Correzione quesiti di Sistemi e reti della simulazione del 3.3.2015

1) Descrivere sinteticamente le tecniche Nat e Pat

i processi di NAT (Network Area Translation) e PAT (Port Address Translation) permettono di connettere ad Internet decine di indirizzi privati di altrettanti dispositivi di rete utilizzando un unico indirizzo pubblico. In pratica il gateway, cioè il dispositivo di uscita su Internet (generalmente il router ADSL), quando riceve una richiesta di accesso ad Internet da un pc della rete locale invia un pacchetto di dati e gli assegna l'indirizzo IP pubblico (NAT) e un numero casuale di porta (PAT). Allo stesso tempo memorizza su una tabella di routing il numero IP privato e il numero di porta. Quando da Internet ritorna il pacchetto di risposta, il router, consultando i dati precedentemente memorizzati, è in grado di consegnare correttamente il pacchetto al computer che ne ha fatto richiesta.

2) Dopo aver spiegato che cosa è la crittografia, criptare il messaggio "Roma bella e grande" applicando il seguente algoritmo: sostituire ciascuna lettera (consonante o vocale) con il carattere di codice ASCII+2 se la posizione è pari (0,2,4 ecc) e con il carattere di codice ASCII-3 se la posizione è dispari(1,3,5 ecc)

La crittografia studia come trasformare un testo in modo che esso non possa essere comprensibile a persone non autorizzate a leggerlo. Il processo che trasforma l'informazione da comprensibile a incomprensibile è chiamato cifratura. Il processo che riconverte l'informazione da incomprensibile a comprensibile è detto decifratura. Per cifrare un messaggio si applica un algoritmo. In questo caso la stringa criptata è Tlo^ _gin^ b dt^pag come si evince dalla tabella.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
R	o	m	a		b	e	l	l	a		e		g	r	a	n	d	e
T	l	o	^		_	g	i	n	^		b		d	t	^	p	a	g

3) Descrivere i rischi e i pericoli per la sicurezza informatica e le principali misure di sicurezza

I rischi e i pericoli principali per la sicurezza dei sistemi informatici e dei dati in esso contenuti, sono i guasti dell'hardware, gli errori del software, gli errori umani, le cause accidentali ed imprevedibili, quali allagamenti, incendi e terremoti, ma soprattutto i malware (virus, worms, trojan ecc) e gli attacchi di hacher, cracker, troller ecc. La sicurezza informatica si attua riducendo i rischi a cui sistemi e dati sono esposti e limitando gli effetti causati dall'eventuale verificarsi di un'azione nociva. Le principali misure di sicurezza, fisica e logico-organizzativa, sono le seguenti:

- protezione fisica (gruppi di continuità, dischi raid, server fault tolerance, controllo degli accessi)
- credenziali di autenticazione (username e password)
- protezione logica (aggiornamento del software,firewal, antivirus, antispam, crittografia)
- backup e restore (disaster recovery)
- buone pratiche

Correzione quesiti di Sistemi e reti della simulazione del 30.4.2015

1) Chiarire il concetto di architettura client/server ed elencare i principali servizi di Intenet

ll termine "client-server" indica un'architettura di rete nella quale un computer client si connette ad un server per la fruizione di un servizio, quale ad esempio la condivisione di una risorsa hardware o software con altri client. In un'architettura client/server generalmente:

- Un server è solitamente in grado di gestire molti client
- Il client spesso deve autenticarsi, cioè eseguire il login, per poter accedere al server
- Il server si occupa di salvare in modo permanente le informazioni inviate dal client

La rete Internet è organizzata sotto forma di una tipica architettura client-server. I servizi disponibili sono tantissimi, i principali sono i seguenti:

1. World Wide Web (Web)
2. File Transfer Protocol (FTP)
3. E-Mail (Posta elettronica)

2) Che cos'è una web application e quali sono le tecnologie principali per realizzarla

