

2013-07-08

1. La certificazione ISO 27001 e' rilasciata in Italia da:

- ☐ OWASP
- ☐ un Organismo di Certificazione Accreditato da OWASP
- ☐ Accredia
- ☒ un Organismo di Certificazione Accreditato da Accredia
- ☐ una Autorità di Certificazione abilitata dall'Agenzia per l'Italia Digitale

2. In IPSEC vengono cifrate le seguenti informazioni:

- ☒ **forse** header di livello 2
- ☐ MAC address
- ☐ trailer di livello 2
- ☐ porta TCP
- ☐ CRC Ethernet

3. Calcolo efficiente di $a^b \bmod q$ mediante il metodo iterativo $b = b_k \dots b_2 b_1 b_0$

```
for (i = k; i >= 0; i--) {  
    d = d*d % q;  
    if (b[i] == 1)  
        d = (d*d) % q;  
}  
return d;
```

4. Definire la resistenza alle collisioni per le funzioni di hash, e discuterne le conseguenze per la sicurezza della firma elettronica

Una funzione **hash** resistente alle collisioni quando è difficile trovare una coppia di messaggi $\langle m1, m2 \rangle$ tali che la funzione *hash* applicata su di essi dia un codice hash uguale, ovvero difficile che $H(m1) = H(m2)$. Questo, nella firma elettronica che è usata per firmare i messaggi, implica che un messaggio firmato è autentico, quindi vuol dire che non è stato manomesso e il messaggio ricevuto dal destinatario è identico a quello spedito dal mittente.

5. Descrivere il NAT, il NATP, e le loro implicazioni per la sicurezza

Il NAT (Network Address Translation) è un meccanismo di mascheramento del router che traduce un indirizzo interno della rete (LAN) in un indirizzo IP pubblico. Ha un rapporto di 1 : 1 Il NATP (Network Address & Port Translation), invece, permette di avere un unico indirizzo IP verso la rete esterna (quello del router) ma molti più indirizzi nella rete interna traducendo anche le porte. Diverse porte corrispondono a diversi host nella rete interna. Rapporto di 1 : *molti*. Questo impedisce a chi è esterno alla rete di conoscere gli indirizzi IP interni.

6. Descrivere l'attacco di tipo DOS noto come "syn flooding"

L'attacco DOS (Denial Of Service) è un attacco che ha lo scopo di mettere fuori uso un server (in genere). Il Syn Flooding è un attacco coordinato e sincronizzato che dà inizio connessioni TCP (da parte dei calcolatori controllati) a ripetizione verso il calcolatore vittima senza completare l'handshake (possibile con indirizzo IP spoofed, visto che la connessione viene solo iniziata). Questo fa sì che il calcolatore vittima non riesca più a gestire nuove richieste di connessione.

2013-09-02

1. La certificazione ISO 27001 riguarda:

- ☒ un information security management system
- ☐ la sicurezza perimetrale e in particolare i firewall
- ☐ l'autenticazione mediante certificati di chiave pubblica
- ☐ i certificati rilasciati da una certification authority accreditata
- ☐ la firma grafometrica

2. Un Proxy HTTP non trasparente:

- ☐ svolge tutte le funzioni richieste ad un Firewall
- ☐ svolge le stesse funzioni di un NAT
- ☐ svolge le stesse funzioni di un NAT
- ☒ sostiene 2 connessioni TCP, una aperta dal client e una aperta verso il server
- ☐ inoltra al server HTTP la richiesta del client, con lo stesso indirizzo IP sorgente

3. Test di primalità di Miller-Rabin

4. Dimostrare che, se M è primo e $x^2 \bmod M = 1$, allora $x = 1$ oppure $x = M - 1$

5. Perché su un packet filter vengono normalmente filtrati i pacchetti IP con l'opzione di source routing? Vengono normalmente filtrati i pacchetti con questa opzione perché è possibile l'*ip spoofing* con TCP su WAN. Un Hacker può impiegare il routing dell'IP di origine per specificare un percorso diretto verso una destinazione e un percorso di ritorno verso l'origine (source routing). In questo modo l'hacker può intercettare o modificare le trasmissioni.

