Il seguente è un elenco di domande (assolutamente non esaustive e scritto un po' velocemente) che forniscono una idea sulla tipologia di domande di esame da 4 cfu.

1. **Sicurezza del software**
   - **1.1.** Buffer overflow: descrivi layout dello stack e tecnica di attacco.
   - **1.2.** Elenca le principali difficoltà nel generare un exploit per una vulnerabilità di tipo buffer overflow.
   - **1.3.** Dai un esempio di programma C vulnerabile e descrivi cosa deve fare l'attaccante per sfruttare la vulnerabilità.
   - **1.4.** Contromisure per gli attacchi buffer overflow (tecnologiche o di processo).
   - **1.5.** Un'architettura con stack che cresce verso l'alto è più o meno vulnerabile ad attacchi di tipo buffer overflow sullo stack?
   - **1.6.** Fai un esempio di sql injection e spiegalo.
   - **1.7.** Fai un esempio di XSS e spiegalo
   - **1.8.** Fai un esempio di XSS persistente e spiegalo.
   - **1.9.** Fai un esempio di CSRF e spiegalo.
   - **1.10.** Analizza la sicurezza nel codice C relativi alla esecuzione di un comando di copia i cui parametri sono passati come argomenti dell'eseguibile.

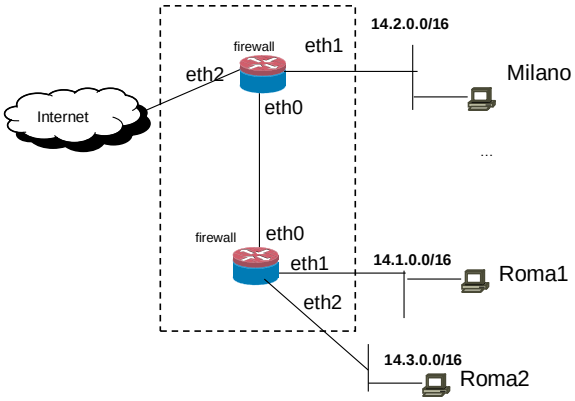
```
int main(int argc, char** argv) {
   char buffer[2000];
   int j;
   strcpy(buffer, "/bin/cp");
   for( j=1; j<argc; j++) {
        strcat(buffer, " ");
        strcat(buffer, argv[i]);
   }
   system(buffer); /*esegue il contenuto di buffer nella shell */
}
```

   - **1.11.** Analizza la sicurezza nel codice C relativi alla esecuzione di un comando di copia i cui parametri sono passati come argomenti dell'eseguibile.

```
int main(int argc, char** argv) {
   /* esegue cp con gli stessi argomenti e lo stesso ambiente del padre */
   execve("/bin/cp", argv, environ);
                          /*environ punta all'ambiente corrente*/
}
```

2. **Sicurezza delle reti.**
   - **2.1.** Vulnerabilità degli switch.
   - **2.2.** Descrivi l'attacco noto come ARP poisoning.
   - **2.3.** Descrivi l'attacco noto come TCP hijecking.
   - **2.4.** Descrivi l'attacco noto come TCP reset e perché è importante per il routing interdominio.
   - **2.5.** Descrivi l'attacco noto come "Internet biggest security hole" nell'ambito del routing interdominio e paragonalo all'ARP poisoning.
   - **2.6.** Descrivi l'attacco noto come SYN flood.
   - **2.7.** Descrivi la tecnica nota come SYN-cookies.
   - **2.8.** Descrivi una vulnerabilità del DNS.
   - **2.9.** Descrivi un firewal stateful
   - **2.10.** Cosa è un Unified Threat Management
   - **2.11.** Dai una configurazione di un firewall, preferibilmente con la sintassi di iptables, che sia equivalente a quella di un rouer-firewall di casa (tipo quelle dei router adsl).
   - **2.12.** Mostra un esempio in cui ci sia un firewall con una regola come contromisura allo spoofing degli indirizzi IP, descrivi la regola usando preferibilmente con la sintassi di iptables.
   - **2.13.** Descrivi le problematiche di scalabilità dei firewall e le soluzioni possibili.
   - **2.14.** Descrivi le componenti principali di un IDS.
   - **2.15.** Descrivi le problematiche di scalabilità dei firewall è una soluzione possibile.

