

A large, light gray watermark of the GRIS logo is centered on the page. It features a stylized, interlocking geometric shape that forms a shield-like emblem. Inside this emblem, the letters "GRIS" are written in a bold, red, sans-serif font, tilted slightly upwards to the right.

Procurando por “Rootkits” em sistemas GNU/Linux



Universidade Federal do Rio de Janeiro
Instituto de Matemática
Departamento de Ciência da Computação
Grupo de Resposta a Incidentes de Segurança

Rio de Janeiro, RJ – Brasil

Procurando por “Rootkits” em Sistemas GNU/Linux

GRIS-2005-T-001

Breno Guimarães de Oliveira

A versão mais recente deste documento pode ser obtida na página oficial do GRIS

GRIS – Grupo de Resposta a Incidentes de Segurança
CCMN Bloco E 2º andar
Sala: I 1021
Av. Brigadeiro Trompowski, s/nº
Cidade Universitária - Rio de Janeiro/RJ
CEP: 21949-900
Telefone: +55 (21) 2598-3309

Este documento é Copyright© 2005 GRIS. Ele pode ser livremente copiado desde que sejam respeitadas as seguintes condições:

É permitido fazer e distribuir cópias inalteradas deste documento, completo ou em partes, contanto que esta nota de copyright e distribuição seja mantida em todas as cópias, e que a distribuição não tenha fins comerciais. Se este documento for distribuído apenas em partes, instruções de como obtê-lo por completo devem ser incluídas. É vedada a distribuição de versões modificadas deste documento, bem como a comercialização de cópias, sem a permissão expressa do GRIS.

Embora todos os cuidados tenham sido tomados na preparação deste documento, o GRIS não garante a correção absoluta das informações nele contidas, nem se responsabiliza por eventuais consequências que possam advir do seu uso.

Índice:

1. Introdução.....	5
2. Instalando e usando o chkrootkit.....	6
3. Instalando e usando o rkhunter.....	7
4. Verificação manual.....	9
5. Conclusão.....	10
6. Referências bibliográficas.....	10

1. Introdução

Antigamente, obter acesso ilegal a uma rede ou sistema era uma tarefa que exigia muito conhecimento específico da parte do invasor. Ainda assim, administradores eram capazes de identificar rápida e facilmente os sinais de uma invasão, bem como restaurar o sistema. A medida que o tempo foi passando, no entanto, novos métodos e programas para esconder rastros foram desenvolvidos, assim como versões modificadas de arquivos do próprio sistema para ocultar arquivos, diretórios e processos, além de permitir elevação de privilégios e acesso irrestrito ao invasor através de comandos especiais e palavras chave.

Rootkits são essencialmente coleções dessas ferramentas, utilizadas por invasores após o comprometimento de um sistema. Em conjunto, costumam incluir executáveis para monitorar o teclado (*keyloggers*), registrar tráfego de rede (*sniffers*), permitir acesso irrestrito ao sistema mesmo sem uma conta válida (*backdoors*) e, principalmente, esconder tudo que foi feito.

Felizmente, novas técnicas de defesa e ferramentas automáticas de varredura foram desenvolvidas para detectar e remover essas e outras “pestes digitais”. Neste tutorial, veremos o funcionamento de duas das mais famosas ferramentas com esse propósito: *chkrootkit* e *rkhunter*. Veremos também alguns métodos manuais de busca que podem auxiliar na descoberta de arquivos e diretórios suspeitos dentro de seu sistema.

Antes de começarmos, alguns aspectos devem ser levados em consideração. Primeiramente, verifique se sua organização possui uma política de segurança ou um procedimento específico para o tratamento de incidentes de segurança. Ao realizar uma varredura em seu sistema, bem como a posterior limpeza do mesmo, desconecte o sistema suspeito da rede (local e Internet). Caso contrário, você corre o risco de um intruso estar conectado ao seu sistema monitorando todas as suas ações, contornando e desfazendo seus passos enquanto você tenta recuperar seu sistema. Se possível, crie uma cópia (*backup*) de seu sistema antes de analisar a intrusão, e trabalhe em cima da cópia. Isso é importante para o caso de precisar restaurar a máquina comprometida ao estágio em que a invasão foi descoberta, e pode ser necessária para uma investigação criminal. Caso disponha de um disco rígido maior ou igual ao disco rígido comprometido, é possível criar uma cópia exata do mesmo através da ferramenta “*dd*”. Supondo que o sistema invadido está no disco `/dev/hdb` e você deseja replicar o mesmo no disco `/dev/hdc`, o comando é:

```
# dd if=/dev/hdb of=/dev/hdc
```

Note que os dados contidos em `/dev/hdc` serão substituídos pela imagem do disco em `/dev/hdb`. Não esqueça de rotular, datar e assinar a cópia, mantendo-a em local seguro

Uma vez identificada a presença de rootkits em seu sistema, é necessário a restauração do mesmo, quer substituindo apenas os programas comprometidos, quer reinstalando o sistema por inteiro. De qualquer forma, note que o ato de restaurar programas destruirá as provas da atividade do invasor em seu sistema, o que pode atrapalhar ou impedir completamente quaisquer investigações. Por isso, é extremamente importante a criação de cópias do sistema antes que qualquer arquivo seja apagado ou substituído.

