2013-07-08

1. La certificazione ISO 27001 e' rilasciata in Italia da:
    1. OWASP
    2. un Organismo di Certificazione Accreditato da OWASP
    3. Accredia
    4. un Organismo di Certificazione Accreditato da Accredia
    5. una Autorità di Certificazione abilitata dall'Agenzia per l'Italia Digitale
2. In IPSEC vengono cifrate le seguenti informazioni:
    1. header di livello 2
    2. MAC address
    3. trailer di livello 2
    4. porta TCP
    5. CRC Ethernet
3. Calcolo efficiente di $a^b \ mod \ q$ mediante il metodo iterativo
4. Definire la resistenza alle collisioni per le funzioni di hash, e discuterne le conseguenze per la sicurezza della firma elettronica
5. Descrivere il NAT, il NAPT, e le loro implicazioni per la sicurezza
6. Descrivere l'attacco di tipo DOS noto come "syn flooding"

2013-09-02

1. La certificazione ISO 27001 riguarda:
    1. un information security management system
    2. la sicurezza perimetralee in particolare i firewall
    3. l'autenticazione mediante certificati di chiave pubblica
    4. i certificati rilasciati da una certification authorityaccreditata
    5. la firma grafometrica
2. Un Proxy HTTP non trasparente:
    1. svolge tutte le funzioni richieste ad un Firewall
    2. svolge le stesse funzioni di un NAT
    3. svolge le stesse funzioni di un NAPT
    4. sostiene 2 connessioni TCP, una aperta dal client e una aperta verso il server
    5. 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 $x^2 \ mod \ M = 1$, 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?
6. Fare un esempio di Broken Authentication o Session Management (OWASP)

2013-09-18

1. Un MAC (message authentication code)
    1. Autentica un utente
    2. Autentica un messaggio con una chiave simmetrica
    3. Autentica un messaggio con una chiave asimmetrica
    4. Autentica un messaggio mediante un protocollo di challenge-response
    5. Rende un messaggio non disconoscibile
2. Il cosiddetto ARP poisoning:
    1. distribuisce un virus su rete locale
    2. distribuisce un virus su rete geografica
    3. provoca una errata associazione tra indirizzi DNS e indirizzi IP
    4. provoca una errata associazione tra indirizzi MAC e indirizzi IP
    5. provoca una errata associazione tra URL http e indirizzi IP
3. Definizione di radice primitiva di un numero q e metodo per generarne una
4. Dimostrare che $ab \ mod \ M = (a \ mod \ M)(b \ mod \ M) \ mod \ M$
5. Disegnare una topologia di rete locale con firewall in HA (high availability)
6. Differenza tra modalità tunnel e transport in una VPN

2014-06-23

1. Descrivere l'attacco DOS basato su ICMP, noto come 'smurf attack'
2. Un certificato di chiave pubblica serve per:
    1. garantire la sicurezza di un firewall
    2. certificare che un firewall usa correttamente le firme elettroniche
    3. garantire con una chiave pubblica le ACL di un firewall
    4. associare in modo certo un soggetto ad una chiave pubblica
    5. associare in modo certo una chiave pubblica a una chiave privata
3. L'attacco noto come XSS (cross site scripting)
    1. permette di eseguire codice sul server attaccato
    2. permette di eseguire codice sul browser della vittima
    3. permette di eseguire codice sia sul browser della vittima che sul server attaccato
    4. usa le credenziali attive sul browser per bloccare il funzionamento del server attaccato
    5. 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 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

    1. il solo payload
    2. il payload e i campi variabili dell'intestazioneIP
    3. il payload e i campi fissi e variabili dell'intestazione IP
    4. il payload e i campi fissi dell'intestazione IP
    5. i soli campi variabili dell'intestazione IPU
3. Un cifrario a sostituzione monoalfabetica
    1. 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
    2. 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
    3. 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
    4. 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
    5. 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
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
2. La firma grafometrica [ ] è la scansione della firma autografa [X] 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)
    1. permette di eseguire codice dannoso sul server web attaccato
    2. permette di eseguire codice dannoso sul browser della vittima
    3. permette di eseguire codice dannoso sia sul browser della vittima che sul server
    4. usa le credenziali attive sul browser per eseguire delle operazioni non desiderate
    5. 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. $(ab)\ mod\ M = [(a\ mod\ M)(b\ mod\ M)]\ mod\ M$
    2. $(ab)\ mod\ M = (a\ mod\ M)\ b\ mod\ M$

2015-07-10

1. Descrivere la funzione di hash SHA-1
2. Il metodo di scambio chiavi di Diffie-Hellman
    1. si basa su particolari attacchi di tipo man in the middle
    2. si basa sulla difficoltà di calcolare il logaritmo discreto
    3. si basa sulla difficoltà di fattorizzare rapidamente un grande numero primo
    4. si basa sulla difficoltà di fattorizzare il prodotto didue grandi numeri primi
    5. si basa sulla difficoltà di calcolare l'esponente modulare
3. L'attacco noto come XSS (cross site scripting)
    1. permette di eseguire codice dannoso sul server web attaccato
    2. permette di intercettare password memorizzate su un database
    3. permette di eseguire codice dannoso sia sul browser della vittima che sul server
    4. usa le credenziali attive sul browser per eseguire delle operazioni non desiderate
    5. 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 $c = m^e\ mod\ n$. Dimostrare che decifrando c otteniamo nuovamente m, ovvero che $c^d\ mod\ n = m$.

