

**Cognome:** \_\_\_\_\_ **Nome:** \_\_\_\_\_ **Matricola:** \_\_\_\_\_

**Sicurezza dei sistemi informatici e delle reti – 18 luglio 2014**

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

**Cognome:** \_\_\_\_\_ **Nome:** \_\_\_\_\_ **Matricola:** \_\_\_\_\_

**Sicurezza dei sistemi informatici e delle reti – 18 luglio 2014**

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

Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

**Sicurezza dei sistemi informatici e delle reti – 18 luglio 2014**

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

**1. Sicurezza del codice.** Analizza la sicurezza nei seguenti stralci di codice C relativi alla esecuzione di un comando di copia i cui parametri sono passati come argomenti dell'eseguibile.

```
1.1. int main(int argc, char** argv) {
    char buffer[2000];
    int j;
    strcpy(buffer, "/bin/cp");
    for( j=1; j<argc; j++) {
        strcat(buffer, " ");
        strcat(buffer, argv[i]);
    }
    system(buffer); /*esegue il contenuto di buffer nella shell */
}
```

```
1.2. int main(int argc, char** argv) {
    char buffer[2000];
    if (strlen(argv[1])>1999)
        /*errore: argomento troppo lungo*/
    strcpy(buffer, "/bin/cp");
    strcat(buffer, argv[1]);
    system(buffer); /*esegue il contenuto di buffer nella shell */
}
```

```
1.3. int main(int argc, char** argv) {
    /* esegue cp con gli stessi argomenti e lo stesso ambiente del padre */
    execve("/bin/cp", argv, environ);
    /*environ punta all'ambiente corrente*/
}
```

Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

**Sicurezza dei sistemi informatici e delle reti – 18 luglio 2014**

```
1.4. int main(int argc, char** argv) {
    int j;
    if (argc>3)
        /*errore: troppi argomenti*/
    for( j=1; j<argc; j++)
        if(argv[j][0]=='-')
            /*errore: opzione per cp!*/
    execve("/bin/cp", argv, NULL); /*stessi argomenti ma ambiente nullo*/
}
```

**2. Sicurezza delle reti.**

**2.1. Descrivi il DDOS noto come syn-flood.**

Che caratteristiche ha il traffico che arriva all'obiettivo dell'attacco?

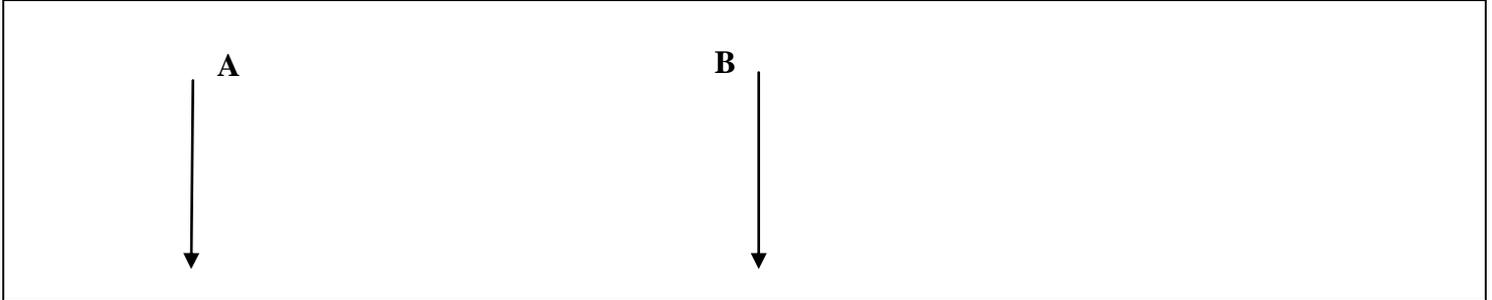
Quali sono le risorse saturate?

