Autenticação em servidores de *e-mail* para envio de alertas de um sistema de detecção de intrusão baseado em *host*

Juliano Schneider dos Santos, Jeferson Campos Nobre
Universidade do Vale do Rio do Sinos (UNISINOS)
juliano.schs@gmail.com, jcnobre@unisinos.br

***Resumo*—A informação, por sua importância e valor, exige proteção adequada para evitar que sua integridade, disponibilidade e confiabilidade sejam afetadas. Uma das ferramentas utilizadas para essa proteção é o sistema de detecção de intrusão. Esse sistema possui características como o envio de alertas para endereços de correio eletrônico possibilitando que providencias sejam tomadas pelos administradores de segurança. O trabalho propõe a implementação de autenticação em servidores de *e-mail* para evitar que mensagens de alertas sejam rotuladas como *spam* e consequentemente descartadas antes de chegar a esses administradores.**

I. Introdução

Informações precisam ser protegidas pois possuem valor agregado. Boa parte das informações estão armazenadas em computadores e a proteção dos dados contidos nestas máquinas é uma constante preocupação de usuários finais e empresas de um modo geral. Existe consenso em reconhecer que a informação é uma peça chave para continuidade e até melhoria dos seus negócios. Tal reconhecimento torna-se mais evidente através da afirmação, apresentada na norma NBR ISO/IEC 17799:2005 [1], de que a informação é um ativo essencial e para tanto necessita ser adequadamente protegida.

Uma das ferramentas que auxilia na proteção das informações é o sistema de detecção de intrusão (*Intrusion Detection System - IDS*). Tal ferramenta possui várias características para manter a segurança da informação. Uma das características é o envio de alertas através de mensagens de *e-mail*. Em uma tentativa não autorizada de acesso a um sistema ou rede de computadores, o IDS gera alertas que podem ser enviadas através de mensagens de *e-mail*. Estas mensagens podem ser descartadas ou bloqueadas pelo servidor de correio eletrônico e consequentemente o administrador de segurança pode não tomar conhecimento do evento gerado. A utilização de técnicas anti-*spam* pelos servidores é uma das possíveis causas do descarte das mensagens.

É de extrema relevância que o detentor da informação seja notificado caso ocorra um evento, principalmente quando ocorrer risco de perda ou furto de dados. A notificação de um evento possibilita a tomada de decisões que visem evitar tais riscos. O alerta deve ser efetivo, ou seja, a mensagem de correio eletrônico deve chegar ao destinatário. Existem alternativas que garantem a entrega de mensagens, porém as mesmas possuem algumas desvantagens, por exemplo, necessidades adicionais de recursos computacionais.

O trabalho tem como principais contribuições: agregar autenticação em servidores de *e-mail* ao IDS e além disso, disponibilizar a proposta de maneira que possa ser estudada, melhorada e utilizada por aqueles que possuem interesse.

O presente artigo apresenta o processo realizado e o resultado alcançado com a implementação da proposta de solução para autenticação em servidores de correio eletrônico. O restante do artigo está organizado da seguinte forma: A seção 2 abrange conceitos a repeito de correio eletrônico e IDS; a seção 3 descreve o problema do envio de mensagens de alerta através de *e-mail*; na seção 4 encontra-se a descrição da implementação e a seção 5 encerra o artigo com apresentação da conclusão.

II. Fundamentação teórica

Esta seção apresenta conceitos a respeito de correio eletrônico, sistema de detecção de intrusão e sobre o IDS OSSEC HIDS. Inicialmente o conteúdo abrange os documentos que compõem e especificam os protocolos do correio eletrônico. Em seguida o assunto sobre sistema de detecção de intrusão aborda suas classificações e estratégias utilizadas para monitoramento de eventos. As principais características do OSSEC e as topologias que podem ser utilizadas servirão para apresentar o sistema de detecção utilizado para a implementação e testes da autenticação em servidores de correio eletrônico.

A. Correio Eletrônico

Correio eletrônico ou *e-mail*, como normalmente é conhecido, é uma forma de comunicação largamente utilizada, tanto em ambientes corporativos quanto em ambientes domésticos. Sua grande aceitação deve-se a simplicidade de uso e em muitos casos a sua informalidade.

