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

Sicurezza dei sistemi informatici e delle reti – 07 febbraio 2011

Tempo a disposizione: 60 (DM509) o 70 (DM270) minuti.
Libri e appunti chiusi. Vietato comunicare con chiunque.
Vietato l'uso di cellulari, calcolatrici, palmari e affini.

Scrivi qui GRANDE 509 o 270

1. Considera il seguente codice C e rispondi alle seguenti domande.

```
int main(int argc, char** argv) {
      char b1[100];
      char b2[1000];
      b2[0]='\0'; /* init b2 with an empty string */
      scanf("%s", b1);
      for (int i=1; i<=20; i++)
          strcat(b2, b1);  /* copy b1 at the end of b2 */
      ...
}
```

1.1. Elenca i problemi di sicurezza che riscontri nel codice sopra riportato.

Scanf: %s non verifica la lunghezza del buffer b1 che è limitato
For(....) strcat(....): copia 20 volte b1 di lunghezza 100 in b2 di lunghezza 1000 provocando overflow.

1.2. Supponi che **`strcat(b2, b1)`** sia sostuito con **`strncat(b2, b1, 100)`** la sicurezza del codice è migliorata, peggiorata o è invariata? Spiega.

Invariata poiché al più 100 caratteri di b1 vengono concatenati a b2 ma questo avviene per 20 volte, per un totale potenziale di 2000 caratteri in b2.

1.3. Supponi che **`strcat(b2, b1)`** sia sostuito con **`strncat(b2, b1, 1000)`** la sicurezza del codice è migliorata, peggiorata o è invariata? Spiega.

Invariata poiché al più 1000 caratteri di b1 vengono concatenati a b2, vedi 1.2

1.4. Suggerisci delle modifiche per eliminare le vulnerabilità riscontrate

Sostituire **"%s"** con **"%99s"**: poiché b1 ha 100 byte di spazio si può leggere al più 99 caratteri.

La parte di codice **for(....) strcat(....)** non è coerente con **b2[1000]**, dipendentemente dalla semantica dell'applicativo si deve o allargare b2 con b2[2000] o cambiare il for con i<=9 ad esempio.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 07 febbraio 2011

2. Sicurezza dei sistemi UNIX

2.1. Descrivi sinteticamente la procedura di login (o grafica, o testuale, o via rete a tua scelta), la sua interazione con PAM e l'effetto sull'UID e sull'EUID.

Il login prevede di delegare a PAM la verifica delle credenziali. L'interazione con l'utente può essere delegata o gestita dal programma chiamante. Dopo l'autenticazione viene effettuato il cambiemnto di utenza per il processo e modificate UID e EUID in base all'utente che ha effettuato l'autenticazione. Viene quindi laciata una shell con tali credenziali.

2.2. Descrivi sinteticamente il ruolo del EUID nel controllo di accesso di una system call generica o puoi fare un sempio a tua scelta se vuoi.

EUID è l'identificatore di utente che viene considerato dal kernel per il controllo di accesso per ciascuna system call. Ad esempio per la verifica di accesso ad un file durante la syscall open() rispetto ai permessi del file stesso. EUID=0 significa permesso da amministratore, altrimenti si effettuano tutti i controlli.

2.3. Descrivi sinteticamente le vulnerability di syslog quando utilizzato via rete.

Quando syslog è usato via rete in architettura c/s, le richieste viaggiano in UDP non autenticati e non cifrati. Non è difficile quindi creare messaggi "fittizi" e saturare i log (aggirabile con ip-sec). Inoltre, è possibile impedire la ricezione di messaggi (vedi arp spoofing).

3. Considera un ambiente ospedaliero altamente informatizzato, in cui molti dei "servizi critici" (cartelle cliniche, controllo apparati medicali, tele-surgery, ecc.) sono basati su tecnologie informatiche e i vari sistemi sono in comunicazione tra di loro mediante reti IP. Si deve predisporre un piano di sicurezza, verrà dato un appalto ad una ditta esterna ma il tuo manager vuole capire le criticità al più presto.

3.1. Suggerisci una policy di 3-4 righe per il tuo manager che non è esperto di tecnologie.

Nella gestione della sicurezza informatica ospedaliera si considerano critici i seguenti aspetti
- Conformità alla normativa sulla privacy per dati sensibili, con particolare attenzione ai dati dei pazienti.
- Affidabilità e continuità di servizio della rete per il corretto funzionamento di apparati medicali e dei servizi di supporto al personale medico, con particolare attenzione ai servizi che hanno un impatto diretto sulla salute dei pazienti.

3.2. Quali sono i rischi più importanti che vedi, anche rispetto alla policy che hai dato e che suggerimenti dai per mitigarli.

