Il seguente è un elenco di domande (assolutamente non esaustive e scritto un po' velocemente) su cui esercitarsi per l'esame.

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.** Fai un esempio di sql injection e spiegalo.
   - **1.6.** Fai un esempio di XSS e spiegalo
   - **1.7.** Fai un esempio di XSS persistente e spiegalo.
   - **1.8.** Fai un esempio di CSRF e spiegalo.
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 con la sintassi di iptables che sia equivalente a quella di un rouer-firewall di casa (tipo quelle dei router adsl).
   - **2.12.** Descrivi le problematiche di scalabilità dei firewall e le soluzioni possibili.
   - **2.13.** Descrivi le componenti principali di un IDS.
   - **2.14.** Descrivi le problematiche di scalabilità dei firewall è una soluzione possibile.
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.
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. Perfect forward secrecy: che garanzie dà? dai un esempio di protocollo dotato di PFS basato su un protocollo a chiave asimmetrica tipo RSA.
6.17. Diffie Hellman. A che serve? Come funziona? Che garanzie dà?

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. Contenuto di un DPS per conformità alla 192/2003
8.3. Analisi del rischio: principi, metodi di valutazione e metodi di mitigazione
8.4. Disaster recovery e business continuity.

Un valido esercizio è porvi delle nuove domande voi stessi.