Simulado 202

1) Existe um área restrita em um site do Apache, no qual requer que os usuários se autentiquem através do arquivo /srv/www/security/site-passwd. Qual comando é usado para modificar a senha dos usuários que já existem, sem perder dados, quando uma autenticação básica está sendo usada.

a) htpasswd -c /srv/www/security/site-passwd passwd usuário
b) htpasswd /srv/www/security/site-passwd usuário
c) htpasswd -n /srv/www/security/site-passwd usuário
d) htpasswd -D /srv/www/security/site-passwd usuário
e) nenhuma das anteriores

2) Considere o seguinte arquivo /srv/www/default/html/restricted/.htaccess. Considere que a diretiva DocumentRoot está configurada no arquivo /srv/www/default/html. Escolha abaixo duas sentenças que são verdadeiras.

a) O Apache irá apenas conceder acesso para http://server/restricted para usuários autenticados conectados em máquinas clientes da rede 10.1.2.0/24
b) Essa configuração irá apenas funcionar se o diretório /srv/www/default/restricted está configurado com AllowOverride AuthConfig limit
c) O Apache irá requerer autenticação para todos os clientes que requisitarem conexões para http://server/restricted
d) Usuários conectados de clientes na rede 10.1.2.0/24 não precisarão se autenticar para acessar http://server/restricted
e) A diretiva poderia ser removida sem alterar o comportamento do Apache para este diretório

3) Qual das seguintes alternativas abaixo não é um tipo de ACL válido quando se está configurando o Squid?

a) src
b) source
c) dstdomain
d) url_regex
e) time

4) O trecho abaixo foi tirado do arquivo de configuração do Squid. Qual das seguintes opções abaixo é verdadeira?

[...]

```
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443
acl Safe_ports port 80 443 1025-65535
acl CONNECT method CONNECT
acl localhost src 10.0.0.0/24

http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
```

[...]

a) Usuários conectados em localhost estarão aptos para acessar sites através deste proxy.
b) É necessário incluir a regra http_access proibindo acesso para todos no final das regras.
c) É possível usar este proxy para acessar sites ativos escutando em nenhuma porta.
d) Este proxy não pode ser usado para acessar servidores FTP escutando em portão padrão.

5) Um gateway conecta os clientes com a Internet usando um proxy Squid. Apenas os clientes da rede 192.168.1.0/24 deve estar habilitados para usar o proxy. Qual das seguintes configurações está correta?

a) acl local src 192.168.1.0/24 http_allow local
b) acl local src 192.168.1.0/24 http_access allow local
c) acl local src 192.168.1.0/24 http access allow local
d) acl local src 192.168.1.0/24 http_access_allow=local
e) acl local src 192.168.1.0/24 httpd_access allow local

6) Para que uma mudança seja efetuada no arquivo de configuração do Samba, é necessário:

a) Reiniciar os processos smbd e nmbd.
b) Enviar um sinal HUP para o processo smbd.
c) Não é necessáio fazer nada, a mudança é automática.
d) Reiniciar o sistema.

7) Um usuário faz uma requisição a um compartilhamento oculto do Samba chamado "confidencial". Como isso pode ser configurado?

a) [confidencial]
comment = compartilhamento oculto
path = /mnt/smb/oculto
writelist = usuario
create mask = 0700
directory mask = 0700

b) [$confidencial$]
comment = compartilhamento oculto
path = /mnt/smb/oculto
writelist = usuario
create mask = 0700
directory mask = 0700

c) [$confidencial]
comment = compartilhamento oculto
path = /mnt/smb/oculto
writelist = usuario
create mask = 0700
directory mask = 0700

d) [%confidencial]
comment = compartilhamento oculto
path = /mnt/smb/oculto
writelist = usuario
create mask = 0700
directory mask = 0700

e) [confidencial$]
comment = compartilhamento oculto
path = /mnt/smb/oculto
writelist = usuario
create mask = 0700
directory mask = 0700

8) Qual das opções abaixo é usada na configuração de um arquivo do Samba para proibir que determinados arquivos estejam visíveis ou acessíveis pelos clientes?

