**Spiegare che cosa si intende per Servizio di Directory, quali funzioni svolge e quali tipi di elementi organizza. Descrivere inoltre, molto brevemente, come i Sistemi Operativi Linux e Microsoft implementino questo servizio**

Un servizio di directory fornisce amministratori di sistema con controllo centralizzato di tutti gli utenti e risorse di tutta la rete. Essi forniscono la capacità di organizzare informazioni e aiuta a semplificare la gestione fornendo un' interfaccia di rete standard per compiti di amministrazione del sistema.
Le risorse condivise sono pubblicate nella directory , gli utenti possono individuare e accedere senza mai sapere su quale macchina le risorse risiedano fisicamente. I file, directory e azioni a cui gli utenti accedono da un singolo punto , possono essere distribuite su più server.
Per operare all'interno di un NOS, servizi di directory diversi necessitano di disporre di un metodo comune di denominazione e riferimento ad oggetti , X.500 definisce l'Electronic Service Directory standard , e ha 3 componenti principali : Dsa , Dua , Dib.
DAP (Directory Access Protocol), gestisce le comunicazioni tra DUA e DSA, ma ha un elevato overhead(--> richiesta di risorse maggiore di quella necessaria)
LDAP è un sottoinsieme di DAP, supporta SSL (Secure Sockets Layer---->protocolli crittografi che permettono una comunicazione sicura dal sorgente al destinatario ), e Integra directory da diversi fornitori.
La struttura logica di Active Directory si basa su unità chiamata domini , infatti la rete di Windows 2000 può avere più domini, organizzati in dominii ad albero. Directory Active utilizza Unità organizzative (UO) per organizzare le risorse all'interno di domini.

**Con riferimento ai Sistemi Operativi analizzati durante il corso, descrivere come si possano avviare e terminare i servizi in Windows ed i daemon in Linux**

**Windows** : fornisce una schermata di controllo dei Servizi di Gestione attraverso il percorso Start> Programmi> Strumenti di amministrazione> Servizi , Fare clic destro su Risorse del computer> Gestione> in MMC, selezionare Servizi e applicazioni> Servizi.
Microsoft Management Console (MMC) permette gestione di reti, computer, servizi e sistemi componenti. I servizi vengono visualizzati in ordine alfabetico per nome , fornendo una descrizione di ciò che ogni servizio fa. L' obiettivi del MMC è quello di semplificare operazioni amministrative attraverso l'integrazione, delegazione, orientamento al compito, e in generale interfaccia semplificazione.

**Deamon** : Generalmente ci sono vari modi per gestire un demone su GNU/Linux: Manualmente tramite script di avvio e arresto forniti dall'init system , Permanentemente tramite script forniti dall'init system ; Tramite il superdemone xinetd ; Tramite script di avvio personalizzato.
Su Ubuntu gli script del sistema di init sono collocati nella directory /etc/init.d , e oltre a “start”, altre opzioni possibili sono stop, restart, reload, status, etc...
Tradizionalmente gli script di startup per Sys V sono posizionati nelle directory /etc/rc.d/init.d o /etc/init.d,e contengono link simbolici a questi script.
Quando un sistema GNU/Linux viene avviato ad uno specifico runlevel, questi link simbolici, associati al runelevel, assicurano l'avvio permanente di servizi, programmi e demoni.
I nomi dei link simbolici si presentano nella seguente forma: Kxxdaemon & Sxxdaemon (S per “Start” , K per “Kill” , xx per l'ordine di esecuzione)
I Super-server si pongono in ascolto di eventuali richieste di demoni o servizi. Si occupano di caricare un demone o un servizio solo dopo aver ricevuto una richiesta. Questo sistema permette di risparmiare memoria in quanto il demone viene avviato solo quando serve. I due super-server usati nelle distribuzioni GNU/Linux sono inetd.d e xinetd.d.
Volendo avviare un demone tramite un proprio script, basta aggiungere l'opportuno comando in /etc/rc.d/rc.local .
L'unico modo per terminare i processi avviati in questo modo è quello di usare il comando kill o killall dopo averne individuato il PID

## Descrivere i metodi di backup.

Il processo di backup implica la copia dei dati
da un computer ad un altro supporto di memorizzazione affidabile per custodirli. Una volta che i dati sono stati archiviati, il sistema amministratore può quindi ripristinare i dati nel sistema da qualsiasi backup precedentemente registrato. Fattori rilevanti per i dispositivi d'archiviazione sono : Costo , Size , gestibilità ,Affidabilità.
Ci sono quattro tipi di procedure di backup:
-Full - sarà il backup di tutto il contenuto del disco rigido (tutti i giorni)
-Parziale - esegue il backup dei file selezionati (al giorno)
-Incrementale - solo i file che sono stati modificati dopo l'ultimo backup verranno selezionati per il backup
-Differenziale - esegue il backup dei file creati o modificati dopo l'ultimo backup normale o incrementale.
Strategie di backup : quali file incorporare , che sia di rete o locale , con quale frequenza farlo , che metodi usare , che tecnologie adottare , ecc...

## Spiegare che cos'è l'attacco DoS, quali sono le varianti più note, e quali contromisure devono essere messe in atto per ridurne gli effetti.

U attacco Denial of Service (DoS) , si verifica quando il sistema preso di mira non ha un efficace servizio protezione di rete , infatti un attacco DoS comune è quello di sovraccaricare un sistema di destinazione con più dati di quelli che può gestire. Gli attacchi hanno origine da un host o un gruppo di host
Ci sono diversi tipi di attacchi DoS:
- attacco buffer overflow è stato progettato per sopraffare il software in esecuzione sul sistema di destinazione (buffer overflow).
- Il ping della morte è un buffer overflow ben noto. L'attaccante invia una richiesta di eco ICMP che sono illegalmente grandi al bersaglio. (carenze specifiche nel software NOS)
- L'attacco sincronizzazione (SYN) TCP , sfrutta il protocollo TCP , invia una grande volume di TCP , provocando un elevato volume di connessioni semiaperte.
- l'attacco Smurf si basa su spoofing del pacchetto IP. Normalmente le richieste di ping
esterni vengono negati e ammesse solo quelle interne , provocando inondazioni e sovraccarico della rete interna.

