Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2019 – 4 CFU (la tesina vale 2 CFU)

SE NON HAI CONSEGNATO LA TESINA NON PUOI SOSTENERE QUESTO ESAME

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2019 – 4 CFU (la tesina vale 2 CFU)

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2019 – 4 CFU (la tesina vale 2 CFU)

SE NON HAI CONSEGNATO LA TESINA NON PUOI SOSTENERE QUESTO ESAME

Tempo a disposizione: 60 minuti. Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di smartphone/watch, calcolatrici e affini.

1. Considera le vulnerabilità di tipo cross-site scripting (XSS). Descrivi il XSS non persistente. Descrivi brevemente il XSS persistente. Descrivi brevemente come l'uso della tecnologia Ajax possa veicolare un XSS persistente.

XSS non persistente.

XSS persistente.

Ajax come veicolo di XSS.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2019 – 4 CFU (la tesina vale 2 CFU)

2. Attacchi DDoS e contromisure.

2.1. Syn-flood. Che tipo di traffico viene inviato sulla rete? Perché tale traffico è un problema per il ricevente?

descrizione del traffico

effetti sul ricevente

2.2. Syn-proxy. Come agiscono? che vantaggio abbiamo ad adottarli?

come agiscono

vantaggi

2.3. Descrivi la contromisura nota come Syn-cookies.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2019 – 4 CFU (la tesina vale 2 CFU)

3. **Piano di sicurezza**. Elenca, e descrivi in una riga, 5 sezioni tipiche di un piano di sicurezza.

1.

2.

3.

4.

5.

4. **Birthday attack**. Descrivi il birthday attack per gli hash crittografici. In particolare, descrivi obiettivo dell'attacco, principio statistico su cui è basato e impatto sulle tecniche di firma digitale.

Obiettivo.

Principio statistico su cui si basa.

Impatto sulla firma digitale.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2019 – 4 CFU (la tesina vale 2 CFU)

5. Gli attacchi al login possono essere classificati in on-line (in cui il prompt di login è accessibile via rete) e off-line (in cui il database utenti/password è disponibile in locale all'attaccante con gli hash delle password). Compila la seguente tabella.

	On-line	Off-line
Che contromisure suggerisci per i due tipi di attacchi?		
Quali sono secondo te le criticità o difficoltà principali per l'attaccante?		
Quali sono secondo te le criticità o difficoltà principali per chi deve mitigare il rischio di un tale tipo di attacchi?		

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 20 settembre 2019 – 4 CFU (la tesina vale 2 CFU)

6. Considera la tecnologia blockchain che è alla base di bitcoin. Rispondi alle seguenti domande sull'algoritmo di consenso noto come "proof of work".

6.1. Cosa deve riuscire a fare un nodo per aggiungere un blocco alla blockchain

6.2. Da che cosa si capisce che un certo nodo della rete è d'accordo circa un certo stato della blockchain?

6.3. Se un attaccante ha più del 50% della potenza di calcolo della rete, che attacco (o attacchi) può instaurare?