data: 31/05/2011

Laboratorio di Amministrazione di Sistema (C62032)

parte A : domande a risposta multipla

1. **Which DoS attack uses fragments with overlapping reassembly information to take advantage of the way IP handles fragmentation?**
   a) SYN attack
   b) Teardrop
   c) ping of death
   d) land

2. **Which two of the following options provide a basic firewall solution by using rules to control network traffic? (Choose two.)?**
   a) proxy services
   b) ip masquerade
   c) packet filters
   d) Network Address Translation
   e) access control lists

3. **Which three OSI model layers are used for packet filtering? (Choose three.)?**
   a) Layer 2
   b) Layer 3
   c) Layer 4
   d) Layer 5
   e) Layer 6
   f) Layer 7

4. **Which of the following is an OS-independent component that is responsible for basic hardware and resource configuration before the OS loads?**
   a) USB ports
   b) SCSI
   c) BIOS
   d) CPU

5. **Which of the following configuration files determines the default runlevel at system startup?**
   a) /etc/rc/init
   b) /etc/inittab
   c) /etc/init/rc.d
   d) /etc/rc.d/inittab

6. **On a computer running Linux, which attribute prevents anyone other than the owner of a file, the directory owner, or root from renaming or removing files in a directory?**
   a) owner bit
   b) no override
   c) lock
   d) sticky bit

7. **Which component of Windows 2000 accommodates many types of scripting languages?**
   a) VBScript
   b) JScript
   c) WSH
   d) ShellScript

8. **How is redundancy built into a server system?**
   a) by including additional hardware components that can take over if other components fail
   b) by including a tape back-up system to preserve data
   c) by adding redundancy software to the system
   d) by keeping duplicates of all data

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

candidato: _____ matricola: _____

data: 31/05/2011

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),.*

#	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	

#	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 parziale	punti
9		
10		
11		
12		

TOTALE

candidato: _____ matricola: _____

Laboratorio di Amministrazione di Sistema (C62032)

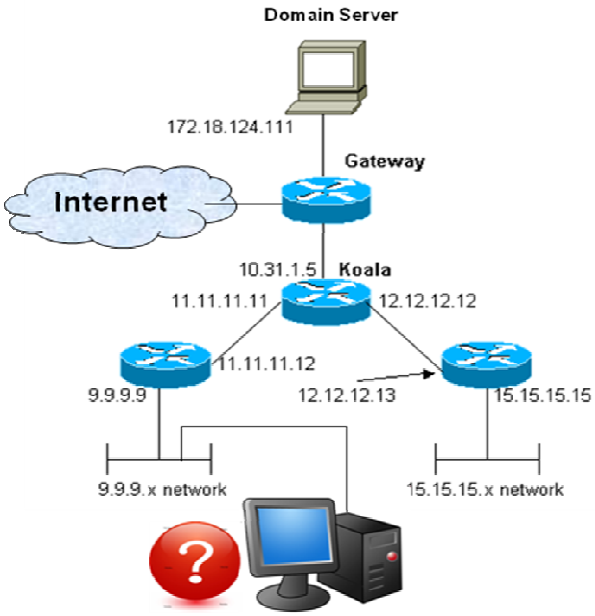
parte B : domande a risposta breve

9. Descrivere come si possono aggiungere o eliminare nuovi utenti o gruppi di utenti, oppure modificare i diritti di un utente o di un gruppo di utenti, in ambiente Linux.

   Vedere le slide 13-19 del modulo "6a. Amministratore di Linux".

   Queste le parole chiave e gli elementi da prendere in considerazione ed opportunamente commentare per comporre una risposta completa:
   - *utente ed account*
   - *chmod*
   - *sudo e root*
   - *useradd e adduser*
   - *passwd*
   - *userdel*
   - *file shadow*
   - *newgrp*
   - *groupadd*
   - *gpasswd*

10. Nella figura sottostante è rappresentata una rete aziendale. L'utente dell'host di indirizzo IP 9.9.9.1 indicato in figura chiama il tecnico gestore di rete perché non riesce ad accedere ad Internet. Indicare quali utility software possono essere utilizzate per verificare il funzionamento dei vari componenti, con quali parametri mandarle in esecuzione, quali problemi hardware e software vengono evidenziati.



   Vedere le slide 11-26 del modulo "8. Ricerca e gestione dei guasti", e le osservazioni fatte in aula.
   Queste le parole chiave che compongono una risposta completa:
   - *ping a vari livelli, per I livelli OSI 1 e 2*
   - *pathping per testare le varie tratte*
   - *ipconfig – ifconfig per verifica delle single schede di rete*
   - *traceroute per verificare la configurazione dei router*
   - *netstat per l'analisi delle connessioni attivate*
   - *e specialmente l'individuazione delle possibili anomalie in base a risposte difformi dalla norma*

candidato: _____ matricola: _____

11. 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
```

.

Vedere la slide 19 del modulo "6b. Shell Scripting", e le altre dello stesso modulo.

12. Con riferimento a quanto descritto in aula, elencare e descrivere i principali rischi della sicurezza attualmente più importanti (client-side software, OS vulnerabilities, zero-days vulnerability).

Vedere le slide 17-31 del modulo "9a. Sicurezza di Rete".

Queste le parole chiave che compongono una risposta completa:

- *Client-side software not pached*
- *Internet facing vulnerable web site*
- *OS remotely exploitable vulnerabilities*
- *zero-day vulnerabilities*
- *Linux vulnerabilities*
- *application patching on Operating Systems and Applications*
- *Client-side exploitation example*

candidato: _____ matricola: _____