## Spiegare che cosa sono i runlevels di Linux, e come possono essere utilizzati nella fase di boot.

I runlevel controllano quale insieme di applicazioni verrà avviato al boot del sistema.
Tradizionalmente le configurazioni riguardanti l'ordine dei runlevel da eseguire al boot sono memorizzate nel file /etc/inittab.
Il processo di init legge tale file e imposta il runlevel
iniziale di conseguenza. Dopo il boot, i runlevel possono essere modificati
utilizzando i comandi init o telinit.
I runlevel sono numerati da 0 a 6 ognuno con una propria fase specifica , passare al runlevel 0 è un caso speciale poichè causa l'arresto della macchina. Il metodo consigliato per spegnere il computer è tramite il comando shutdown.
Importante sarà per verificare la configurazione del server X . Passare i livelli di esecuzione:

- Il livello di esecuzione 5 si avvia il server X automaticamente all'avvio
- Il passaggio a livello di esecuzione 3 (con il comando telinit 3) si spegne

## Spiegare brevemente a cosa servono e come si possono utilizzare i comandi fdisk, mkfs e fsck nei Sistemi Operativi che abbiamo affrontato durante il corso

**fdisk** = fdisk è un comando per creare/modificare/cancellare una partizione. Una volta apportate le modifiche alla partizione, un filesystem deve essere creato sulla partizione. Questo è indicato anche come la formattazione della partizione.
**mkfs**= comando per creare un filesystem in Linux. Una volta che i cambiamenti alla partizione sono stati fatti, un filesystem deve essere creata sulla partizione. Questo è indicato anche come formattazione del partizione.
f**sck**= comando che viene utilizzato per controllare i file system e riparare file danneggiati. Una buona pratica è quella di smontare un sistema prima di archiviarlo.
Utilizzare questo programma di utilità spesso per verificare integrità del file system. Se fsck effettua le modifiche, riavviare il sistema immediatamente.

## Descrivere i principali comandi messi a disposizione dai Sistemi Operativi di Rete della Microsoft per diagnosticare malfunzionamenti (ricerca e gestione dei guasti).

Gli strumenti di diagnostica di rete per Microsoft Windows includono i comandi :

- **ipconfig** viene utilizzato per visualizzare l'indirizzo IP, la subnet mask, e il gateway predefinito per i quali una scheda di rete è configurata.

- **nbtstat** è uno strumento per risolvere i problemi relativi alla risoluzione di nomi NetBIOS su TCP / IP
- **Nslookup** è uno strumento per test e la risoluzione dei problemi dei server DNS. Può essere eseguito in due modalità: interattiva e non interattivo.
- **Netdiag** esegue un serie standard di test di rete e genera un report dei risultati
- **pathping** è la combinazione del comando ping e il comando tracert.

## Descrivere quali comandi e/o strumenti di base del Sistema Operativo Linux possono essere utilizzati per ottenere funzionalità di firewalling

In ambienti ad alto traffico, la soluzione migliore d'adottare è il NAT , mentre in ambienti a basso traffico, come piccoli uffici e casa reti, una soluzione firewall NOS è una
buona scelta.
Linux può usare NOS come un firewall , composto da diverse funzionalità :
- netfilter è un componente del kernel di Linux che permette l'intercettazione e la manipolazione dei pacchetti che attraversano il computer (svolge funzioni di firewall).
- iptables è il programma che permette di configurare netfilter. Raggruppa tutti i controlli che può fare sul traffico in entrata nella cosiddetta INPUT Chain. I controlli sul traffico in uscita sono invece raggruppati nella OUTPUT Chain. La FORWARD Chain serve per il traffico non indirizzato a noi ma che comunque passa per il nostro computer.
Ognuna di queste catene ha una policy, cioè un'azione predefinita da eseguire quando tutti gli altri controlli della catena hanno fallito nel riconoscere se il dato era buono o meno. I valori di policy possono essere:
•ACCEPT lascia passare il pacchetto
•DROP scarta il pacchetto
•QUEUE dirotta il pacchetto nello spazio utente per un’analisi succ.
•RETURN viene eseguita la regola di default della catena

**Spiegare che cos'è il protocollo PPP, quali funzioni svolge in un collegamento per accesso remoto, e come può essere configurato.**

Point-to-Point Protocol (PPP) stabilisce una connessione TCP / IP collegando due computer utilizzando un modem.
Una connessione PPP è progettato per essere utilizzata solo per brevi periodi di tempo in quanto non è considerato una connessione internet "Always-on" .
Da riga di comando si possono eseguire delle operazioni :
-creare un accesso ai file ( /etc/ppp/pap-secrets or /etc/ppp/chap-secrets) ;
-Copy the files (ppp-on and ppp-on-dialer from /usr/share/doc/ppp-2.3.11/scripts)
- Edit this files with your ISP information
La configurazione di PPP può anche essere fatto dalla GUI utilizzando l'interfaccia grafica , la GUI PPP dialer che viene fornito con KDE è il KPPP dialer.

**Descrivere le possibili tecniche che si possono adottare in ambiente Linux per installare nuovi programmi o applicazioni dopo aver completato l'installazione del S.O.**

se si usa Linux Red-Hat 7.X, il file Linuxconf non viene aggiunto al sistema di default. Questo file può essere aggiunto dopo aver completato l'installazione di un gestore di pacchetti , Linux ne ha tre : RPM (x Red-Hat), Debian e tarball. Essi sono utilizzati per installare e rimuovere le applicazioni e programmi nei sistemi Linux dopo il processo di installazione
**Debian** contiene un database dei pacchetti che ha le stesse caratteristiche del database RPM, tuttavia, il Database di Debian è archiviato nella directory / var / lib / dpkg directory.
**RPM** è il tipo più popolare di gestore pacchetti. Esso fornisce gli strumenti necessari, come pacchetto banche dati che sono necessari per installare e rimuovere programmi, tuttavia, non tutte le applicazioni o programmi utilizzano RPM. Prestare attenzione alla compatibilità con RPM attraverso diverse distribuzioni.
**Tarball** sono di gran lunga il tipo più ampiamente supportato del pacchetto disponibile con Linux. Sono un insieme di file compressi che possono essere decompressi e installati su un sistema Linux (utilizzando l'utility qzip). Ogni distribuzione può usare tar per l'installazione o rimuovere le applicazioni e programmi, ma tarball non mantiene un database dei pacchetti (la rimozione del file più difficile) ; Tipicamente contengono file di Sorgente da compilare