Inicialmente o correio eletrônico foi apresentado através de duas propostas publicadas como RFC 821 [2] e RFC 822 [3]. O RFC 821 especifica o protocolo de transmissão e o RFC 822 especifica o formato das mensagens. Cada RFC possui revisões que culminaram nos RFC 5321 [4] e 5322 [5]. O protocolo de transmissão especificado pelo RFC 5321 é conhecido como *Simple Mail Transfer Protocol* (SMTP).

Além dos RFCs citados, o protocolo SMTP possui extensões que complementam sua funcionalidade. Duas destas extensões estão especificadas no RFC 4954 (*SMTP Service Extension for Authentication*) [6] e no RFC 3207 (*SMTP Service Extension for Secure SMTP over Transport Layer Security*) [7]. A RFC 4954 define uma extensão ao protocolo que permite ao cliente SMTP indicar um

mecanismo de autenticação ao servidor, executar a autenticação e opcionalmente negociar uma camada de segurança para uma sessão estabelecida. A RFC 3207 especifica uma extensão que permite proteger a comunicação entre servidor e cliente utilizando o *Transport Layer Security* (TLS).

B. Sistema de detecção de intrusão

Detecção de intrusão pode ser definido como o processo de monitorar eventos em um sistema ou em uma rede de computadores, analisá-los a procura de ameaças ou mesmo possíveis violações de políticas de segurança. Sistema de detecção de intrusão (*Intrusion Detection System* - IDS) é um *software* que automatiza o processo de detecção de intrusão e possui características como: identificar possíveis incidentes; capturar informações sobre eventos e armazená-las; tentar impedir intrusões; reportar ocorrências ao administrador de segurança.

Um sistema de detecção de intrusão pode possuir várias metodologias ou técnicas de descobrir e analisar eventos. As principais metodologias são: a) detecções baseadas em assinatura; b) detecções baseadas em anomalia; c) detecções baseadas na análise de protocolo. Dentre as abrangências do sistema de detecção de intrusão destacam-se duas classificações principais: sistema de detecção baseado em rede (*Network-based Intrusion Detection System* - NIDS) e o sistema de detecção baseado em *host* (*Host-based Intrusion Detection System* - HIDS).

Um NIDS monitora o tráfego de um ou mais segmentos de rede utilizando uma interface de rede diretamente conectada a eles. Levando em consideração fatores como localização do IDS e arquitetura de rede utilizada, implementações de NIDS podem usar métodos distintos para monitoramento do tráfego de rede [8].

O HIDS pode ser configurado para verificar acessos e modificações em arquivos de um sistema, analisar arquivos de *logs*, processos em execução, além de poder monitorar tráfego de rede. Todas estas atividades são realizadas no computador em que o HIDS encontra-se instalado.

C. OSSEC

OSSEC HIDS (***O**pen **S**ource **Sec**urity Host-based Intrusion Detection*) [9] é um IDS baseado em *host* desenvolvido por Daniel Cid, criador e principal mantenedor do projeto. O OSSEC possui várias características, tais como: a) multiplataforma; b) checagem de integridade de arquivos; c) análise de arquivos de *log*; d) detecção de *rootkits*; e) geração e envio de alertas.

O código fonte do OSSEC está sob os termos da licença *GNU General Public License* (GNU/GPL), consequentemente não há restrições quanto a modificações e melhorias em seu código, característica fundamental para o desenvolvimento do presente trabalho.

Existem três tipos de topologias utilizadas pelo OSSEC:

- **instalação do tipo local**: A instalação do tipo local é uma instalação utilizada para proteger um único *host*;
- **instalação do tipo agente**: A instalação do tipo agente é empregada quando existe a necessidade de centralizar informações de vários *hosts* localizados em uma rede de computadores. Cada *host* envia alertas para um servidor OSSEC centralizador, o qual é responsável pelo armazenamento de tais informações;
- **instalação do tipo servidor**: A instalação do tipo servidor tem como objetivo principal receber mensagens de alertas de todos os agentes, armazenando-as e executando medidas necessárias dependendo do tipo de alerta.

Um recurso importante utilizado pelo OSSEC é a capacidade de gerar alertas de incidentes e enviar a notificação destes para um endereço de *e-mail*. No momento em que é instalado, o OSSEC solicita um endereço de correio eletrônico e apresenta o servidor de SMTP a ser utilizado. Contudo, a abordagem de tão somente utilizar a configuração informada pelo usuário mostra-se ineficaz nos casos em que o servidor SMTP exige autenticação ou possui técnicas anti-*spam*.

