Resumo do Relatório de Análise de Logs de Segurança

Visão Geral

Este relatório apresenta uma análise cronológica detalhada de uma série de atividades suspeitas detectadas em diversos logs de segurança. O ataque foi orquestrado a partir do IP `192.168.92.133` e envolveu várias etapas, incluindo escaneamento de portas, acesso FTP, tentativas de conexão SSH, invasão ao MariaDB e obtenção de privilégios de root, culminando no acesso a dados confidenciais.

Principais Eventos

1. **Escaneamento de Portas:** Reconhecimento inicial de serviços ativos, focando em portas comuns de serviços web e e-mail.
2. **Atividades no FTP:** Conexões anônimas bem-sucedidas e download de arquivos com credenciais sensíveis.
3. **Tentativas e Invasão bem-sucedida via SSH:** Múltiplas tentativas falhas seguidas por uma conexão bem-sucedida, indicando possível uso de credenciais obtidas via FTP.
4. **Atividades no MariaDB:** Acesso como usuário 'root' e execução de comandos para localizar informações sensíveis.
5. **Acesso Root Confirmado:** Uso do comando 'su' para obter privilégios de root, permitindo controle total sobre o sistema.
6. **Acesso a Dados Confidenciais:** Leitura de um arquivo confidencial no diretório root, representando uma séria violação de segurança.

Conclusões e Recomendações

Este ataque representa uma violação de segurança significativa, demonstrando a capacidade do atacante de explorar várias vulnerabilidades. Recomendam-se medidas imediatas de resposta a incidentes, incluindo a revisão de políticas de acesso, fortificação de medidas de segurança em servidores FTP e SSH, atualizações de segurança no MariaDB, e uma análise forense detalhada para avaliar o impacto completo do ataque e prevenir incidentes futuros.

Análise Detalhada

Passo 1 - Escaneamento de Portas Detectado nos Logs do iptables

A análise dos logs do iptables revelou uma série de tentativas de escaneamento de portas realizadas pelo IP `192.168.92.133`. Estas tentativas foram registradas no dia *30 de Dezembro às 20:06:04* e se concentraram nas seguintes portas:

- **Porta 80 (HTTP):** Duas tentativas de conexão TCP na porta 80 foram detectadas. Estas conexões usaram o protocolo TCP com a flag SYN, indicando uma tentativa inicial de estabelecer uma conexão, um padrão comum em escaneamentos de portas.
- **Porta 443 (HTTPS):** De maneira similar à porta 80, duas tentativas na porta 443 foram identificadas. Isso sugere um interesse do atacante em identificar serviços web seguros ativos.
- **Porta 8080 (HTTP Alternativo):** Novamente, duas tentativas de conexão na porta 8080 foram registradas, indicando a busca por serviços web configurados em portas alternativas.
- **Porta 995 (POP3S):** Duas tentativas na porta 995 apontam para um possível interesse em serviços de e-mail seguros via POP3.
- **Porta 143 (IMAP):** Foram feitas duas tentativas na porta 143, o que pode indicar uma busca por serviços de e-mail via IMAP.
- **Porta 25 (SMTP):** Duas tentativas na porta 25 foram registradas, demonstrando interesse em serviços de envio de e-mail.

Cada tentativa de conexão apresentou as mesmas características: tráfego de entrada (*IN=eth0*), sem tráfego de saída (*OUT=*), e endereço MAC de origem (*SRC=192.168.92.133*). Todos os pacotes tinham tamanho de 60 bytes, TOS (Type of Service) de 0x00, e um TTL (Time To Live) de 64, com a flag SYN ativada.

Interpretação e Relevância

Este padrão de escaneamento de portas é indicativo de uma tentativa inicial de reconhecimento por parte do atacante. O foco em portas comuns para serviços web (80, 443, 8080), serviços de e-mail (995, 143, 25), e a repetição das tentativas, sugere um esforço sistemático para mapear os serviços disponíveis no sistema alvo.

A escolha dessas portas específicas e a metodologia empregada indicam um possível uso de ferramentas automatizadas de escaneamento de portas, como Nmap ou similares. Este tipo de atividade é geralmente o primeiro passo em um ataque mais amplo, onde o atacante busca identificar pontos de entrada potenciais e serviços vulneráveis.

