

SIMULAZIONE ESAME DI STATO DI ISTRUZIONE SECONDARIA SUPERIORE

Indirizzo: ITIA – INFORMATICA E TELECOMUNICAZIONI

ARTICOLAZIONE TELECOMUNICAZIONI

Tema di: SISTEMI E RETI

Il candidato (che potrà eventualmente avvalersi delle conoscenze e competenze maturate attraverso esperienze di alternanza scuola-lavoro, stage o formazione in azienda) svolga la prima parte della prova e risponda a due tra i quesiti proposti nella seconda parte.

PRIMA PARTE

Un giornale locale negli anni novanta del secolo scorso realizzò una propria banca dati telematica per la distribuzione elettronica di un notiziario settimanale. Gli utenti, previo abbonamento, si collegavano via modem e linea telefonica per la lettura degli articoli e l'invio di posta elettronica.

Da uno studio preliminare risultava che:

- ad ogni articolo erano associati un titolo, un'immagine ed eventualmente un filmato;
- un numero settimanale si componeva di circa cento articoli.

Il nuovo direttore del giornale desidera effettuare l'ammodernamento del sistema, realizzando una nuova rete locale per il collegamento dei computer e di altri dispositivi, la cui collocazione è la seguente:

- un computer e una stampante nell'ufficio del direttore;
- trenta computer distribuiti a due a due negli uffici dei giornalisti;
- due computer e una stampante professionale nell'ufficio dei redattori;
- altre apparecchiature mobili (smartphone, pc portatili, ...) che vengono utilizzate all'occorrenza dai giornalisti o da collaboratori occasionali.

Inoltre, in un locale protetto, vi è un sistema su cui risiedono la banca dati e il server Web.

Il giornale ha un sito web contenente informazioni e una sintesi degli articoli pubblicati accessibili a tutti senza autenticazione; contiene inoltre una sezione riservata agli abbonati, i quali possono accedere agli articoli completi.

Gli abbonati sono circa 5.000.

Il candidato, formulate le opportune ipotesi aggiuntive, sviluppi i seguenti punti:

- 1) proponga un progetto anche grafico dell'infrastruttura di rete, indicando le risorse hardware e software necessarie, esaminandone in particolare l'architettura, gli apparati e le caratteristiche del collegamento della rete ad Internet;
- 2) descriva possibili tecniche di protezione della rete locale e dei server interni dagli accessi esterni;
- 3) proponga i principali servizi (tra cui ad es. identificazione degli utenti, assegnazione della configurazione di rete, risoluzione dei nomi, ...), e ne approfondisca la configurazione di due a sua scelta;
- 4) discuta vantaggi e svantaggi dell'offrire il servizio mediante l'attuale soluzione gestita internamente, oppure utilizzando un servizio esterno (hosting o housing), esponendo le motivazioni che inducono alla scelta.

SECONDA PARTE

Il candidato risponda a due quesiti a scelta tra quelli sotto riportati.

- 1) In relazione al tema proposto nella prima parte, il sito del giornale consente di differenziare gli accessi tra utenti generici non registrati, abbonati al servizio per la consultazione degli articoli completi, direttore e redattori per l'aggiornamento dei contenuti. Il candidato realizzi il modello concettuale e logico della porzione di base di dati che consente di differenziare gli accessi in base alla tipologia di utente.
- 2) Il candidato spieghi il funzionamento dei protocolli HTTPS e SSL.
- 3) I documenti, anche importanti, viaggiano sempre più spesso in rete ponendo in evidenza la necessità di garantire sia l'integrità degli stessi che l'identità del mittente; descrivere le tecniche che garantiscono la sicurezza dei documenti che viaggiano in rete, con particolare riferimento alle tecniche crittografiche a chiave simmetrica e pubblica/privata, nonché la firma elettronica;
- 4) La rete offre agli utenti numerosi servizi Internet, quali posta elettronica, servizio web, FTP, CHAT; si descrivano le caratteristiche salienti di tali servizi.

Durata massima della prova: 6 ore.

È consentito soltanto l'uso di manuali tecnici (references riportanti solo la sintassi, non guide) dei linguaggi utilizzati.

È consentito l'uso del dizionario bilingue (italiano-lingua del paese di provenienza) per i candidati di madrelingua non italiana.

