PORTFÓLIO DE COMPUTAÇÃO FORENSE

5ºSEMESTRE

DATA: 25/09/2024

PROFESSOR: Elisa Antolli Paleari

NOME DO ALUNO: Fernando Henrique Panini

1. Preparação e Coleta de Logs

Ambiente de Análise: Um ambiente seguro foi estabelecido para análise dos logs, garantindo que nenhum dado fosse alterado. Todos os logs foram copiados para um sistema isolado para análise.

Coleta de Logs: Os logs suspeitos extraídos do servidor são os seguintes:

```
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
```

2. Análise dos Logs

Análise Inicial: As entradas do log revelam várias tentativas de login:

- **Tentativas Falhas:** Duas tentativas de login falharam (22:45:01 e 22:45:03) para o usuário root a partir do IP 192.168.1.105.
- **Login Bem-Sucedido:** Uma tentativa de login foi bem-sucedida (22:45:06) para o usuário root a partir do mesmo IP.

IP e Ações do Usuário: O endereço IP de onde as tentativas de login se originaram é 192.168.1.105. Após obter acesso com sucesso, o usuário root abriu uma sessão sudo (22:46:10) e a fechou em (22:47:30). O log não fornece detalhes sobre os comandos executados durante a sessão sudo, o que é uma lacuna crítica.

Determinação de Atividades: Como não temos os comandos executados na sessão sudo, não é possível determinar se as atividades realizadas foram maliciosas. No entanto, o acesso root e o uso do sudo após tentativas de login falhadas são altamente suspeitos e indicam um potencial comprometimento.

3. Relatório de Incidente

Método de Entrada: O método de entrada foi através do protocolo SSH, com várias tentativas de login para o usuário root, culminando em um acesso bem-sucedido.

Atividades Realizadas: Após a autenticação, uma sessão sudo foi aberta, mas sem registros dos comandos executados, não é possível avaliar completamente o impacto.

IP do Invasor: O IP do invasor (ou potencial invasor) é 192.168.1.105.

4. Recomendações de Segurança

1. **Desabilitar o Acesso SSH ao Root:** Impedir que o usuário root faça login via SSH. Isso pode ser feito ajustando o arquivo de configuração SSH (/etc/ssh/sshd_config) para incluir PermitRootLogin no.
2. **Implementar Autenticação de Dois Fatores (2FA):** Reforçar a segurança dos logins SSH com autenticação de dois fatores para dificultar o acesso não autorizado.
3. **Monitoramento Contínuo:** Implementar ferramentas de monitoramento e alerta em tempo real para detectar tentativas de login suspeitas e atividades não autorizadas.
4. **Revisão de Permissões de Usuário:** Avaliar e restringir as permissões de usuários, garantindo que apenas os usuários necessários tenham acesso sudo.
5. **Auditoria de Logs:** Manter uma política de auditoria regular dos logs para identificar padrões de comportamento suspeitos e responder a incidentes rapidamente.
6. **Treinamento de Segurança:** Prover treinamento regular sobre práticas de segurança para os usuários e administradores do sistema.

Implementando essas recomendações, a empresa pode fortalecer sua postura de segurança e minimizar o risco de futuras intrusões.