III. Problema no envio de alertas por *e-mail*

Mensagens de *e-mail* pode ser descartadas devido a técnicas anti-*spam* empregadas por servidores SMTP [10]. Existem várias técnicas para realizar o bloqueio de *spam*, como por exemplo: a) o bloqueio de endereços de correio eletrônico com domínios inexistentes; b) utilização do padrão *Sender Policy Framework* (SPF), que restringe endereços de remetente à uma fonte específica; c) utilização da técnica denominada *Sender Verification Callout* (SVC) que verifica o endereço completo do remetente através da validação do nome de domínio e também o nome do usuário.

Testes simularam o envio de alertas entre o IDS o servidor de correio eletrônico com o intuito de identificar o problema e recolher informações para subsidiar a construção de uma solução. Nestes experimentos as técnicas anti-*spam* dos servidores SMTP testados revelaram-se efetivas pois bloquearam as mensagens de *e-mail* contendo alertas gerados pelo OSSEC. O cenário utilizado nos testes consiste de uma arquitetura de rede simples, composta por dois computadores em uma rede privada que comunicam-se com a Internet através de um roteador. A rede externa é composta por um servidor de correio eletrônico e um usuário conectado a ele. Este usuário representa o administrador de segurança que deve receber notificações do OSSEC instalado nas máquinas da rede interna. A figura 1 ilustra o cenário utilizado nos experimentos práticos e sinaliza o problema abordado, ou seja, as mensagens contendo alertas que não chegam ao destinatário.

Os detalhes do insucesso do envio de mensagens de *e-mail* foram obtidos com a ajuda do *software* Mailsend. Testes simularam o envio de mensagens para os mesmos endereços de correio eletrônico utilizados na configuração do OSSEC. O Mailsend pode ser executado em modo "*verbose*" possibilitando o detalhamento das trocas de mensagens entre o remetente do *e-mail* (cliente) e o destinatário do *e-mail* (servidor). Na análise de tais mensagens concluiu-se necessário três requisitos para a efetiva entrega do alerta ao destinatário:

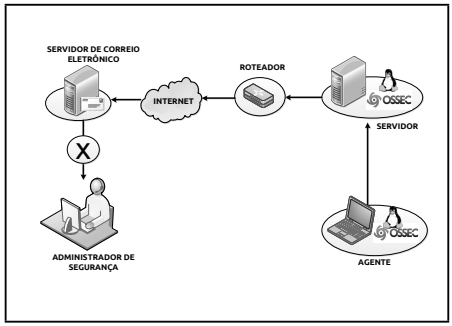

Figura 1. Arquitetura de rede dos experimentos práticos

- **identificação do remetente**: faz-se necessário que o remetente autentique-se no servidor SMTP. Sendo assim, o remetente necessita fornecer nome de usuário e senha válidos para o servidor.
- **camada de segurança**: alguns servidores de correio eletrônico exigem que se estabeleça uma camada de segurança utilizando o protocolo TLS, e somente após estabelecida tal camada efetua-se a autenticação e envio da mensagem de *e-mail*
- **endereço de remetente válido**: certos servidores utilizam métodos auxiliares de validação fazendo com o endereço do remetente seja analisado mesmo após a autenticação ter sido bem sucedida.

Para efetivar a entrega de mensagens de *e-mail* contendo alertas, faz-se necessário um *software* específico que atenda aos requisitos necessários para tal. Estes requisitos referem-se a atender essencialmente as especificações contidas nos RFCs 5321, 4954 e 3207, já mencionados anteriormente.

Uma possibilidade para solucionar a autenticação das mensagens é o *software* Postfix. Com o Postfix é possível envio de mensagens atendendo os requisitos necessários para efetivar a entrega dos alertas.