Non è consentito lasciare l'Istituto prima che siano trascorse 3 ore dalla dettatura del tema.

SOLUZIONE PRIMA PARTE

Ipotesi aggiuntive

La “banca dati” cui si riferisce il testo della simulazione viene interpretata come un DBMS: allo scopo di ottimizzarne sia la gestione che la sicurezza viene installato su un server separato dal server che ospita il sito web.

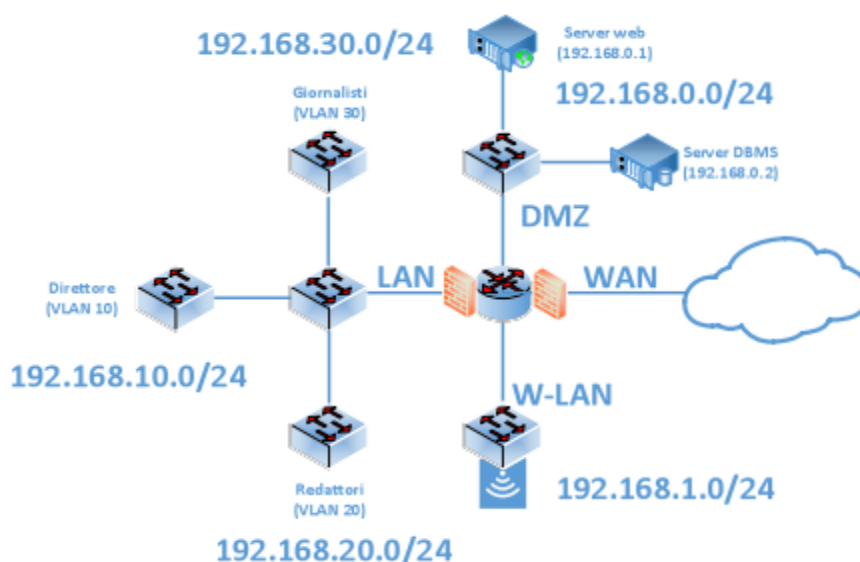
Punto 1: Progetto dell'infrastruttura di rete

Una soluzione classica per la rete del giornale locale è quella che prevede una DMZ per i server accessibili dall'esterno separata dalla rete LAN per il direttore, i giornalisti e i redattori, a sua volta separata dalla rete W-LAN usata dai collaboratori.

Per garantire una maggiore sicurezza è possibile prevedere la separazione delle reti dell'ufficio del direttore, degli uffici dei giornalisti e dell'ufficio dei redattori mediante VLAN: in questo caso il collegamento tra lo switch centrale della rete LAN ed il router sarà di tipo trunk e la relativa interfaccia del router sarà configurata con i 3 diversi indirizzi IP di default-gateway delle 3 VLAN.

Questa soluzione impone uno schema di indirizzamento coerente che prevede 5 reti separate per le quali si utilizzano indirizzi IPv4 privati (statici per la rete LAN e dinamici per la rete W-LAN utilizzando un server DHCP integrato nell'access-point): la configurazione NAT sul router permetterà di associare ad un indirizzo pubblico configurato lato WAN l'indirizzo privato del server web (il server DBMS non sarà invece direttamente accessibile dalla rete esterna).

La subnet mask 255.255.255.0 prevista per tutte le reti coniuga la semplicità di configurazione con il numero di host previsto per ciascuna rete che è sempre inferiore a 253.



Volendo incrementare il livello di sicurezza delle reti LAN e W-LAN è possibile prevedere un altrettanto classica configurazione della rete DMZ utilizzando due router-firewall separati:



Con riferimento alla prima soluzione proposta sono necessari i seguenti dispositivi di rete:

1 router con funzionalità VLAN e firewall	3 porte LAN Ethernet 1Gbps 1 porta WAN per fibra ottica (100Mbps simmetrica)
1 switch ad alte prestazioni con funzionalità VLAN	4 porte Ethernet 1Gbps
1 switch (uffici giornalisti)	32 porte Ethernet 1Gbps
2 switch (ufficio direttore e ufficio redattori)	4 porte Ethernet 1Gbps
1 access-point	autenticazione e crittografia WPA-2, server DHCP