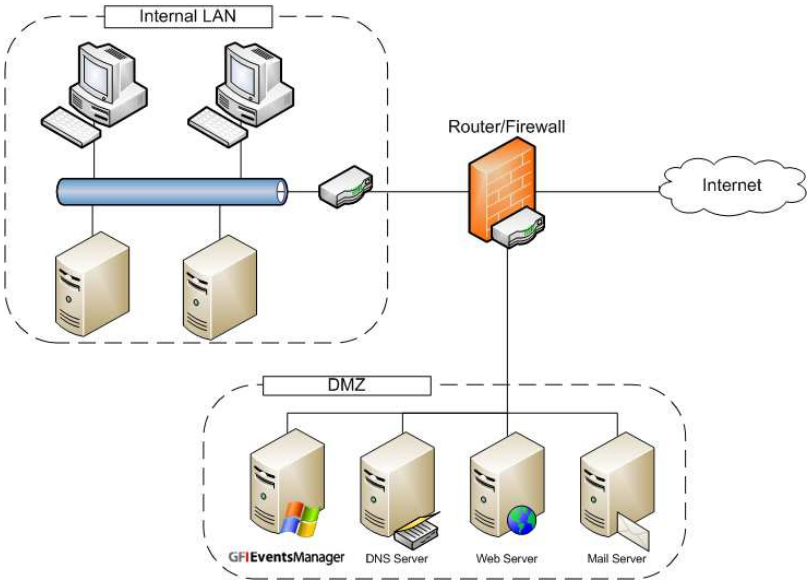
E' un'applicazione disponibile su un server in rete e che non necessita di essere installata nel computer. E' accessibile via web, per mezzo di una intranet o attraverso la Rete Internet, utilizzando un semplice browser. Presenta il vantaggio di essere distribuita ed aggiornata facilmente e di essere accessibile da dispositivi differenti per hardware e sistema operativo. Nella realizzazione di web application le tecnologie più diffuse sono HTML, CSS e Javascript per quel che riguarda la creazione della pagina web lato client e Php per quel che riguarda il lato server. Il server http e il Database più utilizzati sono rispettivamente Apache e MySql, ques'ultimo in abbinamento con il linguaggio Php.

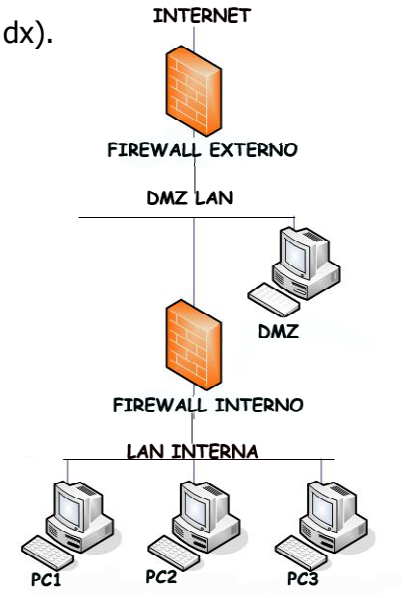
3)Spiegare la differenza tra linguaggi lato client e linguaggi lato server

La differenza sostanziale tra un linguaggio di programmazione lato client (javascript) e un linguaggio di programmazione lato server (php), è che il linguaggio lato client viene interpretato dal browser dell'utente che si collega mentre quello lato server viene interpretato dal server e restituito al browser in HTML. Nella programmazione lato Client il browser residente nel computer client interpreta i codici HTML e i codici di scripting: la pagina viene formattata direttamente sul computer client. Nella programmazione lato Server l'interprete residente nel server interpreta i codici di scripting; i risultati dell'elaborazione vengono trasformati in codici HTML ed inviati al computer client che tramite il browser formatta la pagina a video.

Chiarire il concetto di firewall ed illustrare il funzionamento di una DMZ

Il firewall è un componente hardware o software che serve a proteggere una parte di una rete rispetto all'altra. Di solito si interpone tra una rete locale (LAN) ed Internet (WAN) ed è praticamente un filtro, regolato in base agli obiettivi di sicurezza informatica che si vuole perseguire, che si interpone al traffico di rete per evitare un accesso indiscriminato alla rete locale da parte di intrusi provenienti da Internet. A volte è necessario esporre all'esterno alcuni servizi: ad esempio si deve gestire all'interno della LAN un server di posta elettronica. In tal caso è fortemente consigliata la creazione di una terza zona: la DMZ. Essa è un'area in cui sia il traffico WAN che quello LAN sono fortemente limitati e controllati attraverso una terza interfaccia di rete del firewall (figura sx) oppure utilizzando due firewall (figura dx).





