Segurança Básica

Essas são coisas que todo usuário pode fazer para melhorar a segurança do sistema. Tópicos avançados não serão apresentados aqui, apenas o básico que cada usuário pode implementar facilmente e fornecer uma proteção decente.

Use senhas fortes

A força da sua senha depende de três coisas:

1. Comprimento: uma senha mais longa é uma senha mais forte. Os guias sugerem pelo menos 8 caracteres.
2. Complexidade: Quanto mais variados os caracteres da senha, mais forte é a senha.
3. Dedutibilidade: quanto mais difícil para um invasor derivar uma senha, melhor.

Certifique-se de alterar sua senha com freqüência para que, se alguém estiver tentando decifrá-la, seja necessário reiniciá-la. Veja também o guia definitivo para criar senhas fortes.

Desabilite serviços não utilizados

No Slackware, torne não executáveis quaisquer arquivos rc em `/etc/rc.d` que iniciem serviços que você não usa. Por exemplo:

```
chmod a-x /etc/rc.d/rc.gpm-sample
```

Quanto menos serviços você usa, menores são as chances de que haja um bug que permita a um invasor explorá-lo remotamente.

Configure um Firewall

No Slackware, a maneira mais fácil de fazer isso é usando a adaptação de Alien Bob do Easy Firewall Generator . Apenas gere o firewall, copie a saída para `/etc/rc.d/rc.firewall` e torne-o executável.

```
chmod a+x /etc/rc.d/rc.firewall
```

Outras opções incluem programas de geração de firewall GUI, como Firewall Builder.

X -nolisten tcp

Por padrão, o servidor Xorg escuta a porta 6000 para conexões remotas. Às vezes você quer conexões remotas, mas se não quiser, desabilitá-las é uma boa ideia. A maneira mais fácil de fazer isso é criando este arquivo em `~/.xserverrc` **OU** `/etc/X11/xinit/xserverrc`.

xserverrc

```
#!/bin/sh

exec /usr/bin/X -nolisten tcp
```

Você pode especificar mais opções para o X no mesmo arquivo se precisar do. xserverrc

No Slackware, a escuta de solicitações XDMCP é desabilitada por padrão tanto no xdm quanto no kdm, portanto, é seguro por padrão. Alguém pode perguntar, por que se preocupar em impedir o Xorg de ouvir se esse for o caso? É sempre melhor não confiar nos arquivos de configuração, como exemplificado por um relatório de bug antigo quando xdm ignorou seu arquivo de configuração.

Verifique as portas abertas

Algumas maneiras de verificar se há portas abertas:

```
nmap localhost
nmap YOUR_EXTERNAL_IP_ADDRESS
netstat -luntp
```

Seu endereço IP externo pode ser encontrado em sites como http://whatismyipaddress.com/. Se você não sabe para que uma determinada porta é usada, verifique esse wiki.

Procure por malwares

Os programas a seguir são úteis para detectar rootkits e vírus:

- rkhunter
- ClamAV

Embora não existam muitos malwares para Linux, é uma boa ideia fazer uma varredura de vez em quando.

Fontes

- the ultimate guide for creating strong passwords
- http://slackwiki.com/Basic_Security_Fixes
- http://slackwiki.com/Security_Assessment_using_Nmap

security, software, author htexmexh, translator carriunix

From:
https://docs.slackware.com/ - **SlackDocs**

Permanent link:
https://docs.slackware.com/pt-br:howtos:security:basic_security

Last update: **2021/10/02 02:36 (UTC)**