

Cognome: _____ **Nome:** _____ **Matricola:** _____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2007

Usa questa pagina per la brutta, staccala, non consegnarla.

Cognome: _____ **Nome:** _____ **Matricola:** _____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2007

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2007

Tempo a disposizione: **90 minuti**. Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di cellulari, calcolatrici, palmari e affini.

1. Rispondi alle seguenti domande sulle vulnerabilità del software.

1.1. Descrivi la tecnica di attacco nota come SQL injection facendo un esempio.

Descrizione

esempio

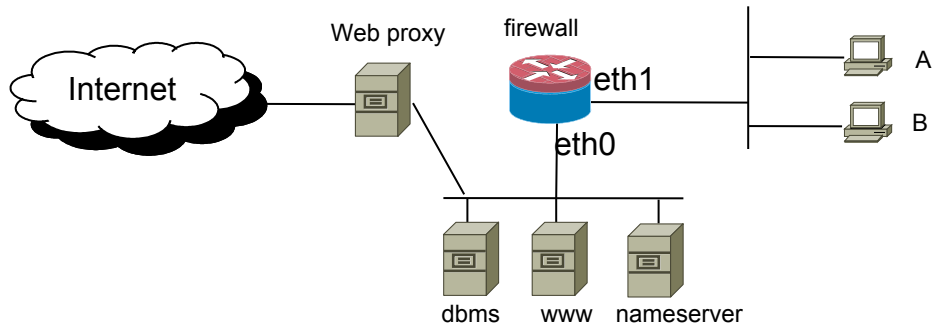
1.2. Input fidato e non fidato. Perché è importante distinguere tra i due casi quando si parla di vulnerabilità del software?

2. Che cosa è il “security target” in Common Criteria?

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2007

3. Considera la rete in figura con la matrice di accesso indicata, in cui i servizi di interesse sono tre: dns, web, e db. La macchina “web proxy” ha solo funzionalità di proxy web sia per richieste in ingresso che in uscita.



	A	A	B	Dbms	www	Nameserver	Internet
Da							
A			-	Rich. db	-	Rich. dns	-
B	-			Rich. db	-	Rich. dns	-
Dbms	Risp. db	Risp. db	Risp. db		Risp. db	-	-
www	-	-	-	Rich. db		-	Risp. web
Nameserver	Risp. dns	Risp. dns	Risp. dns	-	-		Risp./Rich. dns
Internet	-	-	-	-	Rich. web	Risp./Rich. dns	

Rispondi alle seguenti domande.

3.1. Evidenzia sulla matrice di accesso le parti che **non** sono realizzabili con la rete data. Spiegane il perché'.

3.2. Che tecnica suggeriresti per realizzare le parti della matrice di accesso identificate nella domanda precedente?

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2007

3.3. Dai la configurazione del firewall, usando preferibilmente la sintassi di netfilter. Al posto degli indirizzi usa i nomi delle macchine, al posto delle porte usa i nomi dei servizi (dbms, dns, www).

4. Mandatory Access Control vs. Discretionary Access Control. Descrivi i due modelli ed evidenziane vantaggi e svantaggi.

5. Rispondi alle seguenti domande circa la normativa italiana in materia di sicurezza informatica.

5.1. Cosa sono i “requisiti minimi” introdotti dall’allegato B della 196/2003? Dai degli esempi.

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2007

5.2. Che cosa e' il Documento Programmatico di Sicurezza?

5.3. In che rapporto sono il Documento Programmatico di Sicurezza previsto dalla legge 196/2003 e il piano di sicurezza?

6. Descrivi il concetto di perfect forward secrecy e mostra un protocollo che gode di questa proprieta'.

Descrizione

Esempio di protocollo

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2007

7. Radius e 802.1X, mostra il funzionamento dei due protocolli assieme.

8. Rispondi alle seguenti domande sulle Public key Infrastructure

8.1. Descrivi il concetto di certificato.

8.2. Descrivi il modello di PKI oligarchica (quello usato nei browser).

Cognome: _____ Nome: _____ Matricola: _____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2007

8.3. Elenca alcune vulnerabilita' delle PKI e del modello oligarchico.