Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 17 febbraio 2022 – 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 – 17 febbraio 2022 – 4 CFU (la tesina vale 2 CFU)

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

Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 17 febbraio 2022 – 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 "semplicità" e "defence-in-depth". Tra loro c'è una sinergia o un antagonismo? Spiega.

Semplicità

defence-in-depth

sinergia o antagonismo? Spiega.

2. **Perfect forward secrecy** (PFS).

2.1. Quando le chiavi crittografiche private (segreti a lungo termine) vengono pubblicate, un protocollo dotato di PFS cosa garantisce, che un normale protocollo senza PFS non garantisce?

2.2. Mostra il protocollo Diffie-Hellman e spiega perché è dotato della proprietà PFS.

A **B**

Perche è dotato di PFS?

Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 17 febbraio 2022 – 4 CFU (la tesina vale 2 CFU)

2.3. Supponi che un hacker C abbia ottenuto i segreti a lungo termine di A e B e C abbia **accesso in sola lettura al canale di comunicazione** tra A e B. A e B usano un protocollo dotato di PFS. Può C ottenere il contenuto di una comunicazione tra A e B? Perché?

Si o no?

Perché?

3. Sicurezza del codice. Considera il seguente codice che legge da standard input una stringa e chiama il comando "report" passandogli come argomento sulla riga di comando la stringa letta.

```
int main(int argc, char** argv) {
        short len; /* intero di 2 bytes con segno */
        char buffer[1000];
        char cmd[1007];
        read(stdin, &len, 2); /*legge l'intero direttamente in binario*/
        if ( len >= 999 ) {
              . . . /* gestione errore */
        }
        read(stdin, buffer, len);
        buffer[len]='\0';   /*termina con zero*/
        strcpy(cmd, "report ");/* "report <arg>" è un comando fidato che genera output
                                  nel file <arg>*/
        strcat(cmd, buffer);  /* copia buffer in coda alla stringa contenuta in cmd */
        system(cmd);
}
```

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

3.2. Suggerisci delle modifiche al codice per risolvere ciascuna vulnerabilità.

4. Logging. Rispondi alle seguenti domande sul logging e sul protocollo syslog.

4.1. In un sistema che può essere obiettivo di hacking, perché è importante la sicurezza dei log?

4.2. Elenca tre azioni, con una brevissima descrizione, per proteggere l'integrità dei log e per rendere più semplice il loro utilizzo/sfruttamento ai fini dell'auditing.

4.3. Che ruolo ha il protocollo di rete syslog nella gestione dei log in una organizzazione?

5. Smart contracts in Ethereum

Considera il seguente smart contract scritto in solidity eseguito da una blockchain di 25 nodi.

```
contract Prova {
    uint256 valore;
    function  memorizza(uint256 num) public {
        if ( num < 10 ) { valore = num; }
    }
}
```

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

Dove è memorizzata?

Confidenzialità?

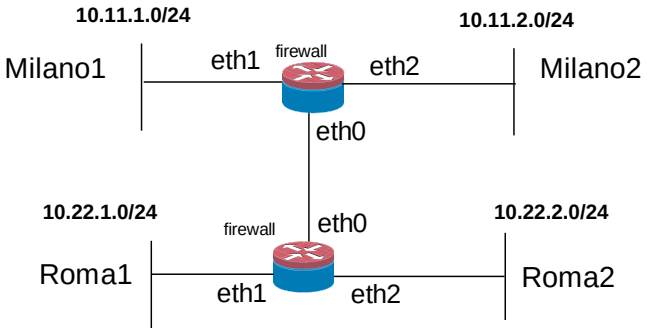
Integrità?

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

Cybersecurity – 17 febbraio 2022 – 4 CFU (la tesina vale 2 CFU)

6. Networking.

Considera la rete in figura con le configurazioni dei firewall date sotto. Non vi sono nat ed il routing è configurato correttamente.



Roma

```
:FORWARD DROP
-A FORWARD –i eth1 –m state --state NEW –j ACCEPT
-A FORWARD –i eth2 –m state --state NEW –j ACCEPT
-A FORWARD –m state --state ESTABLISHED –j ACCEPT
```

Milano

```
:FORWARD DROP
-A FORWARD –i eth0 –s 10.22.2.0/24 –m state --state NEW –j ACCEPT
-A FORWARD –o eth0 –m state --state NEW –j ACCEPT
-A FORWARD –m state --state ESTABLISHED –j ACCEPT
```

6.1. Esprimi la policy realizzata dal sistema dei due firewall, con le configurazioni mostrate, compilando la matrice di accesso corrispondente (supponi un comportamento non malevolo degli utenti). Inserisci Q se passa il primo pacchetto (Query), R se passano solo i pacchetti successivi al primo (Response).

A Da	Roma1	Roma2	Milano1	Milano2
Roma1	-----			
Roma2		-----		
Milano1			-----	
Milano 2				-----

6.2. Supponi che nella rete vi siano utenti malevoli. Date la configurazione di sopra, vedi un modo per aggirare almeno una parte della policy? Descrivi la vulnerabilità e suggerisci una possibile soluzione.

vulnerabilità

soluzione