Exercicios LPIC 102

105.1 Customização e Uso do Ambiente Shell

1. Declare de maneira definitiva, para todos os usuários, uma função que limpe a tela e gere o resultado abaixo ao se digitar "inicio".

"Seja bem-vindo <usuário> Este sistema está ativo desde <1999-01-01 11:11:11>

Bons Estudos!"

* <> indica o uso do resultado de uma variável ou comando

```
~/profile
    inicio () {
        clear;
        echo -n "Seja bem-bindo $USERNAME Este sistema está ativo desde"
        uptime -s
    }
```

2. Configure apenas o seu usuário para executar a função "inicio" em todo novo login.

```
Adicionar em ~/.profile
```

3. Faça que a mesma configuração realizada no passo 2 esteja presente para todos os novos usuários criados a partir de agora.

```
Editar o /etc/.skel/profile
```

4. Muitos usuários andam apagando arquivos indevidamente e depois solicitando que você recupere backups. Para reduzir o problema, você resolve configurar o ambiente para que o comando "rm" sempre peça uma confirmação antes de efetivamente apagar o arquivo ou diretório. Faça a configuração para todos os usuários.

```
/etc/profile
    alias rm="rm -i"
```

105.2 Customização e Criação de Scripts Simples

5. Crie um script que gere o seguinte menu e faça as operações mencionadas:

Escolha a opção desejada:

1 - Fazer uma contagem regressiva começando do número informado como parâmetro

```
seq $1 -1 0 | while read i; do echo -en "\r$i"; sleep 1; done
```

2 - Verificar se o parâmetro informado é um arquivo presente no diretório /etc/

```
if [ "" = "$(find /etc -name $1)" ]; then
    echo "Diretório inexiste"
else
    echo "Diretório existente"
fi
```

*3 - Analisar o /etc/passwd e exibir apenas o nome do usuário (campo 1) e seu ID (campo 3), considerando linhas que possuam /bin/bash
*

```
grep "/bin/bash" /etc/passwd | cut -d: -f1,3
```

Final

```
echo "Comçando o script"

echo "Escolha uma das opções"
echo "1 - Contagem regressiva"
echo "2 - Busca por arquivo no /etc"
echo "3 - Usuarios passwd"

read option

switch option
    case 1:
        seq $1 -1 0 | while read i; do echo -en "\r$i"; sleep 1; done
    case 2:
        if [ "" = "$(find /etc -name $1)" ]; then echo "Diretório inexiste"; else
echo "Diretório existente"; fi
    case 3:
        grep "/bin/bash" /etc/passwd | cut -d: -f1,3
```

106.1 Instalar e Configurar X11

1. Caso não exista, gere o arquivo /etc/X11/xorg.conf em sua instalação do Linux e obtenha as configurações referente ao mouse e teclado.

Caso tenha problemas em gerar o xorg.conf, use como base a URL: https://mg.pov.lt/xorg.conf

```
Xorg -configure
# Buscar os dados no arquivo /etc/xorg.conf
# Encontrar os topicos InputDevice
```

2. Conforme demonstrado na aula, utilize duas máquinas virtuais e teste o uso da variável de ambiente DISPLAY para executar uma aplicação em uma máquina linux e exibi-la em outra.

```
# Verificar o ip da maquina que será cliente
ip a

# Maquina servidor
xhost +IP
# Executar os comandos
```

106.3 Acessibilidade

3. Habilite a configuração de teclado que faz com que a tecla só seja realmente digitada se pressionada por alguns segundos/milissegundos.

```
Slow Key
```

4. Habilite a configuração que permita o uso do teclado para pessoas não conseguem pressionar duas teclas simultaneamente.

```
Sticky Key
```

5. Instalar e utilizar o Screen Magnifier

```
sudo apt install kmag
kmag &
```

107.1 Gerenciamento de Usuários e Grupos

1. Crie os usuários aluno1, aluno2 e aluno3, todos contendo o diretório pessoal no /home e utilizando o shell /bin/bash.

```
useradd aluno1 -m -s /bin/bash
```