**Descrivere le procedure da seguire per aggiungere un nuovo utente e un nuovo gruppo ad un sistema operativo Linux.**

L'utente più importante è rappresentato dall'account di root, chiamato anche superuser. Questo account permette di svolgere le attività di amministrazione del sistema. Nelle versioni recenti di Ubuntu non è presente , è infatti preferibile ricorrere al tool sudo ( root login , su , sudo , ...)
E' possibile aggiungere nuovi utenti in modo interattivo tramite il comando: sudo adduser username
La creazione di un utente è un processo che richiede numerose operazioni come la creazione della home directory e l'impostazione dei permessi di default.
Un amministratore per assegnare o modificare una password ad un utente deve utilizzare il seguente comando: sudo passwd username
Per rimuovere un account: sudo userdel username
Per rimuovere un account, la sua home directory e tutte le directory contenute: sudo userdel -r username
Per disabilitare un account utente senza rimuoverlo è sufficiente rimuovere manualmente la sua password di accesso. Le password sono memorizzate in un unico file: /etc/shadow
L'appartenenza degli utenti ai gruppi è definita dal file /etc/group
Per effettuare il log-in in un altro gruppo dopo l'accesso al sistema, si usa il seguente comando: newgrp **<group name>**
Per creare un nuovo gruppo: sudo groupadd **<group name>**
Il comando useradd è usato per aggiungere utenti a un gruppo , mentre il comando gpasswd permette di amministrare i gruppi attuali.
I permessi sui file e le directory sono gestiti tramite i comandi chown ( imposta l'appartenenza di un file a un determinato utente e gruppo) e chmod (vengono impostati i permessi relativi all'utente proprietario del file, al gruppo e a tutti gli altri ).

**Spiegare come si può mappare localmente un drive remoto nei due ambienti Windows e Linux.**

La mappatura del drive è uno strumento utile che consente ad un amministratore di condividere le risorse che sono memorizzati su un server. Richiede due passaggi: definire il percorso per la risorsa & assegnare un driver letter.
Dopo che l'utente identifica una risorsa di rete da utilizzare a livello locale, la risorsa può essere "mappata" come unità.

W: Per mappare un disco con Windows Explorer, accedere alla cartella sul sistema remoto in Esplora risorse di Windows selezionando Rete> direcrtory> Nome server> nome cartella condivisa.
Un altro modo per farlo è quello di scegliere il menu da Strumenti e quindi scegliere Connetti unità di rete.
Invece di unità di mappatura tramite Esplora risorse, il comando "net use" può essere utilizzato , ed anche incorporato in uno script di accesso che viene eseguito automaticamente quando l'utente si collega alla rete. Con un client Windows: è necessario il demone Samba caricato

L:
Per mappare un drive in un server Linux si usa il comando mount per stabilire una connessione alla directory condivisa sul server. La Local directory designata che punta alla remote share indicata con la prima parte del comando è chiamata il punto di mount di directory. La posizione mount point deve esistere già prima di una share che possa essere mappato ad esso , quindi si creerà la directory con il comando mkdir.

**Descrivere le principali caratteristiche della posta elettronica certificata.**

Posta Elettronica Certificata fornisce al mittente la certezza, a valore legale, dell'invio e della consegna (o meno) dei messaggi e-mail al destinatario.
Permette la trasmissione di tutti i tipi di informazioni e documenti in formato elettronico.
Si può accedere alla propri casella di PEC sia attraverso un client di posta elettronica che attraverso un browser prevede: livelli minimi di qualità del servizio e di sicurezza stabiliti dalla legge; certificazione dell'invio e della consegna del messaggio; l'opponibilità a terzi delle evidenze relative alle operazioni di invio e ricezione di un messaggio.
Importante è che sia il mittente che il destinatario devono utilizzare una PEC affinché il trasferimento sia legale
Fasi:
1.L'utente A invia una mail dal suo computer verso il proprio gestore PEC
2. Il gestore lo prende in consegna, verifica il messaggio e invia al mittente la ricevuta di accettazione
3. Chiude il messaggio in una busta di trasporto certificata e la invia al gestore PEC del destinatario
4. La Busta arriva al gestore del destinatario che invia una ricevuta di presa in carico
5. Il gestore del destinatario, invia il messaggio alla mailbox del destinatario
6.Invia poi la ricevuta di consegna al mittente
I protocolli in uso sono 'sicuri' e diversi dai normali (POP3s ed SMTPs)

**Quali sono i servizi tipici che vengono installati in un server Linux adibito a gestione di una piccola attività commerciale? Descriverne brevemente le funzionalità.**

•**Remote access** (PPP, ISDN, ADSL) : Con una connessione di accesso remoto, si può accedere ad un server da remoto e accedere alla rete con proprio account utente normale, si potrà quindi utilizzare tutte le risorse che sarebbero disponibile dal computer desktop.
I metodi di connessione più conosciuti sono PPP(Point-to-Point Protocol che stabilisce una connessione TCP / IP collegando due computer utilizzando un modem) , ISDN (Invece di usare un modem per la connessione a un computer remoto, ISDN utilizza un terminal adapter) , ADSL(connessione banda larga).
• **Samba** : Il protocollo permette ad un client Windows di operare in una rete Linux come se si trovasse all'interno di una rete di sistemi Windows.
• **NIS**(Network Information Service) : Linux utilizza la propria versione dei servizi di directory chiamata Network Information Service (NIS).

• **LDAP** : è un sottoinsieme di DAP, supporta SSL (Secure Sockets Layer =protocolli crittografi ci che permettono una comunicazione sicura dal sorgente al destinatario ), e Integra directory da diversi fornitori.
• **file-sharing** : la condivisione di file all'interno di una rete domestica o di una azienda si basa su finestre di condivisione file o protocolli condivisione file. La condivisione su internet è spesso fatta utilizzando il FTP , esiste anche la tecnologia P2P , ma ancora non sviluppata da un punto di vista aziendale.
• **FTP** : Molte organizzazioni rendono i file disponibili da remoto per impiegati, clienti e al pubblico in generale attraverso File Transfer Protocol (FTP). I server FTP possono essere configurati per consentire l'accesso anonimo.
• **DNS** : il domain name service protocol traduce in un nome internet un indirizzo IP , i nomi degli host e dei dns che il computer system esegue sono tutti collegati fra loro
• **DHCP** : Dynamic Host Configuration Protocol consente ai computer su una rete IP di ricevere configurazioni rete dal server DHCP. Questi server non dispongono di informazioni sui singoli computer fino a quando le informazioni non vengono richieste. DHCP consente anche il recupero e la capacità di rinnovare automaticamente gli indirizzi IP di rete attraverso un meccanismo Leasing. Questo meccanismo assegna un indirizzo IP per uno specifico periodo, terminato questo verrà assegnato un nuovo indirizzo IP.

