Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 2 luglio 2008

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 2 luglio 2008

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 2 luglio 2008

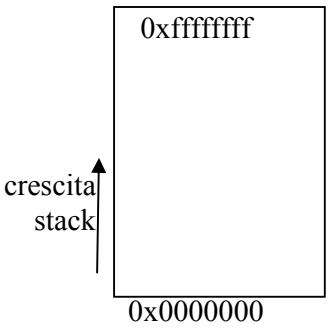
Tempo a disposizione: **60 minuti.** Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di cellulari, calcolatrici, palmari e affini.

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

```
int main(int argc, char** argv)
{
char a[101];
char* d;
getwd(a);    /* ottieni la directory corrente */
d= (char*)malloc(100);
scanf("%9999", d);
…
}
```

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

1.2. Mostra un possibile layout di memoria per lo stack in una architettura in cui lo stack cresce verso l'alto e elenca brevemente alcune delle difficoltà per sfruttare le vulnerabilità riscontrate al punto 1.1.

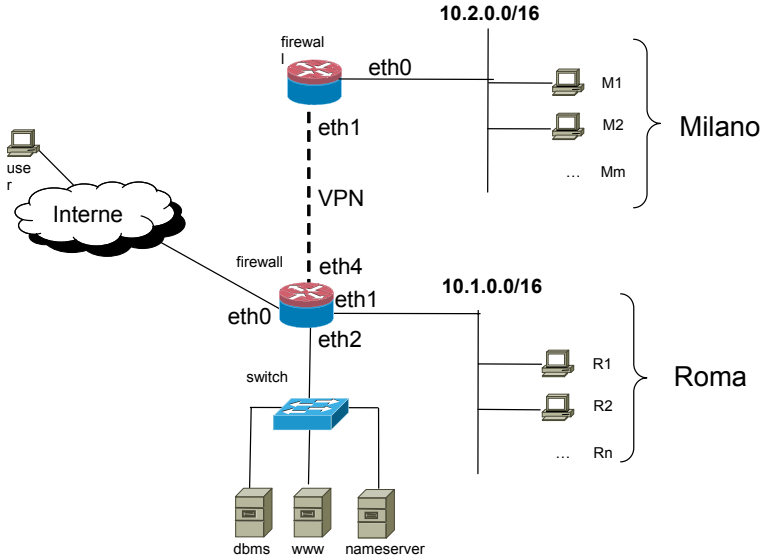


1.3. Considera le vulnerabilità identificate al punto 1.1, cosa dovrebbe fare un wrapper minimale per rendere impossibile un uso malevolo del software?

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

Sicurezza dei sistemi informatici e delle reti – 2 luglio 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	-	-	_____	Rich. & Risp. dns
Internet	Risp. web	Risp. web	-	Rich. Web	Rich.&Risp . dns	_____

Rispondi alle seguenti domande.

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

2.2. Dai la configurazione del **firewall (stateful) di Milano**, usando preferibilmente la sintassi di netfilter considerando la rete di Roma **non fidata**. Nella configurazione bada a prendere delle contromisure **anti-spoofing**. Al posto delle porte usa i nomi dei servizi (dbms, dns, www) e al posto degli indirizzi delle macchine i loro nomi.

(Altro spazio a pagina successiva)

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 2 luglio 2008

2.3. Considera le macchine www, dbms e nameserver a Roma. Il firewall e le macchine sono considerati affidabili, ma lo switch no. Mostra una topologia di rete per tale datacenter che sia tollerante al guasto di uno switch. Quali sono le spese maggiori che secondo te bisogna sopportare per passare dalla configurazione in figura a quella tollerante al guasto di uno switch? Discuti.

3. Rispondi brevemente alle seguenti domande sull'autenticazione nei sistemi UNIX.

3.1. Cosa è PAM?

3.2. Che vantaggi dà rispetto agli approcci tradizionali?

3.3. Descrivi il processo di login (es. tramite terminale, ssh, telnet, ecc.) di un utente in UNIX e mostra il ruolo di PAM?

4. Rispondi alle seguenti domande circa gli aspetti sociali della sicurezza informatica

4.1. Cosa si intende per social engineering (o social hacking)?

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 2 luglio 2008

4.2. Quali sono le vittime tipiche del social engineering?

4.3. In un piano di sicurezza, quali attività possono essere previste per contrastare il fenomeno del social engineering?

4.4. Nell'ambito di un auditing di sicurezza dei processi aziendali quali attività di verifica programmeresti?

5. Un insieme di utenti firmano regolarmente documenti mediante la loro chiave privata. Progetta un servizio T che permetta di sapere che un certo documento è stato firmato prima di un certo istante. Il servizio si può basare su una "autorità temporale" **A** di cui tutti gli utenti si fidano, ma **A** non deve venire a conoscenza del contenuto dei documenti firmati.