No cenário de testes pode-se acompanhar a entrega de uma alerta ao administrador de segurança. A rede interna é composta por dois *hosts*. Um deles contém a instalação do tipo agente do OSSEC. O outro *host* contém a instalação do tipo servidor do OSSEC e também o *software* Postfix. A entrega do alerta acontece da seguinte forma: a) um evento é detectado pelo OSSEC, podendo ter sido um evento no agente ou no próprio servidor; b) OSSEC servidor processa o evento e gera um alerta que deve ser enviado por *e-mail*; c) OSSEC servidor envia a mensagem para o Postfix, neste caso no mesmo computador; d) Postfix recebe a mensagem e repassa para o servidor SMTP externo, procedendo com a autenticação e com utilização de uma camada de segurança caso necessário.

Um *software* responsável somente pelo repasse de mensagens faz com que novos fatores sejam considerados na implementação de um IDS. Um fator a ser considerado é que mais um serviço passa a fazer parte da infraestrutura da rede, ou seja, mais um serviço deve ser monitorado, atualizado e mantido de forma a não se transformar em um risco de segurança. A demanda por recursos de hardware (memória, espaço em disco, consumo de processamento) que o serviço venha a demandar é o outro fator a ser considerado na implementação.

A configuração de um software como o Postfix, agindo como um servidor de *e-mail* para repasse de mensagens ou alertas não resolve satisfatoriamente o problema já que torna-se um recurso externo ao IDS e que deve ser monitorado. A funcionalidade de autenticação através do próprio HIDS elimina a utilização de recursos intermediários para repasse de alertas, criando desta maneira um sistema de detecção com maior autonomia, ou seja, um sistema que pode manter suas características de funcionamento sem a ação de agentes externos.

IV. Implementação

O Mailsend, além de auxiliar nos testes e experimentos práticos, serviu de fonte para implementação da solução, pois o software encontra-se sob a licença GNU General Public License (GNU/GPL). Tanto o Mailsend quanto o OSSEC encontram-se sob a mesma licença, o que possibilita que seus códigos fonte sejam consultados, estudados e modificados livremente.

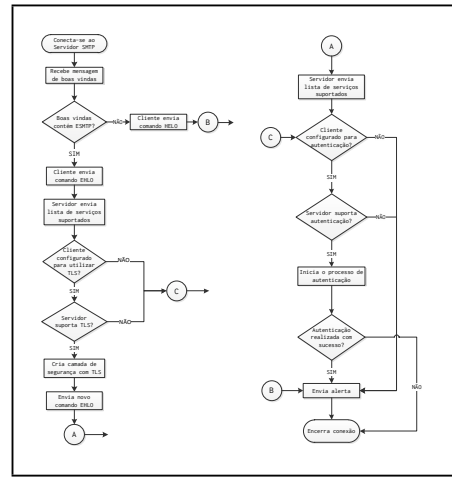

Figura 2. Arquitetura de rede após implementação da solução proposta

A modificação efetiva ocorreu no código fonte do OSSEC, permitindo que o próprio sistema de detecção de intrusão efetuasse a autenticação em servidores SMTP juntamente com a utilização de uma camada de segurança utilizando o protocolo TLS, caso fosse requisitado. A implementação está representada através de um fluxograma com os processos realizados entre o OSSEC e o servidor SMTP (vide figura 2).

O envio da mensagem de *e-mail* contendo alertas, representado pelo fluxograma, segue os seguintes passos:

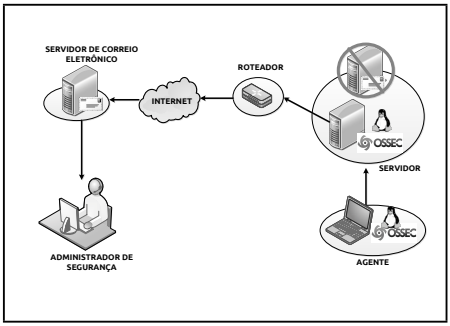

Figura 3. Arquitetura de rede após implementação da solução proposta

1) O IDS inicia uma conexão ao servidor SMTP;
2) O servidor SMTP responde ao IDS com a mensagem de boas-vindas;
3) O IDS analisa se a mensagem de boas-vindas possui o texto `ESMTP` e em caso positivo envia o comando `EHLO`, do contrário envia o comando `HELO`;
4) O servidor recebe o comando `EHLO` e responde com uma lista dos serviços suportados;
5) O IDS verifica se o servidor aceita o comando `STARTLS`. Caso positivo o IDS negocia a criação de uma camada de segurança;
6) Após criada a camada de segurança o IDS envia novo comando `EHLO`;
7) O servidor SMTP responde com nova lista de serviços suportados;
8) O IDS verifica se o servidor oferece a possibilidade de autenticação. Caso positivo inicia o processo de autenticação.
9) Se a autenticação é realizada com sucesso a mensagem de *e-mail* contendo alertas é enviada ao servidor e a conexão é encerrada.