**Spiegare, aiutandosi con qualche esempio, che cosa eseguono i seguenti comandi Linux:**

· **ls** : Lo scopo di tale comando è quello di visualizzare il contenuto della directory corrente.
L'opzione -d elenca le proprietà della directory , l'opzione -l produce un elenco esteso della directory , ecc....
· **grep** : questo comando permette la ricerca di un determinato pattern all'interno di una lista di file. Per effettuare la ricerca di una stringa all'interno di uno o più file, è necessario includere tale stringa fra singoli apici
· **awk** :permette di processare file, ordinare i dati, eseguire operazioni aritmetiche e molto altro. L'utility awk esegue la scansione di un file di input riga per riga alla ricerca di patterns che facciano il match con quelli passati da command line. Nel caso in cui si verifichi un match, awk avanza nella sequenza di programmazione, altrimenti processa la riga successiva del file di input.
· **find** : è usato per trovare la posizione all'interno del file system di una risorsa, supponendo di conoscere almeno parzialmente il suo nome. E' possibile specificare opportuni filtri nella ricerca ed
eseguire comandi attraverso tutto l'albero delle directory.

**Elencare e descrivere molto brevemente quali operazioni si devono eseguire per assemblare un PC.**

· Aprire il case ed installare tutte le prese di corrente
· Attaccare i componento alla scheda madre (CPU, RAM,...)
· Installare la scheda madre inserendola nel case e facendo combaciare tutti i vari collegamenti
· Installare i drive interni (Hard Disk)
· Installare i driver esterni (optival drives, tape)
· Installare le varie schede (video, sonora) , stando attenti a far combaciare tutti i piedini con quelli del case
· Connettere i cavi interni di ogni periferica (power, data: PATA, SATA)
· Connettere i cavi delle periferiche esterne (keyboard, mouse, monitor, Ethernet, power)
Verificare che tutto sia funzionante. Il passo successivo sarà quello di occuparsi della configurazione del Boot

**Elencare e descrivere brevemente le cause dei più comuni attacchi informatici classificati come interni (inside threads) a cui è tipicamente soggetto un sistema informatizzato, e quali sono le più elementari tecniche di protezione adottate**

Le minacce alla sicurezza che hanno origine all'interno di una rete possono essere più dannose di quelle minacce esterne.
Le minacce di alto profilo interne includono comportamenti sleali di dipendenti scontenti che utilizzano il loro accesso per distruggere, rubare, o manomettere i dati.
Lo spionaggio industriale è il tipo più sofisticato di minaccia interna alla sicurezza , dove i dipendenti possono essere avvicinati da aziende concorrenti.
Un problema in crescita per le reti aziendali è la diffusa popolarità della messaggistica istantanea e condivisione di file peer-to-peer , chat e applicazioni di condivisione possono essere vulnerabili ad altri forme di sfruttamento.
Oltre ad una politica di sicurezza ben pianificata, le organizzazioni dovrebbe fornire programmi di formazione per tutti i dipendenti che utilizzano la rete. Dal momento che i dipendenti sono spesso presi di mira come un modo per invadere la rete intranet, è importante istruirli su come prevenire i virus, attacchi DoS, furto di dati e così via. Il danno è più probabile che si verifichi per incompetenza

**Scrivere uno script per ambiente Linux che legga tre variabili intere immesse da tastiera (non da linea di comando) e ne visualizzi la maggiore.**

```
#!/bin/bash
# ricerca del massimo tra tre valori interi
#
echo –n 'Scrivi un intero: ' ; read num1
echo –n 'Scrivi un secondo intero: ' : read num2
echo –n 'Scrivi un terzo intero: ' : read num3
let max=$num1
if [ $num2 > $max ] ;then
  let max=$num2; fi
if [ $num3 > $max ] ; then
  let max=$num3; fi
echo Il massimo è $max
```

**Uno dei principali sistemi per garantire la sicurezza nella gestione e nel trasferimento dei dati è sicuramente la cifratura delle informazioni. Descrivere brevemente la tecnica che adotta chiavi simmetriche e quella con chiavi asimmetriche, specificandone vantaggi e svantaggi e quale tecnica alternativa si adotti maggiormenti nei nostri giorni.**

La crittografia dei file è un modo di crittografia dei dati memorizzati su un disco in modo da risultare illeggibile a chiunque, tranne che per il creatore della dati.
●**DES** è un cifrario a blocchi, agisce su un blocco di lunghezza fissa di testo in chiaro (64 bit) e lo converte in un blocco di testo cifrato della stessa dimensioni utilizzando la chiave segreta. La lunghezza della chiave efficace nel DES è a soli 56 bit. Noto come un cifrario a chiave simmetrica perché la stessa chiave viene utilizzata sia nella crittografia e decrittografia.
•**3DES**: è un sistema di crittografia in grado di crittografare e decrittografare i dati utilizzando una singola chiave segreta. La lunghezza di chiave 3DES è 168 bit poiché 3 fasi di DES con una chiave separata per ogni fase.
Ci sono due tipi di cifratura :
**Cifratura simmetrica** = Molti sono i possibili schemi di cifratura utilizzati: DES, 3DES, AES, RC4, IDEA, … In generale, la forza di uno schema di cifratura dipende dalla lunghezza della sua chiave (perchè la ricerca della chiave risulta più complessa).
**Cifratura asimmetrica** = Ciascun utente ha una chiave pubblica K e una chiave privata K-1 , quest'ultima deve essere mantenuta segreta, non va comunicata a nessuno, e non può essere dedotta da K che è pubblica e disponibile a tutti
La cifratura e decifratura con le chiavi K e K-1 sono commutative.

