OSSEC HIDS

Centralizando a segurança

O que é  ?

- OSSEC é um IDS (Intrusion Detection System) Open Source e multi-plataforma baseado em host, que viabiliza a centralização de eventos em servidores.

Quem é o pai da criança?

- Daniel Cid 

  Fundador e principal desenvolvedor do projeto, atualmente trabalha na Third Brigade como principal pesquisador.

O que ele faz?

- Análise de log´s
- Checagem de Integridade **
- Monitoramento do registro do windows
- Rootkit detection **
- Alertas em tempo real
- Resposta imediata (IPS ou IDS Ativo) **
- Centralização da administração

Por que OSSEC?

LINUX MAGAZINE ONLINE

A revista do profissional de TI

Notícias | Easy Linux | Guia de TI | Linux Park | Livros | Shopping

Home » LM 47 | Segurança Profissional

Principal

- Linux Magazine
- Matérias Online
- Anteriores
- Assinar
- Renovar assinatura

Menu pessoal

login

Esqueceu a senha?

Cadastro

Linux Magazine

LM 47 | Segurança Profissional

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?

A Linux Magazine #47 explica algumas técnicas para manter os invasores fora do seu sistema. Aprenda a caçar e se proteger dos temíveis rootkits, use o popular sistema IDS OSSEC para monitorar invasões à rede e entenda como a virtualização, apesar de trazer muitas vantagens, pode causar impactos negativos sobre a segurança do sistema.

Não está convencido?

LINUXWORLD
Open Source Solutions for the Enterprise

Google™ Custom Search | Search

HOME

EVENTS
CAREERS
ABOUT US

SITE RESOURCES
News
Newsletters
White Papers
Blogs
RSS Feeds
Video
LinuxWorld Podcast
LinuxWorldexpo.com

PARTNER SITES
Demo.com
NetworkWorld.com
JavaWorld.com

Security

LinuxWorld.com > Security >

Top 5 open source security tools in the enterprise

With thousands of open source security packages available, choices can be confusing. Here's the short list of tools that are getting real-world successful deployments.

By Eric Hines, GCIA, CISSP, CEO, Applied Watch Technologies, LinuxWorld.com, 03/12/07

Comments (1) Print article

In the late 1990s, organizations began looking seriously at open source network management and security products. Although some had previously been installed without corporate approval, a fundamental shift occurred within the enterprise as organizations began searching for alternative solutions to commercial network management and security products.

Realizing the considerable cost savings and superior security benefits of open source, companies that were moving to open source in other areas, such as migrating Microsoft Internet Information Server Web servers to the open source Apache Web server, also began considering tools such as the network management software Nagios to replace proprietary products such as HP Openview. While many open source security tools are available, this story reviews the top five tools in production in enterprise environments.

Related links

No results were found for your search.

Your query is too restrictive. You might want to try:
security

RSS

Story tools Sponsored by:

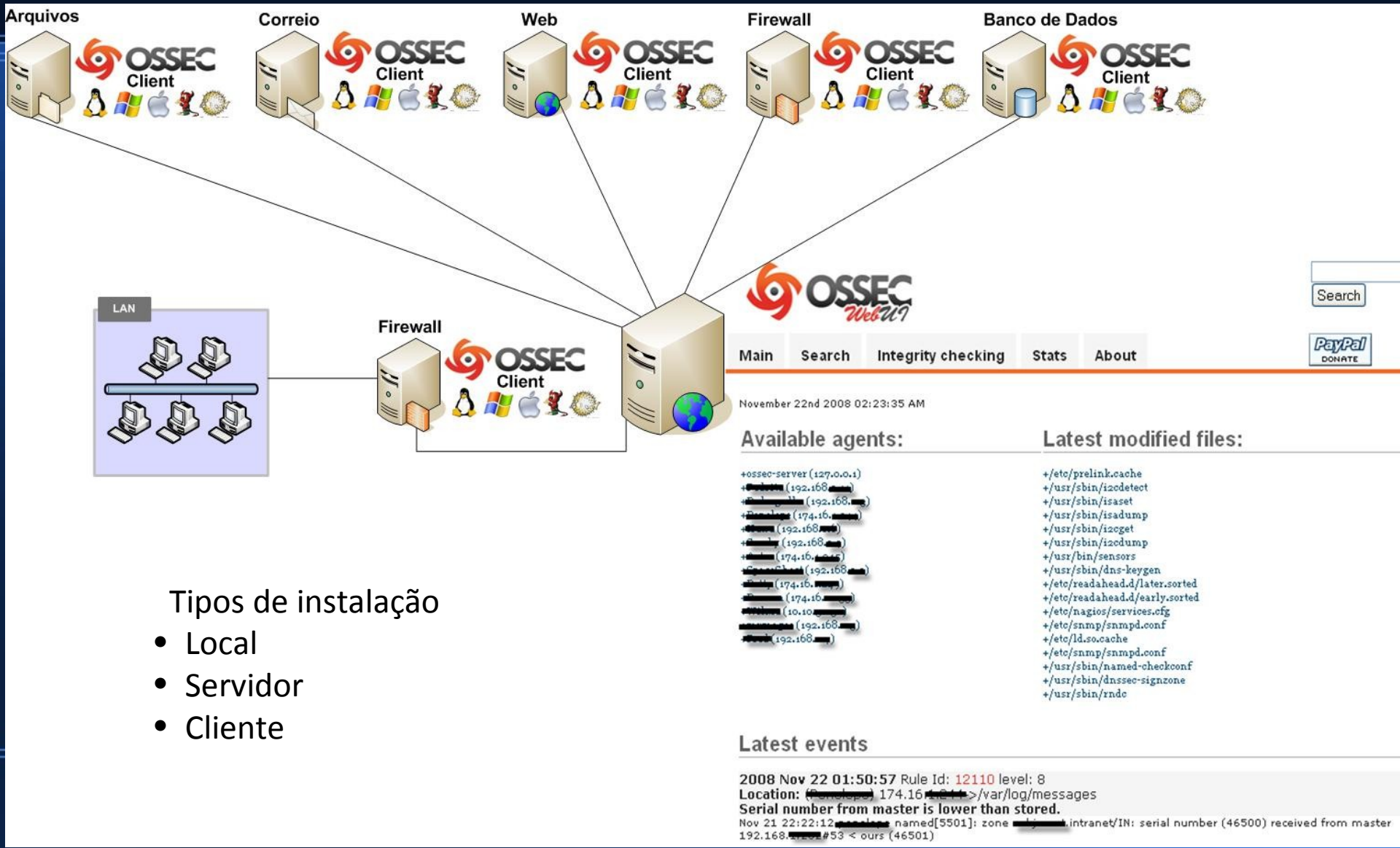
E-Mail article
Print article
Contact author
AIM article
Reddit
Stumble
del.icio.us
Digg
Slashdot It!