a) hide files
b) veto files
c) hide special files
d) hide dot files

9) Qual comando pode ser usado para checar o arquivo de configuração do Samba a fim de encontrar erros?

a) testconfig
b) testparm
c) smbconfig
d) smbtestconfig
e) testsmb

10) Você quer checar quais compartilhamentos estão sendo oferecidos pelo sistema Windows. Qual dos seguintes comandos poderia ser usado por você para executar essa tarefa?

a) showshareswindows
b) smbdlook
c) smbclient
d) smbstatus
e) clientsmb

11) Você adicionou um novo compartilhamento em /etc/exports, mas os usuários concluem que não tem permissão para isso quando eles tentam montar esse compartilhamento. Qual a melhor solução para resolver esse problema?

a) Reiniciar o sistema
b) Adicionar a opção (no_root_squash) na linha adicionada no /etc/exports
c) Reiniciar o NFS
d) Executar o comando exportfs -a
e) Executar o comando export -nfs

12) Para listar o sistema de arquivos disponível de um servidor NFS chamado “4linux”, o comando _____ -e 4linux pode ser usado.

13) Quais dos seguintes daemons devem estar em execução em um servidor NFS?

a) portmap
b) nfsdaemon
c) nfsd
d) xinetd
e) mountd

14) Qual das seguintes linhas abaixo exportarão o diretório /mnt/publico para o host “clientenfs” com acesso de leitura e escrita, assegurando que todas as mudanças serão escritas imediatamente no disco?

a) /mnt/publico clientenfs(rw)
b) clientenfs:/mnt/publico/:rw,sync
c) /mnt/publico clientenfs:rw:sync
d) /mnt/publico clientenfs(rw,sync)
e) clientenfs(rw) /mnt/publico

15) Um host chamado “Tux” com o endereço MAC 00:1d:7d:fe:12:fb deve sempre estar com o endereço 192.168.1.5 oferecido pelo servidor DHCP. Qual as seguintes configurações atinge esse objetivo?

a) host Tux {
hardwareethernet 00:1d:7d:fe:12:fb;
fixed-address 192.168.1.5;
}

b) host Tux {
mac = 00:1d:7d:fe:12:fb;
ip = 192.168.1.5;
}

c) host Tux {
mac-hardware-ethernet 00:1d:7d:fe:12:fb;
fixed-address 192.168.1.5;
}

d) host Tux {
hardware-ethernet 00:1d:7d:fe:12:fb;
fixed-address 192.168.1.5;
}

e) host Tux {
hardware-address 00:1d:7d:fe:12:fb;
fixed-address 192.168.1.5;
}

16) Você deseja designar endereços IP da classe C para seus clientes via DHCP. Qual linha deve ser adicionada no arquivo de configuração dhcpd.conf?

a) bootp-dynamic 192.168.0.0/24;
b) range dynamic bootp 192.168.0.2 192.168.0.255;
c) range dynamic-bootp 192.168.0.2 192.168.0.255;
d) range dynamic_bootp 192.168.0.2 192.168.0.255;
e) range-dynamic-bootp 192.168.0.2 192.168.0.255;

17) Você está usando seu conhecimento em PAM e sshd e deseja ativar senhas em branco. Qual opção você deveria adicionar no arquivo /etc/pam.d/sshd para conseguir isso?

a) auth required /lib/security/pam_unix.so shadow nodelay passwd-no-req
b) auth required /lib/security/pam_unix.so shadow nodelay no-passwd
c) auth required /lib/security/pam_unix.so shadow nodelay nullpass
d) auth required /lib/security/pam_unix.so shadow nodelay nullok

18) Em qual diretório os módulos do PAM são armazenados? Escreva o caminho completo.

_____

19) Qual comando pode ser usado para modificar a senha em uma entrada LDAP? Escreva somente o nome do comando sem o caminho completo.