**Descrivere i compiti dell'Amministratore di Sistema, individuandone Capacità, Requisiti e Responsabilità**

Un amministratore di Sistema deve avere capacità , requisiti validi e retaggio alla responsabilità

***Capacità:***

Di base deve *saper spiegare semplici procedure informatiche istruendo utenti su applicazioni di base , buona conoscenza del S.O. e della sua gestione , e non da meno di vari linguaggi di programmazione. Col tempo acquisirà la capacità di gestione acquisti e configurazione del sistema e dei servizi. Una volta esperto potrà lavorare a stretto contatto con la Direzione.*

**Requisiti**

*Diploma in Informatica con il surplus di una Laurea specialistica magari particolare* , e sicuramente qualche *anno di esperienza*

***Responsabilità:***

*nterfacciarsi con gli utenti , Amministrazione di piccoli sistemi informatici che col tempo potranno divenire di medio/grande dimensioni , gli verranno sottoposti quesiti di mercato a cui dovrà rispondere sapientemente , e avere un ottima politica sugli acquisti.*

**Elencare le fasi elementari che si devono seguire per installare il Sistema Operativo Linux.**

Bisognerà seguire i seguenti passi :

- *Scegliere il sistema di boot più adeguato*
- *Selezionare gli appropriati parametri per l'installazione*
- *Creare ed allocare il file system di Linux (quindi fare un partizionamento)*
- *Selezionare i pacchetti da installare*
- *Installare x-server (opzionale , ma consigliato)*
- *Configurare le opportune impostazioni di sicurezza (account root/amministratore)*
- *Configurare le impostazioni di rete*
- *installazione di pacchetti aggiuntivi nel postinstallazione*
- *Installare e configurare il boot loader*

**Realizzare uno script bash che, in fuzione dei parametri passati tramite linea di comando, esegua il `ping`, l'`ftp` o il `telnet` all'indirizzo IP passato anch'esso tramite linea di comando. Si preveda che, in assenza di argomenti aggiuntivi, lo script visualizzi una riga di help indicante la modalità d'uso dello script**

```
#!/bin/bash
# nome file: multitest
# esegue funzioni diverse in base all'opzione indicata
# provare con $ multitest
# provare con $ multitest --f 127.0.0.1
# provare con $ multitest --p 127.0.0.1
# provare con $ multitest --t 127.0.0.1 21
# provare con $ multitest --help
case $1 in
  --t) telnet $3 $2 ;;
  --f) ftp $2 ;;
  --p) ping $2 ;;
  --help|*)
 echo "Uso: $0 [--help] [--t <IPaddr> <port>] [--p <IPaddr>] [--f <IPaddr>]" ;;
esac
```

**Descrivere a cosa servono, con che S.O. si possono richiamare e come si utilizzano i comandi ifconfig e netstat.**

[linux] **Ifconfig** : è lo strumento utilizzato per impostare e configurare la scheda di rete. Il comando ifconfig può essere immesso nella shell per riportare la configurazione di interfaccia di rete corrente del sistema. La sintassi dei comandi prevede le seguenti opzioni :
Per avere un elenco più sintetico: ifconfig -s
Per attivare/disattivare una interfaccia: ifconfig eth0 up/down
Per assegnare un indirizzo IP / subnet mask: ifconfig eth0 192.168.1.3 netmask 255.255.255.0
Per vedere tutte le interfacce, anche quelle non attive: ifconfig -a

[Windows&Linux] **netstat** : L'utility netstat visualizza tutte le connessioni TCP attive, le porte su cui il computer è in ascolto, statistiche Ethernet, la tabella di routing IP, le statistiche IPv4 e le statistiche Ipv6.
Il comando può agire con varie opzioni : opzione -a permette di vedere i socket non visualizzabili , opzione -t permette di vedere lo stato dei socket tcp , opzione -u permette di vedere lo stato dei socket udp , opzione -n mostra indirizzi numerici host , opzione -p permette di vedere nome e pid dei programmi che hanno instaurato una connessione.

**Descrivere che cosa sono e come si utilizzano i bit di permessi SUID e SGID implementati in ambiente Linux**

**SUID** : modifica l'ID dell'utente che esegue il file. Se un file ha il bit SUID attivato, quando il file verrà eseguito da un qualsiasi utente, il relativo processo avrà gli stessi diritti del proprietario di quel file. diritti del programma in esecuzione : proprietario (SUID=1) o esecutore (SUID=0)
**SGID** : modifica l'ID del gruppo che esegue il file. ID del gruppo del proprietario (SGID=1) o del gruppo dell'esecutore (SGID=0)

Quindi assegnare i permessi per i processi vengono eseguiti utilizzando il SUID (Set User ID) o SGID (Set Group ID) bit, che permette di eseguire il programma con l'autorizzazione di chi è proprietario del file, invece che con i permessi d"utente che esegue il programma.

**Spiegare che cos'è uno script in ambiente Linux, proporne uno qualsiasi e commentarlo. (mod 4° - Amministrazione di Linux e slides Scripti ng di Shell)**

Le distribuzioni GNU/Linux permettono una vasta scelta di linguaggi di scripting. Il sistema più diffuso e integrato per eseguire script è tramite le funzionalità fornite dalla shell. Uno shell script è un file testuale che contiene un numero variabile di comandi scritti in successione. Ogni comando viene eseguito esattamente come se fosse stato inserito nel prompt. Tali script possono contenere logiche di programmazione come loop, condizioni, etc.
Durante il corso abbiamo visto i seguenti comandi :

- echo
- read
- let
- if – then – elif – else – fi
- case – esac
- operatori numerici, booleani, sulle stringhe
- do - done
- for e while
- whiptail
- più i comandi tipici da console

**Quali sono le principali funzioni di un kernel di Sistema Operativo in ambiente Linux? Perché un amministratore dovrebbe ritenere utile ricompilarlo?**

Kernel di un sistema operativo fornisce funzioni quali la gestione della memoria, di basso livello , driver hardware (esclusi i driver video X e i driver di stampa), la programmazione quando i processi specifici ottengono l'accesso alla CPU, consentono programmi di accesso alla rete, e controlli l'accesso al il file system su un disco rigido.
Un amministratore deve assicurarsi che la versione del kernel sia up-to-date.
Alcuni amministratori preferiscono Linux per compilare il loro Kenel proprio da codice sorgente, per cosi ottenere diversi vantaggi: Ottimizzazione del kernel per le massime prestazioni della compilazione per la CPU ; Individual driver configuration, selezionando quali driver sono aggiungere; Capacità di applicare la patch.