Resource Library
Free tools, how-tos and more
Visit today

Tool #1: OSSEC HIDS

HIDS as the No. 1 open source tool due to its recent rapid growth in the enterprise. OSSEC HIDS is a rapidly evolving open source project that offers the first ever open source host intrusion detection and

Como ele funciona?



Tipos de instalação

- Local
- Servidor
- Cliente

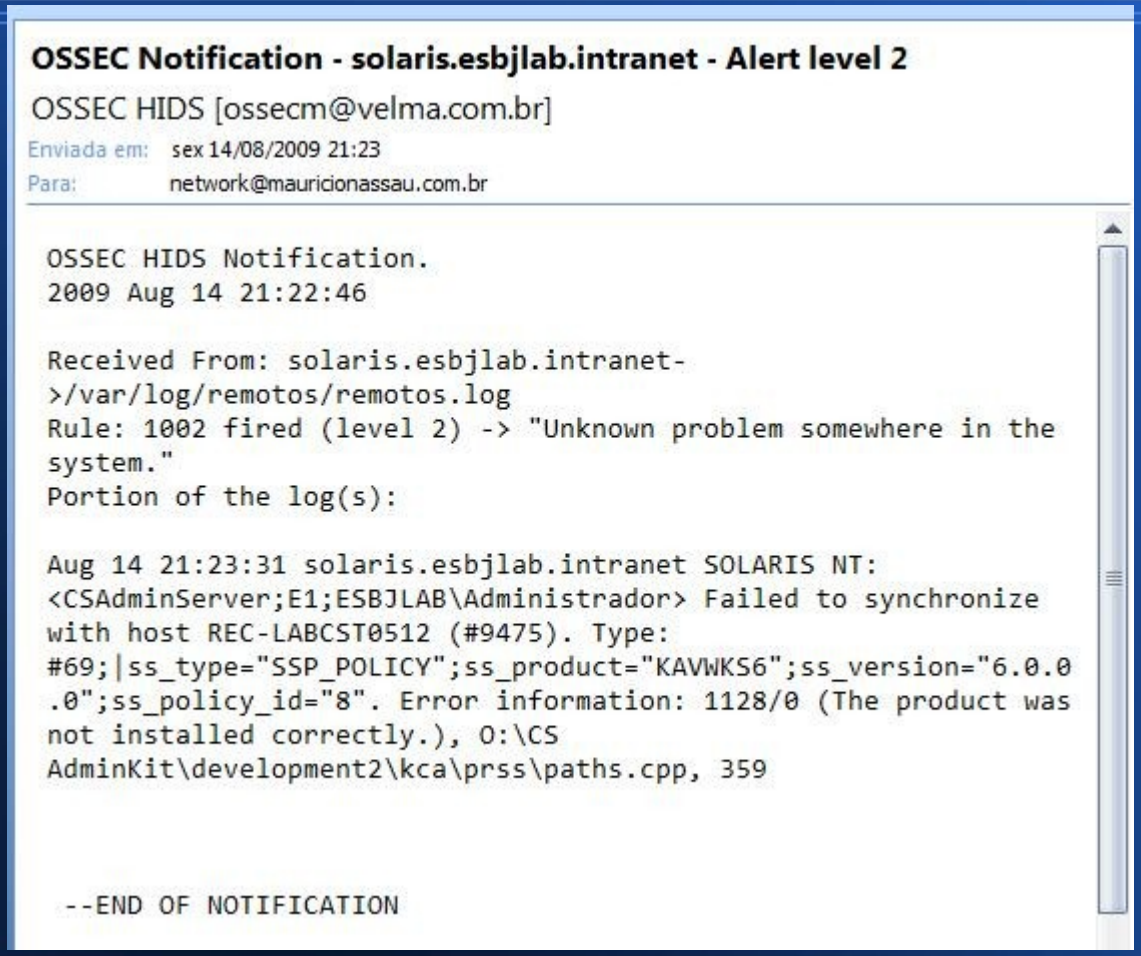
Active Response

```
<!--
<!-- Active Response Config -->
<active-response>
  <!-- This response is going to execute the host-deny
     - command for every event that fires a rule with
     - level (severity) >= 6.
     - The IP is going to be blocked for  600 seconds.
    -->
  <command>host-deny</command>
  <location>local</location>
  <level>6</level>
  <timeout>600</timeout>
</active-response>

 -->

<active-response>
  <!-- Firewall Drop response. Block the IP for
     - 600 seconds on the firewall (iptables,
     - ipfilter, etc).   -->
  <command>firewall-drop</command>
  <location>local</location>
  <level>7</level>
  <timeout>600</timeout>
</active-response>
```

