Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 27 settembre 2013

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 27 settembre 2013

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

Cognome:_____ Nome: _____ Matricola:_____

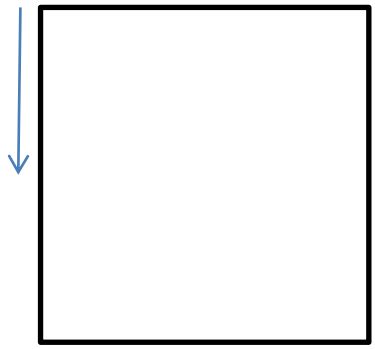
Sicurezza dei sistemi informatici e delle reti – 27 settembre 2013

Tempo a disposizione: 60 (5 cfu) o 70 (6 cfu) minuti. Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di cellulari, calcolatrici, palmari e affini.

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

```
int main(int argc, char** argv) {
      char command[1000];
      int i;
      strcpy(command,'/bin/cp');
      for( i=1; i<argc; i++) {
           strcat(command, " ");
           strcat(command, argv[i]);
      }
      system(command); /*esegue command come comando nella shell del sistema */
}
```

1.1. Mostra lo stack nel momento in cui avviene una delle chiamate strcat(command, argv[i]). Assumi che lo stack cresca verso il basso.



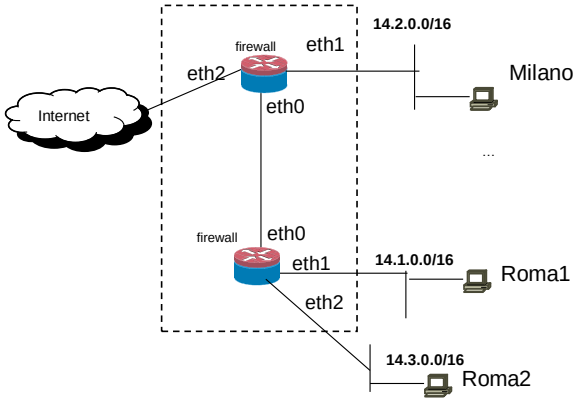
1.2. Elenca i problemi di sicurezza che riscontri nel codice sopra riportato e sottolinea le parti di codice coinvolte. Nel caso di buffer overflow indica il momento in cui l'attacco ha effetto.

1.3. Supponi di **non** poter cambiare il codice e di voler eseguire tale codice con input **non fidato**, che precauzioni prenderesti?

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

Sicurezza dei sistemi informatici e delle reti – 27 settembre 2013

2. Sicurezza delle reti. Considera la rete in figura.



Supponi che le tabelle di routing dei firewall siano correttamente configurate per assicurare la raggiungibilità completa, non ci sia alcun tipo di NAT e le configurazioni dei due firewall siano:

Milano

```
:FORWARD DROP
-A FORWARD -i eth1 -m state --state NEW -j ACCEPT
-A FORWARD -o eth2 -s 14.1.0.0/16 -m state --state NEW -j ACCEPT
-A FORWARD -i eth2 -d 14.3.0.0/16 -m state --state NEW -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

Roma

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

2.1. Mostra la matrice di accesso del sistema dei due firewall per traffico tcp/udp. Inserisci nelle caselle "Q" per richiesta, "R" per risposta o "-" per filtrato.

A / **Da**	Roma1	Roma2	Milano	Internet
Roma1	----------			
Roma2		----------		
Milano			----------	
Internet				----------

2.2. Secondo te è possibile violare la policy mediante spoofing degli indirizzi sorgente? Spiega.

2.3. Secondo te è possibile sostituire "–d 14.3.0.0/16" con altra direttiva che non coinvolge l'esplicita menzione della subnet mantenendo inalterato il comportamento del firewall?

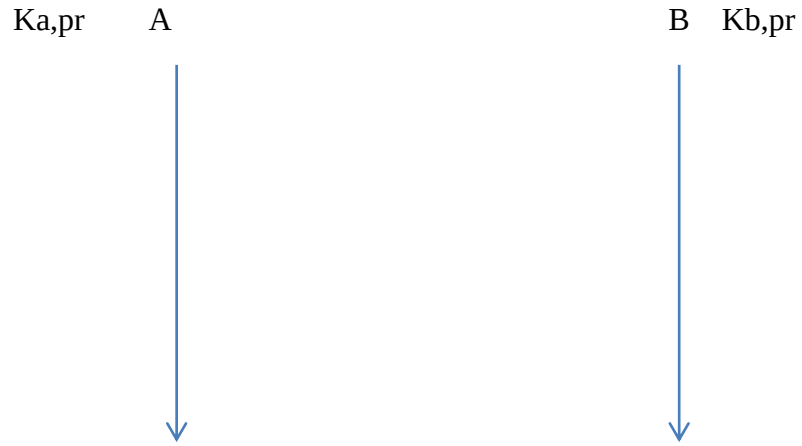
Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 27 settembre 2013

3. Perfect forward secrecy.

3.1. Che significa che un protocollo di mutua autenticazione e scambio di chiave di sessione è dotato di perfect forward secrecy?

3.2. Mostra un protocollo di mutua autenticazione e scambio di chiave di sessione dotato di perfect forward secrecy. Supponi che A e B siano dotati rispettivamente di chiavi private Ka,pr e Kb,pr e le corrispondenti chiavi pubbliche Ka,pub Kb,pub siano note a tutti.



3.3. Che accortezza bisogna prendere nella generazione delle chiavi effimere?

4. Sicurezza dei sistemi.

4.1. Descrivi brevemente 3 azioni di protezione tipiche di una attività di hardening.

4.2. Descrivi una tecnica per la replica dei log di sistema su un server apposito.

4.3. Il database degli utenti di una macchina deve contenere "in qualche forma" anche le password degli utenti. Che probelmi di sicurezza vedi? Che contromisure suggerisci.

5. Sicurezza in azienda. Ti viene chiesto di fare una consulenza per un laboratorio di calcolo universitario a cui gli studenti possono accedere per utilizzare dei pc. Il cablaggio prevede che le macchine, compresa una per l'amministrazione, siano attestate tutte sullo stesso switch (switch con supporto 802.1D, 802.1Q, ecc.). Devi progettare gli aspetti **tecnici e di processo** relativi al soddisfacimento della seguente policy.

a) Conformità alla normativa vigente per quanto riguarda la sicurezza dei dati personali.
b) Isolamento tra le macchine nel senso che un virus o worm su una macchina non deve avere alcun impatto sulle altre attraverso la lan.
c) In caso di segnalazioni da parte della polizia postale, deve essere possibile rintracciare l'utente che aveva in uso una macchina in un certo istante.

5.1. Cosa suggerisci per soddisfare il punto (a) della policy?

5.2. Cosa suggerisci per soddisfare il punto (b) della policy?

5.3. Cosa suggerisci per soddisfare il punto (c) della policy?

6. [solo per 270] Merkel Hash Tree (MHT).

6.1. Descrivi la struttura di un MHT.

6.2. Come è fatta la "prova di non esistenza" di un elemento? Come si fa a verificarla?

6.3. Supponi che un attaccante voglia sostituire un valore di una sola foglia con un altro. Cosa dovrebbe essere in grado di fare rispetto alla funziona di hash su cui si basa il MHT?