Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 15 febbraio 2017 – 6 CFU

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 15 febbraio 2017 – 6 CFU

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

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 15 febbraio 2017 – 6 CFU

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

1. **Sicurezza del codice.** Commenta 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.

1.1.
```
int main(int argc, char** argv) {
        unsigned short len; /* intero di 2 bytes senza segno */
        char buffer*;
        read(stdin, &len, 2); /*legge l'intero direttamente in binario*/
        buffer = malloc(len+1);
        read(stdin, buffer, len);
        buffer[len]='\0';   /*termina con zero*/
        . . .
}
```

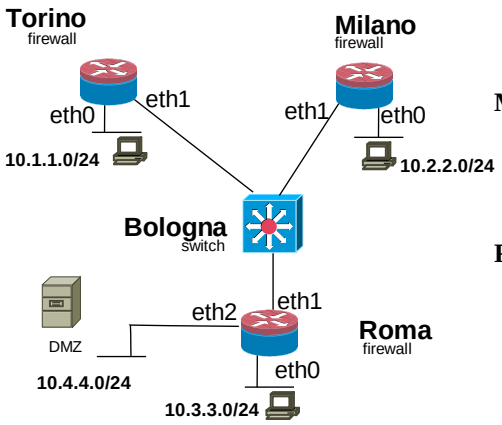
1.2.
```
int main(int argc, char** argv) {
        unsigned short len; /* intero di 2 bytes senza segno */
        char buffer*;
        read(stdin, &len, 2); /*legge l'intero direttamente in binario*/
        if ( len >= 65535 ) {
              . . . /* gestione errore */
        }
        buffer = malloc(len+1);
        read(stdin, buffer, len);
        buffer[len]='\0';   /*termina con zero*/
        . . .
}
```

1.3.
```
int main(int argc, char** argv) {
        short len; /* intero di 2 bytes con segno */
        char buffer[1000];
        read(stdin, &len, 2); /*legge l'intero direttamente in binario*/
        if ( len >= 1000 ) {
              . . . /* gestione errore */
        }
        read(stdin, buffer, len);
        buffer[len]='\0';   /*termina con zero*/
        . . .
}
```

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

Sicurezza dei sistemi informatici e delle reti – 15 febbraio 2017 – 6 CFU

2. Sicurezza delle reti. I firewall delle sedi di Torino, Milano e Roma sono collegate tra loro tramite uno switch come in figura e le loro configurazioni riportate a destra con la notazione usata da iptables.



Torino

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

Milano

```
:FORWARD DROP
-A FORWARD --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i eth1 –s 10.3.3.0/24 --state NEW -j ACCEPT
-A FORWARD -i eth0 --state NEW -j ACCEPT
```

Roma

```
:FORWARD DROP
-A FORWARD --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD –i eth0 –o eth2 --state NEW -j DROP
-A FORWARD –o eth2 --state NEW -j ACCEPT
-A FORWARD –i eth1 –s 10.2.2.0/24 --state NEW -j ACCEPT
-A FORWARD –i eth0 --state NEW -j ACCEPT
```

2.1. Mostra in forma di matrice di accesso la policy di sicurezza realizzata dalle configurazioni dei firewall. Indica con Q (Query) la possibilità di iniziare una comunicazione e con R (Reply) che è solo possibile rispondere ad una comunicazione iniziata dalla controparte.

a / da	Pc Torino	Pc Milano	Pc Roma	DMZ
Pc Torino				
Pc Milano				
Pc Roma				
DMZ				

2.2. Descrivi i problemi di spoofing che trovi nelle configurazioni date, specificando da quali sorgenti possono venire gli attacchi e verso quali destinazioni possono essere eseguiti con successo.

2.3. Dai una soluzione che prevenga i problemi di spoofing trovati al punto precedente cercando di minimizzare il numero di modifiche alla configurazione. Scrivi esplicitamente le configurazioni da aggiungere ai router di Roma Milano e Torino.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 15 febbraio 2017 – 6 CFU

3. Integrità. Rispondi alle seguenti domande.

3.1. Descrivi i principi su cui si basa il modello Biba.

3.2. Descrivi la strutura di un Merkle Hash Tree e la struttura della prova di autenticità del risultato di una query.

Struttura MHT

Prova di autenticità di una query.

4. Privacy.

4.1. Analogie e differenze tra i concetti di confidenzialità e privacy.

4.2. Elenca 5 prescrizioni della legge 196/2003.

1.

2.

3.

4.

5.

Cognome:_____ Nome: _____ Matricola:_____

Sicurezza dei sistemi informatici e delle reti – 15 febbraio 2017 – 6 CFU

5. Protocolli crittografici.

5.1. Descrivi il concetto di perfect forward secrecy.

5.2. Come fa una autorità in possesso dei segreti a lungo termine di A e B a intercettare il contenuto di una comunicazione tra loro? Mostra uno schema.

5.3. Supponi che A e B abbiano come segreto a lungo termine una chiave **simmetrica** K. Mostra un protocollo di mutua autenticazione e scambio di chiave di sessione che sia dotato di perfect forward secrecy.

6. Sicurezza di sistema in Unix. "sudo".

6.1. Dipendentemente dalla configurazione sudo chiede una passowrd. Di quale utente?

6.2. Perché è preferibile usare il comando sudo rispetto ad usare direttamente un utenza amministrativa (ad esempio acceduta con il comando "su")?

6.3. In quali casi una adeguata configurazione di sudo può sostituire efficacemente l'uso di un wrapper?