UNIVERSIDADE PITÁGORAS UNOPAR
POLO DE APOIO, JUNDIAÍ-SP
CURSO SUPERIOR DE SISTEMAS DE INFORMAÇÃO

NOME DO AUTOR: ALISSON HENRIQUE CORREIA

Computação Forense

São Paulo–SP
2024

Computação Forense

Trabalho apresentado à Universidade Pitágoras Unopar
como requisito parcial à aprovação no
Quinto Semestre do curso de
Sistemas de informação.

São Paulo–SP
2024

SUMÁRIO

Introdução

A segurança em ambientes de TI é uma preocupação crescente, especialmente com a sofisticação de ataques cibernéticos e a constante evolução das ameaças. Uma das formas mais comuns de ataques envolve a exploração de serviços expostos, como o SSH, que permite o acesso remoto a servidores. Neste contexto, a análise forense de logs de servidores comprometidos torna-se uma prática essencial para entender a natureza dos ataques, identificar vulnerabilidades exploradas e propor medidas corretivas para evitar futuros incidentes.

Neste trabalho, será apresentada a análise detalhada de um incidente de segurança ocorrido em um servidor Linux, no qual tentativas repetidas de login via SSH resultaram no comprometimento da conta de administrador (root). A partir da análise dos logs fornecidos, identificaremos o ponto de entrada, as atividades realizadas pelo invasor e sugeriremos medidas de segurança para prevenir ataques semelhantes no futuro

Desenvolvimento

Com base nos registros de logs fornecidos, foi desenvolvido um relatório que revela a ação realizada pelo invasor e as soluções para evitar a recorrência num possível evento futuro

Log:

```
Jun 15 22:45:01 server1 sshd[1952]: Failed password for root from 192.168.1.105
port 54022 ssh2
Jun 15 22:45:03 server1 sshd[1953]: Failed password for root from 192.168.1.105
port 54024 ssh2
Jun 15 22:45:06 server1 sshd[1954]: Accepted password for root from 192.168.1.105
port 54026 ssh2
Jun 15 22:46:10 server1 sudo: pam_unix(sudo:session): session opened for user root
by (uid=0)
Jun 15 22:47:30 server1 sudo: pam_unix(sudo:session): session closed for user root
Jun 15 22:48:05 server1 sshd[2001]: Received disconnect from 192.168.1.105 port
54026:11: disconnected by user
Jun 15 22:48:05 server1 sshd[2001]: Disconnected from 192.168.1.105 port 54026
```

Relatório de Incidente de Segurança

1. Resumo do Incidente

Data do incidente: **15 de Junho** Servidor comprometido: **server1** Endereço IP do invasor: **192.168.1.105** Método de entrada: **SSH** Usuário comprometido: **root** Tempo da sessão: **22:45:01 - 22:48:05**

2. Descrição do Incidente

A análise dos logs coletados revelou atividades suspeitas relacionadas a tentativas de login mal sucedidas seguidas por uma tentativa bem-sucedida com o usuário root. A sequência de eventos ocorreu da seguinte forma:

1. **Falhas de autenticação SSH**:
    - **22:45:01**: Tentativa falha de login para o usuário root a partir do IP **192.168.1.105** (porta 54022).
    - **22:45:03**: Segunda tentativa falha de login para root a partir do IP **192.168.1.105** (porta 54024).
2. **Sucesso na autenticação SSH**:
    - **22:45:06**: Autenticação bem-sucedida para o usuário root a partir do IP **192.168.1.105** (porta 54026). Isso indica que o atacante foi capaz de obter ou forçar a senha do root.
3. **Abertura e fechamento de sessão sudo**:

    - **22:46:10**: A sessão sudo foi aberta, indicando que o invasor obteve privilégios elevados. O invasor usou o comando `sudo` para executar comandos com privilégios administrativos.
    - **22:47:30**: A sessão sudo foi encerrada.
4. **Encerramento da conexão SSH**:
    - **22:48:05**: O invasor desconectou do servidor, finalizando a sessão SSH.