La conformità dalla normativa può essere facilmente demandata ad una ditta esterna.
L'identificazione dei servizi critici per l'ospedale non può che essere fatta in cooperazione tra management, tecnici e personale medico. In particolare, una volta identificati i servizi critici e concordati i service level agreement, si devono considerare tutti gli aspetti tecnologici a supporto di tale servizio (connettività di rete, alimentazione elettrica, ecc) e proteggere e/o ridondare i vari elementi in modo da rientrare negli SLA.

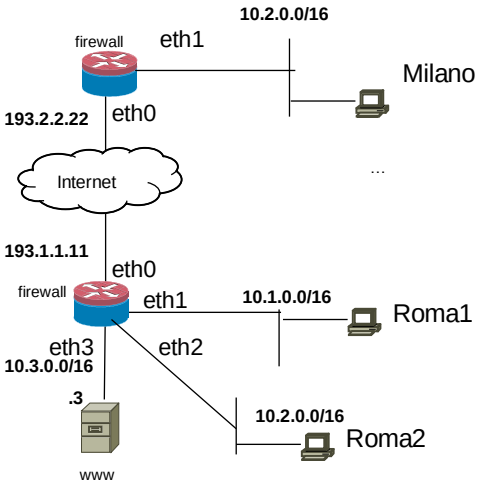
Cognome:_____ **Nome:** _____ **Matricola:**_____

Sicurezza dei sistemi informatici e delle reti – 07 febbraio 2011

3.3. Supponi che una ditta suggerisca per certi sistemi una certificazione Common Criteria EAL 4+ senza specificare null'altro, hai commenti da fare?

L'indicazione EAL 4+ misura la "profondita" con cui un certo prodotto/sistema è stato verificato per la conformità ad un certo security target (caratteristiche di sicurezza). Il security target è più importante di tale misura.

4. Considera la rete in figura.



Le due sedi di Roma e Milano appartengono alla stessa organizzazione ma ciascuna intranet è indipendente. Le interfaccie esterne dei due firewall (eth0) hanno indirizzo ip pubblico e staticamente assegnato dal provider. I due firewall fanno anche da nat. Milano deve poter accedere a www. Per fare questo, il firewall/nat di Roma è staticamente configurato per mostrare il server www con ip 10.3.0.3 su porta 80 come 193.1.1.11 su porta 80. **Www non deve poter essere visibile dal resto di Internet ma solo dalle macchine di Milano e Roma)**. Per il resto, le tre macchine di Roma e Milano devono poter accedere a Internet come iniziatori di comunicazione (di qualsiasi tipo) ma devono essere protette da attacchi provenienti da Internet, e non devono poter comunicare tra di loro. Www non deve poter inziare connessioni.

4.1. Mostra la configurazione dei firewall di Roma e Milano. Ignora il fatto che il firewall fa anche da nat e mostra solo le regole per il filtering.

Milano

:FORWARD DROP
-A -i eth1 -m state --state NEW -j ACCEPT
-A -i eth0 -m state --state ESTABLISHED -j ACCEPT

Roma

:FORWARD DROP
-A -i eth1 -o eth0 -m state --state NEW -j ACCEPT
-A -i eth2 -o eth0 -m state --state NEW -j ACCEPT
-A -i eth1 -o eth3 -m state --state NEW -j ACCEPT
-A -i eth2 -o eth3 -m state --state NEW -j ACCEPT
-A -i eth0 -o eth3 -s 193.2.2.22 --dport 80 -m state --state NEW -j ACCEPT
-A -m state --state ESTABLISHED -j ACCEPT

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

Sicurezza dei sistemi informatici e delle reti – 07 febbraio 2011

4.2. Discuti i rischi di avere www visibile sulla interfaccia esterna, anche se filtrato per accesso solo da Milano

Poiché IP non è autenticato, chiunque può spacciarsi per il firewall di Milano e riuscire ad inserire almeno un pacchetto (un syn) attraverso il firewall. Stabilire una sessione può essere più difficile perché i pacchetti di ritorno seguono il routing verso milano. Ma già il syn può essere usato per fare un DOS.

4.3. Supponi che l'organizzazione voglia aumentare la sicurezza del collegamento tra le sedi. Proponi una tecnologia per realizzare una VPN cifrata tra i due firewall.

Possibili tecnologie sono OpenVPN e IP-SEC ESP tunnel mode

4.4. Supponi di voler mantenere la stessa policy all'interno dell'azienda, cioè i pc di Roma e di Milano non devono poter comunicare tra loro. Ci saranno delle regole di filtraggio apposite. Secondo te, la VPN come viene specificata in tali regole?

