Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 31 gennaio 2008

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 31 gennaio 2008

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 31 gennaio 2008

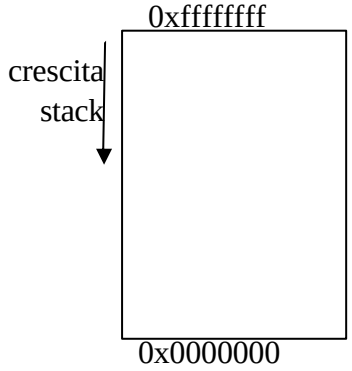
Tempo a disposizione: **60 minuti.** Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di cellulari, calcolatrici, palmari e affini.

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

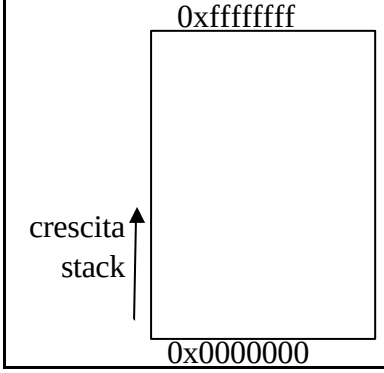
```
int main(int argc, char** argv)
{
char a[100];
char* c;
char* d;
c=getenv("PATH");
d= (char*)malloc(100);
scanf("%99", d);
strncpy(a, c, 1000);  /* copia da c in a */
…
}
```

1.1. Sottolinea il codice che secondo te dà luogo a vulnerabilità e descrivi schematicamente il problema.

1.2. Mostra un possibile layout di memoria per lo stack in una architettura in cui lo stack cresce verso il basso e elenca brevemente alcune delle difficoltà per sfruttare la vulnerabilità.



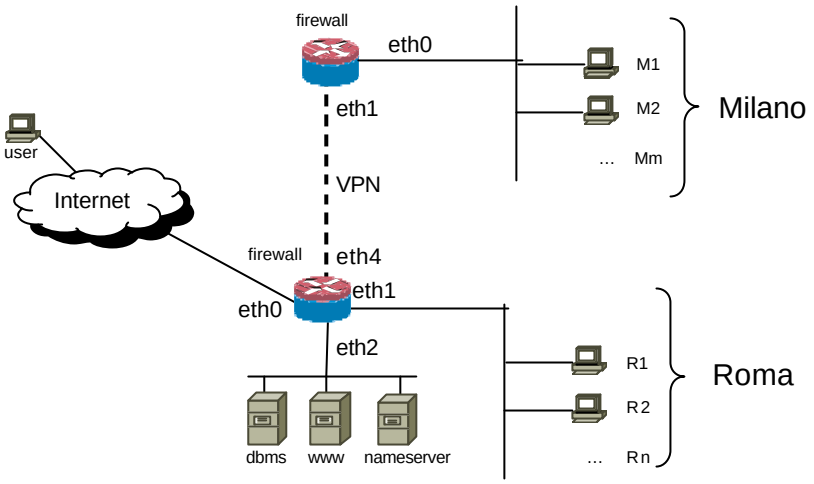
1.3. Considera una architettura con stack che cresce verso l'alto. Mostra il layout di memoria. Pensi che lo sfruttamento della vulnerabilità sia piu' difficile? Discuti brevemente.



2. Considera la rete in figura in cui i servizi di interesse sono tre: **dns, web, e db**.

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

Sicurezza dei sistemi informatici e delle reti – 31 gennaio 2008



A / Da	M1…Mm	R1…Rn	Dbms	www	Nameserver	Internet
M1…Mm	_____	-	-	?	?	Rich. web
R1…Rn	-	_____	-	?	?	Rich. web
Dbms	-	-	_____	Risp. db	?	-
www	?	?	Rich. db	_____	?	Risp. web
Nameserver	?	?	?	?	_____	?
Internet	Risp. web	Risp. web	-	Rich. Web	?	_____

Rispondi alle seguenti domande.

2.1. Gli utenti di Internet e le macchine M1…Mm di Milano e R1…Rn di Roma, devono poter accedere al sito www.securebank.com ospitato sulla macchina www specificando il nome (cioè usando il dns). La macchina "nameserver" è **autorità** per il dominio securebank.com. Completa le caselle della matrice di accesso che contengono "?", **applicando il principio del minimo privilegio**, in modo che l'accesso al sito web sia possibile.

2.2. **Evidenzia sulla matrice di accesso** le parti che non sono realizzabili per mezzo dei firewall.

2.3. Dai la configurazione del **firewall (stateful) di Roma**, usando preferibilmente la sintassi di netfilter, relativamente al **traffico tra le interfacce eth0 e eth2**. Al posto degli indirizzi usa i nomi delle macchine, al posto delle porte usa i nomi dei servizi (dbms, dns, www).

2.4. Supponi che la ditta, al fine di migliorare l'affidabilita' del collegamento ad Internet, decida di acquistare un collegamento anche per la sede di Milano con un ISP differente (con differente Autonomous System). **I firewall sono stateful**. Pensi che l'operazione possa essere compiuta senza precauzioni? Descrivi eventuali problemi ed eventuali soluzioni.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 31 gennaio 2008

3. Descrivi brevemente i concetti di “target of evaluation” e di “security target” in common criteria?

4. Rispondi alle seguenti domande circa l’utilizzo di metodi crittografici per la sicurezza delle trasmissioni.

4.1. Dai un protocollo di **mutua autenticazione e scambio di chiavi** basato su **challenge/response** e chiave **pubblica**.

4.2. Descrivi il concetto di “nonce” e il suo utilizzo nel contesto precedente.

4.3. I numeri casuali possono essere dei buoni nonce? Che precauzioni bisogna prendere?

(per questa risposta c’e’ altro spazio alla pagina successiva)

5. Rispondi alle seguenti domande circa la pianificazione della sicurezza.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 31 gennaio 2008

5.1. Descrivi sinteticamente le parti principali di un piano di sicurezza (una riga per ciascuna parte) **evidenziando** quali parti, secondo te, devono ricevere una **approvazione diretta dal management**.

5.2. Descrivi il rapporto tra Documento Programmatico di Sicurezza previsto dalla legge 196/2003 e il piano di sicurezza rispetto a obiettivi, contenuti e obbligatorietà.

	DPS	**Piano di sicurezza**
Obiettivi		
Contenuti		
Obbligatorietà		
Altro		