Implementação do OSSEC em IPV6

*Roberto Clamer

Resumo: O objetivo deste artigo é apresentar a solução OSSEC – Open Source Security – implementada utilizando o protocolo IPv6, na qual não foi observada restrições quanto a plataforma, entretanto algumas configurações técnicas e conhecimentos específicos do ambiente a ser aplicado, como também informações sobre segurança da informação e diretrizes que devem ser asseguradas, serão importantes para proceder adequadamente com essa implementação.

Palavras-chave: Segurança – Informação – OSSEC – IPV6.

Abstract: The objective of this paper is to present the solution OSSEC - Open Source Security - implemented using IPV6, which was not observed restrictions on the platform, however some settings, skills and expertise to be applied to the environment, as well as information about information security and guidelines to be provided, will be important to properly proceed with this implementation.

Keywords: Security – Information – OSSEC - IPV6.

1 INTRODUÇÃO

A segurança da informação está em foco em todos os países e organizações, principalmente partir do fato que ocorreu recentemente sobre a NSA (National Security Agencie) dos EUA com seu programa PRISM, na qual evidenciou a grande fragilidade das comunicações utilizando-se meios virtuais, com especial foco na utilização da internet.

*Autor: Pós-Graduando MBA em Gerenciamento Estratégico de Projetos pela Faculdade da Serra Gaúcha; Administrador Analista de Sistemas, Coordenador de Tecnologia e Comunicação da empresa Diferro Aços Especiais, docente dos cursos de Graduação em Tecnologia da FTEC – Faculdade de Tecnologia em Caxias do Sul. E mail: bergbah@ibest.com.br.

Trabalho realizado para conclusão do curso EAD-IPv6 realizado pelo NIC.BR;

Os países estão adotando medidas cada vez mais protetivas para garantia dos direitos da informação de sua população, principalmente no que tange ao sigilo das comunicações quanto a informação – um bem jurídico inviolável – que precisa de atenção quando evocamos questões que envolvem a confidencialidade e integridade. Assim como o respeito das decisões de governo sobre processos em análise tática e estratégica, que envolve a comunicação entre chefes de estados desses países e até mesmo chefes de governo entre diversos países.

Dessa forma as organizações, em especial as privadas, estão solicitando e exigindo aos seus governantes que sejam pró-ativos quanto à restrição de acesso às informações que circulam em seu país, ressaltando quanto aos segredos industriais, que precisam do sigilo necessário ao resguardar dados sensíveis quanto a competitividade no mercado corporativo.

Contudo as equipes de tecnologias das empresas estão constantemente atualizando seus conhecimentos técnicos para garantir a disponibilidade das informações, sendo que atualmente o meio da internet é reconhecido como principal acesso básico para a comunicação, pois qualquer ferramenta de aplicação sistêmica utiliza-se da internet para executar suas operações que necessitam trocar dados para o funcionamento adequado e atualizado.

Com a necessidade de mudança constante tecnológica e a demanda crescente de pessoas, organizações e países que utilizam cada vez mais recursos interconectados através da internet, ressaltando o reflexo da evolução na utilização de equipamentos avançados que possuem tecnologia de comunicação para conexão com a internet, destacamos uma mudança importante no que tange ao funcionamento da internet quanto ao protocolo de comunicação TCP/IP, na qual atualmente 95% da estrutura em nível mundial está embasada na versão IPv4, porém é necessário que haja a migração para a versão IPv6 a fim de ampliar a utilização de endereçamentos e consolidar a Internet das Coisas.

Assim, de forma mais evidente, a segurança da estrutura de tecnologia corporativa que comportam informações sensíveis estão e ficarão mais fragilizadas, por isso a implementação de equipamentos para garantir a segurança e monitoramento constante é primordial.

2 FUNDAMENTAÇÃO

A segurança da informação é .....

Protocolo TCP/IP

IPv4

IP66

2.1 OSSEC (Open Source Security)

O OSSEC – Host-based Intrusion Detection System – é um sistema de detecção baseado em hosts (HIDS), escalável, multiplataforma, com análise de logs, checagem da integridade de arquivos, monitoramento constante, detecção de rootkits, que desenvolvido em código aberto e que proporciona uma segurança pró-ativa com resposta instantânea online para alertas necessários.