2. Crie os grupos time1, time2 e time3

```
groupadd time1
```

3. Identifique o UID do aluno1 e o GID do time1

```
grep aluno1 /etc/passwd
```

4. Defina o grupo padrão do aluno1 como time1

```
usermod aluno1 -g time2
```

5. Defina os grupos time2 e time3 como grupos adicionais do usuário aluno1

```
usermod aluno1 -G time1,time3
```

6. Remova o usuário aluno3, inclusive seu diretório /home

```
userdel -r aluno3
```

7. Defina alguma senha para os usuário aluno1 e aluno2

```
passwd aluno1
```

8. Faça com o que o usuário aluno2 fique impedido de logar, em estado de "lock"

```
chage -E0 aluno2
```

9. Faça com que o usuário aluno1 seja forçado a trocar a senha no próximo login.

```
chage -d0 aluno1
```

107.2 Automatização de Tarefas Administrativas através de agendamento

10. Configure o sistema do cron para que o usuário aluno2 não possa usar o serviço

```
echo "aluno3" >> /etc/cron.deny
```

11. Utilizando a cron, crie um agendamento de sistema, que rode um script hipotético chamado /opt/bin/limpeza.sh, todo dia às 07:30, como usuário root.

```
/etc/crontab
    30 7 * * * root /opt/bin/limpeza.sh
```

12. Insira um novo agendamento via cron para o usuário aluno1, para executar um script hipotético chamado /opt/bin/relatorio-semanal.sh, que será executado toda segunda-feira às 08:00

```
echo "0 8 * * 1 aluno1 /opt/bin/relatorio-semanal.sh" > cron.sh
crontab cron.sh
```

13. Insira um novo agendamento via cron para o usuário aluno1, para executar um script hipotético chamado /opt/bin/relatorio-erros.sh, que será executado de segunda a sexta, de hora em hora (minuto 0), mas apenas das 09 às 18.

```
0 * * * 1-5 aluno1 /opt/bin/relatorio-erros.sh
```

14. Use o at para agendar a execução do seguinte comando para daqui a 2 horas: wall "Treinamento de Incêndio, evacuem o prédio"

```
at now +2hour
>   wall "Treinamento de incendio, evacuem o predio"
ctrl+d
```

15. Crie um agendamento usando o at para que às 16:00 seja executado o seguinte comando: echo "Hora do Café"

```
at 16:00
>   echo "Hora do café"
ctrl+d
```

16. Utilizando o systemd-timers, crie um serviço referente à execução do script ~HOME/script-timers.sh e um agendamento para que ele seja executado de Segunda a Sexta, a cada 10 minutos.

```
##   .timer
[Unit]
Description=Agendamento
[Timer]
OnCalendar=*-*-1..5 *:*:/10
[Install]
WantedBy=timers.target

##   .service
[Unit]
Description=Agendamento
[Service]
Type=oneshot
ExecStart=~/script-timer.sh
KillMode=process
TimeoutStopSec=900
```

107.3 Localização e Internacionalização

17. Altere o timezone padrão de sua instalação para Europe/Paris

```
cp -prf /etc/localtime /etc/localtime.bkp
rm -f /etc/localtime
ln -s /usr/share/zoneinfo/Europe/Paris /etc/localtime
```

18. Suponha que o usuário aluno1 deseja que seu timezone seja referente à Santiago no Chile. Identifique o nome correto do timezone e faça a configuração permanentemente, impactando apenas este usuário.

```
/home/aluno1/.profile
    export TZ=America/Santiago
```

19. Restaure o /etc/localtime original de sua instalação

```
rm –f /etc/localtime
cp –prf /etc/localtime.bkp /etc/localtime
```

20. Verifique todas as configurações de localização atual de sua instalação

```
locale
```

21. Faça com que todas as configurações de localização e codificação sigam a definição en_US.UTF-8

```
export LC_ALL=en_US.UTF-8
```

108.1 Manutenção do Horário do Sistema

1. Utilize os comandos *date* e *echo* para criar a frase: "Hoje é dia DD/MM/YYYY. A hora atual é HH:MM"

```
echo -n "Hoje é dia $(date +%d/%m/%Y). A hora atual é $(date +%H:%M)"
```

2. Altere a data atual de seu Linux para 30/12/2017 às 23:00.

```
date 123023002017
```

3. Sincronize o horário do sistema operacional a partir do horário atual do relógio do hardware (BIOS)

```
hwclock --hctosys
hwclock -s
```

