CAPA

Proteja sua rede inteira com o IDS OSSEC

Impenetrável

O sistema de detecção de intrusão OSSEC, de origem brasileira, tem destaque internacional por sua grande competência. Aprenda a instalá-lo e a configurá-lo para a sua rede.

por Marcos Aurelio Rodrigues e Rodrigo Montoro

Ao fazer um projeto de rede, um dos pontos fortes da implementação segura é a segurança em profundidade e a diversificação de controles. Uma rede considerada segura possui muitas camadas de defesa, e um dos principais mecanismos de defesa atuais são os IDSs (*Intrusion Detection Systems*). Sistemas IDS analisam exatamente o que um firewall não consegue: eles são capazes de detectar eventos baseados em regras ou anomalias, executando verificações mais inteligentes que um firewall convencional faria.

O uso de mecanismos IDS se tornaram mais conhecidos por causa do sistemas NIDS (*Network Intrusion Detect Systems*), que são capazes de detectar ataques à rede por meio de sensores instalados em um segmento da rede que receba todo o tráfego (hub, tap ou espelhamento de porta no switch). Apesar de muito eficazes, os NIDSs possuem algumas características que ainda permitem que ataques sejam eficazes. Alguns exemplos de evasão são: ataque *DoS*, *session splicing*, fragmentação de pacotes e codificação de caracteres. Além de algumas técnicas de evasão, os NIDSs também não conseguem detectar ataques que estejam trafegando criptografados.

Para complementar o NIDS, existe também o HIDS (*Host Intrusion Detect System*). O HIDS consegue detectar eventos na estações ou servidores e gerar alertas de forma similar a um sistema NIDS, porém o HIDS roda localmente na máquina, conseguindo detectar eventos que o NIDS não perceberia. O HIDS consegue fazer diversas análises, como da integridade do sistema de arquivos, monitoramento de log, monitoramento de registro, detecção de rootkits e resposta ativa. Para suprir a necessidade desse tipo de defesa foi criado o *OSSEC*[1].

O OSSEC é um sistema HIDS multiplataforma de código-fonte aberto. É uma poderosa ferramenta de análise e integração de logs, verificação de integridade de arquivos, detecção de rootkits, alerta em tempo real e resposta ativa. Suporta diversos tipos de logs e pode ser instalado em vários sistemas operacionais, incluindo Linux, OpenBSD, FreeBSD, MAC OS X, Sun Solaris e Microsoft Windows. Mesmo com a aquisição do projeto OSSEC pela empresa Third Brigade[2], o OSSEC continuará a ser Software Livre. Ele é distribuído sob a licença GNU GPL versão 3, conforme publicada pela Free Software Foundation[3].

O projeto dispõe de vários colaboradores ao redor do mundo e possui como principal desenvolvedor o brasileiro Daniel Cid. Seu desenvolvimento é eficiente não so-

Exemplo 1: Download e verificação do OSSEC

```
# wget http://www.ossec.net/files/ossec-hids-1.5.1.tar.gz
# wget #http://www.ossec.net/files/ossec-hids-1.5.1_checksum.txt
# cat ossec-hids-1.5.1_checksum.txt
# md5 ossec-hids-1.5.1.tar.gzMD5 (ossec-hids-1.5.1.tar.gz) = 1269e02
74cb0debce0d4d30b32fba083
# sha1 ossec-hids-1.5.1.tar.gz
SHA1 (ossec-hids-1.5.1.tar.gz) = 4cc2d8d01a59d81f7e8a8c66fb800152d7f
➥2c15c
```

```
Arquivo  Editar  Ver  Terminal  Abas  Ajuda
# tar -zxvf ossec-hids-1.5.1.tar.gz
# cd ossec-hids-1.5.1

# ./install.sh
  ** Para instalação em português, escolha [br].
  ** 要使用中文进行安装, 请选择 [cn].
  ** Fur eine deutsche Installation wohlen Sie [de].
  ** Για εγκατάσταση στα Ελληνικά, επιλέξτε [el].
  ** For installation in English, choose [en].
  ** Para instalar en Español , eliga [es].
  ** Pour une installation en français, choisissez [fr]
  ** Per l'installazione in Italiano, scegli [it].
  ** 日本語でインストールします・選択して下さい・[jp].
  ** Aby instalować w języku Polskim, wybierz [pl].
  ** Для инструкций по установке на русском ,введите [ru].
  ** Za instalaciju na srpskom, izaberi [sr].
  ** Türkçe kurulum için seçin [tr].
  (en/br/cn/de/el/es/fr/it/jp/pl/ru/sr/tr) [en]: br
```

Figura 1 A instalação do OSSEC é multilíngüe.

mente quanto a correções de falhas, mas também para lançamentos de novos recursos.