**Descrivere le principali caratteristiche delle possibili architetture di una rete Wireless, e le funzioni essenziali di un Access Point.**

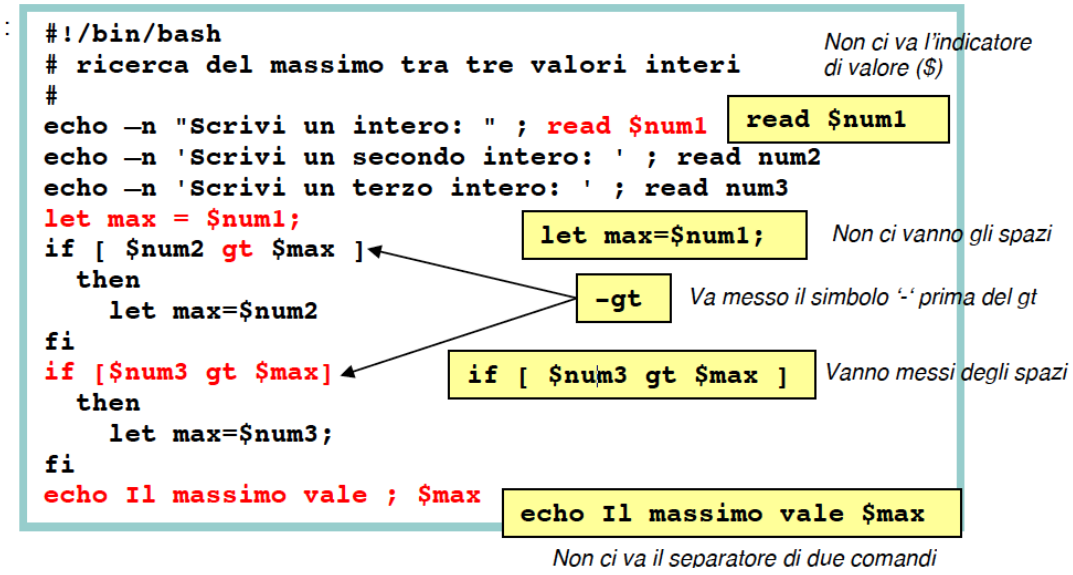
Le reti wireless possono essere divise in : AD HOC LAN( stazioni in grado di comunicare direttamente tra loro senza Access Point) e INFRASTRUCTURED WIRELESS LAN (stazioni che comunicano tra loro utilizzando uno o più Access Point, collegati da un Distribution System)
I compiti degli Access Point sono : collegamento tra rete wireless e rete cablata ; autenticazione, associazione e riassociazione (roaming) ; gestione del risparmio energetico delle stazioni (Power Save Mode) ; sincronizzazione, in modo che tutte le stazioni agganciate ad un AP siano agganciate ad un clock comune. Inoltre gli Access Point possono svolgere funzioni di bridging cioè ponte wireless tra due o più edifici/postazioni (collegamenti punto-punto o multipunto) , stando attenti che le
distanze raggiungibili da 500 m a 10-15 Km purché
siano a vista, tramite antenne direttive.
Elementi da considerare per un buon funzionamento: Access Point baricentrico e a mezza altezza , utenti allineati otticamente all'Access Point ; attenzione alle schermature metalliche ; analisi delle riflessioni ; analisi degli attraversamenti strutturali.

**Che cosa si intende per Security Policy? Chi la emana? Quali ambiti regolamenta? Quali strumenti hardware e software coinvolge?**

1. **Acquisition Assessment Policy**
definisce le responsabilità in materia di acquisizioni aziendali, e definisce i requisiti minimi di una valutazione di acquisizione di essere compilato dal gruppo di sicurezza delle informazioni.
2. **Bluetooth**
Dispositivo di sicurezza comune questa politica prevede più sicurezza per le operazioni Bluetooth. E protegge la società da perdita di identificazione personale e dati aziendali proprietarie.
3. **Dial-in**
Criteri di accesso definisce adeguato accesso dial-in e il suo utilizzo da parte autorizzato personale.
4. **Etica Politica**
definisce le modalità per stabilire una cultura di apertura, fiducia e integrità nelle pratiche di business.
5. **Information Sensitivity Policy**
definisce i requisiti per la classificazione e il fissaggio del Informazioni di organizzazione in un modo appropriato per il suo livello di sensibilità .
6.**Internal Lab Security Policy**
definisce i requisiti per i laboratori interni per garantire che riservate tecnologie di informazione e non siano compromessi, e che servizi di produzione e degli interessi della organizzazione siano protetti da attività di laboratorio.
7. **Personal Communication Devices Policy**
descrive i requisiti di sicurezza per le informazioni personali Dispositivi di comunicazione e segreteria telefonica.

8. **Risk Assessment Policy**
definisce i requisiti e fornisce l'autorità per la team di sicurezza delle informazioni per identificare, valutare, e risolvere i rischi di infrastruttura informativa dell'organizzazione associata condurre gli affari.
9. **Technology Equipment Disposal**
definisce le regole per la cessione dei beni tecnologici obsoleti e riciclaggio materiale informatico
10. **Web Application Security Assessment Policy**
definisce la valutazione di applicazioni Web per identificare potenziali o debolezze realizzate come risultato di involontario miss-configurazione, autenticazione debole, la gestione degli errori insufficienti, la perdita di informazioni sensibili , ecc

**Nel seguente script in bash sono presenti almeno 4 errori sintattici: individuarli, spiegare perché sono degli errori e correggerli:**



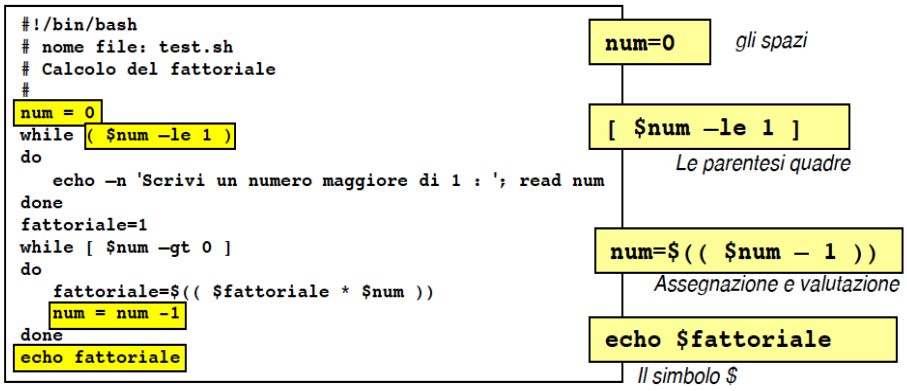

**Che cosa fa il comando cron ? Proporne un esempio di utilizzo**

Cron è un "comando" che permette di pianificare le operazioni da eseguire ad intervalli regolari su un sistema (es: svuota directory / tmp).
Cron è controllato dalle voci nel file / etc / spool / cron and / etc / cron.d directory and file / etc / crontab.
Cron non è un comando, ma piuttosto è un demone che viene eseguito una volta ogni minuto, scansiona i file configuration , ed esegue i compiti specificati. Ci sono due tipi di Cron jobs: cron system e cron utente.
Per creare un sistema Cron Job, è necessario modificare il file / etc / crontab.
Il file inizia con il set di variabili ambientali. Questi impostano alcuni parametri del cron job quali il PATH e MAILTO
Un esempio con cron è la creazione di uno script per l'esecuzione dell'operazione desiderata. Tale script andrà inserito in una delle directory seguenti
/etc/cron. hourly
/etc/cron. daily
/etc/cron.monthly
/etc/cron.weekly
per poter essere eseguito ad intervalli ben definiti (se non specificato, alle 4:00)