_____

20) São comandos do OpenLDAP:

a) ldapad
b) ldapdelete
c) ldapremove
d) ldapmodify
e) ldapadd

21) Quais passos são requeridos para ativar mudanças feitas no arquivo de aliases do Sendmail?

a) Executar o comando newaliases ou sendmail -bi
b) Reiniciar o daemon do sendmail
c) mandar um sinal SIGHUP para o processo do sendmail
d) nenhuma da opções

22) O comando _____ pode ser usado para criar o Maildir no diretório pessoal do usuário quando se usa o servidor de e-mail Postfix. Escreva apenas o nome do comando, sem o caminho completo.

23) Seus usuários requisitaram para você que que as mensagens que chegam para eles que forem duplicadas sejam removidas, qual opção abaixo pode ser usada para fazer um filtro para esse problema?

a) mailfetch
b) mqueue
c) procmail
d) elm
e) rmail

24) Alguns ataques de rede usam pacotes IP com as opções SYN, ACK, PSH, URG, FIN e RST configuradas. Algumas vezes, esse ataque é chamado de “xmas tree pacote”. Para logar todos os pacotes recebidos, você poderia usar:

a) iptables -l INPUT -s 0.0.0.0/0 -d 192.168.0.44/33 --protocol tcp --xmas-pkt -j LOG
b) iptables -l INPUT -s 0.0.0.0/0 -d 192.168.0.44/33 --protocol tcp --cher-pkt -j LOG
c) iptables -l INPUT -s 0.0.0.0/0 -d 192.168.0.44/33 --protocol tcp --cher-pkt -log
d) iptables -l INPUT -s 0.0.0.0/0 -d 192.168.0.44/33 --protocol --tcp-flags SYN,ACK,HSK,PSH,URG,FIN -log
e) iptables -l INPUT -s 0.0.0.0/0 -d 192.168.0.44/33 --protocol tcp --tcp-flags ALL, SYN,ACK,PSH,URG,RST,FIN -j LOG

25) Você decidiu fazer um política padrão de forward com REJECT. Qual regra é necessária para isso?

a) iptables -t mangle -A FORWARD -j REJECT
b) iptables -A FORWARD -j REJECT
c) iptables -A FORWARD REJECT
d) REJECT não é uma política válida

26) Você tem um servidor web executando atrás de um firewall com o IP 192.168.0.5 e você deseja permitir acesso público. O IP externo do firewall é 10.0.0.10. Determine qual (is) regra(s) é/são necessárias para que isso funcione (sua política padrão é ACCEPT para todas as chains):

a) iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-destination 192.168.0.5:80
b) iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 192.168.0.5:80
c) iptables -t nat -A POSTROUTING -m multiport 80,443 -s 10.0.0.10 DNAT --to-destination 192.168.0.5:80
d) nenhuma das opções

27) Para permitir conexões X no servidor SSH, qual linha deve existir no arquivo de configuração do sshd? _____

28) Um administrador consciente do ponto de vista da segurança poderia utilizar DUAS opções no arquivo de configuração do SSH para fazer um ajuste fino:

a) Protocol 2,1
b) PermitEmptyPasswords no
c) Port 22
d) PermitRootLogin yes
e) IgnoreRhosts yes

29) O que deve ser feito em um host para permitir um usuário logar em um host usando uma chave SSH?

a) Adicionar sua chave privada em ~/ssh/authorized_keys
b) Referenciar sua chave pública em ~/.ssh/config
c) Executar o comando ssh-agent no host
d) Adicionar a chave pública em ~/.ssh/authorized_keys
e) Referenciar sua chave privada em ~/.ssh/config

30) Acidentalmente o master boot record (MBR) foi sobrescrita, como posso fazer para recuperar o gerenciador de boot na inicialização?

a) usar o comando grub-install
b) usar o comando install-grub
c) reinstalar o sistema operacional
d) alterar o arquivo /etc/inittab e trocar o runlevel que aponte para o script do grub

31) Onde o código do LILO reside em um sistema que tem dois sistemas operacionais?

a) Na master boot record (MBR)
b) No setor de boot
c) No diretório /boot
d) No início do kernel

32) Você instalou novas bibliotecas, mas elas não estão disponíveis para os programas e não são listadas pelo comando ldconfig -p. Qual arquivo deve ter o caminho para as bibliotecas adicionadas antes de executar o comando ldconfig? Escreva apenas o nome do arquivo, sem o caminho completo: _____

33) Qual comando pode ser usado para verificar a sintaxe do arquivo do Apache 2?

a) apachectl -t
b) testparm
c) apache2ctl -t
d) testapache2 -t

34) Qual comando e sua opção mostra quais são os módulos ativos no Apache? Escreve o comando sem o caminho absoluto: _____

35) Com o comando _____ php5 adiciono o módulo do php no Apache.