Operação

Antes de começar a instalação do OSSEC, é necessário entender as diferenças entre seus modos de operação. A escolha dependerá da quantidade de máquinas a serem analisadas na sua rede:

- Local: usado para proteger uma única máquina;
- Agente: usado para proteger máquinas e relatar eventos a um servidor OSSEC;
- Servidor: usado para fazer a coleta de diversos agentes e também eventos de *Syslog* de outros dispositivos (roteadores, firewalls etc.).

Antes de fazer a instalação do OSSEC em um sistema em produção, é recomendável ter certeza de que o sistema não contenha nenhum rootkit instalado. Para tal tarefa, você pode utilizar softwares como *Rootkit Revealer*[4] ou *Chkrootkit*[5].

Para este artigo, foi utilizada a instalação dos modos *Servidor* e *Agente*. O servidor foi instalado em um sistema OpenBSD 4.3 e o agente em um CentOS 5.2.

Instalação

Para começar a instalação, vamos instalar o OSSEC Server. Faça o download do código-fonte e do arquivo de checksum e verifique a integridade do arquivo baixado (**exemplo 1**).

Para a instalação, vamos descompactar o pacote e executar o script de instalação. A instalação é bem intuitiva, e o OSSEC possui suporte a diversos idiomas. A **figura 1** mostra a primeira tela da instalação, e devemos escolher o português brasileiro (`br`). Depois disso, ele mostrará informações sobre a máquina, como nome da máquina, usuário e versão do sistema operacional (**exemplo 2**).

Após confirmar o tipo de sistema operacional e as demais informações da máquina, vamos optar por fazer a instalação do tipo servidor e decidir qual o diretório de instalação do OSSEC (**exemplo 3**).

O OSSEC pode enviar alertas por email. Para isso, devemos configurar a conta de email a ser utilizada e especificar o servidor SMTP para o envio das mensagens. O endereço de email a ser utilizado é o endereço de destino, ou seja, aquele que receberá as notificações do OSSEC.

Para facilitar a operação, o OSSEC tenta descobrir o endereço do servidor SMTP na rede em que está sendo instalado. Neste artigo, o servidor é *exemplo.org*.

Além de o OSSEC fazer o correlacionamento de logs, ele também pode atuar detectando rootkits e verificando a integridade do sistema de arquivos. Para isso, basta habilitar os mecanismos (*engines*) correspondentes, como mostra o **exemplo 5**.

O OSSEC também é capaz de, ao detectar um evento, realizar uma ação e gerar um alerta; porém, além disso, também usaremos sua resposta ativa (**exemplo 6**). A resposta pode ser ativa tanto do lado do servidor quanto do lado do agente, e pode consistir em bloquear um endereço IP ou desabilitar o acesso de um usuário, por exemplo. Para realizar

Exemplo 2: Exibição de detalhes da máquina

```
OSSEC HIDS v1.5.1 Script de instalação - http://www.ossec.net
   Você está iniciando o processo de instalação do OSSEC HIDS.
   Você precisará de um compilador C pré-instalado em seu sistema.
   Qualquer dúvida, sugestões ou comentários, por favor, mande um
e-mail para
   dcid@ossec.net (ou daniel.cid@gmail.com).
    - Sistema: OpenBSD bolivia.exemplo.org 4.3
    - Usuário: root
    - Host: bolivia.exemplo.org
    -- Aperte ENTER para continuar ou Ctrl+C para abortar. --
```