Chiarire i concetti di crittografia e di cifratura dei dati ed elencare e spiegare sinteticamente le principali funzioni php dedicate alla crittografia dei dati

1. Il termine crittografia indica la scienza che studia i metodi per convertire testi leggibili e in chiaro in stringhe alfanumeriche incomprensibili, chiamate crittogrammi. La cifratura è l'operazione che genera il crittogramma; la riconversione di un crittogramma in un testo in chiaro è un operazione chiamata decifrazione o decifratura. La decifrazione può avvenire attraverso una chiave che può essere di due tipi: pubblica o privata.
2. PHP possiede alcune funzioni dedicate alla crittografia dei dati: tra queste la funzione md5() (Message Digest Algorithm versione 5) è molto diffusa ed utilizzata. L'output generato, per password e/o testi di qualsiasi lunghezza, è una stringa esadecimale della lunghezza di 32 caratteri.

Spiegare che cosa significa che il protocollo HTTP è stateless ed elencare i metodi per mezzo dei quali è possibile comunicare dati tra una pagina PHP e l'altra

HTTP è un protocollo stateless perché non mantiene informazioni sullo stato: ogni richiesta è indipendente da tutte le precedenti e non influenza quelle succesive.

PHP permette di comunicare i dati tra una pagina e l'altra utilizzando:

1. le querystring negli URL passati da una pagina e l'altra.

   Esempio: echo "<a HREF='pagina2.php?cod=200'>....."; Nella pagina2.php il valore cod=200 viene recuperato ad esempio con l'istruzione A$=$_GET["cod"];
2. i campi HTML visibili o nascosti nei form HTML attraverso la Form Action
3. i cookies
4. le sessioni

Spiegare che cos'è una web application ed elencare i vantaggi che presenta rispetto ad una tradizionale applicazione Client/Server

E' un'applicazione accessibile via web, per mezzo di una intranet o attraverso la Rete Internet, utilizzando un semplice web browser. I vantaggi sono i seguenti:

A. facilità di distribuzione e aggiornamento: un'applicazione Web si trova interamente sul server, per cui la pubblicazione sul server coincide con la distribuzione e l'aggiornamento effettuato sul server è automaticamente reso disponibile a tutti gli utenti;
B. accesso multipiattaforma: l'accesso all'applicazione è indipendente dall'hardware e dal sistema operativo utilizzato dagli utenti;
C. riduzione del costo di gestione: l'uso di Internet come infrastruttura per un'applicazione Web riduce notevolmente sia i costi di connettività che i costi di gestione dei client;
D. scalabilità: un'applicazione Web ben progettata può crescere insieme alle esigenze dell'azienda senza particolari problemi.

Spiegare la differenza principale tra il linguaggio PHP e il linguaggio Javascript

1. Entrambi sono linguaggi di scripting interpretati utilizzati all'interno di pagine Web. PHP è un linguaggio di programmazione che viene eseguito dal server e permette di costruire l'output della pagina e quindi di mandarlo al client, di realizzare una connessione al database ed eseguire una query SQL. Inoltre dispone di funzioni di I/O sul filesystem remoto.
2. Javascript viene invece eseguito dal client, cioè dal browser, ed è generalmente utilizzato per controllare la validità dei dati inseriti in un form, per gestire eventi, visualizzare messaggi e finestre del browser.

Che cos'è e come funziona la firma digitale

La firma digitale è il risultato di una procedura informatica che garantisce l'autenticità e l'integrità di messaggi e documenti scambiati e archiviati con mezzi informatici, al pari di quanto svolto dalla firma autografa per i documenti tradizionali. La firma digitale è quindi l'equivalente elettronico di una tradizionale firma apposta su carta e ne assume lo stesso valore legale.

L'elemento che caratterizza la firma digitale è rappresentato dal certificato digitale di sottoscrizione che viene rilasciato dagli enti certificatori. Il certificato di sottoscrizione è un file generato seguendo precise indicazioni e standard stabiliti per legge (al suo interno sono conservate informazioni che riguardano l'identità del titolare, la chiave pubblica attribuitagli al momento del rilascio, il periodo di validità del certificato stesso oltre ai dati dell'Ente Certificatore). Il certificato digitale di un titolare, una volta entrato a far parte dell'elenco pubblico dei certificati tenuto dall'Ente Certificatore, garantisce la corrispondenza tra la chiave pubblica e l'identità del titolare.