2.16. Considera la rete in figura con le configurazioni date.



Roma

```
:FORWARD DROP
-A FORWARD –i eth1 -m state --state NEW -j ACCEPT
-A FORWARD –i eth0 –o eth2 -m state --state NEW -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

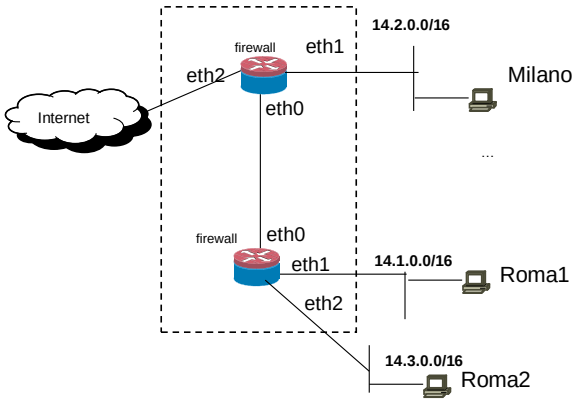
Milano

```
:FORWARD DROP
-A FORWARD –i eth1 -m state --state NEW -j ACCEPT
-A FORWARD –i eth2 –o eth0 -m state --state NEW -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Che matrice di accesso realizzano? (segna Q per query e R per reply)

A **Da**	Roma1	Roma2	Milano	Internet
Roma1				
Roma2				
Milano				
Internet				

2.17. Considera la rete in figura con la matrice di accesso data.



A **Da**	Roma1	Roma2	Milano	Internet
Roma1	----------	QR	Q	Q
Roma2	QR	----------		
Milano	R		----------	Q
Internet	R		R	----------

Mostra delle configurazioni per i fw di Roma e Milano che realizzino tale matrice di accesso. Esprimi le configurazioni preferibilmente seguendo la sintassi di iptables.

3. Principi di progettazione

3.1. Descrivi il principio noto come "minimalità dei diritti" e rapportalo al comportamento tipico di un utente che si vede assegnati diritti maggiori del necessario.
3.2. Descrivi il principio noto come "Default sicuri", fai un esempio
3.3. Descrivi il principio noto come "Semplicità" e perché è importante per la sicurezza informatica.
3.4. Descrivi il principio noto come "Progetto aperto" e il suo ambito di applicazione tipico.
3.5. Descrivi il principio noto come "isolamento" e fai un esempio
3.6. Descrivi il principio noto come "mediazione completa" e spiega come si realizza nell'ambito del software e la sua importanza nell'ambito della certificazione del software.
3.7. Descrivi il principio noto come "defence in depth" e il suo impatto sulla gestione del budget.
3.8. Descrivi il principio noto come "usabilità" e fai due esempi in cui la scarsa usabilità di una contromisura rende un sistema insicuro.
3.9. Descrivi il principio noto come "eterogeneità" e spiega perché è difficilmente applicabile.
3.10. Discuti brevemente la sinergia o l'antagonismo tra i principi eterogeneità e semplicità di progetto.
3.11. Discuti brevemente la sinergia o l'antagonismo tra i principi usabilità e default sicuri.
3.12. Discuti brevemente la sinergia o l'antagonismo tra i principi Isolamento e mediazioni completa.

4. Modelli

4.1. Descrivi il modello noto come AAA e mostra un esempio concreto.
4.2. Descrivi il modello noto come Access Matrix e modella con esso un caso relativo ad un filesystem.
4.3. DAC e MAC, definizioni, differenze, e ambiti applicativi.