Exemplo 3: Escolha da instalação do tipo servidor

```
1- Que tipo de instalação você deseja (servidor, cliente, local ou
➥ajuda)? servidor
    - Escolhida instalação servidor.
2- Configurando o ambiente de instalação.
   - Escolha onde instalar o OSSEC HIDS [/var/ossec]:
     - A instalação será feita no diretório /var/ossec .
```

Exemplo 4: Configuração do email

```
3- Configurando o OSSEC HIDS.
    3.1- Deseja receber notificações por e-mail? (s/n) [s]: s
     - Qual é o seu endereço de e-mail? marcos@exemplo.org
     - Seu servidor SMTP foi encontrado como: exemplo.org.
     - Deseja usá-lo? (s/n) [s]: n
     - Qual é o ip/host de seu servidor SMTP? 192.168.1.2
```

Exemplo 5: Ativação de mecanismos adicionais

```
3.2- Deseja habilitar o sistema de verificação de integridade?
➥(s/n) [s]: s
     - Syscheck (Sistema de verificação de integridade) habilitado.
    3.3- Deseja habilitar o sistema de detecção de rootkits?
➥(s/n) [s]: s
     - Rootcheck (Sistema de detecção de rootkits) habilitado.
```

a ação, ele pode utilizar utilitários como *iptables*, *ipfilter* ou *tcp wrappers*. Além disso, para diminuir os falsos positivos, é possível criar uma lista amiga (*white list*) a fim de evitar que alguns endereços sejam bloqueados.

Em uma instalação do tipo servidor, o OSSEC pode receber alertas por meio de de um canal seguro (porta 1514) ou então do uso do Syslog (**exemplo 7**) para facilitar a integração de logs de outros dispositivos (note, no entanto, que o Syslog utiliza um canal não criptografado como meio de transmissão).

Após respondermos todas as questões do instalador, o OSSEC utilizará o compilador C do sistema para fazer a instalação, como mostra o **exemplo 8**.

Uso do servidor

Agora já podemos iniciar o OSSEC com o comando `/var/ossec/bin/ossec-control star`. Com o servidor funcionando, instalaremos o agente, mas antes disso é preciso criar uma chave para cada agente que se conectará ao servidor. Essa chave é utilizada

Tabela 1: Configurações contidas em ossec.conf

Tag	Descrição
global	Opções globais utilizadas em todo o sistema.
email_alerts	Opções para envio granular de emails de alertas.
rules	Lista com as regras a serem incluídas na análise.
syscheck	Configurações relacionadas à verificação de integridade do sistema.
rootcheck	Configurações relacionadas à detecção de rootkits.
alerts	Opções de alertas para email e logs.
localfile	Arquivos de log que serão monitorados.
remote	Configurações relacionadas a conexões remotas.
client	Opções relacionadas aos agentes.
database_output	Configuração para log em banco de dados.
command	Programa que será ativado na resposta ativa.
active-response	Configurações de resposta ativa.

para a transmissão através do canal seguro. O **exemplo 9** mostra o utilitário `manage_agents`, que, como diz o nome, gerencia os agentes e suas respectivas chaves.

Instalação do agente

Para instalar o agente do OSSEC, podemos utilizar o mesmo pacote baixado para o servidor. No agente, executamos o mesmo script

Exemplo 6: Configuração de respostas automáticas

```
3.4- Respostas automáticas permitem você executar um comando
        específico baseado nos eventos recebidos. Você pode
        bloquear um endereço de IP ou desabilitar o acesso de
        um usuário específico, por exemplo.
        Maiores informações:
        http://www.ossec.net/en/manual.html#active-response
     - Deseja habilitar o sistema de respostas automáticas?
➥(s/n) [s]: s
     - Sistema de respostas automáticas habilitado.
     - Por padrão, nós podemos habilitar o 'host-deny' e
       o 'firewall-drop'. O primeiro adicionará um host
       ao /etc/hosts.deny e o segundo bloqueará o host
       no 'iptables' (se linux) ou no ipfilter (se Solaris,
       FreeBSD ou NetBSD).
     - Eles podem ser usados para parar 'SSHD brute force
       scans', portscans e outras formas de ataque.
       Você pode também realizar  bloqueios baseados nos
       alertas do snort, por exemplo.
     - Deseja habilitar o firewall-drop? (s/n) [s]: s
       - firewall-drop habilitado (local) para níveis >= 6
     - Lista de endereços que não serão bloqueados pela
➥resposta automática:
        - 192.168.1.1
     - Deseja adicionar mais algum endereço a essa lista?
➥(s/n)? [n]:
```