Che cos'è una VPN? E quali vantaggi presenta?

Una VPN è una rete di telecomunicazioni privata che utilizza, come infrastruttura di trasporto, un sistema di trasmissione pubblico e condiviso quale la Rete Internet. Scopo delle reti VPN è offrire alle aziende, a un costo inferiore e sfruttando la rete Internet, le stesse possibilità delle linee private in affitto. Il vantaggio principale è quello di permettere il collegamento tra sedi remote di una stessa società, o genericamente tra reti LAN remote, a costi molto convenienti. Inoltre la VPN garantisce una navigazione anonima sul web in quanto tutti i dati che vengono scambiati sono criptati. In pratica è come se i nostri dati internet passassero attraverso un tunnel che scherma la nostra connessione.

Qual è la differenza tra Nat/PAT e proxy server?

La tecnica NAT/PAT si basa su una tabella di routing contenente la corrispondenza tra i socket interni e i socket esterni in uso (il socket è l'insieme di indirizzo IP e porta di comunicazione).

Quando un client va a visitare una pagina web su un server esterno, il suo indirizzo e la sua porta di origine (socket interno) vengono traslati rispettivamente all'indirizzo IP pubblico e ad un numero di porta casuale (socket esterno), e i due socket vengono registrati nella tabella di routing del router. Quando arriva la risposta dal server WEB esterno, la tabella di routing permette di capire chi voleva quei dati e li manda al client. Questa tecnica lavora ad un livello OSI basso (trasporto), opera modificando solamente le intestazioni dei pacchetti TCP e quindi non è in grado di analizzare il contenuto delle informazioni che tratta. I server PROXY lavorano invece ad un livello OSI più alto, quello applicativo. Il proxy si interpone tra un client ed un server facendo da tramite o interfaccia tra i due host, ovvero inoltrando le richieste e le risposte dall'uno all'altro. Il client si collega al proxy invece che al server, e gli invia delle richieste. Il proxy a sua volta si collega al server e inoltra la richiesta del client, riceve la risposta e la inoltra al client.

I servizi proxy non si occupano dei servizi TCP e IP, ma operano con dei protocolli applicativi come HTTP, FTP, SMTP, POP3 e sono in grado di analizzare e ciontrollare le informazioni su cui lavora.

Quali sono i vantaggi principali della virtualizzazione dei sistemi operativi?

Lo scopo della virtualizzazione è quello di eseguire contemporaneamente più istanze di sistemi operativi (macchine virtuali) in un'unica macchina fisica (host). I sistemi operativi vitrtuali colloquiano con le risorse messe a disposizione dalla macchina fisica attraverso un componente software di livello intermedio generalmente denominata "hypervisor" o "virtual machine monitor". Il vantaggio più ovvio e immediato della virtualizzazione è l'ottimizzazione dell'hardware. Un ambiente virtualizzato è facile da gestire grazie ad una console di monitoraggio che permette di avere tutto sotto controllo, che prevede un unico ambiente per i salvataggi dei dati e la possibilità di aggiungere ulteriori macchine virtuali al sorgere di nuove esigenze. Molto importante è il vantaggio per la sicurezza informatica: i'intero sistema operativo virtuale può essere salvato su un file e ripristinato facilmente, riducendo notevolmente i tempi di indisponibilità in caso di guasto. Ultimo vantaggio, forse il più importante, è la riduzione dei costi.

Spiegare la differenza tra server virtuali e server dedicati

Il server dedicato è una macchina fisica completamente dedicata ad una azienda o un'organizzazione e le risorse hardware non vengono assolutamente condivise con altri. Un server virtuale è una macchina le cui risorse hardware vengono suddivise in più macchine virtuali, grazie all'utilizzo di specifici software di virtualizzazione detti hypervisor. La disponibilità delle risorse hardware assegnate è stabile e sicura e l'ambiente di lavoro è completamente isolato da quello degli altri utenti, tanto che chi lavora su un server virtuale ha l'impressione di lavorare su un vero e proprio server dedicato. Il vantaggio principale di un server virtuale rispetto ad uno dedicato è sicuramente quello economico

Che cos'è il cloud computing e quali i vantaggi presenta?