4. Utilize a pool de servidores do NTP Pool Project para atualizar o horário de sua instalação. Utilize apenas um comando para atualização imediata.

```
ntpdate pool.ntp.org
```

5. Verifique a lista atual de servidores NTP em uso pelos daemons ntpd ou chrony.

```
nptq -p
chronyc sources
```

108.2 Sistema de Logs

6. Crie as seguintes configurações no rsyslog:

- Enviar todos os registros criados pelo facility local7, em qualquer nível, para o arquivo /var/log/local7.log
- Enviar os registros criados pelo facility local7, quando a criticidade for err ou mais crítico, para /var/log/local7.error
- Enviar todos os registros do facility local6 para o servidor de logs remoto 10.0.0.100
- Enviar todos os registros do facility local5, com a criticidade alert ou emerg para o terminal do usuário *admin*.

```
/etc/rsyslog
    local7.*        /var/log/local7.log
    local7.err      /var/log/local7.error
    locat6.*        @10.0.0.100
    local5.alert    admin
```

7. Crie um registro de log para a facility local7, no nível error e utilizando a tag "Exercícios", com a mensagem "Esta é uma mensagem de erro"

```
logger local7.err -t [Exercicios] -p "Essa é uma mesangem de erro"
```

8. Veja os logs do systemd-journal gerados entre as horas 12:00 e 15:00 do dia 15 de Junho de 2017.

```
journalctl --since "2017-06-15 12:00" --until "2017-06-15 15:00"
```

9. Configure o logrotate para rotacionar o log /var/log/local7.log semanalmente, mantendo e compactando os últimos 8 arquivos rotacionados.

```
/etc/logrotate.d/local7.log
    #  /var/log/local7.log {
    #   rotate 8
    #   weekly
    #   compress
    #   notifempty
    # }
```

108.3 Básico sobre Agentes de Envio de Emails (MTA)

10. A partir do terminal Linux, envie um e-mail para o usuário "aluno1" contendo todo o conteúdo do arquivo de configuração principal do rsyslog, com o título "Arquivo do Rsyslog"

```
mail -s "Arquivo do Rsyslog" aluno1 < /etc/rsyslog.conf
```

11. Configure o MTA para que todo e-mail enviado para o usuário "presidente" seja encaminhado para o usuário "secretaria". Considere que não existe no sistema uma conta chamada "presidente".

```
Edite o arquivo /etc/aliases e insira a seguinte configuração:
presidente: secretaria
Execute o comando: # newaliases
```

12. O usuário "aluno1" deseja encaminhar automaticamente todos os e-mails enviados a ele para a conta "lp1". Como ele deve proceder?

```
~/.forward
    lpi1
```

13. Verifique quantas mensagens estão atualmente paradas ou em processamento pelo MTA.

```
mailq | grep -c "^[A-F0-9]"
```

108.4 Gerenciamento de Impressoras

14. Você adquiriu a impressora "HP Photosmart 1115", que foi encontrada na rede pelo cups como socket://10.0.0.150. Configure essa impressora como padrão do Linux. Utilize apenas linha de comando.

```
Inicialmente descubra o driver da impressora pelo comando:
# lpinfo -m|grep "HP Photosmart 1115"
Agora utilize o lpadmin para adicionar a impressora:
# lpadmin -p NomeImpressora -E -v “ socket://10.0.0.150” -m drv:///hpcups.drv/hp-
photosmart_1115.ppd
Definindo a impressora como padrão:
# lpoptions –d NomeImpressora
```

15. Envie para impressão na impressora padrão todo o arquivo /var/log/messages

```
# cat /var/log/messages | lpr
Ou
# lpr /var/log/messages
```

16. Você possui uma impressora chamada ImpressoraReserva, que não é sua impressora padrão. Visualize todos os trabalhos dessa fila e em seguida remova todos os jobs com apenas um comando.

```
Para visualizar utilize o comando:
# lpq –P ImpressoraReserva
Para remover utilize o comando:
# lprm -P ImpressoraReserva –
* o sinal - no final do comando faz com que todos os Jobs sejam removidos. Na sua ausência, apenas o job mais recente será apagado.
```