2. Instalando e usando o chkrootkit

O chkrootkit é uma ferramenta desenvolvida por Nelson Murilo e Klaus Steding-Jessen capaz de identificar uma série de rootkits e sinais de invasão, como a retirada de entradas no registro *wtmp* do sistema, e pode ser encontrado em:

<http://www.chkrootkit.org>

O chkrootkit é compatível com inúmeros sistemas *NIX, como Linux, *BSD, Solaris, entre outros. Até a data de publicação deste tutorial, o chkrootkit estava na versão 0.45. Para instalar, entre na página oficial e obtenha o arquivo “chkrootkit.tar.gz”. Descompacte-o como faria com qualquer outro arquivo .tar.gz:

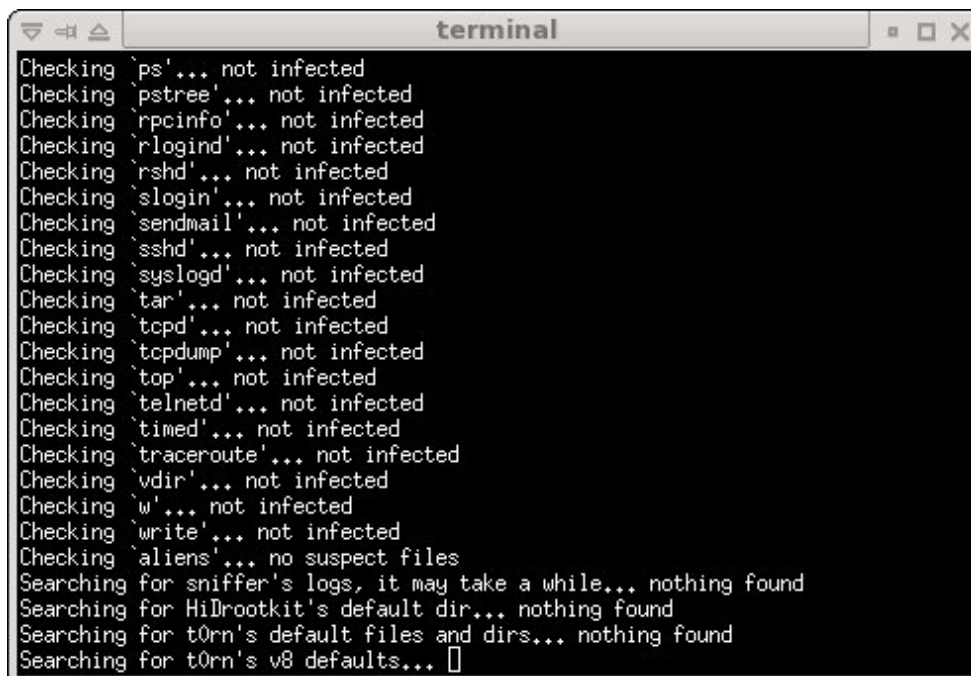
```
$ tar -zxvf chkrootkit.tar.gz
```

Um diretório será criado chamado “chkrootkit-0.45” (o número da versão, ao final do nome do diretório, mudará de acordo com a versão obtida. Adeque os comandos abaixo conforme seu caso específico). Entre no diretório recém criado e execute os comandos abaixo:

```
$ cd chkrootkit-0.45/  
$ make sense
```

Pronto. Para executar o chkrootkit corretamente, é necessário ter privilégios de usuário *root*. Uma vez feito isso, basta digitar “sh chkrootkit” dentro do diretório onde o programa foi descompactado (em nosso caso, “chkrootkit-0.45/”):

```
$ /bin/su  
Password: <digite a senha do usuário root>  
# sh chkrootkit
```



```
terminal  
Checking `ps'... not infected  
Checking `pstree'... not infected  
Checking `rpcinfo'... not infected  
Checking `rlogind'... not infected  
Checking `rshd'... not infected  
Checking `slogin'... not infected  
Checking `sendmail'... not infected  
Checking `sshd'... not infected  
Checking `syslogd'... not infected  
Checking `tar'... not infected  
Checking `tcpd'... not infected  
Checking `tcpdump'... not infected  
Checking `top'... not infected  
Checking `telnetd'... not infected  
Checking `timed'... not infected  
Checking `traceroute'... not infected  
Checking `vdir'... not infected  
Checking `w'... not infected  
Checking `write'... not infected  
Checking `aliens'... no suspect files  
Searching for sniffer's logs, it may take a while... nothing found  
Searching for HiDrookit's default dir... nothing found  
Searching for t0rn's default files and dirs... nothing found  
Searching for t0rn's v8 defaults... []
```

O relatório do chkrootkit é exibido diretamente na tela, mas pode ser redirecionado para um arquivo para posterior análise, como mostra o comando abaixo:

```
# sh chkrootkit > chkrootkit.log
```

Esse comando cria um arquivo texto chamado “chkrootkit.log” contendo toda a saída do programa. Note que, nesse caso, nada irá aparecer na tela até que o programa tenha finalizado sua execução.

