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

Sicurezza dei sistemi informatici e delle reti – 5 febbraio 2009

Tempo a disposizione: **60 minuti.** Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di cellulari, calcolatrici, palmari e affini.

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

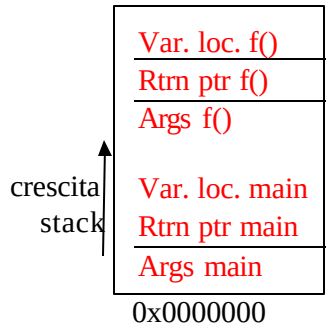
```
int main(int argc, char** argv)
{
char a[1000];
char b[100];
char *c;
c=getenv("CLASSPATH");
scanf("%s", b);
strncpy(a, c, 9999);
...
}
```

1.1. Sottolinea il codice che secondo te può dar luogo a problemi di buffer overflow e descrivi i problemi

scanf("%s", b); nessun controllo sulla lunghezza del buffer

strncpy(a, c, 9999); verifica la lunghezza del buffer ma a e' lunga 1000 bytes mentre la copia puo' essere di 9999 bytes.

1.2. Descrivi schematicamente il layout dello stack in una architettura in cui lo stack cresce verso l'alto.



L'ordine e' dettato dall'ordine in cui avvengono i seguenti eventi:
- preparazione dei parametri
- chiamata a funzione
- allocazione delle variabili locali

e dipende al paradigma di programmazione imperativo

1.3. Considera il o i buffer overflow per il codice mostrato in una architettura con stack che cresce verso l'alto. Per quale chiamata a funzione il return pointer può essere sovrascritto? Quali dati (variabili o altro) vengono sovrascritti dall'overflow?

chiamata a funzione?

Scanf e strncpy

dati sovrascritti?

Supponendo che l'allocazione delle variabili locali di main sia, in ordine crescente di indirizzo, a b c, allora
- nella chiamata a scanf si sovrascrive b, c, gli argomenti della scanf e quindi il return pointer di scanf
- nella chiamata a strncpy sovrascrive b, c, gli argomenti della strncpy e quindi il return pointer di strncpy

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 5 febbraio 2009

2. Rispondi alle seguenti domande su IP sec ESP.

2.1. Tunnel mode

schema di incapsulamento degli header vedi materiale didattico utilizzo tipico (schema e breve descrizione) vedi materiale didattico

2.2. Transport mode

schema di incapsulamento degli header vedi materiale didattico utilizzo tipico (schema e breve descrizione) vedi materiale didattico

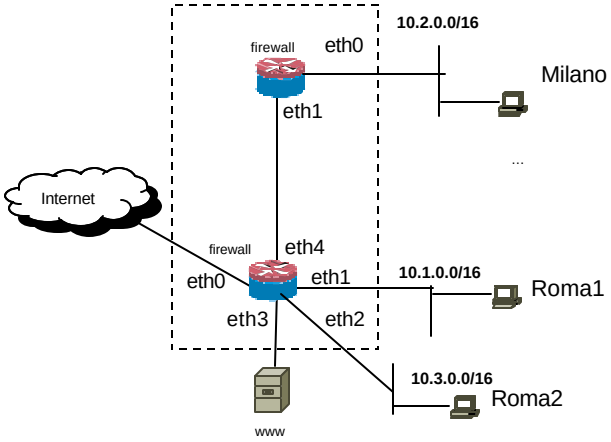
3. Supponi che sul data sheet di un prodotto vi è riportata la dicitura "certified Common Criteria eal 4". Ti viene chiesto di scrivere un rapporto sulla sicurezza di tale prodotto. Come procedi? Che documenti consulti? Perché? Compila la tabella e metti delle note eventualmente sia necessario.

