Year 2020/2021 | Graduation Computer Networks and Systems Engineering | Subject Communications encryption and security

Students Luís Oliveira, Bruno Rodrigues | Supervision Pedro Pinto, Hugo Almeida

OSSEC

INTRODUCTION

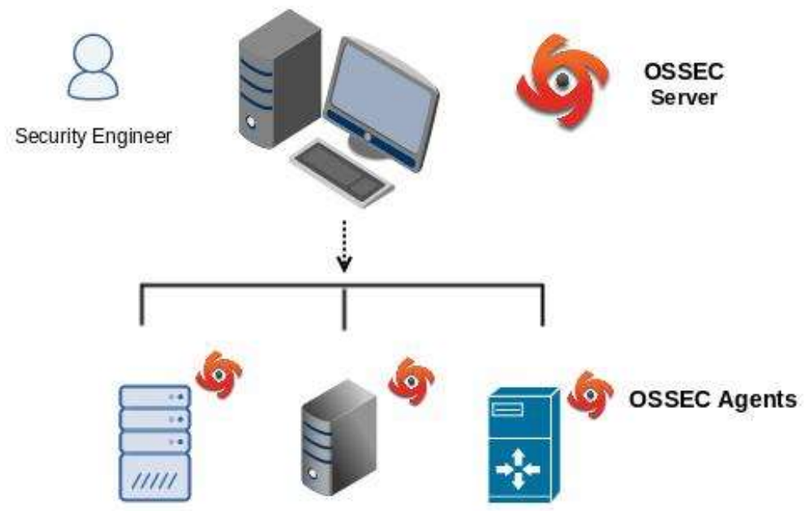
O OSSEC (Open Source Host-based Intrusion Detection System) é uma ferramenta de deteção de invasão baseado em host livre e aberto. Serve também para analisar o tráfego num ambiente computacional.

WORK

O OSSEC é executado em praticamente todos os sistemas operacionais (Linux, Windows, Solaris, Mac OS X, etc).

Com esta ferramenta é possível:

- Análise da integridade dos logs;
- Review da integridade dos ficheiros;
- Deteção de Rootkit em tempo real;
- Deteção de Malware
- Alertas em tempo real;



RESULTS

Tentativa de um ataque brute force através de uma máquina Kali.

Alerta recebido no email configurado pelo administrador, sobre um ataque não conseguido ao servidor.

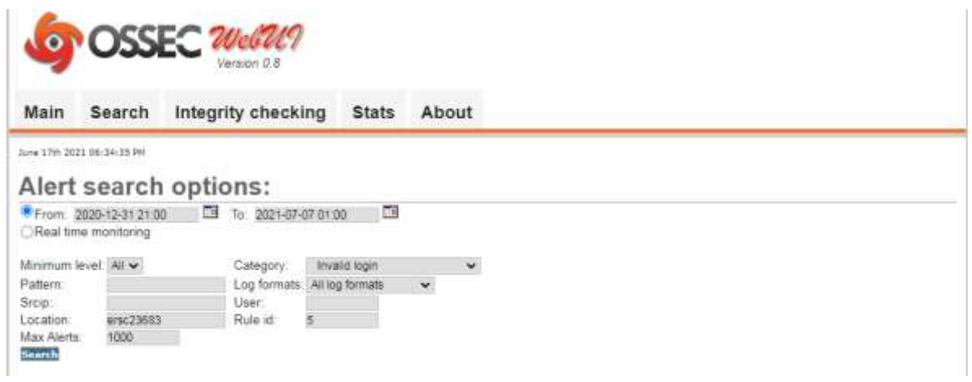
OSSEC HIDS Notification
2021 Jun 11 17:31:29

Received From: ersc23683->/var/log/auth.log
Rule: 5712 fired (level 10) -> "SSHD brute force trying to get access to the system."
Src IP: 192.168.1.160
Portion of the log(s):

Jun 11 17:31:29 ersc23683 sshd[14191]: Failed password for invalid user kali from 192.168.1.160 port 42035 ssh2
Jun 11 17:31:27 ersc23683 sshd[14191]: Invalid user kali from 192.168.1.160 port 42035
Jun 11 17:31:26 ersc23683 sshd[14187]: Failed password for invalid user kali from 192.168.1.160 port 38869 ssh2
Jun 11 17:31:24 ersc23683 sshd[14187]: Invalid user kali from 192.168.1.160 port 38869
Jun 11 17:31:24 ersc23683 sshd[14184]: Failed password for invalid user kali from 192.168.1.160 port 45319 ssh2
Jun 11 17:31:22 ersc23683 sshd[14184]: Invalid user kali from 192.168.1.160 port 45319
Jun 11 17:31:21 ersc23683 sshd[14175]: Failed password for invalid user kali from 192.168.1.160 port 38191 ssh2
Jun 11 17:31:19 ersc23683 sshd[14175]: Invalid user kali from 192.168.1.160 port 38191

--END OF NOTIFICATION

Pode-se fazer uma pesquisa por diferentes categorias: rule ID; user; log format; max alerts; entre outros.



CONCLUSIONS

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

A ferramenta encontra-se disponível na versão gratuita onde existem algumas limitações, e encontra-se também disponível na versão paga para empresas, onde existe número ilimitado de agentes.

REFERENCES & LINKS

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
4. https://www.ossec.net/docs/manual/syscheck/index.html
5. https://bdigital.ufp.pt/bitstream/10284/6184/1/DM_Sheilla%20Nascimento.pdf