Faculdade Impacta - DEVOPS

Relatório
Automação
de
Monitoramento de Logs

Professor: Vanderson Gomes Bossi

Alunos: Joshua Yuuki Onizuka de Souza - **RA** 2400266
Alunos: Paulo Henrique Caldeira - **RA** 2302254

Data: 02/06/2025

Automação de Monitoramento de Logs

Automação de Monitoramento de Logs

1. Introdução

A crescente complexidade dos ambientes computacionais e a constante evolução das ameaças cibernéticas exigem soluções eficazes e automatizadas para a detecção precoce de incidentes de segurança. O monitoramento de logs se torna uma ferramenta essencial para identificar comportamentos anômalos e mitigar riscos de forma proativa.

Neste contexto, o presente projeto acadêmico teve como objetivo implementar uma solução de coleta e automação de logs utilizando ferramentas gratuitas de mercado, com foco em ambientes críticos. A plataforma Wazuh Machine OVA foi utilizada como base para a realização das atividades.

Automação de Monitoramento de Logs

2. Descrição do Projeto

2.1 Eventos Monitorados

Durante o desenvolvimento, foram simulados e coletados os seguintes eventos de segurança:

- Tentativas de login inválidas.
- Modificações em arquivos sensíveis do sistema.
- Execução de comandos suspeitos em shell.
- Alterações em permissões de arquivos.
- Acessos não autorizados em diretórios críticos.

Esses eventos foram escolhidos por representarem situações comuns de risco, como tentativas de invasão, escalonamento de privilégios e manipulações indevidas no ambiente.

Automação de Monitoramento de Logs

2.2 Automação do Monitoramento

1. Script

Arquivo: /var/ossec/etc/rules/local_rules.xml

xml<group name="authentication_failed">

<rule id="100100" level="10">

<if_sid>5710</if_sid> <!-- Ex: regra para falha de login SSH -->

<match>Failed password</match>

<description>Múltiplas falhas de login detectadas</description>

</rule>

</group>

2. Configurar uma Active Response

A Active Response permite que você execute scripts automaticamente quando uma regra for acionada.

Arquivo: /var/ossec/etc/ossec.conf

xml

<active-response>

<command>block_ip</command>

<location>local</location>

<rules_id>100100</rules_id>

</active-response>

Automação de Monitoramento de Logs

3. Script customizado

Script para bloquear IP (pode ser adaptado para qualquer automação)

```
bash

#!/bin/bash

IP=$1

echo "Bloqueando IP $IP"

iptables -A INPUT -s $IP -j DROP
```

Permissão de execução:

```
chmod +x /var/ossec/active-response/bin/block_ip
```

4. Restart o Wazuh Manager

```
systemctl restart wazuh-manager
```

Exemplos de automações que você pode implementar:

- Notificar via e-mail/Telegram se alguém logar fora do horário comercial
- Bloquear IP automaticamente após 5 tentativas de login falhadas
- Gerar um alerta se um usuário tentar usar sudo fora do horário autorizado
- Rodar um script que isola a máquina da rede em caso de evento crítico

2.3 Ferramentas de Monitoramento Pesquisadas

Wazuh

- Plataforma SIEM (Security Information and Event Management) baseada no OSSEC.
- Oferece visualização via Kibana, regras de correlação, controle de integridade e resposta automatizada a incidentes.
- Integra-se facilmente com agentes instalados em hosts Linux e Windows.

Graylog

- Centralizador de logs com painel gráfico customizável.
- Utiliza Elasticsearch e MongoDB como back-end.
- Boa escalabilidade e opções de alertas baseados em condições específicas.

Outras ferramentas consideradas, mas não utilizadas no projeto prático:

- **Elastic Stack (ELK)** – maior curva de aprendizado.
- **OSSEC** – base do Wazuh, porém menos amigável na configuração e visualização.

2.4 Integração e Organização dos Logs

O principal desafio foi consolidar os dados dos logs em um formato acessível e compreensível. Para isso:

- Foi utilizado o **Pandas** no Python para organizar os registros em `.csv`.
- O script foi preparado para exportar relatórios diários com estatísticas dos eventos.
- A integração com Wazuh foi simulada através da análise da documentação e dos arquivos gerados localmente, uma vez que a versão OVA já continha a infraestrutura pré-configurada.