O chkrootkit possui diversos parâmetros que podem ser utilizados, dentre os quais destacamos o “-r <dir>”, que utiliza o diretório <dir> como raiz do sistema (/) na varredura. Tal procedimento é ideal para auxiliar na análise forense de um sistema comprometido, cujo disco rígido foi montado em um sistema limpo executando o chkrootkit. Para mais opções de parâmetros, basta digitar:

```
# sh chkrootkit --help
```

3. Instalando e usando o rkhunter

O “Rootkit Hunter”, conhecido popularmente como “rkhunter”, é uma ferramenta desenvolvida por Michael Boelen capaz de identificar rootkits, backdoors, sniffers e exploits locais, podendo ser obtida em:

http://www.rootkit.nl/projects/rootkit_hunter.html

O rkhunter é compatível com distribuições Linux e *BSD, mas exige que a *shell* do sistema seja a bash (Bourne Again Shell). Para saber qual a shell em execução digite:

```
$ echo $SHELL
```

Até a data de publicação deste tutorial, o rkhunter estava na versão 1.2.3. Para instalar, entre na página oficial e obtenha o arquivo contendo a última versão (em nosso caso, “rkhunter-1.2.3.tar.gz”). Descompacte-o como faria com qualquer outro arquivo .tar.gz:

```
$ tar -zxvf rkhunter-1.2.3.tar.gz
```

Lembre-se de modificar o comando acima caso necessário, substituindo “rkhunter-1.2.3.tar.gz” pelo nome do arquivo obtido. Um diretório chamado “rkhunter” deve ter sido criado no diretório atual. Entre no diretório recém criado e execute o script “installer.sh”, como usuário *root*:

```
$ cd rkhunter/  
$ /bin/su  
Password: <digite a senha do usuário root>  
# sh installer.sh
```


Se o procedimento foi feito com sucesso, o rkhunter foi instalado em um diretório do sistema (geralmente */usr/local/bin/rkhunter*) e pode ser invocado a partir de agora pelo comando “rkhunter”. Note que para executar o mesmo corretamente precisamos estar como usuário *root*.

Antes de usar a ferramenta, conecte-se à Internet para atualizar a base de dados. Isso vai garantir que a verificação em seu sistema será a mais completa possível:

```
# rkhunter --update
```

Terminada a atualização, execute o programa para verificar seu sistema:

```
# rkhunter --checkall
```



```
terminal
/usr/bin/whoami [ OK ]
/usr/sbin/syslogd [ OK ]

[Press <ENTER> to continue]

Check rootkits
* Default files and directories
Rootkit '55808 Trojan - Variant A'... [ OK ]
ADM Worm... [ OK ]
Rootkit 'AjaKit'... [ OK ]
Rootkit 'aPa Kit'... [ OK ]
Rootkit 'Apache Worm'... [ OK ]
Rootkit 'Ambient (ark) Rootkit'... [ OK ]
Rootkit 'Balaar Rootkit'... [ OK ]
Rootkit 'BeastKit'... [ OK ]
Rootkit 'beX2'... [ OK ]
Rootkit 'BOBKit'... [ OK ]
Rootkit 'CiNIK Worm (Slapper, B variant)'... [ OK ]
Rootkit 'Danny-Boy's Abuse Kit'... [ OK ]
Rootkit 'Devil RootKit'... [ OK ]
Rootkit 'Dica'... [ OK ]
Rootkit 'Dreams Rootkit'... [ ]
```

O rkhunter vai exibir na tela todos os testes em andamento, parando em cada etapa para que o usuário possa acompanhar os resultados. Embora útil para acompanhamento em tempo real, o relatório pode passar rápido demais para leitura e análise. Para contornar esse problema, utilize também o parâmetro “--createlogfile”, que gera o arquivo “/var/log/rkhunter.log”, contendo o registro completo de todos os testes realizados e resultados obtidos. Outros parâmetros muito úteis são:

- “--skip-keypress” inicia a varredura em modo não interativo, ou seja, não pede que o usuário pressione a tecla [enter] ao final de cada etapa.
- “--quiet” exibe na tela apenas os testes que acusaram problemas no sistema
- “--rootdir <dir>” utiliza o diretório <dir> como raiz do sistema (/) na varredura. Ideal para auxiliar na análise forense de um sistema comprometido, montado em um sistema limpo.

