

## Laboratorio di Amministrazione di Sistema (CT0157)

### parte A : domande a risposta multipla

1. Which of the following is considered good practice when partitioning a hard disk for a new OS? (Choose two.)
  - a) A third party partitioning tool that supports the operating systems to be installed should be used.
  - b) MS-DOS *fdisk* should be used, as it creates partitions that are compatible with all major operating systems.
  - c) The partitioning tool that comes with the OS should be used to create the partitions for that OS, if no other options are available.
  - d) Partitions should be as large as the disk will allow to provide room for future expansion.
  - e) Partitions should be made as small as possible and FIPS used to adjust them later as necessary.
2. Which are three reasons a company may choose Linux over Windows as an operating system? (Choose three.)
  - a) It is difficult to buy a new computer with a server version of Windows pre-installed.
  - b) There is more application software available for Linux.
  - c) Running a Linux server without a GUI will increase efficiency and reliability. This option is not available in server versions of Windows.
  - d) After a user has purchased a copy of Linux, it can be installed on any number of computers for no additional charge.
  - e) After a user has purchased a copy of Windows, it can be installed on any number of computers for no additional charge.
  - f) By default, users must provide a username and password to log into a Linux system, which improves system security.
3. A technician is troubleshooting a Windows machine that is not communicating with the network server. The technician verifies that the server is not reachable and ipconfig shows that the workstation is configured properly. What should the technician do next?
  - a) ping the default gateway
  - b) ping 127.0.0.1
  - c) check the configuration of the server
  - d) tracert to the server
4. Which setting determines if a program will run with the permissions of its assigned group or the permissions of the user's groups?
  - a) SUID
  - b) SSID
  - c) SGID
5. Which two of the following standards are necessary for proper virus protection? (Choose two.)
  - a) Virus protection software should only be installed on client workstations that have Internet access.
  - b) Virus protection software should only be installed on servers that can be accessed by remote clients.
  - c) Virus protection software should be installed on all workstations and servers.
  - d) All virus warnings should come from at least two network support technicians.
  - e) One person should be responsible for communicating virus alerts to all users.
6. Which of the following situations can be addressed by using the *fsck* command?
  - a) A user has been given the job of creating two new partitions on an existing hard drive.
  - b) A user must change the permissions on three existing files without changing any existing permissions on the directory where the files are stored.
  - c) A user must repair the file structure after an unexpected power failure causes a system to abruptly shut down.
  - d) A user must batch create home directories for seven new users.
7. Which version of Directory Service does Linux use?
  - a) NDS
  - b) NIS
  - c) NFS
  - d) NDAP
8. Which Linux command is used to temporarily change the default gateway of a host?
  - a) arp
  - b) ifconfig
  - c) netstat
  - d) route
  - e) ping

**NB: questo foglio verrà ritirato dopo 15 minuti dall'inizio dell'esame.**

candidato: \_\_\_\_\_ matricola: \_\_\_\_\_

**SPAZIO PER LA VALUTAZIONE:** il candidato riporti su questo lato del foglio le soluzioni relative ai quesiti 1-8 a risposta multipla.

**Criteri di valutazione:** le domande 1-8 valgono un punto per ogni quesito corretto, mentre le domande 9-12 valgono sei punti ciascuna (al massimo, graduati in base alla correttezza della risposta).

**Per chi ha presentato il progetto:** il progetto viene valutato al massimo 12 punti, mentre la seguente prova si intende limitata alle domande dall'1 al 10. I quesiti 1-8 valgono un punto per ogni risposta corretta, mentre le domande 9 e 10 valgono sei punti ciascuna (al massimo, graduati in base alla correttezza della risposta).

#	risposta/e						punti
1	a	b	c	d	e	f	
2	a	b	c	d	e	f	
3	a	b	c	d	e	f	
4	a	b	c	d	e	f	

	valutazione	punti
9		
10		
11		
12		

per chi non ha presentato un progetto



oppure

#	risposta/e						punti
5	a	b	c	d	e	f	
6	a	b	c	d	e	f	
7	a	b	c	d	e	f	
8	a	b	c	d	e	f	

	valutazione	punti
9		
10		
progetto		

per chi ha presentato il progetto

## Laboratorio di Amministrazione di Sistema (CT0157)

*parte B : domande a risposta breve*

9. Descrivere che cosa si intende per Directory Service e come questo servizio venga implementato in Windows e Linux.

*Vedere le slide 31 - 44 del modulo "4. Servizi di Rete"*

*Queste le parole chiave che compongono una risposta completa:*

- *Amministratore centralizzata delle risorse condivise di rete*
- *Electronic Directory Service*
- *X.500, DSA (Directory System Agent), DUA (Directory User Agent) e DIB (Directory Information Base)*
- *Protocollo DAP (Direct Access Control)*
- *Protocollo LDAP (Lightweight DAP)*
- *Windows ed Active Directory*
- *Domain tree ed OUI (Organizational Units)*
- *Domain Controller*
- *Multimaster replication model*
- *ACL (Access Control List) su ogni oggetto di A.D.*
- *Linux e NIS (Network Information Service)*
- *programma linuxconf utilizzato per configurare NIS*

10. Con riferimento alle reti wireless, descrivere brevemente:

- *le bande su cui operano le trasmissioni radio per reti wireless*
- *la terminologia più utilizzata nelle reti WLAN*
- *le due possibili modalità operative delle reti wireless*
- *i compiti richiesti ad un Access Point*
- *vantaggi e svantaggi delle reti wireless*
- *standard IEEE*
- *tecniche di messa in sicurezza delle reti wireless*