Automação de Monitoramento de Logs

3. Evidências e Capturas de Tela

- Execução do script e geração de logs.
- Visualização dos arquivos `.csv` com registros coletados.
- Prints dos dashboards/documentações da ferramenta Wazuh.

```
[root@wazuh-server bin]# cd /var/ossec/etc/rules/local_rules.xml
bash: cd: /var/ossec/etc/rules/local_rules.xml: Not a directory
[root@wazuh-server bin]# cd /var/ossec/etc/rules/
[root@wazuh-server rules]# ls
local_rules.xml  local_rules.xml2
```

```
  GNU nano 8.3
<active-response>
  <command>block_ip</command>
  <location>local</location>
  <rules_id>100100</rules_id>
</active-response>
```

```
[root@wazuh-server bin]# pwd
/var/ossec/active-response/bin
[root@wazuh-server bin]# ls
block-ip             disable-account  firewalld-drop  ip-customblock  kaspersky     npf  restart-wazuh  route-null
default-firewall-drop  firewall-drop  host-deny       ipfw            kaspersky.py  pf   restart.sh     wazuh-slack
```

Automação de Monitoramento de Logs

```
  GNU nano 8.3
#!/bin/bash
IP=$1
echo "Bloqueando IP $IP"
iptables -A INPUT -s $IP -j DROP
```

```
[root@wazuh-server bin]# chmod +x /var/ossec/active-response/bin/block_ip
chmod: cannot access '/var/ossec/active-response/bin/block_ip': No such file or directory
[root@wazuh-server bin]# ls
block-ip              disable-account  firewalld-drop  ip-customblock  kaspersky     npf  restart-wazuh  route-null
default-firewall-drop  firewall-drop    host-deny       ipfw            kaspersky.py  pf   restart.sh     wazuh-slack
[root@wazuh-server bin]# chmod +x block-ip
[root@wazuh-server bin]# ls
block-ip              disable-account  firewalld-drop  ip-customblock  kaspersky     npf  restart-wazuh  route-null
default-firewall-drop  firewall-drop    host-deny       ipfw            kaspersky.py  pf   restart.sh     wazuh-slack
```


Automação de Monitoramento de Logs

4. Conclusão

O que Aprendemos

Este projeto permitiu compreender, na prática, a importância da coleta e do monitoramento de logs como primeiro passo na detecção de ameaças cibernéticas. A experiência demonstrou como a automação pode ser uma aliada poderosa para antecipar problemas e melhorar a postura de segurança de sistemas.

Dificuldades Encontradas

- Dificuldade inicial em entender a estrutura dos logs do Linux.
- Integração com Wazuh exigiu leitura aprofundada da documentação.
- Organização dos dados em formato reutilizável exigiu domínio de bibliotecas Python específicas.

Como Foram Resolvidas

- Utilização de regex e documentação oficial dos arquivos de log.
- Consulta a fóruns técnicos e documentação da Elastic e Wazuh.
- Testes repetidos para validar o funcionamento correto da automação e do script.

Ferramenta Recomendada

A ferramenta mais viável para aplicação real seria o Wazuh, devido à sua robustez, documentação extensa, facilidade de integração com outros sistemas de segurança e visualização via Kibana. Sua estrutura modular e capacidade de gerar alertas em tempo real a torna ideal para ambientes corporativos com demandas críticas de segurança.

Automação de Monitoramento de Logs

5. Considerações Finais

Este trabalho reforça o papel fundamental da automação e do monitoramento ativo em ambientes computacionais. O uso de ferramentas open source como o Wazuh mostra-se não apenas viável, mas estratégico para empresas que desejam implementar um SOC (Security Operation Center) eficaz com recursos limitados.

Mais do que uma entrega técnica, este projeto foi uma experiência de amadurecimento na compreensão da importância da inteligência de logs e da integração entre desenvolvimento e segurança.