Não se esqueça de atualizar a base de dados sempre que for realizar uma verificação. Para mais opções do rkhunter, basta digitar:

```
# rkhunter --help
```


4. Verificação manual

Embora o uso de ferramentas automáticas para a detecção de rootkits seja rápido e eficiente, não há ferramenta capaz de identificar todos os rootkits. Por isso, convém sempre o uso de bom senso – como identificar processos válidos em execução mas que você não utiliza – em uma verificação. Além disso, não conte com utilitários e ferramentas do sistema comprometido como ps, ls, grep, ifconfig, entre outros, pois os mesmos podem ter sido substituídos e modificados para fazer parecer que o seu sistema está normal. Utilize como alternativa ferramentas contidas em locais seguros como CDs, ou obtenha versões confiáveis da Internet (uma boa solução para isso é a ferramenta *BusyBox*, que combina diversos utilitários em um único e pequeno executável, e pode ser obtida em <http://www.busybox.net/>). De preferência, realize todos os testes com o sistema comprometido (ou melhor, com a *imagem* do sistema comprometido) montada em um sistema confiável, de modo que você possa contar com as ferramentas deste e não precise se preocupar com o comprometimento do próprio núcleo (kernel) do sistema, tão comum em rootkits avançados.

O primeiro passo de uma verificação manual é a análise dos registros (*logs*) do sistema. Note que, caso seu sistema tenha de fato sido invadido, existe uma alta probabilidade dos registros da ocorrência terem sido apagados, a menos que o sistema esteja gravando os registros em locais protegidos, como mídias e sistemas que permitem apenas a inclusão de entradas. Verifique seu arquivo `/etc/syslog.conf` para saber onde a ferramenta syslog está gerando seus registros. Geralmente, os registros ficam no diretório `/var/log` e são divididos em diversos arquivos, cada um registrando determinados eventos. Revise-os pacientemente, procurando por qualquer entrada suspeita.

Procure por modificações em executáveis e arquivos de configurações, em especial o conteúdo do seu diretório `/etc`. Compare os arquivos de seu sistema com os originais que utilizou para a instalação. Verifique se existem entradas estranhas em arquivos como `/etc/passwd` ou `/etc/inetd.conf`. Se seu sistema utiliza comandos como `rlogin`, `rsh` e `rexec`, verifique se não há nada de estranho no arquivo `/etc/hosts.equiv` ou em qualquer arquivo “.rhosts” do seu sistema. Finalmente, utilize a ferramenta “*find*” para procurar por arquivos com SUID e SGID. Muitos arquivos de sistema precisam disso, então faça uma comparação dos arquivos que possuem tais características em um sistema legítimo com o sistema suspeito. Para exibir todos os arquivos que possuem os bits SUID e SGID marcados em seu sistema, utilize o seguinte comando:

```
# find / \( -perm -004000 -o -perm -002000 \) -type f -print
```

É possível realizar buscas mais precisas, como por exemplo buscar apenas por arquivos com SUID root ou com SGID kmem, por exemplo. Tais buscas podem ser feitas com os seguintes comandos, respectivamente:

```
# find / -user root -perm -004000 -print
# find / -group kmem -perm -002000 -print
```

Em determinados diretórios, caso saiba qual foi o último arquivo legitimamente modificado, é possível utilizar o *find* para encontrar quaisquer arquivos modificados depois dessa última modificação. Supondo que o nome do arquivo é `arquivo_de_referencia`, bastaria entrar no diretório que desejamos verificar e digitar:

```
# find . -newer arquivo_de_referencia
```

Caso deseje suprimir mensagens de erro retornadas pelo comando *find*, adicione “2>/dev/null” ao final de seu comando de busca.

5. Conclusão

Embora as técnicas para esconder sinais de uma invasão estejam cada vez mais avançadas, recursos e métodos para identificá-las vêm sendo desenvolvidos em igual rapidez. É importante estar sempre atento para indícios de invasões e acessos ilícitos, e realizar testes periódicos em redes e sistemas. Caso algo de estranho seja detectado, desconecte o sistema da rede, faça uma cópia de segurança e inicie o tratamento, para que seu sistema possa estar seguro e de volta a atividade o mais rápido possível.

6. Referências bibliográficas

Dittrich, D. - “Root Kits” and hiding the files/directories/processes after a break-in
(<http://staff.washington.edu/dittrich/misc/faqs/rootkits.faq>)

CERT Coordination Center - *Intruder Detection Checklist*
(http://www.cert.org/tech_tips/intruder_detection_checklist.html)

CERT Coordination Center – *Steps for Recovering from a UNIX or NT System Compromise*
(http://www.cert.org/tech_tips/root_compromise.html)