36) São considerados módulos do Apache:

a) mod_auth
b) mod_rewrite
c) ssl_mod
d) ssl
e) nenhuma das opções

37) São arquivos de configuração do Postfix:

a) /etc/postfix/main.cf
b) /etc/postfix/cf.main
c) /etc/postfix/master.cf
d) /etc/postfix/cf.master
e) /etc/main.cf

38) Qual o arquivo (caminho absoluto) onde ficam os aliases no Postfix?
_____

39) De acordo com um trecho de configuração de DNS analise:

@ IN MX 10 mail.seunome.com.br.
@ IN MX 30 outroserver.outroserver.com.br.

a) o mail.seunome.com.br tem menor prioridade do que outroserver.outroserver.com.br
b) o mail.seunome.com.br tem maior prioridade do que outroserver.outroserver.com.br
c) o mail.seunome.com.br tem a mesma prioridade que outroserver.outroserver.com.br
d) essa configuração não tem a ver com prioridade e sim o TTL

40) Para que o modo de utilização anônimo funcione no vstpd qual seria a diretiva que deveria estar no arquivo vsftpd.conf?

a) listen=Yes
b) anonymous=Yes
c) anonymous_enable=Yes
d) anonymous-enable=Yes
e) anonymous_only=Yes

41) São consideras portas de um servidor FTP:

a) 22
b) 23
c) 21
d) 25
e) 20

42) Com quais comandos posso verificar se um serviço está executando normalmente em relação a testes de portas? Escolha 3 opções.

a) netstat
b) iptables
c) nmap
d) tcpd
e) fuser

43) Qual comando ftp é usado para listar diretórios locais a partir de um servidor ftp?

a) ls
b) dir
c) !ls
d) ?ls
e) %ls

44) Um servidor SSH está configurado para usar TCP WRAPPER e apenas hosts da rede classe C 192.168.1.0 deve ter permissão para acessá-lo. Qual das seguintes linhas abaixo poderia aplicar isso no arquivo /etc/hosts.allow?

a) ALLOW:192.168.1.0/255.255.255.0:sshd
b) sshd:192.168.1.0/255.255.255.0:ALLOW
c) 192.168.1.0/255.255.255.0:ALLOW:sshd
d) tcpd:sshd:192.168.1.0/255.255.255.0:ALLOW
e) sshd:ALLOW:192.168.1.0/255.255.255.0:ALLOW

45) Qual arquivo define os níveis de mensagens escritas nos arquivos de log? Escreve apenas o nome do arquivo. _____

46) Você deseja se certificar que seu sistema não está sobrecarregado com usuários executando múltiplos agendamentos. Uma política foi estabelecida em que apenas o administrador do sistema poderá criar agendamento ou definir quem poderá agendar tarefas. Como poderia ser feito isso?

a) Criar um arquivo vazio chamado /etc/cron.deny
b) Criar um arquivo chamado /etc/cron.allow com os nomes que terão permissão para agendar as tarefas
c) Criar um arquivo chamado /etc/cron.deny contendo todos os nomes de usuários
d) Criar duas arquivos vazios chamados de /etc/cron.allow e /etc/cron.deny

47) Quais são os campos em sua ordem correta para um agendamento de tarefa com o cron?

a) minuto, hora, dia da semana, dia do mês, mês
b) minuto, hora, mês, dia do mês, dia da semana
c) minuto, hora, dia do mês, mês, dia da semana
d) hora, minuto, dia do mês, mês, dia da semana

48) Quando você olha o arquivo /etc/passwd, você observa que todos o campos de senha contém um “x”. O que isso significa?

a) Que a senha não está encriptada.
b) Que você está usando senhas shadow.
c) Que todas as senhas estão em branco.
d) Que todas as senhas expiraram.