O arquivo `sendmail.c` do OSSEC é o fonte que possui os códigos de envio dos alertas através de correio eletrônico. As principais modificações foram realizadas neste arquivo. Com as modificações realizadas, o processo de envio alertas por *e-mail* tem a possibilidade de ser configurado com a opção de autenticar-se ou não no servidor SMTP e com possibilidade de criar uma camada de segurança com TLS.

A figura 3 demonstra a implementação com os objetivos alcançados, ou seja, entrega de alertas ao administrador de segurança e eliminando a intervenção de agentes externos, no caso, um servidor de correio eletrônico somente para repasse das mensagens.

V. Conclusão

Servidores de correio eletrônicos possuem técnicas anti-*spam* com o intuito de evitar a disseminação do *spam*. Contudo, estas técnicas acabam bloqueando e descartando mensagens legítimas sem o conhecimento do destinatário. Do mesmo modo em que afeta mensagens consideradas legítimas, um sistema de detecção de intrusão que utiliza *e-mail* para alertar o administrador de segurança acaba diretamente prejudicado.

Para que o sistema de detecção seja efetivo seus alertas precisam ser efetivos, ou seja, é necessário que o destinatário receba a notificação. Técnicas anti-*spam* de servidores de correio eletrônico impedem a efetividade da ferramenta.Constatado o problema, testes foram realizados na busca de uma solução. Inicialmente utilizou-se uma solução que mostrou-se não ser a ideal, principalmente por fazer uso de um agente externo ao sistema de detecção de intrusão. Com o auxílio de *softwares* de código fonte aberto, implementar autenticação em servidores SMTP no próprio sistema de detecção mostrou-se a solução adequada para o problema.

Devido ao grande número de servidores de *e-mail* faz-se necessário que testes sejam realizados constantemente para que a implementação atinja de maneira satisfatória seu objetivo. Nos testes efetuados os resultados foram satisfatórios, no sentido em que obteve-se sucesso no envio dos alertas e consequente recebimento por parte dos destinatários. Garantir que o destinatário receba o alerta através de mensagens de *e-mail* confere maior confiabilidade e autonomia ao sistema de detecção de intrusão. Além de constantes realizações de testes, a inclusão do IDS na árvore de desenvolvimento de uma distribuição GNU/Linux, como o Debian, serviria para uma maior divulgação na comunidade de software livre.

Referências

[1] NBR-ISO/IEC, *ABNT NBR ISO/IEC 17799 – Tecnologia da informação – Técnicas de segurança – Código de prática para gestão de segurança da informação*, 2nd ed. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

[2] J. B. Postel, *Simple Mail Transfer Protocol*. IETF, RFC 821, 1982.

[3] D. H. Crocker, *Standard for the Format of ARPA Internet Text Messages*. IETF, RFC 822, 1982.

[4] J. C. Klensin, *Simple Mail Transfer Protocol*. IETF, RFC 5321, 2008.

[5] P. W. Resnick, *Internet Message Format*. IETF, RFC 5322, 2008.

[6] R. Siemborski and A. Melnikov, *SMTP Service Extension for Authentication*. IETF, RFC 4954, 2007.

[7] P. Hoffman, *SMTP Service Extension for Secure SMTP over Transport Layer Security*. IETF, RFC 3207, 2002.

[8] K. Scarfone and P. Mell, in *Guide to Intrusion Detection and Prevention Systems*. Gaithersburg, MD: National Institute of Standarts and Tecnology, 2007, special Publication 800-94.

[9] A. Hay, D. Cid, and R. Bray, *OSSEC Host-Based Intrusion Detection Guide*. Burlington: Syngress Publishing, Inc, 2008.

[10] T. R. Surmacz, in *Reliability of e-mail delivery in the era of spam*, IEEE Computer Society. 2nd International Conference on Dependability of Computer Systems, 2007, pp. 198–204.