109.1 Fundamentos de Protocolos de Internet

1. Considerando uma máquina cujo IP é 192.168.100.15 e possui a máscara 255.255.255.0. Responda às seguintes perguntas:

- O IP da Rede

```
192.168.100.0/24
```

- O IP de Broadcast da Rede

```
192.168.100.255
```

- A Classe de IPs (A, B ou C)

```
C
```

- Quantas máquinas podem ser alocadas na mesma rede

```
254
```

- O CIDR equivalente à esta máscara

```
/24
```

- Qual máscara deve ser utilizada para que esta rede seja dividida em 2

```
/25
```

2. Em uma mesma rede física temos hosts configurados com os IPs e Máscaras abaixo:

- A) 192.168.10.20 / 255.255.255.0
- B) 192.168.10.30 / 255.255.0.0
- C) 192.168.20.30 / 255.255.0.0
- D) 172.16.12.1/24
- E) 172.16.12.100/24
- F) 172.16.10.100/25
- G) 172.16.10.150/25

- H) 172.16.10.200/25

Indique com quais outros hosts cada host consegue se comunicar. Por exemplo, o Host A consegue comunicação com os hosts X e Y, e etc.

Você pode realizar testes definindo IPs manualmente em VMs e utilizando o comando ping.

```
A - B
B - A,C
C - B
D - E
E - D
F - Null
G - H
H - G
```

109.2 Configuração Básica de Redes

3. Utilizando o NetworkManager, crie uma nova conexão de nome "nova-rede", do tipo ethernet, que associe a interface enp0s3 ao ip 192.168.8.100, máscara 255.255.255.0 e gateway 192.168.8.1

```
Utilize os comandos abaixo:
# nmcli connection add type ethernet con-name nova-rede ifname enp0s3 ip4
192.168.8.100/24 gw4 192.168.8.1
# nmcli connection up nova-rede
```

109.3 Resolução de Problemas de Redes

4. Verifique se há uma rota padrão ativa em seu host Linux

```
route -n
ip route show
```

5. Identifique qual porta está sendo utilizada pelo processo "cupsd"

```
netstat -nalpt|grep cupsd
ss -nalpt|grep cupsd
```

6. Verifique se a porta utilizada pelo processo "cupsd" está aceitando conexões

```
telnet 0 631
netcat 0 631
```

7. Utilizando o comando ip, defina o IP da Interface enp0s3, ou sua primeira interface, para o IP 172.16.32.100, máscara 255.255.255.0 e defina o gateway como 172.16.32.1

```
ip address flush dev enp0s3
ip address add 172.16.32.100/24 dev enp0s3
ip route add default via 172.16.32.1
```

109.4 Configuração de Cliente DNS

8. Configure manualmente sua VM Linux para utilizar como servidores de DNS os IPs abaixo:

- 8.8.8.8
- 8.8.4.4

```
Edite o arquivo /etc/resolv.conf e inclua as linhas abaixo:
nameserver 8.8.8.8
nameserver 8.8.4.4
```

9. Configure sua máquina Linux para associar o nome "roteador-padrao" ao IP 100.100.100.100

```
# /etc/hosts
100.100.100.100     roteador-padrão
```

10. Consulte informações do domínio lpi.org utilizando o servidor DNS Público de IP 1.1.1.1 ao invés das configurações definidas no /etc/resolv.conf.

```
dig lpi.org @1.1.1.1
```

11. Verifique se seu Linux é capaz de obter o IP associado ao endereço www.debian.org

```
host www.debian.org
```

110.1 Realizar tarefas de segurança do sistema

1. Configure o sudo para que o usuário "aluno1" (crie se não exisitir) tenha permissão de executar os comandos poweroff, reboot e shutdown.

```
# Editar o arquivo "/etc/sudoers" e adicionar as seguintes confguraaçes
    Cmnd_Alias Exercicio = /sbin/poweroff /sbin/rebootf /sbin/shutdown
    aluno1 ALL=Exercicio
    # O usuário deverá executar os comandos precedido pelo comando “sudo”
```

2. Faça que um comando que mostre a última vez que cada usuário do sistema fez login mas exclua os usuários que nunca logaram no sistema.

```
lastlog | grep -v "Never logged in"
```

