

Sobre vírus e o Linux

Contribuição de Gabriel "Pnordico" Menezes
08 de dezembro de 2008

Após muitas discussões e "conversas informais" sobre este assunto eu decidi absorver as principais referências e deixar aqui a minha tentativa de elucidar, de uma vez por todas (por mais difícil que isso seja), este tema, destruindo mitos, expondo a verdade, afirmando, confirmando e convencendo de uma vez por todas que o Linux (assim como todos os outros Unix e Unix-like) são sistemas extremamente seguros e confiáveis.

- 1- Considerações Iniciais
- 2- Existe vírus para Linux?
- 3- Mas existem antivírus para Linux...
 - 4- Os vírus do Windows rodam no Linux? E pelo Wine?
 - 5- Mas eu já li sobre máquinas Linux sofrendo ataques
 - 6- Existem outros fatores que contribuem para que o Linux seja seguro?
 - 7- Mas isso torna o sistema invulnerável?
 - 8- E na Internet?
 - 9- Engenharia Social? Que ameaça é essa?
 - 10- E as aplicações multiplataforma?
- I- Créditos

1- Considerações Iniciais Versão/Revisões: 5 (Sex 23 abr 2010 13:01)

Considerando o objetivo deste artigo não vou me ater aos conceitos de "vírus, worms, trojans ou código malicioso", tratando todos eles por "vírus".

Sobre este assunto dá para escrever um livro, portanto procurarei ser o mais direto possível e tratar dos questionamentos mais comuns.

Este texto será constantemente atualizado. Caso você ache que algum ponto ficou em aberto, entre em contato comigo através do e-mail ou orkut e peça educadamente para que sua dúvida seja abordada.

2- Existe vírus para Linux? A resposta teórica para essa pergunta é "Sim, existe..." e essa ameaça tem nome: "Rootkit". Mas isso quer dizer que eu posso ser infectado apenas por estar navegando pela internet (como acontece em outros sistemas)?

A resposta é "Não". O rootkit para atuar precisa ser instalado no sistema e essa instalação precisa ser feita como root. Isso quer dizer que é quase impossível você "pegar" um rootkit acidentalmente. As poucas pessoas confiáveis que já viram algum rootkit (é difícil até encontrar alguém que já tenha se deparado com algum) sabem que o rootkit foi instalado por uma outra pessoa (que tinha acesso de administrador na máquina, acesso físico e senha de root, uma pessoa que estava mal intencionada).

Recentemente ocorreu uma situação atípica, porém rapidamente detectada, onde um usuário mal intencionado de um site de temas, wallpapers e descanso de tela para o GNOME, aproveitou-se da disponibilização de pacotes através desse site e disponibilizou um pacote infectado com um rootkit.

Isso não mostra a vulnerabilidade do sistema em si, mas mostra que devemos tomar cuidado e não podemos instalar pacotes de fontes desconhecidas. A recomendação nesse caso é apenas utilizar os repositórios oficiais.

Portanto a resposta pra essa pergunta pode ser: "Sim, existe, mas ninguém nunca viu"

Saiba mais sobre rootkits

Detectando rootkits: <http://www.guiadohardware.net/dicas/detectando-rootkits.html>

Sobre Vírus e Linux

Vírus no Linux? http://www.cic.unb.br/docentes/pedro/trabs/virus_no_linux.html

Bliss, a Linux virus (Inglês) <http://math-www.uni-paderborn.de/~axel/bliss/>

3- Mas existem antivírus para Linux... Existem. ClamAV, Avast... No total são 25 listados pelo SuperDownloads. Mas qual o real objetivo desses antivírus (AV)? Onde e em quais casos eles são usados?

Esses softwares de AV são utilizados quando existe troca de dados entre uma máquina Linux e uma máquina Windows, assim você evita que a máquina Windows seja infectada por um arquivo que estava "inofensivo" na máquina Linux.

Isso quer dizer que o antivírus no Linux serve para proteger as máquinas Windows, pois os vírus são "inofensivos e inativos" no Linux. Para evitar que máquinas Windows sejam infectadas por esses arquivos (levados pela rede ou por pendrive, por exemplo) surgiu a necessidade de fazer o scan destes arquivos antes deles serem transportados para as máquinas Windows, assim surgiu a necessidade da existência de softwares antivírus que rodem no Linux.

