

Insegurança

O filme "Karate Kid" ensina algumas lições valiosas para a segurança de sistemas.
por Kurt Seifried



stockxpert

Tenho notado uma tendência preocupante nos últimos cinco anos. O estado da segurança no Linux não parece estar melhorando. Isso não significa que não tenhamos tido grandes avanços tecnológicos: o SELinux já está disseminado e vários fornecedores entregam sistemas com serviços desativados e firewalls habilitados por padrão. Porém, em geral, o número e os tipos de falhas não mudaram muito, ou talvez estejam até piorando.

Em 2007, a Red Hat emitiu um total de 371 alertas de segurança com identificadores CVE, cada um representando pelo menos uma falha de segurança única, e às vezes mais de uma. A Mandriva não fica muito atrás, com 350 alertas. Porém, o Debian, com 444, e o Gentoo, com 539, nos levam a temer algo.

Não fui eu que escrevi

A primeira coisa que deve ser lembrada é que a maioria dos softwares incluídos pelos distribuidores de Linux não foi escrita por eles. A maioria das ferramentas de espaço de usuário num sistema Linux é reempacotada e talvez alterada pelo distribuidor, mas, além da resolução de falhas, a maioria dos distribuidores não altera em profundidade os softwares. Isso leva a vários problemas, tais como

permissões de arquivo fracas. Um exemplo perfeito dessa questão é a falha CVE-2002-0849. Em 2002, descobri que o principal software para iSCSI no Linux, produzido pela Cisco, incluía a senha CHAP (*Challenge Handshake Authentication Protocol*) num arquivo (`/etc/iscsi.conf`) legível por qualquer usuário. Com essa senha, um agressor conseguiria acessar os dados no volume iSCSI como se fosse o servidor, ignorando quaisquer restrições de arquivos ou outros mecanismos de segurança.

Então, eu rapidamente informei isso à Cisco, que consertou o problema e todos seguiram suas vidas.

Agora já é 2008 e, se verificarmos uma lista de vulnerabilidades de segurança, vamos encontrar o CVE-2007-5827: "iSCSI Enterprise Target (iscsitararget) 0.4.15 usa permissões fracas para `/etc/ietd.conf`, o que permite que usuários locais obtenham senhas".

Ninguém aprende nada?

Se você conferir o diretório `/etc/` em busca de arquivos com senhas, certamente encontrará algumas em pouco tempo. A **tabela 1** mostra todos os que eu obtive rodando os seguintes comandos como usuário comum:

```
$ grep -i password /etc/*  
$ grep -i password /etc/*/*
```

Encontrar essa classe de ameaças – e consertá-las – deveria ser trivial para a maioria dos fornecedores. A funcionalidade do sistema não deve ser afetada, pois a maioria dos serviços de rede é iniciada como root, lê seus arquivos de configuração e depois reduz seus privilégios.

Geralmente, basta remover as permissões de leitura irrestrita desses arquivos para solucionar o problema. Uma simples linha adicional no script `%post` de um pacote RPM – por exemplo, para executar `chown o-r [arquivo]` – seria suficiente.

Entretanto, os distribuidores não fazem isso e ignoram solenemente o problema, ou simplesmente se recusam a resolvê-lo. Mas o que isso tem a ver com o Karate Kid?

Assim como o Karate Kid, o administrador de sistemas padrão precisa aprender caratê (segurança de sistemas), caso contrário os vilões o atacarão num beco e usarão sua cabeça e rins como saco de pancadas (tornar-se root no sistema e tomá-lo para si). Muitos administradores ganharam inimigos involuntariamente; ativistas, empresas concorrentes, criminosos e outros ficariam felizes em dominar servidores alheios para vários motivos, incluindo o armazenamento de informações roubadas, ataques a sites, captura de informações de clientes etc.

