

Prevenção

Invasores de redes têm várias formas engenhosas de escalar privilégios e ocultar sua presença no sistema. A melhor proteção é mantê-los fora.

por **Tim Schürmann e Joe Casad**

Logo quando você pensava que havia dominado a arte de proteção contra invasões, os cibercriminosos descobrem novas técnicas para atravessarem sua segurança. Os agressores usam qualquer vantagem possível para ficarem escondidos e ganharem controle. Então, você não deve usar tudo que estiver disponível para mantê-los do lado de fora?

As matérias de capa deste mês são dedicadas a manter os invasores fora do seu sistema. Em nosso primeiro artigo, estudamos uma técnica poderosa para manter suas portas do firewall fechadas para todos os usuários – mas ainda aberta ao tráfego de máquinas amigáveis.

E se alguém invadisse seu sistema Linux e substituísse o programa *login* por uma variante maliciosa? O novo *login* descobre o seu nome de usuário e sua senha e envia os dados coletados por meio de um buraco em seu firewall para algum servidor em outro ponto da Internet. Ninguém suspeita do novo *login*, embora o invasor saiba que um administrador de sistema atencioso pode se perguntar sobre a mudança no tamanho do arquivo.

Mas criminosos na Internet têm uma forma de cobrir seus rastros. Junto com a ferramenta *login* alterada, o meliante inclui uma variante do programa *ls*. Essa nova versão do *ls* mascara

mudanças de tamanho e data do programa *login*.

O agressor também decide substituir vários outros programas do sistema que funcionam juntos para coletar informações e ocultar qualquer vestígio da intrusão. Até programas antivírus são inúteis, pois também são enganados pelas ferramentas manipuladas.

Essa situação não é, de forma alguma, ficção. Os invasores frequentemente trazem uma coleção de ferramentas para capturar informações, abrir *backdoors* e esconder suas atividades. Esse conjunto de armas é conhecido como *rootkit*.

Um *rootkit* geralmente contém vários componentes que realizam várias tarefas:

- ◆ um cavalo de tróia deposita o *rootkit* no sistema;
- ◆ um *sniffer* analisa o tráfego de rede e obtém as credenciais de acesso;
- ◆ em alguns casos, *keyloggers* registram as teclas pressionadas para capturar senhas ou PINs antes de o sistema criptografá-las;
- ◆ uma *backdoor* fornece ao invasor acesso ao sistema.

Todas essas atividades são camufladas pela substituição de arquivos de sistema e, para *rootkits* atuais, redirecionamento de chamadas de API. Outros componentes depois põem o computador em uso – possivelmente para distribuir spam ou desferir ataques de negação de serviço.

Inovação

No início, os *rootkits* simplesmente substituíam ferramentas de sistema populares como *ls*, *passwd* e *ps*. Os especialistas em segurança rapidamente aprenderam a detectar esses *rootkits* básicos e os programadores de malwares aprenderam, em seguida, como atuar no kernel em si.

Se um agressor conseguir injetar código malicioso no kernel, o código ofensivo do kernel pode capturar e redirecionar qualquer requisição.

Rootkits rodando no espaço do kernel são particularmente difíceis de descobrir. No Linux, *rootkits* de kernel costumam ser injetados por meio de um módulo do kernel, o que explica por que são conhecidos como *rootkits* LKM (*loadable kernel module*).



Os desenvolvedores de rootkits usam várias técnicas para infestar o kernel. Uma opção é manipular o retório de memória via `/dev/kmem`.

Firmware

Rootkits de firmware oferecem um vetor alternativo de ataque. Eles infectam o firmware do PC e sobrevivem a uma reinicialização. Alguns rootkits ficam bem à vontade nas rotinas de firmware do ACPI. Um disco de recuperação limpo não é muito útil contra esse tipo de ameaça.

Pílula azul

A última tendência são os rootkits virtualizados. Um rootkit virtualizado funciona como uma máquina virtual: a primeira etapa é o rootkit modificar o processo de inicialização para que seja carregada uma máquina virtual antes do sistema operacional. O sistema operacional que você acha que está rodando no hardware na verdade roda numa máquina virtual. Isso dá ao rootkit controle total sobre o computador, sem que o sistema operacional ou o usuário perceba qualquer coisa. O nome dessa técnica – *Blue Pill* [1] – é uma alusão ao filme *Matrix*, em que a pílula azul mantém uma pessoa no mundo virtual. A técnica para detectá-la se chama *Blue Pill Detection*.