**Con riferimento al cablaggio strutturato ed alle caratteristiche fisiche dei mezzi fisici utilizzati, analizzare brevemente i seguenti elementi: cablaggio orizzontale, cablaggio verticale e dorsale di campus.**

Il Cablaggio strutturato è un metodo per creare un sistema di cablaggio organizzato che può essere facilmente compresi e gestiti da installatori , amministratori di rete e qualsiasi altra tecnico abile con i cavi.
Regole di cablaggio strutturato per reti LAN : aspetto per una soluzione di connettività completa , piano per la crescita futura , mantenere la libertà di scelta per i venditori.
Nello strutturare un palazzo (studentato) , bisognerà stare attenti al cablaggio orizzontale e verticale.
**cablaggio orizzontale**: ogni piano dovrà avere un armadio di distribuzione piano, che con una portata massima di 90m porterà la rete all'area di lavoro , che poi verrà "smistata" ai dispositivi dell'utente.
**cablaggio verticale** : ogni edificio dovrà avere un armadio di distribuzione d'edificio , dal quale verrà portata la rete a tutti i piani (ad ogni armadio distribuzione piano) con una portata massima di 6m fra un piano e l'altro.

**Nel seguente script in bash sono presenti 4 errori sintattici: individuarli e correggerli**




**Descrivere quali tecniche si possono adottare per rendere sicura la trasmissione/ricezione di una e-mail. Si faccia riferimento alla tecnica PGP (Pretty Good Privacy) descritta a lezione.**

Pgp è un programma che permette di usare autenticazione e privacy crittografica (crittografia assimetrica).
Associato a S/MIME , sono disponibili plug-in che implementano sicurezza per i dispositivi mail più conosciuti (outlook , mozilla thunderbird , ecc...)
Oltre a PGP , programmi di protezione di posta elettronica più diffusi sono Kerberos, Fuoco Trust e MailMarshal

**Descrivere un possibile attacco informatico, analogo a quello presentato in aula. Quali considerazioni fondamentali si possono ricavare da questo scenario?**

**Fase0: Attacker Places Content on Trusted Site**
l'attaccante comincia inserendo un contenuto malevolo in un sito web attendibile di terzi. Il contenuto immesso dall'attaccante include codice per lo sfruttamento di software lato client non adeguatamente aggiornato
**Fase1: Client-Side Exploitation**
un utente sulla rete interna aziendale naviga in Internet da una macchina Windows con software lato client non adeguatamente aggiornato,
come ad esempio un lettore multimediale , un visualizzatore di documenti o un componente della suite di Office. Dopo aver caricato il contenuto malevolo dal sito, il browser dell'utente vittima invoca la vulnerabililtà del lato client del programma passandogli il codice exploit dell'attaccante. Questo codice
permette all'attaccante di installare o eseguire programmi sulla macchina vittima, utilizzando i privilegi dell'utente che ha lanciato il browser. L'attacco è parzialmente limitato perché questo utente può eseguire
programmi solo con i privilegi utente.
**Fase2 : Establish Reverse Shell Backdoor Using HTTPS**
il codice dell'attaccante installa un programma backdoor connection sulla macchina vittima. Questo programma permette all'aggressore un accesso alla shell della macchina vittima, utilizzando
l'accesso HTTPS dalla macchina attaccante a quella vittima attaccata.
Il traffico backdoor sembra quindi essere regolare traffico cifrato web in uscita per quanto riguarda il firewall.
**FASE3-4 : Dump Hashes and Use Pass-the-Hash Attack to Pivot**
l'attaccante usa l'accesso alla shell del sistema vittima per caricare in locale un programma che sfrutti le debolezze della macchina per aumentare gradualmente i propri privilegi. Questo
programma permette (o almeno cerca) al malintenzionato di passare su questa macchina dall'account utente con limitati privilegi a quello di totale controllo del sistema. L'attaccante ora può scaricare gli hash delle password per tutti gli account di questo computer locale, tra cui l'account di amministratore locale sul sistema.
Ora però , invece di violare ed utilizzare l'account di amministratore locale, l'attaccante utilizza un programma Windows pass-the-hash per scoprire l'autenticazione a un'altra macchina Windows sulla rete aziendale nterna, un sistema client completamente aggiornato e protetto su cui il
nuovo utente vittima ha privilegi amministrativi completi . Utilizzando Server Message Block (SMB), il protocollo basato sulle hash degli utenti e non sulle loro password, permettendo al
malintenzionato di accedere al file system o eseguire programmi sul sistema completamente protetto con privilegi di amministratore locale. Utilizzando questi privilegi, l'attaccante ora scarica anche le hash delle password per tutti gli account locali di questa macchina Windows, che era regolarmente protetta.
**Fase5: Pass the Hash to Compromise Domain Controller**
l'attaccante utilizza una chiave hash della password di un account locale sul client Windows perfettamente protetto per accedere al sistema controller di dominio, di nuovo con un attacco passthe-hash per ottenerne l'accesso alla shell.
Poiché la password per l'account amministratore locale è identica alla password di un account amministratore di dominio, gli hash delle password per i due account sono identici. Pertanto, l'utente malintenzionato può accedere al controller di dominio con privilegi completi di amministratore di dominio, avendo il controllo completo su tutti gli altri account e le macchine presenti.
**Fase6-7 : Exfiltration**
Con i privilegi completi di amministratore di dominio, l'attaccante compromette ora la macchina server che memorizza i dati riservati dell'organizzazione.
Estrae ed analizza queste informazioni sensibili, composte generalmente da oltre 200 MB di dati. L'attaccante invia dal server questi dati attraverso Internet, sempre utilizzando HTTPS per criptare le informazioni, riducendo al minimo le probabilità di essere scoperto.

