Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 07 febbraio 2011

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 07 febbraio 2011

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

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.

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.

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.

1.4. Suggerisci delle modifiche per eliminare le vulnerabilità riscontrate

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.

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.

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

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.

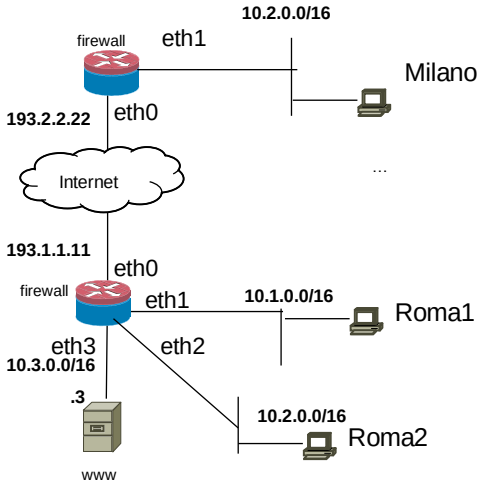
3.2. Quali sono i rischi più importanti che vedi, anche rispetto alla policy che hai dato e che suggerimenti dai per mitigarli.

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?

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

Roma

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

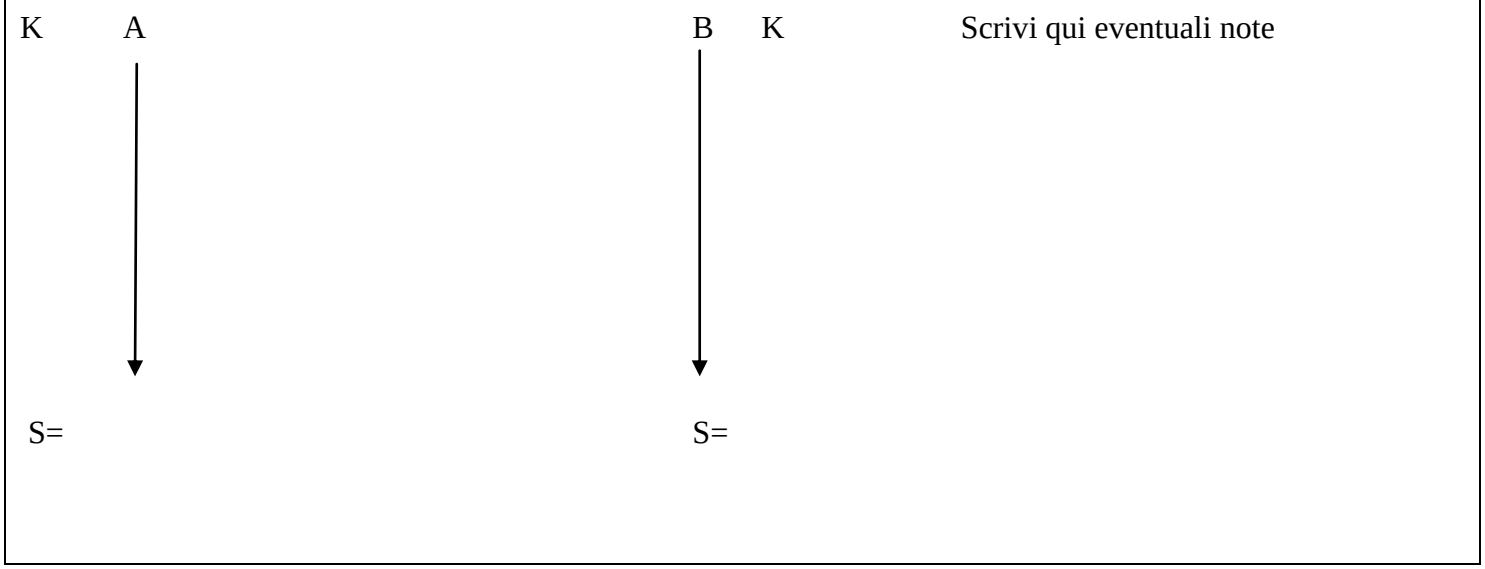
4.3. Supponi che l'organizzazione voglia aumentare la sicurezza del collegamento tra le sedi. Proponi una tecnologia per realizzare una VPN cifrata tra i due firewall.

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?

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.



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.**

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.