

Corso Specialista Sistemi Ambiente Web

Test conoscenze acquisite - 01.12.2003 (un punto per risposta)

Configurazione e Gestione server IIS

- 1 **E' possibile avere sul medesimo server differenti siti FTP?**
 - A Sì, adoperando identità distinte
 - B No, perchè non sarebbero identificabili univocamente nella rete IP
 - C Solo con il protocollo HTTP ver. 1.1

- 2 **Quante connessioni sono adoperate tra un client FTP ed il server?**
 - A Una, per trasmettere i dati ed i segnali di controllo (segnalamento in banda)
 - B Dipende se il client domanda il modo attivo o passivo
 - C

- 3 **Qual è il vantaggio della autenticazione anonima per un sito FTP?**
 - A I tempi di reazione sono piu' bassi
 - B L'autenticazione utente non ha senso perchè le restrizioni Windows non valgono per i siti FTP
 - C L'utenza/parola chiave non vengono trasmessi in "chiaro" sulla rete

- 4 **E' possibile avere sul medesimo server differenti siti WEB?**
 - A Sì, adoperando identità distinte
 - B No, perchè non sarebbero identificabili univocamente nella rete IP
 - C Solo se viene adoperato il protocollo HTTP ver. 1.1

- 5 **Adoperando i permessi di accesso web, puo' restringere l'accesso a singoli utenti o gruppi?**
 - A No
 - B Sì
 - C Sì, se si configura esplicitamente l'accesso per tali utenti

- 6 **Come procede per restringere l'accesso ad un sito web per utenti o gruppi?**
 - A Adopera le restrizioni di accesso web
 - B Adopera le restrizioni di accesso Windows (per NTFS)
 - C Non è possibile restringere l'accesso a livello server IIS

- 7 **La configurazione del protocollo SSL su un sito IIS presuppone...**
 - A la mappatura dei certificati dei clienti (browser)
 - B la sola configurazione della porta SSL (443)
 - C l'esistenza di un certificato pubblico per il sito

- 8 **L'uso dell'indirizzo IP permette di restringere l'accesso...**
 - A solo per siti web
 - B per siti web e FTP
 - C solo siti FTP

- 9 **L'home directory di un sito web ...**
 - A puo' essere locata solo nell'area di memoria del server
 - B puo' essere locata nell'area di memoria di altri server (cartella condivisa)
 - C non puo' essere locata nell'area di memoria di un controller di dominio

- 10 **Per quale motivo la carta di rete di un server IIS viene configurata con piu' indirizzi IP?**
 - A Per motivi di ridondanza (nel caso un indirizzo non funzioni)
 - B Per poter configurare diversi siti (virtual hosting)
 - C Per incrementare la stabilità del server

Corso Specialista Sistemi Ambiente Web

Test conoscenze acquisite - 01.12.2003 (un punto per risposta)

Risposte a scelta multipla con una sola risposta corretta per domanda (1 punto per risposta)

Gli aspetti di sicurezza

- 1 **Quando lei introduce il suo nome utente e parola chiave, che processo ha luogo?**
 - A Di autorizzazione per l'accesso ai files locali del PC
 - B Di autenticazione delle sue credenziali per l'accesso al PC
 - C Di autorizzazione per l'accesso ai files raggiungibili tramite connessioni di rete

- 2 **Nella maschera login del PC (nome utente / parola chiave), c'è un terzo campo. A che serve?**
 - A Il campo serve a distinguere il login locale da quello nel dominio
 - B Il campo serve solo all'Amministratore di sistema
 - C Il campo è facoltativo e non deve essere riempito

- 3 **Quale componente di rete suggerisce per ostacolare lo sniffing in una LAN?**
 - A Switch
 - B Hub
 - C Router

- 4 **In che modo viene settata la scheda di rete da uno sniffer?**
 - A Modo passivo
 - B Modo promiscuo
 - C Modo attivo