1. L'hacker cambia il proprio indirizzo IP in modo da farlo corrispondere all'indirizzo IP del client valido, in questo caso si parla di indirizzo spoofato.
2. L'hacker poi costruisce un percorso che conduce al server, ovvero il percorso diretto che i pacchetti dovranno prendere per giungere al server e per tornare all'host dell'hacker, utilizzando l'indirizzo del client valido come ultimo tratto del percorso per giungere al server.
3. L'hacker utilizza il percorso di origine per inviare al server una richiesta del client.
4. Il server accetta la richiesta dell'hacker come se questa provenisse dal client valido e poi restituisce la risposta all'host dell'hacker.
5. Ogni risposta alle richieste da parte del client valido viene inviata

all'host dell'hacker.

6. **Fare un esempio di Broken Authentication o Session Management (OWASP)**

1. Le credenziali di accesso di un utente sono salvate in chiaro
2. Il session ID è visibile nell'URL
3. Password, Session ID, e altre credenziali vengono inviate tramite un canale non cifrato.

2013-09-18

1. **Un MAC (message authentication code)**

- ☐ Autentica un utente
- ☒ Autentica un messaggio con una chiave simmetrica
- ☐ Autentica un messaggio con una chiave asimmetrica
- ☐ Autentica un messaggio mediante un protocollo di challenge-response
- ☐ Rende un messaggio non riconoscibile

2. **Il cosiddetto ARP poisoning:**

- ☐ distribuisce un virus su rete locale
- ☐ distribuisce un virus su rete geografica
- ☐ provoca una errata associazione tra indirizzi DNS e indirizzi IP
- ☒ provoca una errata associazione tra indirizzi MAC e indirizzi IP
- ☐ provoca una errata associazione tra URL http e indirizzi IP

3. **Definizione di radice primitiva di un numero q e metodo per generarne una**

2. Generazione:

1. Generare $\alpha < q$ a caso, tale che α sia relativamente primo con q
2. fattorizzare $q - 1$ ($f_1 \times f_2 \times \dots \times f_j = q - 1$)
3. **se** esiste f tale che $\alpha^{(q-1)/f} \bmod q = 1$
 - allora **torna al passo 1**
 - altrimenti **restituisce** α

4. **Dimostrare che $(ab) \bmod M = (a \bmod M)(b \bmod M) \bmod M$**

Siano

- $a \bmod M = x$ con $x < M$
- $b \bmod M = y$ con $y < M$

Allora $(\exists k, j)$ tale che:

- $Mk + x = a$
- $Mj + y = b$

Pertanto:

$(ab) \bmod M = ((Mk + x)(Mj + y)) \bmod M = (MkMj + Mky + Mjx + xy) \bmod M = xy \bmod M = (a \bmod M)(b \bmod M) \bmod M$ rimane xy perché gli altri sono tutti multipli di M

5. **Disegnare una topologia di rete locale con firewall in HA (high availability) ESTERNO - ROUTER - SWITCH - (FIREWALL - FIREWALL) - SWITCH - (HOST1, HOST2, HOST3, ...)**

6. **Differenza tra modalità tunnel e transport in una VPN** In **Transport mode** la cifratura e l'autenticazione avviene su **computer** mittente e destinatario:

- Protegge da Sniffing/Spoofing su rete locale
- Rende visibili su internet indirizzi mittente e destinatario
- Richiede speciale configurazione del computer utente (non trasparente)
- Necessario per traffico da postazione mobile

In **Tunnel mode** la cifratura e l'autenticazione su **firewall** o **router**

- **Non protegge** da Sniffing/Spoofing su rete locale
- Nasconde gli indirizzi dei singoli computer (mittente e destinatario) ma non gli indirizzi della rete mittente e destinataria
- È trasparente all'utente singolo
- Veloce, prodotti affidabili per router/firewall