3. Conte quantas vezes o usuário "lpi1" logou no sistema no mês atual

```
last | grep -c "lpi1"
```

4. Defina as seguintes características na conta do usuário "aluno1"

- O usuário deve trocar a senha a cada 2 meses

```
passwd -x60 aluno1
chage -M60 aluno1
```

- O usuário pode trocar a senha no máximo 1 vez por semana

```
passwd –n7 aluno1
chage -m7 aluno1
```

- 1 semana antes da senha expirar, o usuário deve receber avisos

```
passwd –w7 aluno1
chage –W7 aluno1
```

- Após a senha expirar o usuário tem uma semana para trocar a senha antes que a conta fique inativa

```
passwd –i7 aluno1
chage –I7 aluno1
```

5. Gere um arquivo chamado /tmp/relatorio_suid.out contendo todos os arquivos do sistema, e apenas os arquivos, que possuem a permissão de SUID definida.todo o sistema

```
find / -perm -4000 -ls > /tmp/relatorio_suid.out
```

6. Configure o sistema para que o usuário "aluno1" só possa realizar 2 logins simultâneos no sistema.

```
# /etc/secutiry/limits.conf
lpi2    hard    maxlogins   2
```

7. Identifique todas as portas TCP em estado LISTEN na sua estação/VM Linux no momento.

```
netstat -tlpn | grep TCP
# Esse limite será aplicável para logins em terminaisf não nas abas do simulador de terminal
```

8. Faça um mapeamento de todas as portas abertas nos hosts de sua rede interna. Em um ambiente corporativo, peça permissão ao administrador da rede.

```
nmap IP/Máscara (ex: nmap 192.168.8.0/24)
```

110.2 Configurar Segurança do Host

9. Disponibilize o serviço de FTP através do xinetd

```
No diretório /etc/xinet.d/ adicione um arquivo com as seguintes confguraaçes:
service fp
{
    fags         = REUSE
    socket_typpe = stream
    wait         = no
    user         = root
    server       = /usr/sbin/in.fpd
    log_on_failure += USERID
    disable      = no
}
```

10. Configure o TCP Wrapper para que aceite apenas conexões da rede local ou do localhost para o serviço ftpd.

```
# /etc/hosts.allow
    in.fpd: 10.0.0.*
    in.fpd: 127.0.0.1
# /etc/hosts.denyp
    in.fpd: ALL
```

110.3. Protegendo dados com Encriptação

11. Crie uma segunda máquina virtual utilizando a opção "Clone" do VirtualBox. Faça com que o usuário aluno1 da máquina1 consiga conectar via SSH no usuário lpi1 da máquina2, sem a necessidade de digitar usuário e senha.

```
# Na máquina1f logado como aluno1f gere as chaves:
ssh-keypgen -t rsa -b 1024
# Dentro do diretório /home/lpi1/.sshf copie o conteúdo do arquivo id_rsa.pub Na
máquina2f logado como lpi1f crie ou edite o arquivo
# ~/.ssh/authorized_keys
# e adicione o conteúdo copiado da chave pública do aluno1.
# Realize um teste de conexão.
```

12. A partir da máquina1, execute remotamente o Firefox do servidor X remoto

```
ssh -X lpi1@IP "firefox"
```

13. Realize todos os procedimentos para que o usuário aluno1 da máquina1 possa enviar um arquivo criptografado que será lido pelo usuário lpi1 na máquina2.

```
Na máquina 2f logado como lpi1:
    Gerar as chaves: # gpg --gen-keyp
    Exportar a chave pública: # gpg --output arquivo.pub --export "Identfcaaão"
    Enviar a chave via SCP para a máquina1f usuário aluno1. Em uma das máquinas o
openssh-server deve estar instalado
Na máquina 1f logado como aluno1:
    Importar a chave pública do lpi1: # gpg --import arquivo.pub
    Criptografar o arquivo: # gpg --recipient "Identfcaaão" --output arquivo-
criptografado.gpg --encryppt arquivo-origem.out
    Enviar o arquivo-criptografado.gpg via SCP para a máquina2.
Na máquina 2f logado como lpi1:
    Descritpgrafar o arquivo: # gpg --output arquivo-descriptografado.txt --
decryppt
arquivo-criptografado.gpg
```