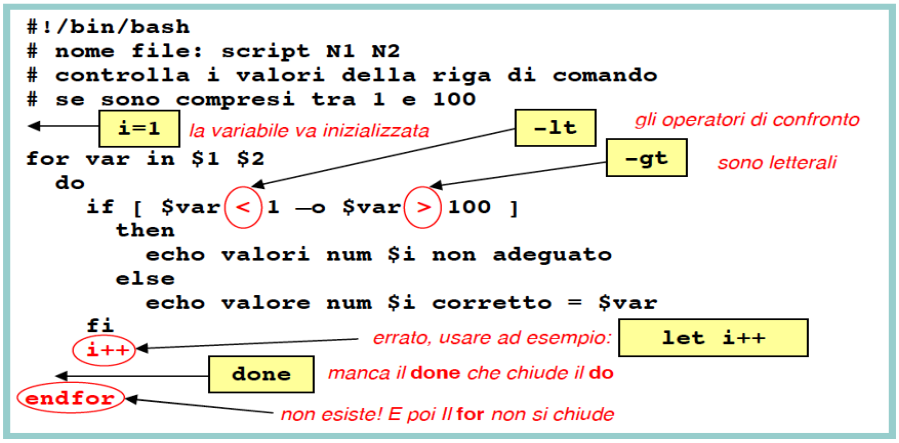
**Realizzare uno script bash che verifichi la presenza o meno di un dato file. Il nome del file da cercare deve essere passato allo script utilizzando la riga di comando. Si preveda che, in assenza di argomenti aggiuntivi, lo script visualizzi una riga di help indicante la modalità d'uso dello script.**

```
#!/bin/bash
#
# script che controlla se un dato file esiste
# il nome del file deve essere passato come argomento
# della linea di comando

if [ $# -ne 1 ]
then
     echo "Uso:  $0  nome-file"
     exit 1
fi

if [ -f $1 ]
then
     echo "Il file $1 esiste"
else
     echo "Spiacente ma il file $1 non esiste."
fi
```

**Che cos'è, in un sistema Linux, un CORE DUMP? Quando si verifica, che cosa determina, a cosa serve**

Core dump è una registrazione della memoria che un programma stava usando al momento del crash. L'obiettivo di Core Dump è quello di permettere ai programmatori di studiare il file , di capire esattamente che cosa ha causato il programma di crash.
Per individuare i file di base (non solo) su un sistema Linux si usa il comando : find core /-name
Le principali proprietà del file Core sono: Il proprietario del file indica che ha eseguito il programma ; La data di creazione del file core è la data in cui il crash si è verificato e quando il core dump è stato creato; Creating Program properties dei file core vi diranno che programma si è bloccato e ha generato il file di core dump (usare gdb).
Al fine di gestire in modo efficace i processi di sistema su un Sistema Linux, è importante essere in grado di determinare quali processi sono in esecuzione su un sistema ,e quali sono critici e non critici , quindi quelli che sono attualmente in esecuzione su un possono essere visti usando il comando ps (es: ps -A –forest)
Il comando top ha funzioni molto simili allo strumento di prestazioni di Windows 2000 , il quale fornesce dettagliate informazioni riguardanti CPU e RAM. Il comando kill può essere usato per terminare il processo (kill –s signal pid)

**Nel seguente script in bash sono presenti almeno 5 (o 6) errori: individuarli, spiegare perché sono degli errori e correggerli.**



**Elencare e descrivere brevemente quali caratteristiche hardware dovrebbe avere un fileserver di rete dimensionato per un piccolo laboratorio universitario (tipicamente 20 utenti), con particolare riferimento alle caratteristiche descritte nel Capitolo 2 "Hardware standard del PC".**

Un file server dovrebbe avere :

**Hardware:**

· Un buon Case e collegamenti alla corrente
· SchedaMadre
· CPU multicore
· buona RAM
· Hard Disk and RAID organisation
• schede video , audio , rete ben cnfigurate
· Backup system

**Software:**

· Network Operating System
· LDAP
· NFS o Active Directory
· IIS
· e tutto quello che può garantire un efficace e sicuro funzionamento

**Dopo essere stati accreditati presso un server linux tipo quello utilizzato nelle esercitazioni di laboratorio (Ubuntu Server) come utente XXX appartenente al gruppo sudoers, elencare e commentare i comandi necessari per eseguire le seguenti operazioni:**

```
$ mkdir test
$ cd test
```

**Scrivere (con un editor a scelta) uno script che stampi la tabellina del 9 (dallo 0 al 90)**

```
$ gedit test.sc
     #!/bin/bash
     # nome file: test.sc
     for a in 0 1 2 3 4 5 6 7 8 9 10
     do
          echo " 9 * " $a = $(( 9 * $a ))
          echo -n
     done
```

*oppure*

```
a=0
while [ "$a" -le 10 ]
do
  echo " 9 * " $a = $(( 9 * $a ))
  echo -n
  let "a+=1"
done
```

**Salvare lo script e provarlo, mandandolo in esecuzione**

```
$ chmod a+rwx test.sc
$ ./test.sc
9 * 0 = 0
9 * 1 = 9
9 * 2 = 18
9 * 3 = 27
9 * 4 = 36
9 * 5 = 45
9 * 6 = 54
9 * 7 = 63
9 * 8 = 72
9 * 9 = 81
9 * 10 = 90
```

## Le principali Outside Threats

Il furto di dati si verifica quando un utente non autorizzato o programma software ottiene illegalmente informazioni private che è memorizzata o trasmessa su una rete (packet sniffing e sistema di effrazioni).
La distruzione dei dati avviene quando un non autorizzata persona o un programma software irrompe in un sistema e eliminazione di dati.
Un Denial of Service (DoS) è progettato per degradarsi prestazioni del server o rimuoverlo dalla rete completamente.
Diverse fonti esterne possono causare attacchi:

- Gli hacker - i veri desideri degli hacker di sezionare i sistemi e programmi per vedere come funzionano.
- Crackers - quelli che sfondano a sistemi informatici per manomettere, sottrarre o distruggere i dati.
- Virus - che provoca un po 'di imprevisti e di solito indesiderabile evento.
- Worms - un virus autoreplicante che non altera i file, ma risiede nella memoria attiva e si duplica.
- Cavallo di Troia - è un programma che si presenta come un altro programma per ottenere informazioni

## Creare uno script che produca una lista numerata dei file della directory corrente che soddisfano ad una stringa-condizione passata al file come argomento della linea di comando

```
#!/bin/bash
# nome file: script8 condizione
# ad esempio ./script8 “*.txt”
# enumera i file della directory corrente che
# soddisfano alla condizione specificata
#
let i=0
for file in `ls $1`
do
let i++
echo $1: $file
done
```