Quadro 1: Compilar ou não compilar

As instruções para os administradores sugerem a compilação dos detectores de rootkits antes do uso. Porém, como se pode imaginar, isso é um problema caso o rootkit já tenha controle do sistema. Nesse caso, o compilador talvez já esteja comprometido e crie uma versão manipulada do detector. Por esse motivo, deve-se tentar compilar o detector imediatamente após a instalação do sistema, ou usar um sistema comprovadamente limpo.

Prevenção

Rootkits são muito difíceis de detectar após sua instalação no sistema. Antes de serem instalados, no entanto, é possível identificá-los com programas antivírus e buscadores de rootkits (ou detectores de rootkit), que usam assinaturas ou heurística para identificar os culpados (veja também o [quadro 1](#)).

A melhor forma de parar um rootkit é não deixá-lo entrar. Os artigos desta edição discutem algumas técnicas para manter invasores do lado de fora, antes que fiquem confortavelmente instalados.

Contudo, apesar de todos os nossos esforços, você jamais ficará seguro o suficiente para ignorar a possibilidade de um rootkit se esgueirar através das suas defesas. As seções a seguir discutem algumas estratégias para remoção de rootkits.

Verificação visual

Como os resultados em sistemas em execução não são inteiramente conclusivos, deve-se desligar o suspeito e reiniciá-lo a partir de uma fonte sabidamente limpa. Ela pode ser um disco de recuperação, por exemplo. O verdadeiro teste é verificar todos os arquivos suspeitos, conferindo-os contra um sistema limpo. Isso geralmente é feito comparando-se o sistema atual com um *snapshot* do sistema obtido diretamente após a instalação. Para impedir que o rootkit afete os resultados da comparação, armazene o snapshot original numa mídia somente leitura.

Obviamente, um becape completo do sistema precisa de espaço significativo em disco. Como alternativa,

pode-se apenas criar *checksums* para verificar a integridade dos arquivos. Para fazer isso, o buscador de rootkit calcula uma assinatura para cada arquivo; se o rootkit tentar alterar o arquivo, o checksum será automaticamente alterado e não coincidirá com o calculado na última atualização.

Chkrootkit

Um dos buscadores de rootkit mais populares para Linux é o *Chkrootkit* [2]. A ferramenta de Nelson Murilo e Klaus Steding-Jessen engloba uma coleção de pequenos programas em C especialmente escritos para detectar uma anomalia específica. Após descompactar o arquivo, compile os aplicativos com o sugestivo comando:

```
make sense
```

```

w@mer@linux:~/src/chkrootkit$ ./chkrootkit
Searching for RKLP files and dirs... nothing found
Searching for Dvocki rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for ShitC... nothing found
Searching for Omega Worm... nothing found
Searching for Sadini/IIS Worm... nothing found
Searching for Merkit... nothing found
Searching for Showtee... nothing found
Searching for OptiKit... nothing found
Searching for T.R.K... nothing found
Searching for Mithra... nothing found
Searching for LXC rootkit... nothing found
Searching for Romanian rootkit... nothing found
Searching for Sackit rootkit... nothing found
Searching for Volo rootkit... nothing found
Searching for Gold2 rootkit... nothing found
Searching for TIZ worm default files and dirs... nothing found
Searching for Annoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for SHKIT rootkit default files and dirs... nothing found
Searching for AjeKit rootkit default files and dirs... nothing found
Searching for z0rMf rootkit default files and dirs... nothing found
Searching for Madalin rootkit default files... nothing found
Searching for Fe rootkit default files... nothing found
Searching for ESRK rootkit default files... nothing found
Searching for rootbor... nothing found
Searching for BAYLER rootkit default files... nothing found
Searching for common ssh-scanners default files... nothing found
Searching for suspect PHP files... nothing found
Searching for anomalies in shell history files... Warning: '' is linked to another file
Checking 'asp'... not infected
Checking 'binshell'... not infected
Checking 'lrm'... chkproc: nothing detected
chkdirs: nothing detected
Checking 'revx6cs'... not found
Checking 'sniffer'... eth1: PF_PACKET(/sbin/dhccdd)
Checking 'v5000'... not infected
Checking 'vted'... chkutep: nothing detected
Checking 'scalper'... not infected
Checking 'slapper'... not infected
Checking 'z2'... chklastlog: nothing detected
Checking 'chkutep'... chkutep: nothing detected
linux:~/src/linux/oliver/chkrootkit$

```

Figura 1 O *Chkrootkit* rodou uma vez e não encontrou qualquer rootkit conhecido.