**2.2. Che ruolo può avere un firewall nella protezione dai syn-flood?**

**2.3. Descrivi una tecnica per effettuare load balancing su più firewall in modo che traffico relativo alla stessa connessione passi per lo stesso firewall.**

### 3. Protocolli crittografici.

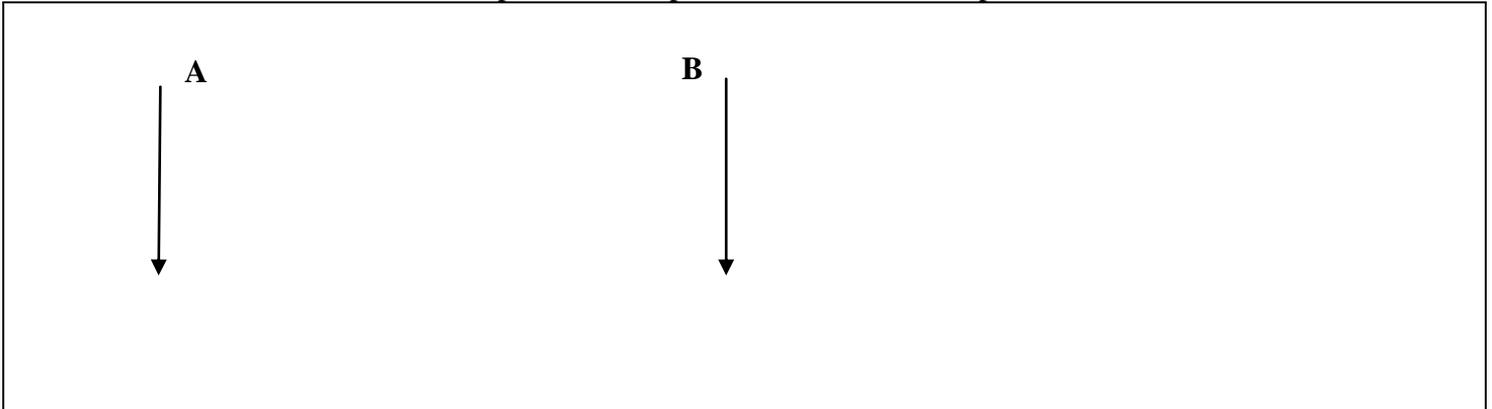
3.1. Supponi che un server B sia dotato di una chiave privata. Un client A, in possesso della relativa chiave pubblica, deve autenticare B. Mostra **il più semplice** protocollo di autenticazione basato sull'approccio challenge-response **in cui il server decifra il challenge**.



3.2. Considera il protocollo al punto 1. Che tipo di attacco crittoanalitico (tra ciphertext only, known plaintext, chosen plaintext) si può instaurare facendo solo richieste legittime a B?

3.3. Considera il protocollo al punto 1. Se un attaccante possiede un messaggio cifrato con la chiave pubblica di B e ne vuole conoscere il contenuto come può sfruttare B?

3.4. Fornisci una variante del protocollo al punto 1 che non abbia i problemi elencati.



### 4. Principi di progettazione

4.1. Progetto aperto. Perché è considerato un principio importante?

Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

**Sicurezza dei sistemi informatici e delle reti – 18 luglio 2014**

**4.2.** Default sicuri. Perché è considerato un principio importante?

**4.3.** Mediazione completa. Perché è considerato un principio importante?

**4.4.** Nell'ambito dei sistemi operativi come si realizza il principio di mediazione completa?

**5. Pianificazione**

**5.1.** Perché è importante avere un piano di sicurezza?

**5.2.** Quali sono gli obiettivi dell' "analisi del rischio"

Cognome: \_\_\_\_\_ Nome: \_\_\_\_\_ Matricola: \_\_\_\_\_

**Sicurezza dei sistemi informatici e delle reti – 18 luglio 2014**

**5.3.** In che rapporto è, in un piano di sicurezza, la parte relativa all'analisi del rischio con "l'analisi dello stato attuale" e con le "contromisure"?

Con l'analisi dello stato attuale:

Con le contromisure:

**6. Sicurezza in ambiente Windows.** Supponi di voler idealmente creare una matrice di accesso che rappresenti lo stato di sicurezza di un sistema Windows.

**6.1.** Cosa identificheresti come soggetti?

**6.2.** Cosa identificheresti come oggetti?

**6.3.** Che cosa identificheresti come diritti?