Exemplo 7: Uso do Syslog para envio e análise dos logs

```
    3.5- Deseja habilitar o syslog remoto (514 udp)? (s/n) [s]: s
     - Syslog habilitado.
    3.6- Ajustando a configuração para analisar os seguintes
logs:
      -- /var/log/messages
      -- /var/log/authlog
      -- /var/log/secure
      -- /var/log/xferlog
      -- /var/log/maillog
   - Se quiser monitorar qualquer outro arquivo, modifique
     o ossec.conf e adicione uma nova entrada para o arquivo.
     Qualquer dúvida sobre a configuração, visite
➥http://www.ossec.net/hids/ .
     - Pressione ENTER para continuar -
```


PARTICIPE DO PRINCIPAL
EVENTO DE PHP DA AMÉRICA LATINA

php CONFERENCE BRASIL 08

27, 28 e 29 de Novembro
UNIFIEO • OSASCO-SP

PALESTRANTES INTERNACIONAIS
PRESENÇAS CONFIRMADAS:

- Christopher Jones
  Desenvolvimento de Produto, Oracle
- Todd Trichler
  Gerente Sênior de Produto, Oracle Technology Network
- Luke Crouch
  Engenheiro de Software, Sourceforge.net

Diamond
Borland
LOCAWEB SERVIÇOS DE INTERNET
msdn
ORACLE
ScriptCase
INGRAM MICRO
IBM Premier Business Partner

Silver
dextra Coding your Business

Hospedagem
HostNET

Apoio Institucional e Infra-Estrutura
CENTRO UNIVERSITÁRIO FIEO UNIFIEO

Apoio
DICAS-L WWW.DICAS-L.COM.BR
br-linux.org Ano 10
DINAMIZE
HTML STAFF

Mídia Oficial
LINUX MAGAZINE

Apoio Cultural
TEMPO REAL LIVRARIA DO PROFISSIONAL DE INFORMÁTICA

Promoção e Realização
TEMPO REAL EVENTOS

www.phpconf.com.br

Exemplo 8: Instalação automatizada do sistema

```
5- Instalando o sistema
   - Executando o Makefile
...
   - O Sistema é OpenBSD.
   - O script de inicialização foi modificado para executar o OSSEC
➥HIDS durante o boot.
   - Configuração finalizada corretamente.
   - Para iniciar o OSSEC HIDS:
                /var/ossec/bin/ossec-control start
   - Para parar o OSSEC HIDS:
                /var/ossec/bin/ossec-control stop
   - A configuração pode ser vista ou modificada em /var/ossec/etc/
➥ossec.conf
      Obrigado por usar o OSSEC HIDS.
      Se você tiver alguma pergunta, sugestão ou encontrar algum
      "bug", nos contate através do e-mail contact@ossec.net ou
      utilize nossa lista de e-mail:
      ( http://www.ossec.net/main/support/ ).
      Maiores informações podem ser encontradas em
➥http://www.ossec.net
      -  Pressione ENTER para continuar  -
- Adicione as seguintes linhas na configuracao do seu firewall:
       Maiores informações em:
       http://www.ossec.net/en/manual.html#active-response-tools
        table <ossec_fwtable> persist #ossec_fwtable
        block in quick from <ossec_fwtable> to any
        block out quick from any to <ossec_fwtable>
   - Você precisa adicionar cada um dos clientes antes que estejam
➥autorizados a acessar o servidor.
     Execute o 'manage_agents' para adicioná-los ou removê-los:
     /var/ossec/bin/manage_agents
     Maiores informações em:
     http://www.ossec.net/en/manual.html#ma
```

de instalação, mudando apenas o modo de operação em relação ao usado no servidor. Nesse momento, escolhemos novamente o idioma português brasileiro, como mostra a **figura 1**.