Diversamente dal software tradizionale che viene eseguito su un PC locale, nel cloud computing le applicazioni vengono eseguite tramite Internet. Se si utilizza un'applicazione di posta sul Web come GMail o un altro servizio online si ha già a che fare con il cloud computing. I vantaggi principali del Cloud Computing, a fronte del pagamento di un canone mensile e di una minore velocità di esecuzione rispetto a quella delle applicazioni tradizionali sul Pc locale , sono i seguenti: è possibile lavorare da qualsiasi PC o tablet connesso al Web, non ci sono costi di manutenzione, la sicurezza è elevata, i costi aumentano e diminuiscono in base alle esigenze, non si devono fare investimenti pesanti per l'acquisto dei software. .

Elencare i punti in comune tra il linguaggio PHP e il linguaggio Javascript

Javascript e Php sono i linguaggi di scripting più diffusi: entrambi riprendono per molti versi la sintassi del C . Sono linguaggi a tipizzazione debole. Per tipizzazione si intende l'associazione tra una variabile ed un tipo di dato e per "tipizzazione debole" o "tipizzazione dinamica", si intende che una variabile non deve essere dichiarata ed è in grado di cambiare il proprio tipo durante l'esecuzione del programma.

Spiegare che cos'è una web application ed elencare i vantaggi che presenta rispetto ad una tradizionale applicazione Client/Server

E' un'applicazione accessibile via web, per mezzo di una intranet o attraverso la Rete Internet, utilizzando un semplice web browser. I vantaggi sono i seguenti:

E. facilità di distribuzione e aggiornamento: un'applicazione Web si trova interamente sul server, per cui la pubblicazione sul server coincide con la distribuzione e l'aggiornamento effettuato sul server è automaticamente reso disponibile a tutti gli utenti;
F. accesso multipiattaforma: l'accesso all'applicazione è indipendente dall'hardware e dal sistema operativo utilizzato dagli utenti;
G. riduzione del costo di gestione: l'uso di Internet come infrastruttura per un'applicazione Web riduce notevolmente sia i costi di connettività che i costi di gestione dei client;
H. scalabilità: un'applicazione Web ben progettata può crescere insieme alle esigenze dell'azienda senza particolari problemi.

Descrivere le principali caratteristiche del linguaggio php

php (acronimo di Hypertext Preprocessor, ultima verisone 5.4.3 del maggio 2012) è un linguaggio di scripting interpretato, utilizzato principalmente per la realizzazione di pagine web dinamiche e per lo sviluppo di applicazioni web lato server. L'elaborazione di codice PHP sul server produce codice HTML da inviare al browser dell'utente che ne fa richiesta. PHP riprende per molti versi la sintassi del C e del Perl ed è un linguaggio a tipizzazione debole: dalla versione 5 è stato migliorato il supporto al paradigma di programmazione ad oggetti. PHP è in grado di interfacciarsi a molti database tra cui MySql, Oracle, PostgreSql e Microsoft SQLServer. Soprattutto con MySql forma un binomio inscindibile, sicuramente il più diffuso del Web. La presenza di alcuni costrutti derivati dal C permette di utilizzare php per agire a basso livello: tuttavia è fondamentalmente un linguaggio di alto livello, grazie anche alle oltre 3.000 funzioni del nucleo di base e alle numerosissime librerie. Inoltre è gratuito, open source e multipiattaforma.

Spiegare che cos'è una Intranet e proporre una soluzione che permetta di realizzare un Web Server Intranet

Il termine Intranet indica una rete privata generalmente utilizzata all'interno di un'azienda commerciale, di un ente pubblico o di un'organizzazione. Essa implementa gli stessi protocolli di Internet. Uno degli usi più comuni di una Intranet è quello di rendere disponibili pagine web in una rete privata: un Pc della rete funge da Web Server e su di esso viene installata una web application, cui potranno accedere gli utenti della Intranet tramite un browser.

Facendo riferimento al SO Windows, una soluzione molto diffusa per realizzare un Web Server Intranet, è quella di utilizzare Wamp Server, un software libero che permette di installare in macchine con So Windows, il Server Apache, il Data Base MySql e il linguaggio lato server php.