2014-06-23

1. **Descrivere l'attacco DOS basato su ICMP, noto come “smurf attack”** E' un tipo di attacco ICMP echo request (in gran numero) dove B (un reflector) è un broadcast di rete o sottorete. Il mittente ha indirizzo IP *spoofed* uguale all'indirizzo della vittima A, che si trova sulla stessa rete o sottorete.
2. **Un certificato di chiave pubblica serve per:**
 - ☐ garantire la sicurezza di un firewall
 - ☐ certificare che un firewall usa correttamente le firme elettroniche
 - ☐ garantire con una chiave pubblica le ACL di un firewall
 - ☒ associare in modo certo un soggetto ad una chiave pubblica
 - ☐ associare in modo certo una chiave pubblica a una chiave privata
3. **L'attacco noto come XSS (cross site scripting)**
 - ☐ permette di eseguire codice sul server attaccato
 - ☒ **FORSE** permette di eseguire codice sul browser della vittima
 - ☐ permette di eseguire codice sia sul browser della vittima che sul server attaccato
 - ☐ usa le credenziali attive sul browser per bloccare il funzionamento del server attaccato
 - ☐ usa le credenziali di accesso ad un sito per aprire una pagina protetta su un altro sito
4. **Nello standard ISO 27001, che cos'è lo “statement of applicability”**
5. **Dimostrare che, se $N = pq$ e p e q sono primi, allora $\Phi(N) = (p-1)(q-1)$, dove Φ (Phi) è la funzione di Eulero**
6. **Discutere l'interazione tra NAT e reti private virtuali**

2014-07-11

1. **Descrivere la metodologia di analisi dei rischi definita da OWASP**
2. **In IPSEC con AH il MAC autentica**
 - ☒ il solo payload
 - ☐ il payload e i campi variabili dell'intestazione IP
 - ☐ il payload e i campi fissi e variabili dell'intestazione IP
 - ☐ il payload e i campi fissi dell'intestazione IP
 - ☐ i soli campi variabili dell'intestazione IP
3. **Un cifrario a sostituzione monoalfabetica**
 - ☐ sostituisce ad ogni singola lettera del testo in chiaro un'altra lettera, in base ad una sostituzione che può cambiare più volte man mano che si procede nello scorrimento del testo stesso
 - ☐ sostituisce ad ogni coppia di lettere del testo in chiaro un'altra coppia di lettere, in base ad una sostituzione che può cambiare più volte man mano che si procede nello scorrimento del testo stesso
 - ☐ sostituisce ad una n-upla di lettere del testo in chiaro un'altra n-upla di lettere, in base ad una sostituzione che può cambiare una sola volta man mano che si procede nello scorrimento del testo stesso
 - ☐ sostituisce ad una n-upla di lettere del testo in chiaro un'altra n-upla di lettere, in base ad una sostituzione che può cambiare più volte man mano che si procede nello scorrimento del testo stesso
 - ☒ sostituisce ad una n-upla di lettere del testo in chiaro un'altra n-upla di lettere, in base ad una sostituzione che non può mai cambiare man mano che si procede nello scorrimento del testo stesso
4. **Definire che cos'è una funzione di hash resistente alle collisioni**
5. **Differenza tra un packet filter e un firewall applicativo**
 1. **Packet Filter:**
 - Filtra in base a:
 - Direzione del pacchetto
 - Direzione della connessione
 - Indirizzo IP (sorgente e destinazione)
 - Servizio (porta sorgente e destinazione)
 - Difficoltà con alcuni protocolli
 - Non mantiene log
 - Difficile monitorare attacchi mentre avvengono
 2. **Application Proxy**
 - Connessioni dirette tra interno ed esterno sono **proibite**
 - Possibili solo connessioni attraverso il firewall
 - Ogni servizio dev'essere configurato
 - Non trasparente
 - richiede host dedicato
 - Prestazioni medie
 - Sicuro
 - Mantiene log sofisticati

- E' in grado di riferire il traffico agli utenti
6. **Algoritmo per calcolare l'inverso moltiplicativo in aritmetica modulo n**