Tabela 1: Arquivos com senhas

Programa	Arquivo	Variável com senha
Dovecot	/etc/dovecot.conf	ssl_key_password
FreeRADIUS	/etc/raddb/eap.conf	private_key_password
FreeRADIUS	/etc/raddb/mssql.conf	password
FreeRADIUS	/etc/raddb/postgresql.conf	password
FreeRADIUS	/etc/raddb/radiusd.conf	várias senhas
FreeRADIUS	/etc/raddb/snmp.conf	smux_password
FreeRADIUS	/etc/raddb/sql.conf	password
FreeRADIUS	/etc/raddb/users	User-Password
HSQLDB	/etc/init.d/hsqldb	TLS_PASSWORD
libpurple	/etc/purple/prefs.xml	password string
OpenHPI	/etc/openhpi/openhpi.conf	MULTIPLE
pam_pkcs11	/etc/pam_pkcs11/pam_pkcs11.conf	ldap passwd
quota	/etc/warnquota.conf	LDAP_BINDPW
Squid	/etc/squid/squid.conf	MULTIPLE
Tomcat	/etc/tomcat/server.xml	connectionPassword

No entanto, diferentemente do Karate Kid, a maioria de nós não possui um Sr. Miyagi para derrotar os malvados estudantes da Cobra Kai, não apenas salvando-nos de uma surra como também ensinando-nos a lutar melhor que eles. Os maus elementos lutam sujo. Muito sujo.

Lições aprendidas

O que aprendemos com a história de Karate Kid?

- ▶ É improvável uma trégua: no filme, eles pedem uma trégua enquanto o mocinho treinava. No mundo real, criar uma página web ou enviar emails aos spammers pedindo uma trégua enquanto se aprende a criar e administrar sistemas seguros não vai funcionar. Entretanto, pode-se conseguir algum espaço e limitar a quantidade de tempo gasto em requisições de usuários para se focar na melhoria dos sistemas, o que vale a pena.
- ▶ Encontre um mentor: encontrar um mentor normalmente

é uma boa idéia. Eu já gastei tempo suficiente (re)inventando a roda para saber que às vezes gastar dinheiro num livro é uma opção bem mais simples e rápida. Porém, ter alguém para ensiná-lo e responder suas dúvidas é ótimo. Vários grupos e organizações incentivam a segurança da informação, tais como ISC², ISACA e ISECOM. Muitas têm um regulamento e programas de incentivo ao aprendizado e à educação, e é provável que você encontre alguma disposta a ajudá-lo.

- ▶ Aprenda a lutar mesmo contundido: ao se encarar um agressor, você se debaterá com leis e regulamentos, e o vilão não joga limpo. Ele pode inundar suas caixas de mensagem com milhares de emails, e enquanto você lida com isso, ele entrará no servidor web e roubará todos os registros de clientes. Tenha um plano com antecipação para estar preparado caso os sistemas sejam comprometidos.

▶ Se preciso, chute a cara do seu adversário: diferentemente do Karate Kid, ninguém ganha pontos por estilo ao lidar com agressores. Fazê-los com rapidez e eficiência permite que se prossiga para o próximo problema. Algumas vezes, já vi pessoas procurarem a “melhor” solução para um problema de segurança em vez de buscarem simplesmente uma “boa”. Jamais uma solução será perfeita – sistemas e redes mudam, novos ataques serão encontrados e novas defesas serão descobertas. Aprender a despachar agressores rapidamente lhe oferecerá mais tempo para ser gasto na criação de sistemas melhores e para se concentrar na prevenção.

Conclusão

Se você quiser um sistema seguro, precisará trabalhar para conseguí-lo – poucos fornecedores entregam um desses pronto.

Além disso, provavelmente será necessário trabalhar para encontrar o tempo e a energia para gastar treinando e criando sistemas e redes melhores. Embora isso nem sempre seja fácil, qualquer outra coisa servirá apenas para manter o *status quo* e prolongar a dor. ■

Mais informações

[1] Karate Kid, na Wikipédia: http://pt.wikipedia.org/wiki/The_Karate_Kid

Sobre o autor

Kurt Seifried é consultor de segurança da informação especializado em redes e Linux desde 1996. Ele frequentemente se pergunta como a tecnologia funciona em grande escala, mas costuma falhar em pequena escala.