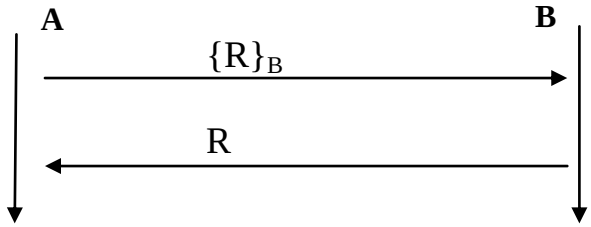
5. Sicurezza dei sistemi

5.1. Quali sono le quattro tipologie di informazioni che possono essere potenzialmente usate per l'autenticazione?
5.2. Hardening: punti di forza, applicabilità, difficoltà, strumenti.
5.3. Che cosa è un wrapper? quando si usa? cosa fa?
5.4. Attacchi on-line e off-line ai meccanismi di autenticazione con password: metodi, punti di forza e difficoltà, contromisure.
5.5. IDS: falsi positivi e falsi negativi, cosa sono? che problemi danno? quanto sono critici nell'utilizzo di un IDS?
5.6. Syslog. Casi d'uso. Punti di forza e debolezze.
5.7. Sudo. Casi d'uso. Punti di forza e debolezze.
5.8. PAM. Casi d'uso. Punti di forza e debolezze.

6. Tecniche crittografiche

6.1. Definizione e proprietà di una funzione di hash crittografica.
6.2. Definizione e proprietà di un metodo di crifratura simmetrico.
6.3. Definizione e proprietà di un metodo di crifratura asimmetrico.
6.4. Applicazioni degli hash crittografici
6.5. Applicazioni dei metodi di cifratura simmetrici

6.6. Applicazioni dei metodi di cifratura asimmetrici
6.7. Birthday attack: principio ed esempio di attacco
6.8. Attacchi brute force all'hash con e senza database, perché sono difficili da applicare?
6.9. Rainbow tables: come funzionano? che vantaggi danno? che contromisure si possono prendere?
6.10. Key rollover: che vantaggi dà? quando è necessario adottarlo?
6.11. Discuti le necessità poste sulla generazione di numeri casuali in crittografia e i problemi più comuni delle implementazioni.
6.12. Dai un esempio di protocollo di autenticazione one-way con chiave asimmetrica e uno con chiave simmetrica e discuti il problema dell'attacco replay e il concetto di nonce.
6.13. Dai un esempio di protocollo di mutua autenticazione con chiave simmetrica vulnerabile ad attacco reflection.
6.14. Segreti a lungo termine vs. segreti a breve termine, cosa sono? perché sono necessari entrambi?
6.15. Scambio di chiave di sessione e tcp session hijack: che tipo di impatto hanno questi due aspetti sul progetto di protocolli di trasporto crittografici (tipo ssl).
6.16. Descrivi il concetto di perfect forward secrecy.
6.17. PFS: ome fa una autorità in possesso dei segreti a lungo termine di A e B a intercettare il contenuto di una comunicazione tra loro? Mostra uno schema.
6.18. Fornisci un protocollo di mutua autenticazione e scambio di chiave di sessione dotato di perfect forward secrecy basato su RSA.
6.19. Fornisci un protocollo di mutua autenticazione e scambio di chiave di sessione dotato di perfect forward secrecy in cui l'autenticazione è basata su RSA e lo scambio di chiavi su Diffie-Helman.
6.20. Diffie-Hellman. A che serve? Come funziona? Che garanzie dà?
6.21. Supponi che un server B sia dotato di una chiave privata. Un client A, in possesso della relativa chiave pubblica, deve autenticare B e lo fa con il seguente protocollo di tipo challenge-response.



R: challenge (nonce) generato da A

Qual è il tipo di attacco crittoanalitico più vantaggioso tra ciphertext only, known plaintext, chosen plaintext che un attaccante che sniffa la rete può instaurare? Fornisci una variante del protocollo per impedire tale attacco.
Se il nonce è prevedibile il protocollo è vulnerabile? Se sì, qual è l'attacco?
Se il nonce è usato più di una volta il protocollo è vulnerabile? Se sì, qual è l'attacco?
Fornisci una variante del protocollo che sfrutta solo funzioni di hash, e si basi su un segreto condiviso.