2015-06-25

1. **Descrivere il formato dello Authentication Header Ipsec (AH) e commentare il significato e l'utilizzo di ogni campo** Campi:
 - Next Header (8) - Identifica il protocollo superiore in IPv4 (next header in IPv6)
 - Length (8) - utile perché la lunghezza di Data varia a seconda dello SPI
 - Reserved (16)
 - SPI (32, Security Parameters Index) - Identifica un indice dell'algoritmo e delle chiavi crittografiche
 - Data ($N \times 32$) - codici di autenticazione (MAC - Message Authentication Code) riferiti a tutto il pacchetto, ma dove i campi variabili (TTL, checksum) sono uguali a 0
2. **La firma grafometrica**
 - ☐ è la scansione della firma autografa
 - ☒ comprende la scansione della firma autografa e altri dati biometrici cifrati
 - ☐ comprende la scansione della firma autografa e altri dati biometrici non cifrati
 - ☐ è l'encryption RSA, fatta con la chiave privata, del digest del documento da firmare
 - ☐ è il digest dell'encryption RSA, fatta con la chiave privata, del documento da firmare
3. **L'attacco noto come CSRF (cross site request forgery)**
 - ☐ permette di eseguire codice dannoso sul server web attaccato
 - ☐ permette di eseguire codice dannoso sul browser della vittima
 - ☐ permette di eseguire codice dannoso sia sul browser della vittima che sul server
 - ☒ usa le credenziali attive sul browser per eseguire delle operazioni non desiderate
 - ☐ intercetta i cookie presenti sul browser per utilizzarli successivamente come autenticazione
4. **Nello standard ISO 27001, che cosa sono i "controlli" e in base a quali criteri vengono selezionati?**
5. **Per quale motivo il one-time pad è più sicuro di un cifrario di Vernam con una chiave di lunghezza fissa?**
6. **Dimostrare le due seguenti proprietà:**
 1. $(ab) \bmod M = [(a \bmod M)(b \bmod M)] \bmod M$
 2. $(ab) \bmod M = (a \bmod M) b \bmod M$

2015-07-10

1. **Descrivere la funzione di hash SHA-1**
2. **Il metodo di scambio chiavi di Diffie-Hellman**
 - ☐ si basa su particolari attacchi di tipo man in the middle
 - ☒ si basa sulla difficoltà di calcolare il logaritmo discreto
 - ☐ si basa sulla difficoltà di fattorizzare rapidamente un grande numero primo
 - ☐ si basa sulla difficoltà di fattorizzare il prodotto di due grandi numeri primi
 - ☐ si basa sulla difficoltà di calcolare l'esponente modulare
3. **L'attacco noto come XSS (cross site scripting)**
 - ☐ permette di eseguire codice dannoso sul server web attaccato
 - ☐ permette di intercettare password memorizzate su un database
 - ☐ permette di eseguire codice dannoso sia sul browser della vittima che sul server
 - ☐ usa le credenziali attive sul browser per eseguire delle operazioni non desiderate
 - ☒ può ottenere cookie del browser e utilizzarli successivamente come autenticazione
4. **Descrivere la vulnerabilità OWASP nota come "insecure direct object reference"**
5. **Che cos'è una marca temporale (timestamp)?**
6. **Consideriamo il cifrario RSA con modulo $n = pq$, esponente privato d ed esponente pubblico e . Sia il messaggio da cifrare $m = iq < n$. Cifrando m otteniamo $c = m^e \bmod n$. Dimostrare che decifrando c otteniamo nuovamente m , ovvero che $c^d \bmod n = m$.**

2015-09-02

1. **Differenza tra disaster recovery e sistemi di backup**
2. **Il numero di moltiplicazioni necessario per cifrare o decifrare con RSA è**
 - ☐ lineare rispetto al modulo
 - ☐ lineare rispetto al numero di bit del modulo
 - ☐ esponenziale rispetto al modulo
 - ☐ esponenziale rispetto al numero di bit del modulo
 - ☐ esponenziale rispetto al numero di bit delle chiavi
3. **Un certificato di chiave pubblica**
 - ☐ contiene la chiave privata in chiaro di una Certification Authority
 - ☐ contiene la chiave privata cifrata di una Certification Authority
 - ☒ **forse** contiene una firma della Certification Authority
 - ☐ contiene il nome dell'organismo accreditato per la certificazione ISO 27001
 - ☐ contiene la chiave privata cifrata dell'organismo accreditato per la certificazione ISO 27001