L'access-point e lo switch con funzionalità VLAN sono dispositivi configurabili ed in quanto tali utilizzano un proprio indirizzo IP per esporre un servizio di configurazione normalmente nella forma di un server web embedded. Il contesto descritto non giustifica connessioni a 10Gbps, per cui l'intero cablaggio è realizzato con cavi Ethernet UTP categoria 6 con banda di 1Gbps. Per la tecnologia di connessione alla rete Internet è necessario prevedere un contratto con un ISP specializzato per un servizio FTTB/FTTH (Fiber To The Building/Home) che preveda almeno 100Mbps sia in upstream che in downstream: l'elevata banda in upstream è resa necessaria dagli accessi quotidiani di almeno 5000 utenti che, per le caratteristiche del servizio offerto, hanno probabilmente distribuzione temporale ampiamente concentrata.

Punto 2: Tecniche di protezione della rete locale e dei server interni

La protezione della rete e dei server da accessi esterni non desiderati è realizzata mediante un insieme di tecniche implementate a diversi livelli dello stack ISO/OSI:

- protezione della rete W-LAN con standard WPA-2 e autenticazione degli accessi mediante un server Radius che realizza un servizio AAA (Authentication, Authorization, Accounting)
- regole di firewall sul router per realizzare la DMZ dei server e limitare l'accesso alle reti LAN e W-LAN
- uso del protocollo TLS per l'accesso dall'esterno al server web (HTTPS)
- autenticazione degli accessi al servizio web, eventualmente mediante ricorso ad un servizio SSO (Single Sign On)
- limitazione della configurabilità del router, dello switch core della rete LAN e dell'access-point della rete WLAN.

Si forniscono di seguito esempi essenziali delle liste delle regole di firewall per il router nell'ipotesi che il server Radius appartenga ad una quarta VLAN di servizio con indirizzo 192.168.40.0/24 e abbia indirizzo IP 192.168.40.1.

Interfaccia WAN in ingresso*

protocollo	indirizzo origine	porta origine	indirizzo destinazione	porta destinazione	permesso
TCP	qualsiasi	qualsiasi	192.168.1.X 192.168.10.X 192.168.20.X 192.168.30.X	qualsiasi	concesso solo per connessione stabilita
TCP	qualsiasi	qualsiasi	192.168.0.1	80 (HTTP) 443 (HTTPS)	concesso
UDP	qualsiasi	53 (DNS)	qualsiasi	qualsiasi	concesso
qualsiasi	qualsiasi	qualsiasi	qualsiasi	qualsiasi	negato

* deve essere valutata l'abilitazione del protocollo ICMP

Interfaccia LAN in uscita

protocollo	indirizzo origine	porta origine	indirizzo destinazione	porta destinazione	permesso
TCP	192.168.1.X	qualsiasi	qualsiasi	qualsiasi	negato
UDP	192.168.1.X	qualsiasi	192.168.40.1	1812 (RADIUS) 1813 (RADIUS)	concesso
TCP	qualsiasi	qualsiasi	qualsiasi	qualsiasi	concesso solo per connessione stabilita
UDP	qualsiasi	53 (DNS)	qualsiasi	qualsiasi	concesso
ICMP	qualsiasi	-	qualsiasi	-	concesso
qualsiasi	qualsiasi	qualsiasi	qualsiasi	qualsiasi	negato

Punto 3: servizi e relativa configurazione

La rete del giornale locale espone i seguenti servizi:

- servizio web sul server 192.168.0.1 pubblicamente accessibile;
- servizio DBMS sul server 192.168.0.2 accessibile esclusivamente dal server web e dai computer della rete LAN;
- servizio DHCP integrato nell'access-point della rete W-LAN.

Per il servizio web è possibile installare un server Apache (disponibile sia come demone per S.O. Linux che come servizio per S.O. Windows), la cui configurazione avviene modificando il file testuale "httpd.conf"; è in particolare necessario configurare le porte di ascolto del servizio, (tipicamente TCP 80 per HTTP e TCP 443 per HTTPS, ma possono essere diverse se si configura il NAT sul router con una tecnica di port-forwarding).

L'abilitazione TLS necessaria per il supporto HTTPS può essere effettuata attivando il modulo OpenSSL integrato e richiede un certificato del server: data la tipologia pubblica del servizio offerto è necessario che il certificato sia generato da una CA (Certification Authority) accreditata da AgID (Agenzia per l'Italia Digitale).