Documento consultato.	Perche?
Target of Evaluation (nei documenti di certificazione del prodotto)	Per identificare quale versione del prodotto è certificata in quale configurazione
Security Target ed eventualmente il Protection Profile correlato (nei documenti di certificazione del prodotto)	Per verificare quali sono gli obiettivi di sicurezza che sono stati certificati e in quale "ambiente" di sicurezza.
Evaluation Assurance Level (nello standard CC)	Per verificare il livello di profondità con cui sono state effettuate le verifiche, di fatto à il significato della dicitura "EAL 4"
Note:	

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 5 febbraio 2009

4. Considera la rete in figura.



Supponi che le tabelle di routing dei firewall siano correttamente configurate per assicurare la raggiungibilità completa e le configurazioni dei due firewall siano le seguenti:

Milano

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

Roma

```
:FORWARD DROP
-A FORWARD -s 10.1.0.0/16 [eth1] -m state --state NEW -j ACCEPT
-A FORWARD -o eth3 -m state --state NEW -j ACCEPT
-A FORWARD -o eth0 -m state --state NEW -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

4.1. Mostra la matrice di accesso del sistema di firewall evidenziato dal tratteggio per traffico tcp/udp regolare, cioè senza spoofing. Iinserisci nelle caselle "Q" per richiesta, "R" per risposta o "-" per filtrato.

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

4.2. Considera traffico con **spoofing** di indirizzi. Considera la seguente matrice di traffico. Compila inserendo

- "S" dove il sistema di firwall non riesce a filtrare tale traffico in disaccordo con la politica
- "N" dove il sistema di firewall filtra correttamente
- "OK" dove il sistema non filtra ma ciò è previsto dalla politica

A / **Da**	Milano	Roma1	Roma2	www	Internet
Milano	----------	S	S	OK	OK
Roma1	N	----------	OK	OK	OK
Roma2	N	S	----------	OK	OK
www	N	S	S	----------	OK
Internet	N	S	S	OK	----------

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 5 febbraio 2009

4.3. Suggerisci le azioni che faresti sulla configurazione dei firwall per rendere il filtraggio più sicuro.

Specificare sempre nelle regole che prevedono un match sulla sorgente l'interfaccia di ingresso oppure inserire delle regole anti-spoofing negando le reti "interne" come sorgenti sulle interfacce esterne.

5. Ti viene chiesto di fare una consulenza per un Internet Café in cui il pubblico può accedere ad Internet dalle macchine del locale. Il cablaggio prevede che le macchine siano attestate tutte sullo stesso switch (switch di buona qualità con supporto 802.1D, 802.1Q, ecc.). La consulenza prevede che tu debba progettare gli aspetti tecnici e di processo relativi al soddisfacimento della seguente policy:

a) Conformità alla normativa vigente per quanto riguarda le norme antiterrorismo
b) Conformità alla normativa vigente per quanto riguarda la sicurezza dei dati personali
c) Isolamento tra le macchine nel senso che un virus o worm su una macchina non deve avere alcun impatto sulle altre attraverso la lan.

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

Bisogna
- identificare gli utenti con un documento di riconoscimento prima di consentirgli l'accesso ad Internet
- mantenere dei log degli accessi ad Internet degli accessi per eventuali future indagini.

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

I soli dati personali trattati riguardano le informazioni relative all'accesso degli utenti alle macchine e i log. Per le macchine in cui vengono tenuti tali dati si deve essere conformi all'allegato B della 196/2003 (password, antivirus, aggiornamenti, backup, ecc.). Redazione del DPS (molto semplice in questo caso).

Poiche' le macchine degli utenti possono contenere temporaneamente dati personali (es. documenti) si deve fare in modo che tali dati siano in qualche modo "tutelati" ma non trattati direttamente dall'organizzazione che gestisce l'Internet Cafe', infatti il loro trattamento non e' strettamente necessario per l'attivita'. Le macchine andranno quindi ripulite (ad esempio automaticamente) tra un utilizzo e il prossimo.

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

Oltre ad un antivirus e' possibile mettere ciascuna macchina su una VLAN separata. Se lo switch supporta funzionalita' anti-worm (conteggio del numero di connessioni attivate per unita' di tempo) possono forse essere utili ma questo puo' interferire con strumenti peer-to-peer (emule, skype. ecc)