4. Come funziona un firewall ridondato (anche detto “HA” – high availability)
5. Che tipo di cifrario implementa una macchina a rotori, e quali sono le sue debolezze?
6. Fare un esempio concreto di Cross-Site Scripting (XSS)

2016-06-16

1. **Descrivere il funzionamento di un attacco basato su “Buffer Overflow”**
2. **Secondo OWASP, il livello di rischio legato ad una vulnerabilità dipende da:**
 - ☒ facilità di sfruttarla e impatto del corrispondente attacco
 - ☐ facilità di enumerare le password dei corrispondenti utenti (brute force)
 - ☐ posizione della vulnerabilità nella OWASP top ten
 - ☐ numero di exploit di quella vulnerabilità / numero di exploit totali
 - ☐ si rimanda allo standard ISO 27001
3. **Una banconota elettronica / bitcoin**
 - ☐ contiene un numero seriale visibile a tutti, in modo da evitare la doppia spesa
 - ☐ ha un valore economico conosciuto da tutti, in modo da rendere possibile la spesa
 - ☐ contiene un numero seriale “blinded”, ovvero nascosto
 - ☐ contiene un valore economico “blinded”, ovvero nascosto
 - ☐ ha un valore economico, ma non ha un numero seriale
4. **Il concetto di “Business Continuity”**
5. **Dimostrare che, se $X|Y$ e $X|Z$, allora $X|(iY + jZ)$ per ogni intero i, j**
6. **Spiegare il funzionamento e lo scopo della “Anti-replay window” in una VPN con IPSEC**

2016-07-12

1. Descrivere il metodo di generazione delle chiavi del cifrario RSA, e discuterne la complessità computazionale
2. La protezione da memory corruption nota come “canarino”:
 - ☐ viene realizzata dal sistema operativo
 - ☐ viene realizzata dal layer IPC
 - ☒ viene realizzata dal compilatore
 - ☐ viene realizzata dal programmatore
 - ☐ non è realizzabile in pratica
3. Il NAPT (network address and port translation)
 - ☐ permette di avere un solo indirizzo interno, diverso dall'indirizzo pubblico esterno
 - ☐ permette di avere più indirizzi interni, purché identici agli indirizzi pubblici esterni
 - ☐ permette di avere più indirizzi interni, purché meno numerosi di quelli esterni

- ☒ permette di avere piu' indirizzi interni, anche con un solo indirizzo pubblico esterno
 - ☐ permette di avere un solo indirizzo interno, e piu' indirizzi pubblici esterni
4. Perché una funzione Hash(M) definita come *XOR* dei blocchi di M non è collision resistant
 5. Effetti della frammentazione IP sul comportamento di un firewall di tipo packet filter
 6. Si consideri questo programma C:

```
int main(int argc, char** argv) {  
    int cookie;  
    char buf[80];  
    gets(buf);  
    if (cookie == 0x41424344)  
        printf("you win!");  
}
```

Spiegare in concreto come eseguirlo, sfruttando la vulnerabilità della “gets” per forzare l’output “you win”

2016-09-02

1. Descrivere il metodo ricorsivo per il calcolo dell'esponente modulare e discuterne la complessità.

```
int expmod (int a, int b, int q) {
    if (b == 0)
        return 0;
    if (b % 2 == 0)
        return sq(expmod(a, b/2, q)) % q;
    else
        return sq(expmod(a, b-1, q)) % q;
}
```

2. La tecnica nota come ARP poisoning

- ☐ realizza un buffer overflow sul server ARP
- ☐ realizza un buffer overflow sul firewall
- ☐ invia una risposta ARP con indirizzi IP modificati
- ☒ invia una risposta ARP con indirizzi MAC modificati
- ☐ invia una risposta ARP causando un buffer overflow