A instalação da ferramenta é baseada em arquivos XML, com gerenciamento centralizado utilizando de arquitetura local ou cliente/servidor na qual possibilita através de consultas a boas práticas já desenvolvidas, uma aplicação segura por padrão, devido ao fato de que existem modelos de configurações com privilégios mínimos pré-definidos por usuário que segregam as permissões dos processos realizados pela própria aplicação, na qual possui no modo de operação cliente e servidor utilizando-se da criptografia na comunicação.

Os processos internos executados pelo OSSEC:

1) Analyslsd – Processo principal responsável pela análise.
2) Remoted – Responsável por receber os registros remotos.
3) LogCollector – Responsável por analisar os arquivos logs coletados.
4) Agentd – Responsável por encaminhar os logs para o server.
5) Maild – Responsável por enviar e-mails.

6) Execd – Responsável por executar as respostas.
7) Monitord – Responsável por monitorar o estado dos agentes.

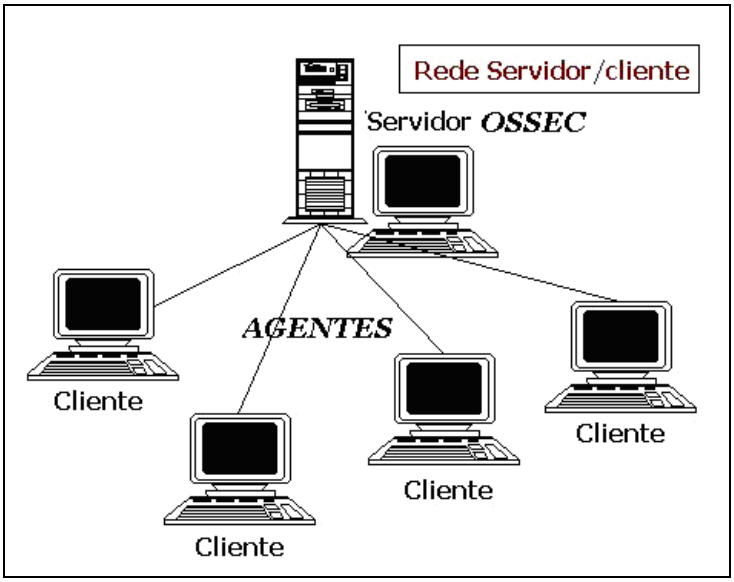


Figura 1: Aplicação OSSEC Cliente X Servidor

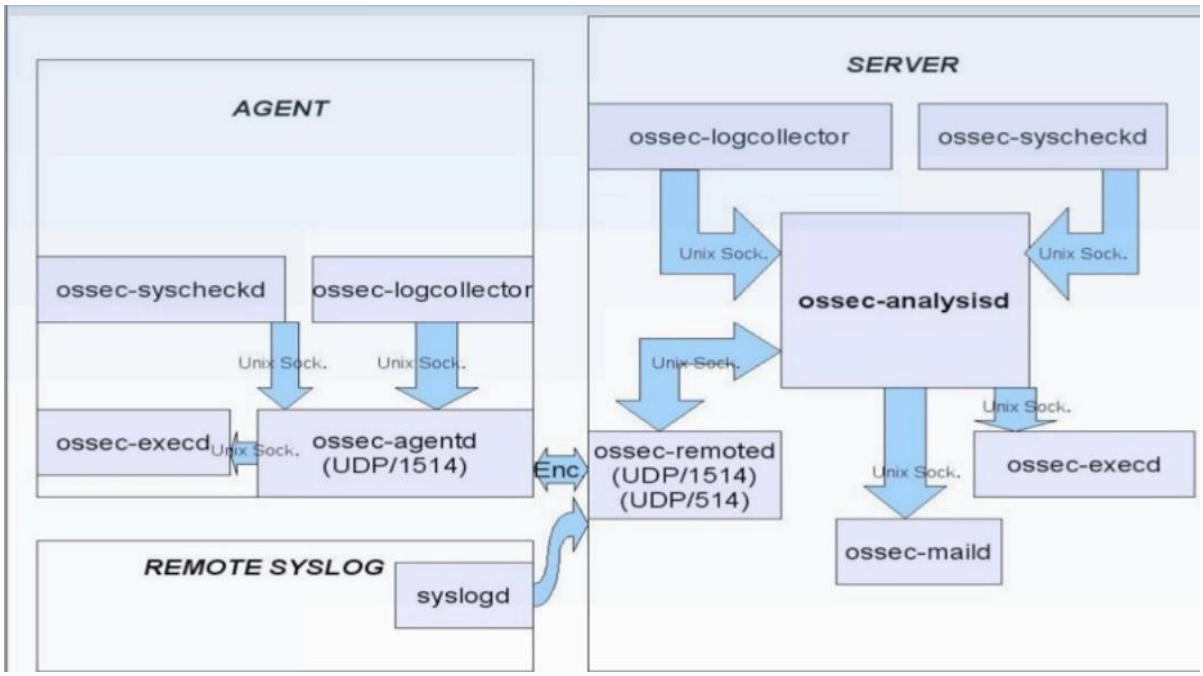
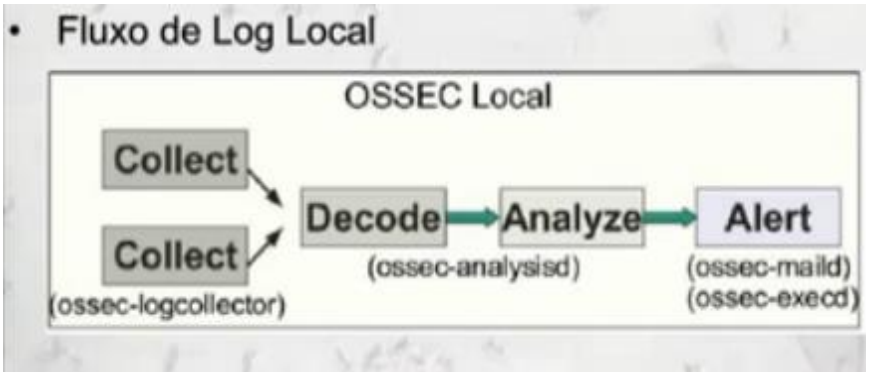


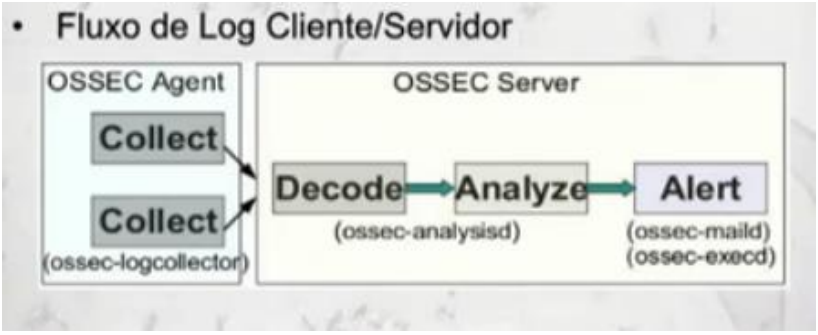
Figura 3: Arquitetura OSSEC

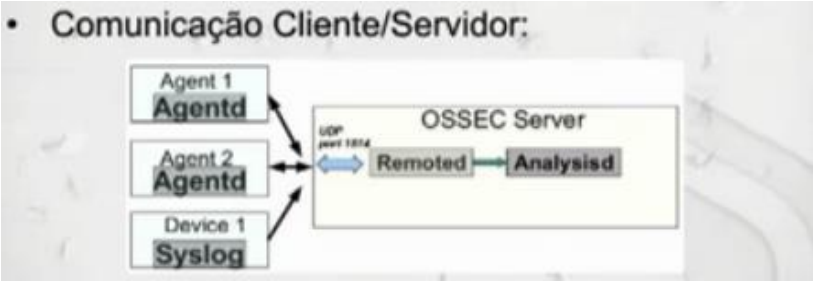
2.1.1 Análise de Logs

Utiliza-se de técnicas como compressão de arquivos para armazenamento e segurança, através da criptografia com chaves compartilhadas do blowfish, com comunicação pela porta UDP:1514.