Recomendações Iniciais de Segurança

Com base nesta análise, recomenda-se:

- Implementar um sistema de detecção de intrusão (IDS) para identificar e alertar sobre tais atividades de reconhecimento no futuro.
- Realizar uma revisão e fortificação das configurações de segurança em todas as portas identificadas, assegurando que apenas os serviços necessários estejam acessíveis e devidamente protegidos.
- Monitorar continuamente os logs do iptables e outros sistemas de segurança para detectar tentativas similares de reconhecimento ou ataque.

Passo 2 - Atividades Suspeitas no Servidor FTP

A análise dos logs do servidor FTP revelou atividades significativas e suspeitas originadas do mesmo IP `192.168.92.133`, detectado anteriormente no escaneamento de portas. As atividades no FTP ocorreram logo após o escaneamento, em *30 de Dezembro, começando às 20:59:57*. Os eventos chave incluem:

- **Múltiplas Conexões:** Foram registradas várias tentativas de conexão ao servidor FTP pelo IP suspeito, indicando uma tentativa persistente de estabelecer uma conexão.
- **Logins Anônimos bem-sucedidos:** O atacante conseguiu fazer login no servidor FTP como usuário anônimo repetidas vezes, usando o endereço de e-mail "IEUser@" como senha. Isto sugere que o servidor FTP estava configurado para permitir acessos anônimos, uma vulnerabilidade significativa.
- **Download de Arquivos Sensíveis:** Em *21:00:18 e 21:00:22*, o atacante realizou o download de dois arquivos, `credentials_DB.txt` e `credentials_SSH.txt`, que pelo nome, indicam conter informações de credenciais. Esta ação é um forte indicativo de acesso não autorizado a dados sensíveis.

Interpretação e Relevância

Essas atividades no servidor FTP são críticas pois indicam não apenas a exploração bem-sucedida de uma vulnerabilidade (acesso FTP anônimo), mas também a obtenção de informações potencialmente sensíveis. O fato de o atacante ter direcionado o download para arquivos específicos sugere um conhecimento prévio ou uma pesquisa direcionada de informações valiosas armazenadas no servidor.

Recomendações de Segurança para o Servidor FTP

Diante dessas descobertas, as seguintes medidas de segurança são recomendadas:

- **Desativar Acesso Anônimo:** Remover a permissão de acesso anônimo ao servidor FTP, exigindo autenticação de todos os usuários.
- **Revisão dos Arquivos Hospedados:** Verificar todos os arquivos disponíveis no servidor FTP, removendo ou protegendo dados sensíveis que não devem ser acessíveis publicamente.
- **Monitoramento e Auditoria:** Implementar um sistema de monitoramento robusto para detectar acessos suspeitos e atividades anômalas no servidor FTP. Além disso, realizar auditorias regulares nos logs para identificar tentativas de acesso e possíveis vulnerabilidades.
- **Atualização e Fortificação de Segurança:** Atualizar o software do servidor FTP para a versão mais recente, aplicando todas as correções e fortificações de segurança disponíveis.
- **Treinamento e Conscientização:** Realizar treinamentos com a equipe de TI para conscientizar sobre as melhores práticas de segurança, especialmente no que diz respeito à configuração e manutenção de servidores FTP.

Passo 3 - Tentativas e Invasão bem-sucedida via SSH

A análise dos logs de SSH revela uma série de eventos críticos que ocorreram imediatamente após as atividades no servidor FTP. Estes eventos, originados do mesmo IP `192.168.92.133`, incluem tentativas de acesso e uma invasão bem-sucedida ao sistema via SSH.

1. **Tentativas de Acesso SSH:** Entre *20:59:57 e 20:59:58*, o atacante tentou múltiplas conexões SSH. Estas tentativas envolveram diferentes tipos de chaves de host, incluindo ssh-dss, ssh-rsa, ecdsa-sha2-nistp384, e ecdsa-sha2-nistp521. Várias dessas tentativas falharam devido à "não correspondência do tipo de chave de host", sugerindo tentativas de exploração de vulnerabilidades ou uso de várias credenciais obtidas.

2. **Invasão bem-sucedida via SSH:** Em *21:00:51*, ocorreu uma invasão bem-sucedida ao SSH. O atacante conseguiu fazer login com o usuário "target", indicando o uso de credenciais válidas. A presença de uma conexão bem-sucedida logo após as tentativas fracassadas sugere que o atacante pode ter obtido as credenciais corretas, possivelmente das informações baixadas anteriormente do servidor FTP.