3. Análise das Atividades

A partir do log, fica claro que o invasor utilizou o usuário **root** para realizar atividades com privilégios elevados durante a sessão sudo. No entanto, o log não oferece detalhes específicos sobre os comandos executados durante essa sessão. A ausência de informações detalhadas sobre as atividades exatas realizadas durante o uso do `sudo` impede uma análise mais detalhada sobre as alterações feitas no sistema.

4. Ponto de Entrada

O invasor conseguiu comprometer o servidor através de tentativas repetidas de login por SSH (provavelmente usando um ataque de força bruta ou possivelmente através de uma senha fraca). Após duas tentativas falhas, o invasor obteve sucesso na terceira tentativa de login.

5. Recomendações de Segurança

Baseado na análise, aqui estão algumas recomendações para prevenir incidentes semelhantes no futuro:

1. **Desativar login direto como root**:
    - Desativar o login SSH para o usuário root e, em vez disso, utilizar um usuário com privilégios limitados que possa elevar permissões usando `sudo` quando necessário.
2. **Habilitar autenticação por chave SSH**:
    - Exigir a autenticação por chave pública SSH para o acesso remoto ao servidor, eliminando a necessidade de login por senha.
3. **Implementar políticas de senhas fortes**:
    - Exigir senhas fortes e complexas para todas as contas, incluindo root e usuários com privilégios administrativos.
4. **Implementar limitação de tentativas de login**:
    - Utilizar ferramentas como **fail2ban** ou **SSHGuard** para bloquear temporariamente endereços IP após várias tentativas de login falhas, mitigando ataques de força bruta.
5. **Monitoramento de atividades privilegiadas**:
    - Configurar monitoramento para registrar comandos executados durante sessões `sudo`. Isso pode ser feito utilizando logs mais detalhados ou soluções de auditoria como **Auditd**.
6. **Utilizar um firewall para limitar o acesso SSH**:
    - Restringir o acesso SSH apenas a endereços IP confiáveis e conhecidos. Isso pode ser configurado utilizando **firewalls** como **UFW** ou **iptables**.
7. **Auditoria e monitoramento de logs**:
    - Configurar alertas automáticos para atividades suspeitas, como várias tentativas de login falhas e atividades privilegiadas. Sistemas de

monitoramento de logs como **OSSEC** ou **Splunk** podem ser usados para essa finalidade.

6. Conclusão

O incidente analisado revela um comprometimento do servidor através de um ataque de força bruta ou senha comprometida no serviço SSH. É necessário revisar as práticas de segurança em torno do acesso ao servidor, implementando métodos de autenticação mais seguros e monitorando atividades suspeitas regularmente.

Considerações Finais

As atividades realizadas permitiram o desenvolvimento de habilidades práticas fundamentais na análise forense de logs de sistemas comprometidos. Através da análise dos registros fornecidos, foi possível identificar padrões de comportamento malicioso, determinar o ponto de entrada do ataque e avaliar as ações realizadas pelo invasor. Além disso, o exercício proporcionou a oportunidade de elaborar um relatório detalhado, descrevendo o incidente e propondo recomendações de segurança para evitar novos ataques.

Esse processo reforça a importância do conhecimento técnico para interpretar evidências e aplicar contramedidas eficazes. A análise de logs, combinada com a capacidade de propor soluções preventivas, é essencial para melhorar a postura de segurança das organizações. A experiência obtida com esta prática capacita o aluno a lidar com cenários reais de segurança cibernética, compreendendo tanto a identificação de vulnerabilidades quanto a implementação de medidas de proteção adequadas.

Referências

Aula de: **Computação Forense**
Tutores: Elisa Antolli Paleari
Conteúdo fornecido por Faculdade Anhanguera

Curso de Computação forense
Tutor: Eduardo Santos
Conteúdo: https://www.youtube.com/playlist?list=PLGs72hmHIIDTWXm7_cTIdD-iPiaqAHNxT