Ou seja: "Eles existem, mas você não precisa deles pra usar seu Linux"

4- Os vírus do Windows rodam no Linux? E pelo Wine? Programas de Windows são para Windows. Linux não é Windows! Vírus para Windows não são feitos para rodar em Linux, portanto não vão rodar. É tão simples como dizer "você

não vai conseguir rodar um .exe [Binário/executável do Windows] no Linux".
Já os "vírus do Windows rodando no Wine" geram muitas discussões e dúvidas.

Você pode até conseguir fazer com que o "vírus" rode no Wine, vai fazer ele executar algumas de suas funções, baixar alguns arquivos talvez, mas ele não vai funcionar da mesma forma que funcionaria no Windows, porque o Wine não é o Windows, o Wine NÃO É UM EMULADOR DE WINDOWS.

Qual a diferença?

O Windows é um sistema operacional e possui seus arquivos de configuração, sua árvore de diretórios, seus serviços do sistema e sua rotina de inicialização e é justamente em alguns (ou todos) desses pontos que os vírus atuam. Os vírus pra Windows geralmente se aproveitam de vulnerabilidades e alteram a inicialização e/ou alguns serviços do sistema para que o próprio vírus rode na inicialização do sistema. Como o Wine não executa uma rotina de inicialização, um vírus instalado no Wine não será executado automaticamente bem como pode não funcionar, já que o Wine não possui as vulnerabilidades do Windows (sendo o Wine apenas uma implementação das APIs do Windows)

Um vírus sendo executado no Wine pode acabar baixando arquivos para o \$HOME do usuário, mas isso só acontece porque o Wine configura o \$HOME do usuário como um link para os "Meus Documentos" das aplicações Windows, então, na verdade, o vírus não está baixando um arquivo para seu \$HOME, ele está baixando um arquivo para "Meus Documentos" que na configuração do Wine está apontando para o seu \$HOME (e isso é configurável).

No caso do vírus ter sido programado pra rodar perfeitamente no wine e ser compatível com o Linux (o que é um tremendo desperdício de esforço e nem sabemos se isso é possível, sendo esta uma situação hipotética) ele dependeria de inúmeras brechas de segurança deixadas pelo usuário que levaria uma eternidade para citar, mas seguem alguns exemplos: Seria necessário que o usuário configurasse o wine para ter acesso ao /, configurasse o / com o chmod 777 recursivo dando acesso total do usuário ao sistema ou que o wine fosse executado como root, o wine deve ter suporte às funções necessárias para executar comandos no Linux, entre muitas outras. É tão difícil de imaginar que essa opção é considerada como impossível ou inviável, como eu disse, um desperdício de esforço em algo que provavelmente não funcionaria.

Resumindo: "Não existem vírus que façam isso e, mesmo que existissem, não causariam danos significativos"

5- Mas eu já li sobre máquinas Linux sofrendo ataques Nenhum sistema é perfeito ou livre de vulnerabilidades. Mas o que acontece para uma máquina ser atacada?

Normalmente essa máquina está rodando algum serviço (como apache, ssh, telnet) mal configurado que acaba gerando alguma falha na segurança. Sem comentar que muitas pessoas mal intencionadas usam de recursos como a engenharia social para obter as senhas, convencer as pessoas a executarem comandos, executarem serviços (como iniciar o ssh), entre outras coisas. Muitas vezes o "ataque" começa no usuário e só depois parte para o sistema, principalmente se o ofensor tiver acesso físico (pode mexer na máquina livremente).

6- Existem outros fatores que contribuem para que o Linux seja seguro? Sim, mas isso é assunto para outros artigos. Caso tenha interesse: A política de permissão dos sistemas Unix/Unix-like em geral. Isso pode ser demonstrado pelo fato de serem raras as notícias de problemas com Linux, MacOS, BSDs, Solaris (tanto que quando acontece a "mídia especializada" faz o maior alvoroço). Por outro lado, aparecem problemas a todo momento no Windows que a mesma "mídia especializada" parece tratar como "comuns".

Um outro fator importante é o fato do desenvolvimento se dar através do código aberto. O fato do software ser livre contribui para que falhas de segurança sejam localizadas e corrigidas com maior agilidade, pois ao invés de ter apenas uma empresa cuidando disso, existe toda uma comunidade de usuários do mundo todo realizando essa tarefa a todo o tempo.

7- Isso torna o sistema invulnerável? Não! De maneira alguma.