Interpretação e Relevância

A sequência de tentativas fracassadas seguidas por um acesso bem-sucedido é preocupante, pois indica que o atacante estava experimentando diferentes abordagens até conseguir o acesso. O sucesso final sugere que o atacante obteve acesso a credenciais válidas, o que representa uma grave falha de segurança.

Recomendações de Segurança para o SSH

Com base nessa análise, as seguintes medidas de segurança são recomendadas:

- **Alteração de Credenciais:** Imediatamente alterar todas as senhas e chaves SSH, especialmente para contas com elevados privilégios.

- **Revisão das Políticas de Segurança SSH:** Implementar políticas rigorosas para o uso de SSH, incluindo chaves fortes e restrição de tipos de chave permitidos.

- **Autenticação de Dois Fatores:** Considerar a implementação de autenticação de dois fatores para o acesso SSH, adicionando uma camada extra de segurança.

- **Monitoramento e Auditoria:** Intensificar o monitoramento e a auditoria dos logs SSH para detectar tentativas de acesso não autorizado e padrões suspeitos de atividade.

- **Treinamento de Conscientização de Segurança:** Promover treinamentos regulares para a equipe de TI, enfatizando a importância de práticas de segurança fortes no uso e gerenciamento do SSH.

Passo 4 - Atividades Suspeitas no MariaDB

Após as ações bem-sucedidas no servidor FTP e no SSH, a análise dos logs do MariaDB indica uma série de operações suspeitas realizadas pelo atacante. Estas atividades foram registradas imediatamente após o acesso ao SSH, começando em *21:01:01* do dia *30 de Dezembro*. Os principais eventos incluem:

- **Conexão Inicial:** O atacante estabeleceu uma conexão com o MariaDB como usuário 'root', indicando um alto nível de acesso.
- **Comandos Executados:** Foram realizadas várias operações, incluindo `select @@version_comment` para verificar a versão do banco de dados, `show databases` para listar todos os bancos de dados disponíveis, e `SELECT DATABASE()` para identificar o banco de dados ativo.
- **Foco em Dados Específicos:** O atacante executou comandos para listar e acessar tabelas específicas, como visto no comando `show tables` e na consulta `select * from important_change_password`, indicando uma busca direcionada por informações sensíveis ou críticas.

Interpretação e Relevância

A habilidade do atacante de acessar o MariaDB como usuário 'root' é extremamente preocupante, pois sugere um controle quase total sobre o banco de dados. A execução de comandos específicos para localizar e acessar dados sensíveis indica um conhecimento prévio ou um objetivo claro, potencialmente visando roubo de dados ou manipulação de informações críticas.

Recomendações de Segurança para o MariaDB

Diante desses achados, as seguintes medidas são urgentemente recomendadas:

- **Alteração de Credenciais e Privilégios:** Mudar imediatamente as senhas de todos os usuários do banco de dados, especialmente do usuário 'root'. Além disso, revisar e restringir os privilégios dos usuários para limitar o acesso apenas ao necessário.
- **Análise de Integridade dos Dados:** Realizar uma auditoria completa para verificar se houve alteração, exclusão ou roubo de dados sensíveis.
- **Implementação de Controles de Acesso Mais Rígidos:** Reforçar as políticas de controle de acesso ao banco de dados, incluindo autenticação multifatorial e limitações nas conexões remotas.
- **Monitoramento e Auditoria Contínua:** Estabelecer um sistema de monitoramento contínuo para detectar atividades anômalas e acessos não autorizados ao MariaDB.
- **Atualização e Patches de Segurança:** Garantir que o MariaDB esteja atualizado com as últimas versões e patches de segurança aplicados para corrigir quaisquer vulnerabilidades conhecidas.

Passo 5 - Acesso Root Identificado nos Logs de Auditoria

A análise dos logs de auditoria revela um evento crítico de segurança: o atacante conseguiu obter privilégios de root no sistema. Este evento ocorreu em *30 de Dezembro às 21:01:34*, logo após as atividades suspeitas no MariaDB. Detalhes relevantes incluem:

- **Uso do Comando 'su':** O log registra o uso do comando `su`, que é utilizado para mudar a identidade do usuário, neste caso, para o usuário root. Isso é indicado pela linha `type=PROCTITLE msg=audit(1703980894.518:1302): proctitle="su"`.
- **Execução bem-sucedida:** O log mostra que o comando foi executado com sucesso, alterando a identidade do usuário para root. Isso é evidenciado pelo `exit=0` na linha de `type=SYSCALL`.
- **Rastreamento do Caminho de Execução:** Os logs detalham os caminhos dos arquivos executáveis e bibliotecas envolvidas, como visto nas linhas `type=PATH`.
- **Contexto da Execução:** O diretório atual (*cwd*) registrado é `"/home/target"`, indicando o local a partir do qual o comando 'su' foi executado.

