OSSEC

Criptografia e Segurança nas Comunicações

Docentes: Hugo Almeida /Pedro Pinto

Luís Oliveira
24833
l.oliveira@ipvc.pt
Turno A
ERSC
ESTG-IPVC
2020/2021

Bruno Rodrigues
23683
bfiliperodrigues@ipvc.pt
Turno A
ERSC
ESTG-IPVC
2020/2021

INTRODUÇÃO

A busca por soluções para auxiliar no dia-a-dia é constante, e neste contexto será apresentado uma ferramenta open source para o controlo da rede. Para encontrar estas soluções, neste artigo vamos falar da ferramenta OSSEC.

O OSSEC é um sistema de detecção de invasões baseado em host livre e aberto. Este possui uma arquitetura centralizada e multi - plataforma.

Este é também uma ferramenta poderosa que serve para garantir a segurança da informação em ambientes de redes.

OBJETIVOS

- Demonstrar a utilização do OSSEC;
- Verificar a fiabilidade e a capacidade desta ferramenta.

CENÁRIO

O OSSEC foi instalado na máquina Linux/Ubuntu. Configuramos a interface web onde é possível procurar por data, verificar a quantidade de alertas por regra, por nível, verificar a integridade do computador e o status do computador, ou seja, permite a verificação dos logs e os incidentes reportados. Configuramos também os alertas que são recebidos no email. Sempre que haja um alerta de elevado risco, é notificado o email que foi configurado.

Foram adicionados os agentes ao servidor, que servem para adicionar as máquinas.

Foi utilizada a máquina Kali Linux, para realizar vários ataques e testar o funcionamento do OSSEC.

DESENVOLVIMENTO

O OSSEC é uma plataforma completa para monitorizar e controlar o sistema.

Está disponível em várias plataformas, como Linux, Solaris, Windows e Mac OS X.

O OSSEC permite que os administradores configurem alertas sobre os quais desejam ser alertados e permite que estes se destaquem em aumentar a prioridade de alertas críticos. A integração com smtp, sms e syslog permite que os administradores fiquem atentos aos alertas, enviando notificações para o email. Opções de resposta ativa para bloquear um ataque no momento também está disponível.

O OSSEC pode ser utilizado com agente e sem o controlo de um agente, como por exemplo os rooters e as firewalls.

Esta ferramenta também permite que sempre que haja uma alteração no sistema, o administrador é automaticamente notificado através da deteção do rootkit.

A resposta ativa permite que o OSSEC execute uma ação imediata quando os alertas são acionados.

Integridade do ficheiro, é o processo que verifica a integridade e autenticidade de um ficheiro, ou seja, o objetivo é identificar os ficheiros modificados sem o consentimento do administrador do sistema.

O OSSEC permite realizar o controlo de integridade de ficheiros, sem o agente estar instalado. É bastante útil para controlar firewalls e rooters.

O OSSEC pode receber e analisar os eventos syslog a partir de uma grande variedade de firewalls, switches e rooters. Este suporta todos os rooters Cisco, Cisco PIX, Cisco FWSM, Cisco ASA, Juniper Routers, Netscreen firewall, Checkpoint, entre outros.

RESULTADOS

Os resultados obtidos foram os pretendidos. Como podemos visualizar nas duas primeiras imagens, conseguimos criar os agentes e adicioná-los ao servidor.

De seguida, podemos ver que a interface web do OSSEC foi configurada e permite-nos visualizar o que se passa na rede.

Foi realizada uma tentativa de ataque brute - force ao servidor, e como podemos ver na imagem 4, este ataque foi negado e alertado ao administrador.

Seguidamente, foi configurado no ficheiro para que os alertas superiores ou iguais a nível 7 fossem alertados ao administrador através do email.

Por fim na imagem 6, conseguimos observar a resposta ativa a ser utilizada e os alertas a serem acionados.