- 5 **Secondo lei, nella moderna crittografia il metodo viene tenuto riservato?**
 - A Sì, altrimenti i moderni computers potrebbero decriptare facilmente il testo cifato
 - B Sì, metodo e cifra devono essere riservati perchè legati tra loro
 - C No, al fine che la validità del metodo possa essere verificata dai crittoanalisti

- 6 **Qual è l'idea di base della crittografia a chiave segreta (simmetrica)?**
 - A Ogni partner possiede due chiavi, tra loro simmetriche
 - B I due partners conoscono la medesima chiave
 - C La chiave deve essere generata da un ente certificatore fidato

- 7 **DES è un metodo di crittografia a chiave simmetrica.**
 - A Falso
 - B Vero
 - C Vero, ma il metodo è oramai obsoleto (superato)

- 8 **Per quale motivo la cifratura simmetrica non è adatta in un contesto globale?**
 - A Recenti ricerche hanno mostrato come l'uso della chiave segreta sia poco sicuro
 - B Il numero delle chiavi cresce con legge quadratica al crescere dei partners
 - C Al crescere del numero dei partners diventa difficile trovare chiavi differenti

- 9 **Quale è la lunghezza della chiave nel metodo DES originario?**
 - A 64
 - B 1024
 - C 128

- 10 **Qual è l'idea di base della cifratura a chiave pubblica (asimmetrica)?**
 - A Esistono due chiavi (privata, pubblica) matematicamente legate tra loro
 - B La coppia di chiavi (pubblica, privata) viene generata da un ente pubblico
 - C La coppia di chiavi (pubblica, privata) è disponibile a tutti su server dedicati

Gli aspetti di sicurezza (continuazione)

- 11 **La chiave nei metodi di cifratura pubblica è piu' lunga che nei metodi a chiave segreta.**
A Questo spiega perchè la cifratura pubblica è piu' sicura
B Il paragone non ha senso perchè i metodi sono differenti
C Non è vero, la chiave è piu' corta
- 12 **Quale svantaggio presenta la cifratura pubblica rispetto a quella privata?**
A Lo scambio delle chiavi con i partners è piu' laborioso
B La chiave privata viene compromessa piu' facilmente della chiave segreta
C I tempi di cifratura sono piu' lunghi anche con i moderni calcolatori
- 13 **Perchè si usano i metodi di cifratura ibridi?**
A Uniscono i vantaggi della chiave pubblica e privata
B Non sono patentati e quindi gratuiti
C Sono i soli che funzionano nel contesto di Internet
- 14 **Come viene ottenuto un messaggio compresso?**
A Tramite la check-sum
B Tramite la funzione di hash
C Tramite la cifratura RSA
- 15 **Qual è la maggiore criticità della cifratura a chiave pubblica?**
A L'associazione della chiave pubblica al suo proprietario
B La generazione delle chiavi da parte dell'Ente certificatore
C La distribuzione delle chiavi tra i due partners
- 16 **Un certificato X.509 contiene...**
A La chiave privata del soggetto certificato
B La chiave pubblica del soggetto certificato
C La chiave di sessione del soggetto certificato
- 17 **Un certificato X.509 viene rilasciato solo dopo verifica dell'identità personale**
A Vero
B Dipende dal livello del certificato, a basso livello non c'è verifica
C Falso
- 18 **Per poter firmare digitalmente un email,**
A devo conoscere la chiave pubblica del destinatario
B devo conoscere la chiave privata del destinatario
C adopero la mia chiave privata e non devo conoscere le chiavi del destinatario
- 19 **Per poter cifrare un email,**
A devo conoscere la chiave pubblica del destinatario
B devo conoscere la chiave privata del destinatario
C adopero la mia chiave privata e non devo conoscere le chiavi del destinatario
- 20 **Il protocollo SSL...**
A viene adoperato solo per cifrare lo scambio dati browser / server (HTTP)
B opera a livello di trasporto e puo' assicurare anche altri traffici (es. POP3)
C opera a livello di rete ed è trasparente per tutte le applicazioni