Interpretação e Relevância

A obtenção de privilégios de root é um marco crítico em um ataque, pois dá ao invasor controle total sobre o sistema. Este acesso permite ao atacante realizar quase qualquer ação no sistema, desde a manipulação de dados até a instalação de backdoors e softwares maliciosos.

Recomendações de Resposta a Incidentes de Segurança

Considerando a gravidade deste acesso root, as seguintes ações de resposta a incidentes são urgentemente recomendadas:

- **Isolamento e Análise Forense:** Imediatamente isolar a máquina afetada da rede para prevenir a propagação do ataque ou vazamento de dados. Iniciar uma análise forense para entender completamente o escopo do incidente.
- **Revisão de Privilégios e Políticas de Senha:** Revisar as políticas de privilégios e senhas, especialmente para contas com acesso root, para garantir que apenas usuários autorizados possam obter tais privilégios.
- **Monitoramento Intensificado:** Aumentar o monitoramento em todos os sistemas para detectar quaisquer atividades suspeitas que possam indicar ações do invasor com privilégios de root.
- **Revisão e Correção de Vulnerabilidades:** Realizar uma revisão abrangente de segurança em todo o sistema para identificar e corrigir quaisquer vulnerabilidades que possam ter sido exploradas para obter acesso root.
- **Plano de Recuperação e Resiliência:** Desenvolver e implementar um plano de recuperação para restaurar os sistemas afetados e reforçar a resiliência contra ataques futuros.

Passo 6 - Acesso a Arquivo Confidencial Confirmado nos Logs de Auditoria

A análise final dos logs de auditoria revelou um acesso não autorizado a um arquivo altamente confidencial. Este evento ocorreu em *30 de Dezembro às 21:01:43*, imediatamente após a confirmação do acesso root pelo atacante. Os detalhes chave incluem:

- **Acesso ao Arquivo `important_data.txt`:** O log mostra que o arquivo `important_data.txt` foi acessado. Este arquivo, localizado no diretório root, é marcado como altamente confidencial.
- **Uso do Comando 'cat':** O atacante utilizou o comando `cat` para ler o conteúdo do arquivo, conforme indicado pelo `type=PROCTITLE` e `type=EXECVE` nos logs.
- **Contexto de Execução:** O diretório atual (*cwd*) registrado como `"/root"` confirma que o atacante estava operando no diretório root, com plenos privilégios.
- **Registro Detalhado da Atividade:** Os logs fornecem informações detalhadas sobre o caminho do arquivo, permissões, e a execução bem-sucedida do comando, evidenciando o acesso não autorizado.

Interpretação e Relevância

O acesso a um arquivo confidencial no diretório root por um atacante não autorizado é uma indicação clara de uma violação de segurança grave. Este acesso permite ao atacante obter informações sensíveis, que podem ser usadas para fins maliciosos ou vazadas, causando danos significativos à organização.

Recomendações de Resposta a Incidentes de Segurança

Diante deste acesso não autorizado a dados confidenciais, as seguintes ações de resposta a incidentes são recomendadas:

- **Avaliação Imediata do Impacto:** Determinar a natureza das informações acessadas e avaliar o potencial impacto da violação de dados.
- **Notificação e Conformidade Legal:** Se necessário, notificar as autoridades e partes afetadas de acordo com as leis e regulamentações de proteção de dados.
- **Medidas de Contenção e Remediação:** Implementar medidas imediatas para conter a violação e prevenir acessos futuros a dados confidenciais.
- **Reforço de Políticas de Segurança de Dados:** Revisar e fortalecer as políticas e práticas de segurança de dados, incluindo a criptografia de arquivos confidenciais e a implementação de controles de acesso mais rigorosos.
- **Revisão de Acessos e Permissões:** Realizar uma auditoria completa nos acessos e permissões do sistema para garantir que apenas usuários autorizados tenham acesso a informações confidenciais.