Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 18 febbraio 2014

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 18 febbraio 2014

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 18 febbraio 2014

Tempo a disposizione: 70 minuti. Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di smartphone, calcolatrici e affini.

1. **Protocolli crittografici.**

1.1. Fornisci un esempio di protocollo di autenticazione one-way vulnerabile a "replay attack".

A (client) B (server)

Descrivi l'attacco:

1.2. Fornisci un esempio di protocollo di mutua autenticazione vulnerabile a "reflection attack".

A (client) B (server)

Descrivi l'attacco:

2. **Confronta** il normale Piano di Sicurezza con il Documento Programmatico di Sicurezza.

	Piano di sicurezza	**Documento Programmatico di Sicurezza**
Obiettivi		
Obbligatorietà		
Contenuti		
Altro		

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 18 febbraio 2014

3. **Sicurezza del codice.** Analizza la sicurezza nei seguenti stralci di codice C relativi alla lettura di una stringa da standard input in cui la lunghezza della stringa è codificata in binario con due bytes all'inizio della stessa.

3.1.
```
int main(int argc, char** argv) {
        short len; /* intero di 2 bytes con segno */
        char buffer[100];
        read(stdin, &len, 2); /*legge l'intero direttamente in binario*/
        read(stdin, buffer, len);
        buffer[len]='\0';   /*termina con zero*/
        . . .
}
```

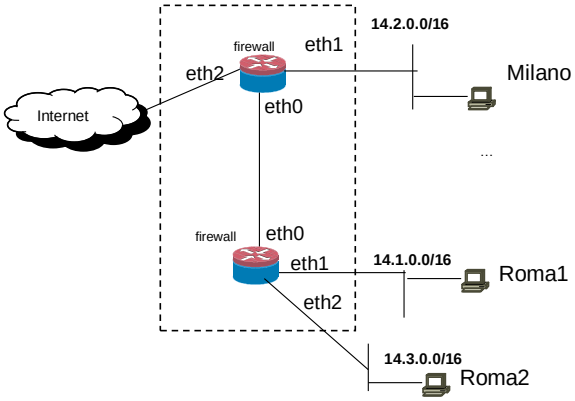
3.2.
```
int main(int argc, char** argv) {
        short len; /* intero di 2 bytes con segno */
        char buffer[100];
        read(stdin, &len, 2); /*legge l'intero direttamente in binario*/
        if ( len+1 > 100 ) {
              . . . /*gestione errore*/
        }
        read(stdin, buffer, len);
        buffer[len]='\0';   /*termina con zero*/
        . . .
}
```

3.3.
```
int main(int argc, char** argv) {
        short len; /* intero di 2 bytes con segno */
        char buffer[100];
        read(stdin, &len, 2); /*legge l'intero direttamente in binario*/
        buffer=malloc(len+1);
        read(stdin, buffer, len);
        buffer[len]='\0';   /*termina con zero*/
        . . .
}
```

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

Sicurezza dei sistemi informatici e delle reti – 18 febbraio 2014

4. Sicurezza delle reti. Considera la rete in figura.



Supponi che le tabelle di routing dei firewall siano correttamente configurate per assicurare la raggiungibilità completa, non ci sia alcun tipo di NAT e la configurazione del firewall di Roma sia la seguente.

Roma

```
:FORWARD DROP
-A FORWARD –i eth1 -m state --state NEW -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

4.1. Supponi di voler realizzare la seguente matrice di accesso per il sistema dei due firewall ("-" indica che non può passare traffico).

A / **Da**	Roma1	Roma2	Milano	Internet
Roma1	----------	Query	-	-
Roma2	Reply	----------	Reply	Reply
Milano	-	Query	----------	Query
Internet	-	Query	Reply	----------

Dai la configurazione del firewall di Milano per realizzare tale matrice di access, se possibile, o spiega perché è impossibile. (Usa preferibilmente la sintassi di iptables/netfilter).

4.2. Discuti l'impatto dell'eventuale presenza di costrutti tipo "–s 14.3.0.0/16" (match indirizzo ip sorgente) nella configurazione del firewall di Milano sulla sicurezza.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 18 febbraio 2014

5. Sicurezza dei sistemi. Controllo di accesso per il filesystem in Unix.

5.1. Il controllo di accesso per il filesystem in Unix è discrezionario o mandatorio? perché?

5.2. Considera la seguente configurazione di permessi e compila la matrice di accesso sottostante.

```
drwxr-xr-x      root root       /etc/
-rw-r--r--      root root       /etc/passwd
-rw-r-----      root shadow     /etc/shadow
drwxr-xr-x      root root       /etc/ssl/
drwx--x---      root ssl-cert   /etc/ssl/private/
-rw-r--r--      root ssl-cert   /etc/ssl/private/certificate
drwxr-xr-x      root root       /bin/
-rwxr-sr-x      root shadow     /bin/expiry
```

Nella matrice di accesso considera sempre che gli utenti accedono a file e directory tramite i propri processi che assumiamo essere lanciati dalla propria home. I diritti da indicare nella matrice di accesso sono i seguenti.

File: **R** (apertura file in lettura), **W** (apertura file in scrittura), **X** (esecuzione)

Directory: **L** lettura lista dei file, **A** aggiunta di un file, **D** cancellazione di un file, **S** usare la directory in un pathname specificato per una qualsiasi system call.

oggetto (file) → **soggetto (utente) ↓**		file: passwd	file: shadow	directory: /etc/ssl/	directory: /etc/ssl/ private/	file: certificate	file: expiry
utente	**gruppo**						
pippo	pippo						
shadow	shadow						
apache	ssl-cert						
root	root						

5.3. Commenta brevemente qui le tue risposte per le colonne relative a “private”, “certificate”, “expiry” e alla riga relativa a “root”.

private

certificate

expiry

root

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 18 febbraio 2014

6. Sicurezza in ambiente Windows. Security reference monitor.

6.1. Quali è l'output del security reference monitor?

6.2. Quali sono gli input del security reference monitor?

6.3. Riporta l'algoritmo applicato dal security reference monitor?