*Vedere le slide 8 - 29 del modulo "3C. Progettazione di una rete - wireless"*

*Queste le parole chiave che compongono una risposta completa:*

- *S-Band ISM tra 2.4 e 2.5 GHz. E C-Band ISM tra 5.725 e 5.875 GHz*
- *Spettro distribuito*
- *BSA (Basic Service Area), AP (Access Point), STA (Station), DS (Distribution System), BSS (Basic Service Set), ESS (Extended Service Set)*
- *Ad Hoc e Infrastructured Wireless*
- *Bridging tra cablata e wireless*
- *Autenticazione, associazione e riassociazione, roaming*
- *costi, tempi della messa in opera e logistica semplificata, facilità di riorganizzazione, scalabilità, flessibilità, reti temporanee*
- *inaffidabilità, sicurezza, roaming, multipath fading, estensione limitata, mancanza di standardizzazione, inquinamento elettromagnetico*
- *IEEE 802.11 a, b, g, n*
- *Disabilitazione DHCP*
- *AP con indirizzo dinamico*
- *Autenticazione dell'accesso*
- *SSID, WEP, WPA e WPA2*

## Laboratorio di Amministrazione di Sistema (CT0157)

*parte riservata a chi non presenta il progetto*

11. Nelle recenti distribuzioni UBUNTU del Sistema Operativo Linux di default l'accesso come amministratore (root) è stato disabilitato per problemi di sicurezza.

Descrivere:

- quali sono i vantaggi, in termine di sicurezza, che questa scelta comporta
- quale alternativa viene suggerita per poter eseguire comandi con diritti amministrativi di root
- quali sono i comandi che occorre digitare per utilizzare l'account amministratore.

*Vedere le slide 1 - 3 del modulo "Lab2-ShellScripting"*

*Queste le parole chiave che compongono i singoli punti della risposta:*

- quali sono i vantaggi, in termine di sicurezza, che questa scelta comporta
  - *Nel caso di processo non affidabile, bloccarsi con l'utenza generica è totalmente diverso che bloccarsi con diritti amministrativi.*
  - *Gli utenti non devono imparare e ricordarsi anche la password di amministratore*
  - *Aumenta la consapevolezza di quando si eseguono operazioni critiche*
  - *Non è necessario scoprire l'identificativo dell'amministratore perché (root) è noto a priori, mentre l'identificativo del generico utente, anche quando usa sudo, deve essere scoperto o indovinato.*
  - *Ogni volta che si richiama sudo, la richiesta viene registrata sul file di log /var/log/auth.log*
- quale alternativa viene suggerita per poter eseguire comandi con diritti amministrativi di root
  - il ricorso al comando sudo*
- quali sono i comandi che occorre digitare per utilizzare l'account amministratore.
  - a) *aprire una sessione terminale per digitare comandi da CLI*
  - b) *impostare la password per l'account root, digitando il comando*  
*sudo passwd root*  
*dovrà essere immessa inizialmente la password dell'account personale utilizzato per accedere al server, e poi quella (nuova) scelta per l'utente root*
  - c) *a questo punto l'account root è stato riabilitato, come verificabile se si usano i comandi su e/o sudo.*
  - d) *L'account root è stato riabilitato, ma solo per utilizzi limitati nel tempo e non è ancora possibile accreditarsi come root fin dal login iniziale. Questa operazione richiede l'accesso al file di configurazione lightdm.conf.*

12. Utilizzo di un sistema operativo Linux come Firewall.

- Descrivere le principali funzioni svolte dai programmi ipchains, iptables, ufw e netfilter.
- Illustrare lo scopo dei tre canali INPUT chain, OUTPUT chain e FORWARD chain di iptables.
- Che valori possono assumere le relative policy?
- Con iptables, se si vuole aggiungere la regola che consenta l'ingresso di traffico diretto ad un server interno alla rete, quale comando occorre eseguire?
- Con ufw, se si vuole aggiungere la regola che impedisce qualsiasi traffico proveniente dall'host 11.22.33.44, quale comando occorre eseguire?

*Vedere le slide 85 - 90 del modulo "9. Sicurezza di Rete"*

*Queste le parole chiave che compongono i singoli punti della risposta:*

- Descrivere le principali funzioni svolte dai programmi ipchains, iptables, ufw e netfilter  
*netfilter è la componente del kernel che permette l'intercettazione e la manipolazione dei pacchetti che attraversano il computer.*  
*ipchains è stato il primo programma di Linux pensato per configurare netfilter e svolgere di conseguenza funzioni di firewalling. Successivamente è stato introdotto iptables, che permette di implementare anche funzionalità NAT e stateful packet filtering.*  
*Per la distribuzione Ubuntu ipchains è stato rimpiazzato dal programma ufw (uncomplicated firewall), più semplice da utilizzare.*
- Illustrare lo scopo dei tre canali INPUT chain, OUTPUT chain e FORWARD chain.  
*INPUT chain      traffico in entrata al firewall*  
*OUTPUT chain    traffico in uscita al firewall*  
*FORWARD chain   traffico non indirizzato al firewall, ma che lo deve attraversare*
- Che valori possono assumere le policy?  
*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*
- Con iptables, se si vuole aggiungere la regola che consenta l'ingresso di traffico diretto ad un web server interno alla rete, quale comando occorre eseguire?  
  
*\$ sudo iptables -A INPUT -p tcp -dport 80 -j ACCEPT*
- Con ufw, se si vuole aggiungere la regola che impedisce qualsiasi traffico proveniente dall'host 11.22.33.44, quale comando occorre eseguire?  
  
*\$ sudo ufw deny from 11.22.33.44 [to any port]*