49) Você criou um novo usuário adicionando uma linha no arquivo /etc/passwd:
leo::1001:1001:Leonardo Amorim:/home/leo:/bin/bash

Você então cria o diretório home dele e usa o comando passwd para setar sua senha.
No entanto, o usuário leo lhe chama dizendo que não consegue logar. Qual é o problema?

a) O usuário não pode alterar sua senha
b) O usuário leo não tem permissão no diretório /home/leo
c) O usuário não pode digitar seu login
d) Você não pode deixar a senha de um usuário em branco quando o cria

50) Linus Torvalds, tem um login que é linus, ele pede para que você administrador mude a senha, pois ele a esqueceu. Como fica a linha de comando para mudar a senha dele? Escreva apenas o nome do comando e seu parâmetro. _____

51) Como seria o comando para adicionar outro IP a uma mesma placa de rede que já tem um endereço IP?

a) ifconfig eth0 192.168.0.2
b) ipconfig eth0 192.168.0.2
c) ifconfig eth0:0 192.168.0.2
d) ipconfig eth0:0 192.168.0.2

52) Qual comando pode ser usado para verificar quais arquivos estão abertos? Escreva apenas o nome do comando sem o caminho completo. _____

53) Qual a porta que o portmap utiliza?

a) 53
b) 3128
c) 111
d) 22
e) 445

54) Você está tentando iniciar o sistema e modificar a senha de root, que você não sabe. O que você deve digitar no prompt do LILO?

a) linux /etc/passwd
b) linux norootpass
c) linux disable passwords
d) linux init=/bin/bash
e) linux passwd=0

55) Como ativar o módulo ip_forward que é responsável pelo encaminhamento de pacotes?

a) echo 0 > /proc/sys/net/ipv4/ip_forward
b) echo 1 > /proc/sys/net/ipv4/ip_forward
c) echo 0 > /proc/sys/net/ipv4/ipforward
d) echo 1 > /proc/sys/net/ipv4/ipforward
e) nenhuma das opções

56) Como você faria para liberar a porta 3128 na configuração do firewall para que o Squid possa receber conexões?

a) iptables -A INPUT -i eth0 -p tcp –dport 3128 -j ACCEPT
b) iptables -A OUTPUT -i eth0 -p tcp –dport 3128 -j ACCEPT
c) iptables -A INPUT -i eth0 -p tcp –sport 3128 -j ACCEPT
d) iptables -A INPUT -i eth0 -p tcp –dport 3128 -x ACCEPT

57) O comando _____ lista os dispositivos usb conectados.

58) O comando _____ verifica o cache de endereços ARP do seu computador. Escreva o comando sem parâmetros.

59) Você precisa adicionar um usuário chamado “linus” no Samba. O comando _____ faz isso. Escreva o comando com os parâmetros e argumentos.

60) Existem 7 campos no arquivo /etc/passwd. Qual das seguintes opções estão na ordem correta?

a) nome do usuário, UID, senha, GID, diretório home, shell, comentário
b) nome do usuário, senha, UID, GID, comentário, diretório home, shell
c) nome do usuário, GID, senha, UID, diretório home, shell, comentário
d) UID, nome do usuário, senha, GID, diretório home, shell, comentário

61) Qual o nome e o caminho completo para o principal arquivo de log do sistema?
_____

62) Qual permissão padrão do diretório /tmp?

a) 0777
b) 0755
c) 7777
d) 1777

63) Qual dos seguintes comandos executará um script chamado “MeuScript.sh” todos os dias às 10:30 da noite?

a) * 22 30 * * MeuScript.sh
b) 22 30 * * * MeuScript.sh
c) 30 22 * * * MeuScript.sh
d) * * * 22 30 MeuScript.sh

64) Qual dos logins abaixo é válido no sistema?

a) Linus Torvalds
b) ltorvalds
c) Linus T
d) L.T.

65) O identificador de usuário (UID) inicial é definido no arquivo (escreva o caminho completo)
_____