Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 8 febbraio 2010

Scrivi qui GRANDE 509 o 270

Tempo a disposizione: **60/70 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 dir[99999];
char *command;
scanf("%999999s",dir);
command=malloc(sizeof(dir)+20);
sprintf(command, "ls –l %s", dir);
system(command);
...
}
```

1.1. Descrivi i problemi di sicurezza che riscontri nel codice sopra riportato.

scanf("%999999s",dir);
legge più caratteri di quanti dir ne possa contenere.

sprintf(command, "ls –l %s", dir);
system(command);
esegue codice inserito dall'utente

1.2. Se tu fossi responsabile della sicurezza dell'esecuzione di quel codice ma non puoi cambiarlo, come ti comporteresti. Rispondi nei due casi in cui l'input è **fidato** e in cui l'input è **non fidato**

Input fidato

Nessuna precauzione

Input non fidato

Si dovrebbe effettuare un wrapping in modo da verificare l'input prima che questo sia processato.

1.3. Supponi di poter cambiare il codice, che cosa suggeriresti ai programmatori per migliorarne la sicurezza?

Correggere la scanf (o aumentare la taglia di dir[])
Considerare un altro modo per eseguire la lettura della directory che non sia quello di richiamare "ls" su suna shell oppure eseguire dei test molto stretti sull'input prima della creazione del comando.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 8 febbraio 2010

2. Considera il concetto di hash crittografico

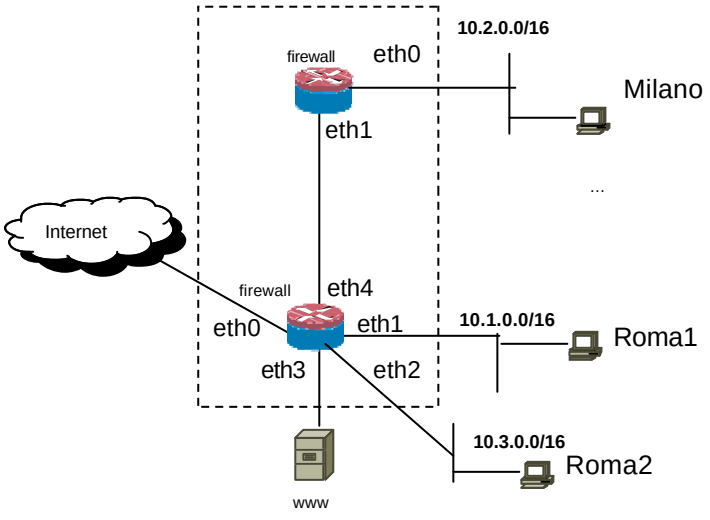
2.1. Descrivi l'attaco di tipo birthday, mostrando un esempio

Vedi materiale didattico

2.2. Descrivi l'attacco per mezzo di rainbow table e la struttura del database utilizzato.

Vedi materiale didattico

3. 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:

Milano

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

Roma

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 8 febbraio 2010

```
:FORWARD DROP
-A FORWARD -i eth1 -m state --state NEW -j ACCEPT
-A FORWARD -i eth2 –o eth0 -m state --state NEW -j ACCEPT
-A FORWARD -i eth4 –o eth3 -m state --state NEW -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

3.1. Mostra un 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**	Milano	Roma1	Roma2	www	Internet
Milano	----------	-	-	Q	-
Roma1	-	----------	Q	Q	Q
Roma2	-	R	----------	-	Q
www	R	R	-	----------	-
Internet	-	R	R	-	----------

3.2. Supponi di avere un secondo ISP presso milano. Ciascuna sede usa il suo ISP per tutte le comunicazioni. Nessuna ridondanza sul fault dell'ISP. Il link tra le sedi è usato solo per le comunicazioni tra le due sedi. Descrivi la configurazione del routine e del firewalling, o problemi che riscontrati che ne impediscono la realizzazione (ignora l'esistenza di www).

Routing: ciascuna sede annuncia su Internet le proprie rotte e in modo che il traffico di ritorno raggiunga ciascuna sede attraverso il firewall giusto.

Firewalling: configurazione stateful standard, ciascuna sede considera esterne le interfacce verso l'isp e fidato il traffico che proviene dal link tra le sedi.

3.3. Come sopra, ma Entrambe le sedi usano l'ISP di Roma se questo è disponibile, altrimenti usano l'ISP di Milano. Il link tra le sedi è utilizzato anche per l'accesso ad Internet dalla sede di Milano in situazione normale e da Roma in caso di backup. Descrivi la configurazione del routine e del firewalling, o problemi che riscontrati che ne impediscono la realizzazione (ignora l'esistenza di www).

Routing: ciascuna sede annuncia tutte le reti su Internet, ma da Roma le annuncia divise in "more specific". I due router si annunciano l'uno con l'altro la default (con priorità router di Roma, dettagli variano a seconda della tecnologia usata (rotte statiche o IGP o iBGP).
Firewalling: configurazione stateful standard, ciascuna sede considera esterna l' interfaccia verso l'isp, interna quella verso la sede e "ibrida" quella del link tra le sedi. Su quest'ultima, il traffico che viene dall'altra sede (ma non da internet) deve essere considerato interno. Ciò si può fare o mettendo una regola per indirizzi sorgenti (nel qual caso bisogna però inserire filtri anti-spoofing) o "dividendo" il link tra le sedi in due circuiti virtuali distinti (o due vlan), uno per il traffico da internet e uno per il traffico dall'altra sede.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 8 febbraio 2010

4. Documento Programmatico di Sicurezza e Piano di Sicurezza.

4.1. Confronta i due documenti

	DPS	**Piano di sicurezza**
Obiettivi	Vedi materiale didattico	
Contenuti		
Obbligatorietà		
Altro		

4.2. Descrivi, per ciascuno dei due documenti, quale è il rapporto con la normativa antiterrorismo specificando cosa i due documenti conterranno in relazione a tale normativa.

Rapporto con il DPS
Il dps conterrà dovrà considerare i trattamenti dei dati personali imposti dalla normativa antiterrorismo.

Rapporto con il Piano di Sicurezza
Il PdS considererà la conformità alla normativa e quindi anche alla legge antiterrorismo.

5. Descrivi le maggiori vulnerabilità degli switch e delle reti locali.

Vedi materiale didattico

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 8 febbraio 2010

6. **[solo per 270]** Descrivi le proprietà della struttura dati autenticata (ADS) Merkle Hash Tree e il metodo per produrre un **certificato** della **presenza** di un elemento in tale struttura e il metodo per produrre un certificato della **assenza** di un elemento in tale struttura.

MHT

Vedi materiale didattico

Certificazione della presenza di un elemento

Vedi materiale didattico

Certificazione della assenza di un elemento

Vedi materiale didattico