Logs suportados: Unix Pam, OpenSSH, Solaris telnetd, Samba, Sudo, Proftpd, Pureftpd, MS FTP Server, Solaris FTP, Imapd, Postfix, SendMail, MS Exchange, Apache, MS Internet Information Service, Iptables, Netscreen, Cisco PIX/ASA/FWSM, Cisco IOS, Snort, Nmap, Symantec AV, Named, Squid, MS Win event logs, entre outros.

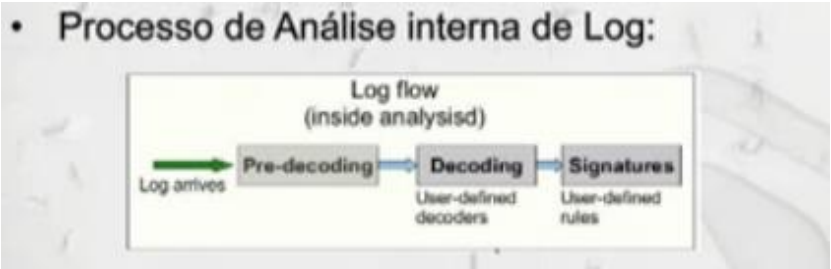






O processo de análise de logs é realizado através das funções:

1) Pré-decoding: Extração de campos conhecidos como time, IP, etc.
2) Decoding: Utilizando-se de expressões pré-definidas.
3) Assinaturas: Utilizando-se de regras pré-definidas.



2.1.2 Checagem da Integridade de Arquivos

```
<rule id="100345" level="12">
<if_matched_group>syscheck</if_matched_group>
<description>Changes to /var/www/htdocs – Critical file!</description>
<match>/var/www/htdocs</match>
</rule>
```

2.1.3 Monitoramento

```
<!-- SSHD messages -->
<group name="syslog,sshd,">
<rule id="5700" level="0" noalert="1">
<decoded_as>sshd</decoded_as>
<description>SSHD messages grouped.</description>
</rule>

<rule id="5704" level="4">
```

```
<if_sid>5700</if_sid>
<match>fatal: Timeout before authentication for</match>
<description>Timeout while logging in (sshd).</description>
</rule>
<rule id="5705" level="10" frequency="4" timeframe="360">
<if_matched_sid>5704</if_matched_sid>
<description>Possible scan or breakin attempt </description>
<description>(high number of login timeouts).</description>
</rule>
```

2.1.4 Detecção de Rootkits

2.1.5 Alertas

```
<rule id="100101" level="10">
<if_group>authentication_success</if_group>
<time>7 pm 6:
30 am</time>
<description>Login during nonbusiness
hours.</
description>
</rule>
```

3 METODOLOGIA

Foi utilizada a metodologia de análise qualitativa descritiva, pois houve a necessidade no entendimento completo do objeto de estudo, na qual apresenta diversas variáveis a serem consideradas no momento dos testes da aplicação.

O procedimento utilizado através da simulação na coleta de dados experimental, registrando de forma sintética as principais situações realizadas para adequação da ferramenta ao contexto descrito.

4 RESULTADOS

5 CONSIDERAÇÕES FINAIS

6 REFERÊNCIAS

ZUCCO, Jerônimo. **Implementando o OSSEC HIDS**. Publicação 2010 Artigo disponível em ftp://ftp.registro.br/pub/gts/gts16/TutorialOSSEC/Implementando_OSSEC.pdf

http://www.dicas-l.com.br/arquivo/ossec_hids.php#.UhPVvH_lexk

Site: http://www.ossec.net/

Download: http://www.ossec.net/?page_id=19