Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 20 luglio 2021 – 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:_____

Cybersecurity – 20 luglio 2021 – 4 CFU (la tesina vale 2 CFU)

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

Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 20 luglio 2021 – 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. **Principi.** Discuti brevemente i principi di progettazione "isolamento" e "defence-in-depth". Tra loro c'è una sinergia o un antagonismo? Spiega.

Isolamento

defence-in-depth

sinergia o antagonismo? Spiega.

2. **Piano di sicurezza.** Elenca 6 sezioni tipiche di un piano di sicurezza e descrivi ciascuna in una riga,.

1.

2.

3.

4.

5.

6.

Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 20 luglio 2021 – 4 CFU (la tesina vale 2 CFU)

3. **Sicurezza del codice.** Considera il seguente codice che legge da standard input una stringa che poi aggiunge degli asterischi per farne un titolo. La stringa in input è rappresentata nel formato in cui i byte del contenuto della stringa sono preceduti dalla sua lunghezza L (in bytes), espressa in binario con un intero di 2 bytes.

```
int main(int argc, char** argv) {
        unsigned short len; /* intero di 2 bytes senza segno */
        char buffer*;
        char title[1000];

        read(stdin, &len, 2); /*legge l'intero direttamente in binario*/
        buffer = malloc(len+1);
        read(stdin, buffer, len);
        buffer[len]='\0';   /*aggiunge il terminatore zero finale*/
        sprintf(title, "*** %s ***", buffer )
              /*mette in title il contenuto di buffer con gli asterischi attorno,
                sprintf() è come printf ma non stampa, scrive solo su title che
                deve essere preallocata */
}
```

3.1. Elenca le vulnerabilità che pensi siano presenti in questo codice con una breve descrizione di ciascun problema.

3.2. Per ciascuna vulnerabilità trovata, suggerisci una contromisura.

Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 20 luglio 2021 – 4 CFU (la tesina vale 2 CFU)

4. Smart contracts in Ethereum

Considera il seguente smart contract scritto in solidity.

```
contract Test {
    uint256 number;
    function storeNum(uint256 num) public {
        if ( num < 100 ) { number = num; }
    }
}
```

4.1. Che caratteristiche di sicurezza ha la sua esecuzione in confronto ad un software standard?

4.2. Considera la variabile di stato **`number`**. Dove è memorizzata? Cosa puoi dire della confidenzialità del suo contenuto? Cosa puoi dire sull'integrità del suo contenuto?

Dove è memorizzata?

Confidenzialità?

Integrità?

5. Perfect forward secrecy (PFS).

5.1. Un protocollo dotato di PFS cosa garantisce che un normale protocollo non garantisce?

Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 20 luglio 2021 – 4 CFU (la tesina vale 2 CFU)

5.2. Supponi che la magistratura autorizzi la polizia all'intercettazione di una comunicazione tra A e B. La comunicazione usa un protocollo dotato di PFS. La magistratura fornisce alla polizia i segreti a lungo termine di A e B (cioè le loro chiavi private di autenticazione). Come procede la polizia per l'intercettazione?

5.3. Mostra un protocollo di mutua autenticazione e scambio di chiave di sessione dotato di PFS.

6. Attacchi DDoS e contromisure.

6.1. Syn-flood: descrivi il traffico che viene inviato sulla rete dall'attaccante, descrivi gli effetti di tale traffico sul sistema ricevente?

descrizione del traffico

effetti sul sistema ricevente

Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 20 luglio 2021 – 4 CFU (la tesina vale 2 CFU)

6.2. Syn-proxy. In quale posizione useresti un syn-proxy? Che azione ha un syn-proxy sul traffico? Che vantaggio porta il suo uso?

dove useresti un syn-proxy?

come agisce un syn-proxy sul traffico?

Che vantaggio porta il suo uso?

6.3. Descrivi la contromisura nota come Syn-cookies.