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.

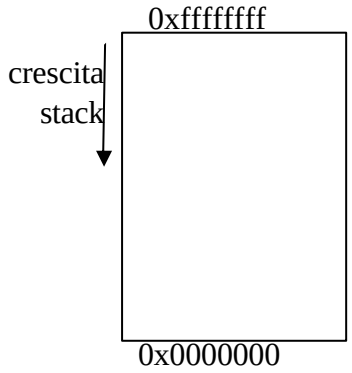
1. Considera il seguente codice C e rispondi alle seguenti domande.

```
int main(int argc, char** argv)
{
char a[100];
char* c;
char* d;
c=getenv("PATH");
d= (char*)malloc(100);
scanf("%99s", 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.

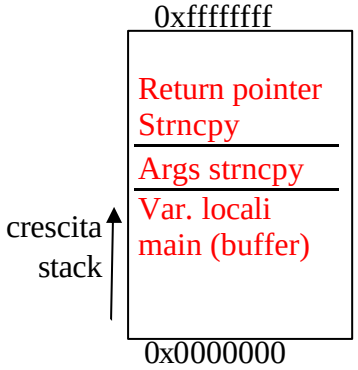
Strncpy copia fino a 1000 caratteri dalla stringa puntata da c al buffer a che è lungo 100 bytes. La stringa puntata da c può essere decisa da chi lancia il programma poiché è fornita in input mediante la variabile d'ambiente "PATH".

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.



Vedi materiale didattico

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.

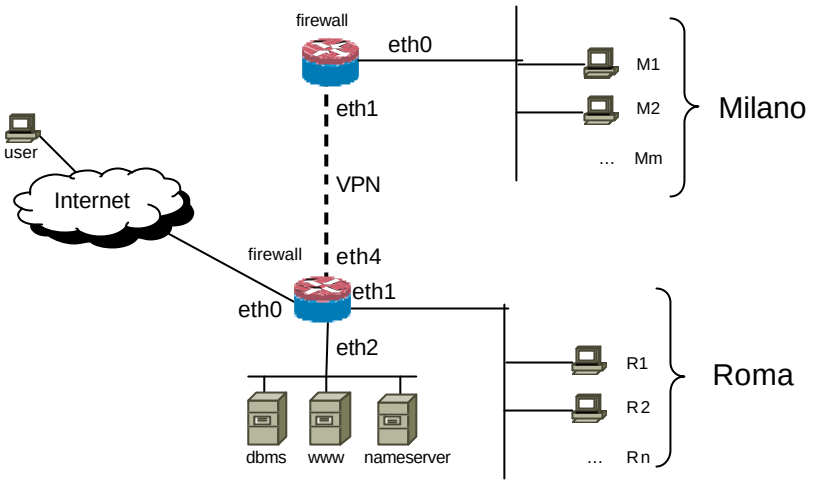


La vulnerabilità può essere sfruttata mediante la sovrascrittura del return pointer della funziona che sta riempiendo il buffer (scanf, strcpy, ecc.), infatti in questa configurazione il buffer si trova a indirizzi inferiori di quello di tale return pointer. Generalmente le difficoltà sono analoghe (forse leggermente più semplice poiché non si devono sovrascrivere le variabili locali della funzione che dovrà ritornare).

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

Sicurezza dei sistemi informatici e delle reti – 31 gennaio 2008

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



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

*questi elementi non sarebbero da togliere secondo il minimo privilegio ma il testo non lo richiedeva.

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).

```
:FORWARD DROP
-A FORWARD -i eth0 -o eth2 -p tcp -d www --dport www -m state --state NEW -j ACCEPT
-A FORWARD -i eth0 -o eth2 -p udp -d nameserver --dport dns -m state --state NEW -j ACCEPT
-A FORWARD -m state --state ESTABLISHED -j ACCEPT
```

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

Sicurezza dei sistemi informatici e delle reti – 31 gennaio 2008

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.

Problema: E' necessario che i pacchetti relativi ad una stessa connessione passino per lo stesso firewall.
Alcune possibili soluzioni:
- usare la seconda linea solo come backup in modo che solo un firewall sia attivo per volta. Per fare cio' e' necessario che su Internet il routing interdominio instradi sempre verso il firewall attivo (il firewall attivo deve annunciare la rotta in BGP, l'altro no o un less specific).
- usare il firewall di milano per la sede di milano e quello di roma per la sede di roma. In tal caso le due sedi devono avere due prefissi differenti e annunciati in maniera distinta su Internet. Tale soluzione non assicura backup.
- come sopra ma con backup. Si puo' annunciare su internet una less specific che verra' usata dai router quando non viene annunciata la rotta specifica. Si deve far in modo che i router/firewall facciano essi stessi l'annuncio della meno specifica (da entrambi) e della piu' specifica (ciascuno la sua).

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

Vedi materiale didattico

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**.

Un possibile protocollo:

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

Per il concetto di nonce: vedi materiale didattico.

Il nonce è usato come challenge. E' importante che i nonce usati come chanllenge siano usati una sola volta altrimenti l'autenticazione potrebbe essere vulnerabile ad un reply attack.

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

Un numero casuale è un buon nonce se il numero è scelto da un insieme abbastanza vasto e generato a partire da un "seed" non prevedibile e/o riproducibile. In tal caso con altissima probabilità ciascun numero verrà generato una sola volta

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 31 gennaio 2008

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

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**.

Vedi materiale didattico

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	Documentare le misure di sicurezza per i dati personali.	Documentare come l'organizzazione affronta il problema della sicurezza al fine ridurre rischi economici.
Contenuti	Dati personali, trattamenti, sicurezza dei trattamenti, responsabilità	Analisi e pianificazione della sicurezza ad ampio spettro secondo le necessità dell'organizzazione.
Obbligatorietà	Obbligatorio per legge 196/2003	Facoltativo
Altro		Può prevedere la redazione del DPS al fine di essere conformi alla normativa.