Per il servizio DBMS è possibile installare un server My-SQL (disponibile sia come demone per S.O. Linux che come servizio per S.O. Windows), la cui configurazione può essere effettuata semplicemente utilizzando l'applicazione My-SQL Workbench che consente di impostare tra gli altri i seguenti parametri:

- tipologia degli storage engine;
- set di caratteri;
- password dell'utente amministratore;

- utenti e relativi privilegi e password;
- porta di ascolto (normalmente TCP 3306).
- numero di connessioni contemporanee
- client affidabili

La configurazione del server DHCP integrato nell'access-point (accessibile dai client wireless sulla porta UDP 67) che realizza la rete W-LAN sarà limitata all'impostazione dei parametri della rete stessa (sotto l'ipotesi che l'indirizzo 192.168.1.1 sia attribuito all'access-point stesso):

- network: 192.168.1.0
- netmask: 255.255.255.0
- default-gateway: 192.168.1.254
- address-range: 192.168.1.2 – 192.168.1.253
- DNS-address: fornito da ISP
- lease-time: 36000s (10h)

Nell'ipotesi di disporre di un unico indirizzo IP pubblico per l'interfaccia WAN verso la rete Internet, nel router deve essere configurato il servizio NAT:

- statico di tipo port-forwarding per rendere accessibile il server web associando il suo indirizzo IP privato (192.168.0.1) all'indirizzo IP pubblico esclusivamente per le porte 80 (HTTP) e 443 (HTTPS)
- dinamico (IP overloading) per le quattro reti interne (la rete W-LAN e le tre VLAN che costituiscono la rete LAN) che necessitano di accedere alla rete Internet esterna esclusivamente come client (navigazione web, servizi di posta elettronica, ...).

Punto 4: confronto tra soluzione interna e hosting/housing esterno

La soluzione di rete proposta è qualitativamente carente per quanto riguarda affidabilità e sicurezza, in particolare del servizio web ad accesso pubblico.

Essendo la rete priva di ridondanza dei dispositivi (router, switch e server) e della connettività Internet, la disponibilità del servizio è infatti soggetta ad interruzione in presenza di un qualsiasi guasto, o temporanea mancanza di alimentazione o di connettività.

Inoltre, anche per la tipologia del servizio offerto, è possibile prevedere “attacchi” relativamente frequenti finalizzati a limitare la disponibilità del servizio stesso, o ad alterare i contenuti esposti.

Infine, l'erogazione di un servizio pubblico disponibile senza soluzione di continuità richiede la presenza o reperibilità continuativa di personale tecnico in grado di mantenere il servizio stesso e intervenire in caso di interruzione della disponibilità.

Per questi motivi la soluzione interna risulta al tempo stesso insoddisfacente sotto il profilo qualitativo ed estremamente costosa anche in ragione della tipologia di connettività alla rete Internet che impone. La soluzione esterna prevede in questo caso l'acquisto di un servizio di hosting standard (web server + DBMS) che qualsiasi data-center (ad esempio Aruba S.p.A.) offre a costi contenuti garantendo parametri di sicurezza e di disponibilità

irraggiungibili per una soluzione interna di una piccola organizzazione, evitando al tempo stesso l'acquisto e la gestione tecnica dei server e di un'infrastruttura di rete resa complessa dalla presenza della DMZ.

La prevedibile distribuzione temporale degli accessi al sito web del giornale, concentrati in alcune ore della giornata, rende il servizio descritto il candidato ideale per una soluzione cloud di noleggio di un server virtuale con configurazione (numero di CPU, quantità di memoria RAM, banda di networking, ...) variabile in funzione del traffico e/o dell'ora, permettendo di ottimizzare sia la qualità del servizio stesso che il suo costo.

