzati dal Titolare del trattamento (es. direttamente o tramite i responsabili)

h. Il DPO è come responsabile dei dati di un'azienda, risponde dei danni in caso di data breach

i. I servizi che usano dati personali devono essere pensati per proteggere questi dati durante tutte le fasi di comunicazione (in transit) ma non è responsabilità del titolare proteggerli quando i dati sono memorizzati (at rest)

---

a. Un dispositivo di firma sicuro in grado di memorizzare in maniera tamper-proof le chiavi crittografiche (segrete) può essere usato per generare delle Qualified Signature

b. Un documento è stato firmato con quattro firme sequenziali. Se rimuovo le ultime due firme apposte, la verifica delle prime due non fallisce

c. Per verificare con successo una Qualified Electronic Signature, la chiave pubblica deve provenire da un Qualified Certificate

d. Un documento firmato con Advanced Electronic Signature può essere usato in tribunale

e. Se un documento è firmato da più persone usando firme parallele, ogni firma dipende da quelle di tutti gli altri

f. Il Time Stamp generato da una Time Stamp Authority (TSA) è la firma digitale applicata ad una valore ricevuto da un'entità esterna (es. digest) concatenato ad un valore temporale calcolato dalla TSA stessa

g. Un Qualified Certificate può essere usato per rappresentare l'identità digitale di un server ed è necessario per la generazione di Advanced Digital Signature

h. Le detached signature sono sconsigliate perché, essendo formata da due parti separate, è più semplice forgiare firme valide senza conoscere i segreti crittografici

i. PKCS#7 e CMS definiscono un formato di firma digitale di tipo enveloping

---

a. Le curve ellittiche servono a implementare algoritmi a chiave pubblica più efficienti di quelli tradizionali (campi finiti) a parità di livello di sicurezza raggiunto

b. con le CRL posso chiedere ad un server creato appositamente (es. disponibile via Internet) se un determinato certificato, identificato dal suo serial number, è valido in un preciso momento del presente o passato

c. la firma digitale di un documento è il risultato di un'operazione che coinvolge l'uso di un parametro asimmetrico segreto e del digest del documento stesso

d. l'uso di esponenti RSA pubblici come 3 e 17 rendono possibile la fattorizzazione del modulo n

e. se il server OCSP mi conferma che il certificato è valido, posso considerare validi anche documenti firmati mesi prima (sempre che tutte le altre verifiche crittografiche siano corrette nel periodo di validità del certificato)

f. SHA-2 è stato deprecato dal NIST perché esistono attacchi che ne riducono la forza sotto agli 80 bit

g. se uso il protocollo ESP di IPsec v2, posso autenticare l'header del TCP

h. l'uso delle Key Derivation Function è limitato nella pratica perché non sono abbastanza efficienti sia a livello di computazione che di uso della memoria

---

Scegli le risposte affermative:

a. gli IPS sono stati progettati per velocizzare ed automatizzare la risposta alle intrusioni o anomalie rilevate

b. un HIDS può verificare le intrusioni in uno specifico server, ad esempio monitorando che alcuni file non vengano modificati e analizzando i log dei sistemi operativi ed altri servizi attivi

c. un NIDS è uno scanner di rete che identifica le porte aperte sui sistemi e ne riconosce le vulnerabilità note

d. le politiche di risposta agli incidenti devono anche cercare di limitare gli errori umani, es. spiegando a tutto il personale come minimizzare i rischi associati al phishing (awareness)

e. un Security information and event management (SIEM) è un particolare tipo di IPS che si integra con i firewall per reagire agli eventi di sicurezza

f. per prevenire o anticipare le intrusioni, i componenti di un IDS dovrebbero monitorare i comportamenti anomali esclusivamente all'interno del mio sistema informativo

g. un SOC dovrebbe aggregare tutto il personale che si occupa di prevenire e monitorare gli attacchi contro i sistemi informativi dell'azienda ma anche rispondere agli incidenti rilevati

h. gli honey pot possono servire a sviare gli attaccanti dai veri asset aziendali

i. il vulnerability management e patch management, se applicati correttamente e adottati a livello aziendale, sono utili a prevenire gli incidenti informatici