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
    1. lineare rispetto al modulo
    2. lineare rispetto al numero di bit del modulo
    3. esponenzialerispetto al modulo
    4. esponenziale rispetto al numero di bit del modulo
    5. esponenziale rispetto al numero di bit delle chiavi
3. Un certificato di chiave pubblica
    1. contiene la chiave privata in chiaro di una Certification Authority
    2. contiene la chiave privata cifrata di una Certification Authority

    3. contiene una firma della Certification Authority
    4. contiene il nome dell'organismo accreditato per la certificazione ISO 27001
    5. 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:
    1. facilità di sfruttarla e impatto del corrispondente attacco
    2. facilità di enumerare le password dei corrispondenti utenti (brute force)
    3. posizione della vulnerabilità nella OWASP top ten
    4. numero di exploit di quella vulnerabilità / numero di exploit totali
    5. si rimanda allo standard ISO 27001
3. Una banconota elettronica / bitcoin
    1. contiene un numero seriale visibile a tutti, in modo da evitare la doppia spesa
    2. ha un valore economico conosciuto da tutti, in modo da rendere possibile la spesa
    3. contiene un numero seriale "blinded", ovvero nascosto
    4. contiene un valore economico "blinded", ovvero nascosto
    5. 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":
    1. viene realizzata dal sistema operativo
    2. viene realizzata dal layer IPC
    3. viene realizzata dal compilatore
    4. viene realizzata dal programmatore
    5. non è realizzabile in pratica

3. Il NAPT (network address and port translation)
    1. permette di avere un solo indirizzo interno, diverso dall'indirizzo pubblico esterno
    2. permette di avere più indirizzi interni, purché identici agli indirizzi pubblici esterni
    3. permette di avere piu' indirizzi interni, purche' meno numerosi di quelli esterni
    4. permette di avere piu' indirizzi interni, anche con un solo indirizzo pubblico esterno
    5. 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
2. La tecnica nota come ARP poisoning
    1. realizza un buffer overflow sul server ARP
    2. realizza un buffer overflow sul firewall
    3. invia una risposta ARP con indirizzi IP modificati
    4. invia una risposta ARP con indirizzi MAC modificati
    5. invia una risposta ARP causando un buffer overflow
3. Il Syn flooding
    1. è un attacco di buffer overflow
    2. è un attacco DOS che può essere utilmente abbinato ad IP spoofing
    3. è un attacco DOS, non abbinabile ad IP spoofing
    4. richiede una modifica del layer TCP del server
    5. permette di modificare i cookie di sessione

4. Dimostrare che esistono infiniti numeri primi e discuterne le conseguenze in crittologia
5. Discutere il concetto di non disconoscibilità nella firma elettronica
6. Descrivere il concetto di DMZ, con una possibile topologia di rete, e spiegare perché è utile per la sicurezza di una rete locale

2016-09-19

1. Descrivere un metodo percalcolare la radice primitiva a di un primo q, dimostrarne la correttezza
2. Una VPN (virtual private network)
    1. separa una LAN in reti virtuali che si comportano come se fossero fisicamente distinte
    2. separa una LAN in due o più LAN con indirizzamenti IP distinti
    3. separa una LAN in due o più reti virtuali attraverso un proxy
    4. è realizzata a livello 2 della pila ISO/OSI
    5. è realizzata a livello 3 della pila ISO/OSI
3. Una funzione di hash resistente alle collisioni
    1. rende impossibili le collisioni
    2. rende improbabili le collisioni
    3. rende computazionalmente difficile la generazione di collisioni
    4. dato un input produce un codice (hash code) che autentica l'input stesso
    5. 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 informatico)
6. Descrivere il funzionamento del NAPT (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:
    1. Probabilità = $f(gravità\ del\ rischio, vulnerabilità)$
    2. Gravità del rischio = $f(probabilità, impatto)$
    3. Probabilità = $f(agente\ della\ minaccia, impatto)$
    4. Impatto = $f(impatto\ tecnologico, probabilità)$
    5. Gravità del rischio = $f(impatto\ tecnologico, impatto\ di\ business)$
3. In una VPN "tunnel"
    1. è tutto cifrato, tranne il MAC address
    2. l'indirizzo IP del solo terminatore sorgente è cifrato
    3. gli indirizzi IP di entrambi i terminatori sono cifrati
    4. il reale indirizzo IP sorgente è cifrato
    5. 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”:
    1. In ogni momento una sola blockchain è valida
    2. In ogni momento sono valide più blockchain che condividono una sottocatena iniziale
    3. La blockchain è resa valida dalla firma di una terza parte fidata
    4. La blockchain è resa valida da un voto di maggioranza sulla rete peer to peer
    5. La blockchain è resa valida da un MAC (message authentication code)
3. Un firewall con HA (High Availability):
    1. È normalmente realizzato in una configurazione con load-balancing
    2. È normalmente realizzato in una configurazione con DNS round-robin
    3. È normalmente realizzato in una configurazione con fail-over
    4. È un firewall application-aware
    5. 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:
    1. Si comporta in modo diverso a seconda del sistema operativo vittima
    2. Si comporta in modo diverso per applicazioni Web e per sistemi mobile
    3. Cambia ad ogni sua “riproduzione”
    4. Cambia ad ogni sua “esecuzione”
    5. Cambia ad ogni scansione dell’antivirus
3. Una VPN IPSEC:
    1. Cifra ma non può autenticare
    2. Autentica ma non può cifrare
    3. Si situa nella pila ISO-OSI sopra il livello link
    4. Si situa nella pila ISO-OSI sopra il livello di rete
    5. 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 $ax + by = \ MCD(a, b)$