3. Il Syn flooding

- ☐ è un attacco di buffer overflow
- ☒ è un attacco DOS che può essere utilmente abbinato ad IP spoofing
- ☐ è un attacco DOS, non abbinabile ad IP spoofing
- ☐ richiede una modifica del layer TCP del server
- ☐ permette di modificare i cookie di sessione

4. Dimostrare che esistono infiniti numeri primi e discuterne le conseguenze in crittologia (EUCLIDE)

- Supponiamo che p sia l'ultimo numero primo.
- Sia $q = 2 \times 3 \times 5 \times \dots \times p$ il prodotto dei numeri primi fino a p .
- Se $q + 1$ è primo, p non era l'ultimo.
- Se $q + 1$ non è primo, è divisibile per $r > p$ con r primo (in quanto non è divisibile per alcun primo fino a p).
- Di nuovo $r > p$ quindi p non è l'ultimo primo

Questo viene utilizzato nello scambio di chiavi **Diffie-Hellman** in cui si utilizza l'aritmetica modulo n che dev'essere primo. Un numero troppo piccolo rende lo scambio di chiavi poco sicuro e vulnerabile ad attacchi di forza bruta, quindi serve un numero sufficientemente grande da rendere un tale attacco computazionalmente impossibile.

5. Discutere il concetto di non disconoscibilità nella firma elettron-

ica. Il documento informatico munito di firma digitale o firma elettronica avanzata sembrerebbe in realtà non disconoscibile; Infatti per verificare la firma apposta su un foglio è necessario procedere ad un esame grafo-logico, nel caso di documento informatico sottoscritto con firma digitale basta verificare la corrispondenza della firma con la chiave pubblica del presunto sottoscrittore per accertarne la provenienza. Conseguentemente, il disconoscimento della firma digitale **sarebbe precluso**, perché con la corrispondenza tra la chiave pubblica e la chiave privata vengono accertate sia la **provenienza** del documento che **l'assenza di alterazioni** del medesimo. L'unica ipotesi di falsità materiale che può configurarsi (atteso che le alterazioni materiali del documento sono da escludere grazie alla funzione di hash), è che la firma sia apposta da **persona diversa dal legittimo proprietario** del dispositivo di firma. Di conseguenza, l'oggetto del disconoscimento non sarà relativo alla firma ma all'effettivo utilizzo della firma digitale da parte del titolare.

6. **Descrivere il concetto di DMZ, con una possibile topologia di rete, e spiegare perché è utile per la sicurezza di una rete locale.**
Una demilitarized zone (DMZ), è una sottorete isolata, fisica o logica, che contiene dei servizi informatici offerti da un'azienda, accessibili sia da reti esterne non protette (WAN), che da workstation interne alla stessa azienda (intranet) e il cui scopo è quello di far usufruire questi servizi nella maniera più sicura possibile, senza compromettere la sicurezza della rete aziendale. Questa zona si trova nell'ambito di una topologia di rete chiamata Screened Subnet.

2016-09-19

1. Descrivere un metodo per calcolare la radice primitiva a di un primo q , dimostrarne la correttezza
2. Una VPN (Virtual Private Network)
 - ☒ separa una LAN in reti virtuali che si comportano come se fossero fisicamente distinte
 - ☐ separa una LAN in due o più LAN con indirizzi IP distinti
 - ☐ separa una LAN in due o più reti virtuali attraverso un proxy
 - ☐ è realizzata a livello 2 della pila ISO/OSI
 - ☐ è realizzata a livello 3 della pila ISO/OSI
3. Una funzione di hash resistente alle collisioni
 - ☐ rende impossibili le collisioni
 - ☐ rende improbabili le collisioni
 - ☒ rende computazionalmente difficile la generazione di collisioni
 - ☐ dato un input produce un codice (hash code) che autentica l'input stesso
 - ☐ dato un input produce un codice (hash code) che cifra l'input stesso
4. Descrivere il cifrario di Vigenère
5. Discutere il concetto di IT Risk Management (gestione del rischio infor-

matico)