7. Applicazioni delle tecniche crittografiche

7.1. Public Key Infrastructures: descrivi il concetto di certificato, di certification authority e di catena di certificati.
7.2. Quali sono i punti critici di una PKI?
7.3. Descrivi SSL e il concetto di cipher suite.
7.4. Descrivi SSL e l'handshake con autenticazione RSA.
7.5. IP-Sec: descrivi la struttura del pacchetto per il servizio Encapsulated Security Payload nelle due varianti tunnel mode e transport mode.
7.6. Autenticazione di livello 2: EAP, RADIUS e loro utilizzo per l'auteticazione di un hot spot wifi.
7.7. Descrivi il concetto di one time password e dai un esempio di tecnica realizzativa.

8. Pianificazione

8.1. Contenuto di un piano di sicurezza

8.2. Analisi del rischio: principi, metodi di valutazione e metodi di mitigazione
8.3. Disaster recovery e business continuity.

9. Strutture dati autenticate

9.1. Descrivi la struttura dati autenticata nota come "Merkle Tree". Fornisci la complessità computazionale della tempo necessario per creare una prova di esistenza di un elemento e dello spazio occupato da tale prova.
9.2. Considera un Merkle tree e supponi che un client conosca solo il root-hash. Che cosa bisogna fornire a tale client per provare l'esistenza di un elemento nell'albero? su quale proprietà degli hash crittografici si basa tale prova? perché?.
9.3. Considera un Merkle tree e supponi che un client conosca solo il root-hash. Che cosa bisogna fornire a tale client per provare la non esistenza di un elemento nell'albero? su quale proprietà degli hash crittografici si basa tale prova? perché?
9.4. Supponi di usare un Merkle Tree per verificare che un cloud provider C restituisca correttamente i dati di un dataset. Sia il dataset sia il Merkle Tree sono memorizati in C e i client conoscono solo il root-hash. Mostra un protocollo (con un diagramma di sequenza) per eseguire una query autenticata con la verifica di integrità.
9.5. Supponi di usare un Merkle Tree per verificare che un cloud provider C restituisca correttamente i dati di un dataset. Sia il dataset sia il Merkle Tree sono memorizati in C e il client conosce solo il root-hash. Mostra un protocollo (con un diagramma di sequenza) per eseguire una aggiornamento del dataset e del Merkle Tree in C e del root-hash sul client.

10. DLT e blockchain

10.1. Quali sono gli elementi che devono essere specificati per descrivere un DLT unpermissioned? Descrivi ciascuno brevemente
10.2. Descrivi la struttura della blockchain di Bitcoin, focalizzando su blocchi transazioni e utxo, mostrando anche cosa rende la blockchain una struttura dati autenticata.
10.3. Descrivi, senza entrare nei dettagli, con che tecnica il possessore di un indirizzo nel creare una transazione fornisce la prova che è proprio lui il possessore dell'indirizzo.
10.4. Descrivi l'algoritmo di consenso Proof of Work usato in Bitcoin.
10.5. Dato un indirizzo bitcoin come si può risalire alla quantità di Bitcoin disponibili per tale indirizzo?
10.6. Descrivi il ciclo di vita di una transazione in Bitcoin, da quando viene "richiesta" da un client a quando è confermata.
10.7. Descrivi l'attacco Sybil ad una rete Bitcoin.
10.8. Descrivi l'attacco 51% ad una rete Bitcoin.
10.9. Che significa che in Bitcoin possono esistere dei "fork"? come viene risolto il problema?
10.10. Bitcoin prevede che venga generato un blocco in media ogni 10 minuti circa. Che tecnica viene usata per mantenere approssimativamente costante tale frequenza?

Un valido esercizio è porvi delle nuove domande voi stessi.

Un compito da 4 cfu è composta da 5 o 6 domande, di cui 3 tendenzialmente teoriche e 2 o 3 in cui si deve risolvere un quesito con un tempo a disposizione tra i 45 e i 60 minuti. Ad esempio un compito potrebbe essere composto dalle seguenti domande

8.2 Analisi del rischio….
6.1 Hash crittografico
10.4 Bitcoin PoW
2.17 Considera la rete in figura con la matrice di accesso data. Mostra una configurazione….
1.10 Analizza la sicurezza nel codice C…
tempo a disposizione 45 minuti