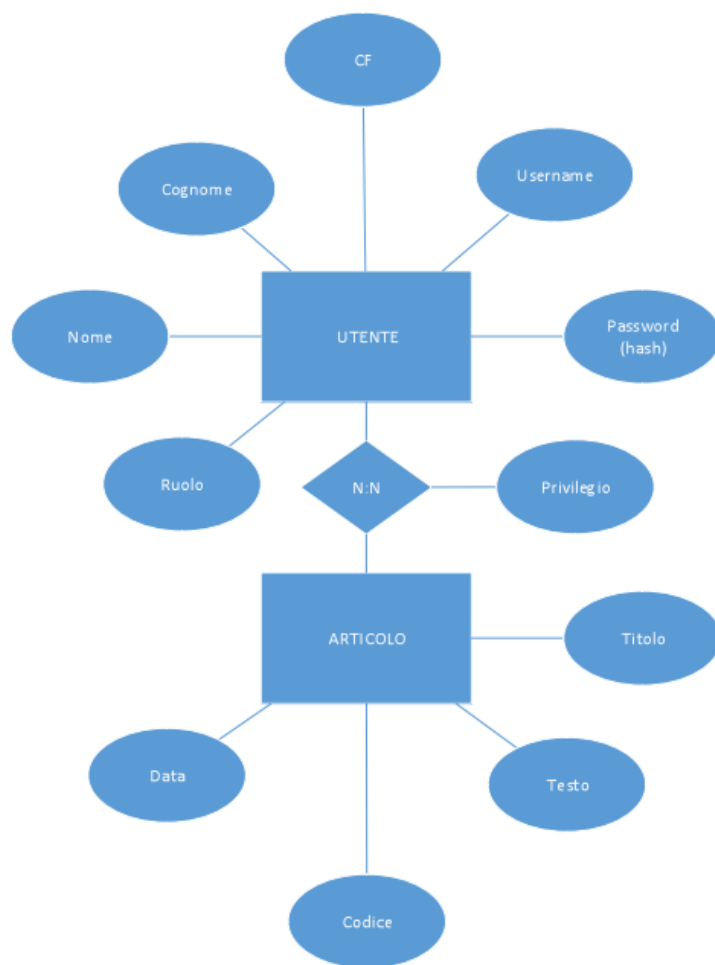
SOLUZIONE SECONDA PARTE

Quesito 1

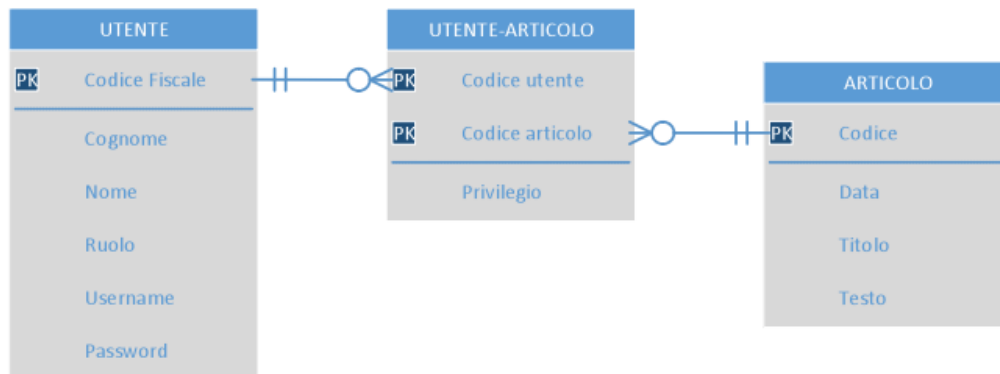
Nell'ipotesi che i privilegi di accesso ad uno specifico articolo da parte di uno specifico utente possano essere:

- nessuno (nel caso di articoli non pubblicamente disponibili);
- solo lettura (nel caso di articoli pubblicamente disponibili o riservati per gli utenti registrati);
- lettura e scrittura (per gli utenti interni del giornale: direttore, redattori e giornalisti)

il seguente diagramma E/R modella la porzione di un database relazionale che permette di autenticare gli utenti e di attribuire loro i corretti privilegi di accesso agli articoli:



Tenendo conto che le password degli utenti, per motivi sia di sicurezza che di privacy, devono essere memorizzate in forma cifrata mediante una funzione hash, il database relazionale risultante può essere così schematizzato (è previsto un utente “anonimo” che ha i privilegi di un qualsiasi utente non registrato):



Quesito 2

Nell'unità A4 riportate le informazioni sul protocollo HTTPS, mentre nell'unità C3 sono riportate le informazioni relative al protocollo SSL.

Quesito 3

Nel modulo B sono riportate le informazioni sulla sicurezza delle informazioni che viaggiano in rete, le quali garantiscono l'autenticità e l'integrità dei documenti, nonché la firma elettronica.

Quesito 4

Nel modulo A sono riportate le informazioni sui servizi Internet