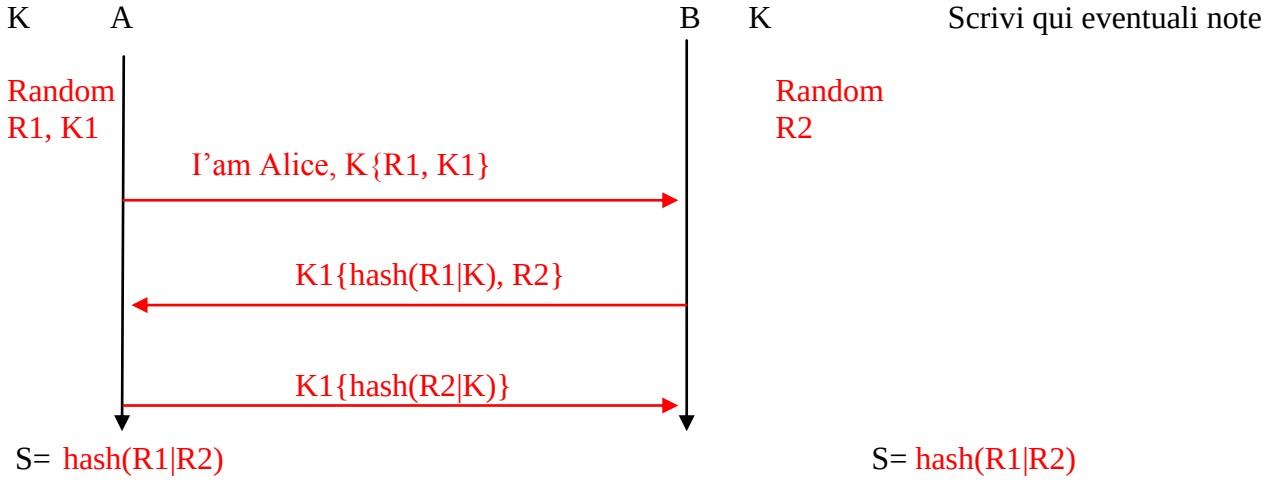
In tali regole la VPN verrà specificata con un nome di interfaccia (qualsiasi tipo di tunnel appare come una nuova interfaccia a livello IP). Il filtraggio con indirizzi IP sarebbe vulnerabile allo spoofing.

5. Alice e Bob hanno un segreto condiviso **K**. Mostra un protocollo di **mutua autenticazione** e scambio di chiave di **sessione** (**S**) che

- faccia uso di chiavi simmetriche (**K, K_1, K_2,** ecc.) e nonce (**R_1**, **R_2**, ecc.) ma non di chiavi asimmetriche,
- **non** sia vulnerabile ad attacco del tipo known plaintext
- usi il segreto condiviso **K per cifrare solo il primo messaggio**

Usa la notazione suggerita tra parentesi nel testo per chiavi e nonce.

Una possibile soluzione



6. [solo per 270] Strutture dati autenticate e sicurezza del cloud computing.

6.1. Per quanto riguarda la sicurezza, quali sono le principali differenze da tenere in considerazione tra servizi informatici in public cloud rispetto a medesimi servizi gestiti in proprio? **Dai una lista coincisa.**

In una public cloud non si può fare auditing delle procedure seguite dal service provider per rispettare le clausule contrattuali (es, SLA) e non si può fare forensic in caso di incidente, e alle volte è anche difficile dimostrare che c'è stato un incidente.

Alcuni aspetti critici sono i seguenti: adeguatezza delle precauzioni per confidenzialità e integrità dei dati, rispetto della normativa sulla privacy, adeguatezza dell'infrastruttura hw e sw per la disponibilità e la durabilità, procedure di accesso all'infrastruttura fisica, procedure per la gestione del software, la gestione di infrastruttura piattaforma e applicazione possono essere in capo a entità distinte.

6.2. Supponi di usare uno storage remoto e non fidato per un database. Supponi di avere una struttura di Merkle Hash Tree per la verifica dell'integrità. Supponi di memorizzare il basis direttamente nel servizio di storage, e solo li. Se un client vuole verificare l'integrità delle sue query che rischi corre ad usare tale basis? Spiega.

Il basis rappresenta l'hash dell'intera struttra dati nel suo stato in un certo istante. Quando lo stato cambia il basis cambia. Tenere il basis in uno storage non fidato rende possibile per l'attaccante sostituire basis e MHT con una versione differente (o precedente) ma comunque tra loro consistenti.

NOTA
Una possibile soluzione di compromesso è quella di affiancare un timestamp al basis e firmare la coppia. In questo modo siamo certi della "anzianità" del contenuto del MHT. Si può poi adottare una politica di aggiornamento periodico del timestamp del basis. C'è ovviamente un compormesso tra efficienza (frequenza dell'aggiornamento) e la possibilita di un attaccante di riportare indietro al struttura dati di un certo lasso temporale.