Alerta por e-mail



OSSEC Notification - solaris.esbjlab.intranet - Alert level 2

OSSEC HIDS [ossecm@velma.com.br]

Enviada em: sex 14/08/2009 21:23

Para: network@mauricionassau.com.br

```
OSSEC HIDS Notification.
2009 Aug 14 21:22:46

Received From: solaris.esbjlab.intranet-
>/var/log/remotos/remotos.log
Rule: 1002 fired (level 2) -> "Unknown problem somewhere in the
system."
Portion of the log(s):

Aug 14 21:23:31 solaris.esbjlab.intranet SOLARIS NT:
<CSAdminServer;E1;ESBJLAB\Administrador> Failed to synchronize
with host REC-LABCST0512 (#9475). Type:
#69;|ss_type="SSP_POLICY";ss_product="KAVWKS6";ss_version="6.0.0
.0";ss_policy_id="8". Error information: 1128/0 (The product was
not installed correctly.), O:\CS
AdminKit\development2\kca\prss\paths.cpp, 359



 --END OF NOTIFICATION
```

- Envio de e-mail com classificação de eventos
- Envia e-mail de eventos desconhecidos

Biblioteca de rules

apache_rules.xml
mcafee_av_rules.xml
proftpd_rules.xml
syslog_rules.xml
arpwatch_rules.xml
msauth_rules.xml
pure-ftpd_rules.xml
telnetd_rules.xml
asterisk_rules.xml
ms-exchange_rules.xml
racoon_rules.xml
sshd_rules.xml
local_rules.xml
postfix_rules.xml
symantec-av_rules.xml
mailscanner_rules.xml

attack_rules.xml
ms_ftpd_rules.xml
rules_config.xml
vmpop3d_rules.xml
cisco-ios_rules.xml
mysql_rules.xml
sendmail_rules.xml
vmware_rules.xml
courier_rules.xml
named_rules.xml
smbd_rules.xml
squid_rules.xml
zeus_rules.xml
imapd_rules.xml
policy_rules.xml
postgresql_rules.xml

vpn_concentrator_rules.xml
firewall_rules.xml
netscreenfw_rules.xml
solaris_bsm_rules.xml
vpopmail_rules.xml
ftpd_rules.xml
ossec_rules.xml
sonicwall_rules.xml
vsftpd_rules.xml
hordeimp_rules.xml
pam_rules.xml
spamd_rules.xml
web_rules.xml
ids_rules.xml
pix_rules.xml
symantec-ws_rules.xml

Criando Rules

```
<!-- Tornamos ESSI modifications -->

 <rule id="60000" level="2">
    <match>bad owner name (check-names)</match>
<!--    <options>alert_by_email</options> -->
    <description>Hosts cadastrado no dominio com algum caracter especial.</description>
  </rule>

<rule id="60001" level="2">
    <match>dansguardian: Error connecting via ipc to log</match>
    <description>Dansguardian nao esta conseguindo gravar logs de acesso.</description>
  </rule>

<rule id="60002" level="2">
    <match>failed while receiving responses: not exact</match>
    <description>A zona de DNS mudou durante a transferencia.</description>
  </rule>

<rule id="60003" level="9">
    <match>dansguardian: Error connecting to proxy</match>
    <description>O servico de PROXY esta offline.</description>
  </rule>

<rule id="60004" level="7">
    <match>The product was not installed correctly</match>
    <match>Failed to synchronize with host</match>
    <description>O Antivirus nao esta funcionando corretamente.</description>
  </rule>
```

Dúvidas?

Referências

www.ossec.net
www.linuxmagazine.com.br
www.linuxworld.com

Contato

toronto.garcez@gmail.com

Obrigado!! ;)