6. Descrivere il funzionamento del NAT (network address and port translation) e le sue conseguenze per la sicurezza di una rete

2017-06-12

1. Descrivere il concetto di DDOS (distributed denial of service)
2. Per effettuare un'analisi del rischio secondo la metodologia OWASP, si utilizza la formula:
 - ☐ Probabilità = $f(\text{gravità del rischio}, \text{vulnerabilità})$
 - ☒ Gravità del rischio = $f(\text{probabilità}, \text{impatto})$
 - ☐ Probabilità = $f(\text{agente della minaccia}, \text{impatto})$
 - ☐ Impatto = $f(\text{impatto tecnologico}, \text{probabilità})$
 - ☐ Gravità del rischio = $f(\text{impatto tecnologico}, \text{impatto di business})$
3. In una VPN "tunnel"
 - ☐ è tutto cifrato, tranne il MAC address
 - ☐ l'indirizzo IP del solo terminatore sorgente è cifrato
 - ☒ gli indirizzi IP di entrambi i terminatori sono cifrati
 - ☐ il reale indirizzo IP sorgente è cifrato
 - ☐ il reale indirizzo IP sorgente è in chiaro
4. Definire e illustrare graficamente il concetto di "Merkle Tree"
5. Spiegare il "bit s" nel controllo di accesso ai sistemi Unix, e perché può essere pericoloso in presenza di vulnerabilità di un eseguibile
6. Algoritmo iterativo per calcolare in modo efficiente l'esponente modulare e sua complessità

2017-07-14

1. **Descrivere il ciclo Plan-Do-Check-Act secondo lo standard ISO-27001**
2. **Nel contesto della "Blockchain":**
 - ☐ In ogni momento una sola blockchain è valida
 - ☐ In ogni momento sono valide più blockchain che condividono una sottocatena iniziale
 - ☐ La blockchain è resa valida dalla firma di una terza parte fidata
 - ☒ La blockchain è resa valida da un voto di maggioranza sulla rete peer to peer
 - ☐ La blockchain è resa valida da un MAC (message authentication code)
3. Un firewall con HA (High Availability):
 - ☐ È normalmente realizzato in una configurazione con load-balancing
 - ☐ È normalmente realizzato in una configurazione con DNS round-robin
 - ☒ È normalmente realizzato in una configurazione con fail-over
 - ☐ È un firewall application-aware
 - ☐ È un firewall di tipo packet-filter che evita la perdita di pacchetti
4. **Definire il metodo di scambio di chiavi di Diffie-Hellman**
5. **Discutere, nel metodo di scambio di chiavi di Diffie-Hellman come descritto nella domanda 4, la complessità computazionale di ciascun passo**
6. **Descrivere il protocollo ESP (encapsulating security payload) nelle reti private virtuali IPSEC**

2017-09-18

1. **Descrivere brevemente tre delle top ten vulnerabilities di una Web application secondo Owasp**
2. **Un virus polimorfo:**
 - ☐ Si comporta in modo diverso a seconda del sistema operativo vittima
 - ☐ Si comporta in modo diverso per applicazioni Web e per sistemi mobile
 - ☒ Cambia ad ogni sua “riproduzione”
 - ☐ Cambia ad ogni sua “esecuzione”
 - ☐ Cambia ad ogni scansione dell’antivirus
3. **Una VPN IPSEC:**
 - ☐ Cifra ma non può autenticare
 - ☐ Autentica ma non può cifrare
 - ☐ Si situa nella pila ISO-OSI sopra il livello link
 - ☒ **forse** Si situa nella pila ISO-OSI sopra il livello di rete
 - ☐ Si situa nella pila ISO-OSI sopra il livello di trasporto
4. **Discutere i limiti di un firewall di tipo packet filter**
5. **Spiegare perché il teorema della domanda 5 serve per il calcolo dell’inverso moltiplicativo in RSA**
6. **Dimostrare che dati due interi a e b , esistono altri due interi x e y , tali che $ax + by = MCD(a, b)$**