Após isso, o script mostrará informações sobre a máquina, exatamente como fez na instalação do servidor. Na estação usada neste artigo, essa etapa é mostrada no **exemplo 10**. Dessa vez, optaremos por instalar o agente e decidiremos em qual diretório será feita a instalação (`/var/ossec/`, como mostra o **exemplo 11**).

Durante a instalação do agente, definimos o endereço do servidor OSSEC já instalado (`192.168.1.3`, no **exemplo 12**) e novamente habilitamos a verificação do sistema de arquivos, a detecção de rootkits e a resposta ativa. O OSSEC então começará novamente o processo de compilação e configuração do sistema (**exemplo 13**).

Comunicação servidor/agente

Para fazer a configuração da comunicação entre o servidor e o agente, é necessário importar a chave do servidor no agente. Para isso, abra dois terminais, um conectado ao servidor e outro ao agente. Primeiramente, vamos extrair a chave no lado servidor (**exemplo 14**) e em seguida copiá-la para o cliente (**exemplo 15**).

Ao final da importação, é necessário reiniciar tanto o servidor quanto o agente com o comando:

```
/var/osec/bin/ossec-control
➥restart
```

Configuração

Após a instalação do OSSEC, não há mais muito o que alterar para iniciar a operação. A estrutura de configuração do OSSEC é em XML, e todos os arquivos que a compõem se localizam no subdiretório `etc/` do diretório onde o OSSEC foi instalado. O arquivo principal é o `ossec.conf` e toda configuração fica dentro da seção principal `<ossec_config>`. Alguns sub-elementos dela são:

- `<global>`: opções gerais em instalações dos tipos servidor e local.
- `<alerts>`: opções de alerta do tipo email e log.
- `<remote>`: opções relacionadas a conexões remotas e de agentes (somente em instalações do tipo servidor)
- `<localfile>`: configuração relacionada a logs monitorados.

O **exemplo 16** mostra duas seções que definem o monitoramento do tipo de log syslog para alertas de segurança de um sistema Linux.

Alertas

Todo alerta possui um nível entre 0 e 15, sendo 15 o mais grave e 0 o mais trivial. Para definir quando um alerta deve ser

Exemplo 9: Gerenciamento de agentes

```
# /var/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v1.5.1 Agent manager.      *
* The following options are available: *
****************************************
    (A)dd an agent (A).
    (E)xtract key for an agent (E).
    (L)ist already added agents (L).
    (R)emove an agent (R).
    (Q)uit.
Choose your action: A,E,L,R or Q: A
- Adding a new agent (use '\q' to return to the main menu).
   Please provide the following:
    * A name for the new agent: paraguai
    * The IP Address of the new agent: 192.168.1.4
    * An ID for the new agent[001]:
Agent information:
    ID:001
    Name:paraguai
    IP Address:192.168.1.4
Confirm adding it?(y/n): y
Agent added.
```

Exemplo 10: Informações da máquina agente

```
OSSEC HIDS v1.5.1 Script de instalação - http://www.ossec.net
  Você está iniciando o processo de instalação do OSSEC HIDS.
  Você precisará de um compilador C pré-instalado em seu sistema.
  Qualquer dúvida, sugestões ou comentários, por favor, mande
➥um e-mail para
  dcid@ossec.net (ou daniel.cid@gmail.com).
   - Sistema: Linux paraguai.exemplo.org 2.6.18-53.el5
   - Usuário: root
   - Host: paraguai.exemplo.org
   -- Aperte ENTER para continuar ou Ctrl+C para abortar. --
```

Exemplo 11: Tipo de instalação cliente e local de instalação

```
1- Que tipo de instalação você deseja (servidor, cliente,
➥local ou ajuda)? cliente
    - Escolhida instalação cliente.
2- Configurando o ambiente de instalação.
   - Escolha onde instalar o OSSEC HIDS [/var/ossec]:
      - A instalação será feita no diretório /var/ossec .
```

enviado por email e quando deve ser transmitido por log, podemos alterar o conteúdo das tags `<log_alert_level>` e `<email_alert_level>`. A forma exibida na seção `<alerts>` do **exemplo 16** gera logs somente para alertas acima de 1, enquanto somente alertas acima de 7 serão enviados por email.

É necessário também citar alguns arquivos de configuração e suas respectivas sintaxes.