1-Nem todas as ameaças são vírus (conforme veremos adiante);

2-Como citado em (5) existem outros fatores ou programas que podem criar vulnerabilidades no sistema, entre eles estão:

- Sistema desatualizado com pacotes antigos que podem ter falhas de segurança;
- Política de segurança e acesso/permissões de usuários pouco efetivas;
- Senhas "fracas" (fáceis de adivinhar ou descobrir por força bruta ou engenharia social)
- Serviços mal configurados que podem permitir acesso remoto não autorizado (ssh ou apache, por exemplo)
- Instalação de pacotes de origem desconhecida onde podem ter sido inserido qualquer tipo de código malicioso
- Execução de comandos desconhecidos por parte do usuário (executar um comando que você não sabe o que faz pode ter consequências desastrosas).

Como se proteger?

Depende muito do caso. Algumas regras são básicas e devem ser seguidas, como:

- Manter o sistema atualizado;
- Utilizar apenas repositórios oficiais;
- Manter rodando apenas os serviços necessários e mantê-los bem configurados;
- Evitar usar senhas fáceis/fracas;

- Manter uma política séria de permissões e acesso de usuários;
- Apenas fazer algo se souber exatamente o que está fazendo;
- Utilizar as ferramentas de segurança de acordo com a sua necessidade.

Como deixar o sistema mais seguro

Linux Security HOWTO (Principal obra em questão de segurança em sistemas Linux)

General System Security (Para sistemas baseados no RedHat)

Securing Debian Manual (Para sistemas baseados no Debian)

Hardening Linux usando controle de Acesso Mandatário (Security-Enhanced Linux SELinux)

Introdução ao SELinux

8- E na Internet? A internet é um lugar hostil para os desavisados. Os crackers se aproveitam da distração e/ou ingenuidade dos usuários para roubar dados pessoais. Muita atenção deve ser dada às "ameaças virtuais", pois as citadas aqui independem do sistema operacional utilizado, porque o usuário é enganado ou convencido a enviar os dados pessoais diretamente para o criminoso.

- Phishing: Através de um site falso (que é criado como uma cópia do site verdadeiro) o usuário desavisado digita os dados pessoais e senha e estes são enviados diretamente para o criminoso.

- Scripts maliciosos: Aproveitando-se de alguma vulnerabilidade de algum site específico o cracker faz com que o usuário execute algum script (normalmente clicando em algum link desconhecido que aponta para o script) e acaba tendo acesso aos dados pessoais e/ou senha do usuário. (Esse tipo de vulnerabilidade já foi muito utilizada para roubar contas e comunidades no Orkut)

- Scam: Emails falsos que pedem informações pessoais por email alegando "recadastramento". Empresas sérias jamais pedem informações pessoais por email.

- Engenharia Social: Em sistemas de informação, é uma prática condenável que vai de encontro às regras de convívio em sociedade.

Aprenda um pouco mais sobre segurança na Web

GoogleBlog - Security (Em Inglês)

Como evitar ser fisgado (Sobre Phishing)

9- Engenharia Social? Que ameaça é essa? A segurança da informação em sistemas computacionais passou a receber cada vez mais atenção com o passar dos tempos e o advento de novas tecnologias através de ferramentas em hardwares e softwares cada vez mais avançados. Porém nessa equação existe uma variável que independe tanto das ferramentas de hardware quanto de software, o controlador do sistema, o detedor da informação e das senhas de acesso: O ser humano. E é justamente esse o foco da Engenharia Social.

Um ataque baseado em engenharia social parte de um princípio simples: O elemento mais vulnerável de qualquer sistema de segurança da informação é o ser humano.

É uma prática moral e socialmente condenável, pois, em muitas consiste em obter a confiança ou confundir o indivíduo fazendo com que sejam reveladas informações pessoais, críticas e/ou confidenciais e usar essas informações para qualquer fim, lícito ou não.

Aprenda mais sobre Engenharia Social

Entendendo e Evitando a Engenharia Social

Na Wikipedia (Inglês)

10- Aplicações Multiplataforma EM DESENVOLVIMENTO

I- Créditos Este texto foi escrito com a colaboração (direta ou indireta) de todos os que participaram deste tópico na Linux Brasil e:

Gabriel Pnord - Autoria e revisões

Marcos Miklos - Revisão, sugestões e links

Rhoy - Sugestões e revisão

Bruno Yporti - Sugestões e revisão

Cesar Augusto - Sugestões e revisão