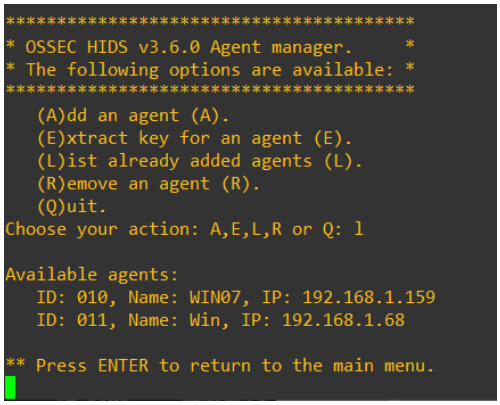


Fig1 – Adição dos agentes

Fig2 – Adição do agente ao servidor

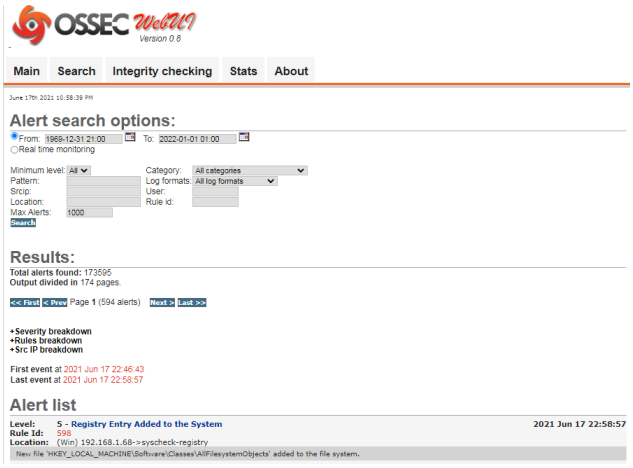


Fig3 - Interface Web

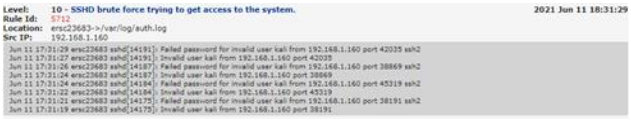


Fig4 – Tentativa de ataque brute – force

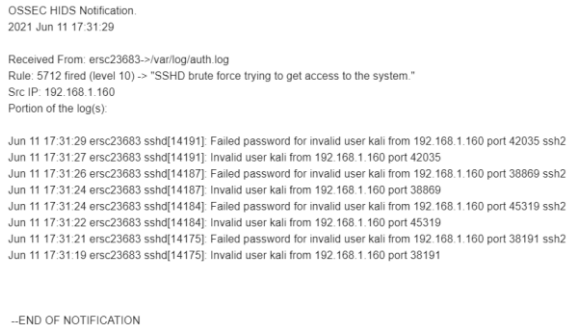


Fig5 – Notificação email

Fig6 – Resposta ativa

CONCLUSÃO

Apesar de ser uma ferramenta de simples utilização e fácil instalação, o OSSEC não deixa de ser uma boa opção para controlar a rede. Entre as suas principais finalidades, a análise de logs e verificação de integridade ganham destaque devido à facilidade da compreensão dos dados apresentados durante a monitorização.

Ferramenta Open Source poderosa para a deteção de intrusos e com um funcionamento muito simples de se entender.

Por fim, esta é a versão gratuita, mas existe a versão paga com mais funcionalidades, para implementar nas empresas.

Luís Oliveira – nº24833

Bruno Rodrigues – nº23683

REFERÊNCIAS

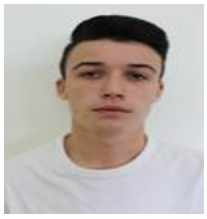
1 - https://www.ossec.net/

2 - https://www.guiadoti.com/?s=OSSEC

3 - https://docplayer.com.br/20277733-O-que-e-o-ossec-como-funciona.html

Realizado por:

Luís Oliveira, nº24833, Autoavaliação:13



Bruno Rodrigues, nº23683, Autoavaliação: 13