O diretório principal das configurações do OSSEC, considerando os caminhos de instalação escolhidos neste artigo, é `/var/ossec/etc/`, e os arquivos são:

- `ossec.conf`: arquivo principal de configuração do OSSEC. Contém as configurações descritas na **tabela 1**.
- `decoder.xml`: arquivo que contém os decodificadores dos logs recebidos pelo OSSEC. Os decodificadores separam algumas informações para a segunda parte das análises que são as regras.
- `internal_options.conf`: possui algumas informações de configuração para depuração e ajuste fino; deve ser modificado com cuidado.

Outro diretório importante é o `/var/ossec/rules/`, que contém as regras responsáveis por analisar o conteúdo dos logs. Cada arquivo dentro dele contém um conjunto de regras para definição da gravidade das mensagens no log de um aplicativo, assim como um identificador geral para cada mensagem do log.

Por exemplo, o arquivo `apache.rules.xml` define, entre outras centenas de regras, que a mensagem `authentication failed`, quando encontrada nos logs do Apache, deve receber o nível 5 e ser categorizada entre as mensagens de falha na autenticação. Enquanto isso, em `attack_rules.xml` é

Exemplo 12: Recursos ativos no agente

```
3- Configurando o OSSEC HIDS.
    3.1- Qual é o endereço de IP do servidor OSSEC HIDS?:
➥192.168.1.3
     - Adicionando IP do servidor 192.168.1.3
    3.2- Deseja habilitar o sistema de verificação de integridade?
➥(s/n) [s]: s
     - Syscheck (Sistema de verificação de integridade) habilitado.
    3.3- Deseja habilitar o sistema de detecção de rootkis?
➥(s/n) [s]: s
     - Rootcheck (Sistema de detecção de rootkits) habilitado.
    3.4 - Deseja habilitar o sistema de respostas automáticas?
➥(s/n) [s]: s
```

Exemplo 13: Instalação automatizada do agente

```
3.5- Ajustando a configuração para analisar os seguintes logs:
      -- /var/log/messages
      -- /var/log/secure
      -- /var/log/maillog
   - Se quiser monitorar qualquer outro arquivo, modifique
     o ossec.conf e adicione uma nova entrada para o arquivo.
     Qualquer dúvida sobre a configuração, visite
➥http://www.ossec.net/hids/ .
     - Pressione ENTER para continuar -

5- Instalando o sistema
   - Executando o Makefile
...
   - Para se comunicar com o servidor, você primeiro precisa
     adicionar este cliente a ele. Quando você tiver terminado,
     use a ferramenta 'manage_agents' para importar a chave de
     autenticação do servidor.
     /var/ossec/bin/manage_agents
     Maiores informações em:
     http://www.ossec.net/en/manual.html#ma
```

definido que mensagens que coincidirem com a expressão regular:

```
ftpd[\d+]: \S+ FTP LOGIN FROM \.+
➥0bin0sh
```

devem receber nível 14 (alto), pois caracterizam um *exploit* de estouro de buffer contra versões do servidor FTP *wu-ftpd* anteriores à 2.6, e serão agrupadas como tentativa de exploit (`exploit_attempt`).

Além desses arquivos, há dezenas de outros, abrangendo desde o servidor VoIP *Asterisk* até o monitor de máquinas virtuais *VMware*, passando por roteadores Cisco com sistema *IOS*, regras de firewall, bancos de dados *MySQL*, sistema *PAM* e servidores de email Microsoft *Exchange*.

Evidentemente, é possível e relativamente fácil criar novas regras e decodificadores, uma vez que seja compreendida a sintaxe dos arquivos.

Exemplo 14: Extração da chave do servidor

```
# /var/ossec/bin/manage_agents
**********************************
* OSSEC HIDS v1.5.1
Agent manager.       *
* The following options
are available: *
**********************************
     (A)dd an agent (A).
     (E)xtract key for an agent E).
     (L)ist already added agents (L).
     (R)emove an agent (R).
     (Q)uit.
Choose your action: A,E,L,R or Q: e
Available agents:
     ID: 001, Name: paraguai, IP:
➥192.168.1.4
Provide the ID of the agent to extract
➥the key (or '\q' to quit): 001
Agent key information for '001' is:
MDAxIHBhcmFndWFpIDE5Mi4xNjguMS40IDk
➥1YmRjMzM4Y2M2Mzk4M2ExNmI4
➥MmE4ZjE1N2RkY2EzYzBjNDA0MjNhOGJkMj
➥ljZTFiZjhjNjllOTdiMjEyYjQ=
```

Conclusão

Atualmente vivemos uma era da segurança da informação em que os ataques se tornam mais complexos e inteligentes a cada dia, sendo que a segurança em perímetro vem se tornando algo obrigatório nas empresas. Há pouco tempo atrás, era comum utilizar sistemas HIDS somente em máquinas expostas à Internet e nos servidores mais críticos. Porém, visto o aumento dos ataques a estações de trabalho e malwares com suporte a SSL, é crescente a necessidade de rodar HIDS em todas as máquinas, e o OSSEC certamente é uma das melhores soluções nesse campo, por suportar uma grande quantidade de sistemas operacionais e oferecer as vantagens do Software Livre. ■

Exemplo 15: Importação da chave pelo agente

```
[root@paraguai ossec-hids-1.5.1]# /var/ossec/bin/manage_agents
****************************************
* OSSEC HIDS v1.5.1 Agent manager.       *
* The following options are available: *
****************************************
     (I)mport key from the server (I).
     (Q)uit.
Choose your action: I or Q: I
* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.
Paste it here (or '\q' to quit): MDAxIHBhcmFndWFpIDE5Mi4xNjguMS40IDk1Y
mRjMzM4Y2M2Mzk4M2ExNmI4MmE4ZjE1N2RkY2EzYzBjNDA0MjNhOGJkMjljZTFiZjhjNjl
lOTdiMjEyYjQ=
Agent information:
     ID:001
     Name:paraguai
     IP Address:192.168.1.4
Confirm adding it?(y/n): y
Added.
```

Exemplo 16: Monitoramento de syslog para alertas em Linux

```
<localfile>
      <log_format>syslog</log_format>
      <location>/var/log/secure</location>
</localfile>
  <alerts>
      <log_alert_level>1</log_alert_level>
      <email_alert_level>7</email_alert_level>
</alerts>
```

Mais informações

[1] Página do OSSEC: http://www.ossec.net

[2] Third Brigade: http://3rdbrigade.com

[3] FSF: http://www.com.br.com.br

[4] Rootkit Revealer: http://www.fsf.org

[5] Chkrootkit: http://tinyurl.com/465pg7

Sobre os autores

Marcos Aurelio Rodrigues (deigratia33@gmail.com) é consultor de segurança e infra-estrutura, certificado CCNA, MCSO e Comptia Security +, e possui mais de oito anos de experiência em administração e infra-estrutura de sistemas e rede, além de ser mantenedor da comunidade Snort-br.

Rodrigo "Sp0oKeR" Montoro (spooker@gmail.com) é certificado LPI, RHCE, SnortCP e MCSO, trabalha como Analista de Segurança e possui dez anos de experiência em sistemas de código aberto, em especial ferramentas de segurança, com as quais tem forte envolvimento.

seres

Uma empresa tão livre quanto a sua imaginação.

Pensando na sua liberdade de pensamento, a F13 Tecnologia oferece produtos, soluções e seruiços em Linux e Softwares livres, como suporte técnico presencial ou remoto e cursos de formação com certificação, tais como:

- Formação Linux com ênfase na LPI (4 módulos totalizando 160 horas)
- Formação PHP (3 módulos totalizando 120 horas)
- Firewall Auançado (40 horas)
- Controle de uersões com CVS, SVN e Trac (8 horas)
- Virtualização com Xen (40 horas)
- Seruiço de diretórios com OpenLdap (40 horas)
- Correio Eletrônico Auançado (40 horas)
- Voip & Asterisk com ênfase em DialPlan (40 horas – Curso ministrado por instrutor com certificação OCAP)
- Administração de Bancos de Dados Liures (PostgreSQL e MySQL – 40 horas)

F13 TECNOLOGIA

(85) 3252.3836

www.f13.com.br