FACULDADE DE TECNOLOGIA IBRATEC - UNIBRATEC

NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO

Segurança da Informação

MARCUS DIEGO DE OLIVEIRA CASTELO BRANCO

APT-SEC: FERRAMENTA PARA ADMINISTRAÇÃO DE ATUALIZAÇÕES DE PACOTES EM SISTEMAS DEBIAN GNU/LINUX

RECIFE

2017

MARCUS DIEGO DE OLIVEIRA CASTELO BRANCO

APT-SEC: FERRAMENTA PARA ADMINISTRAÇÃO DE ATUALIZAÇÕES DE PACOTES EM SISTEMAS DEBIAN GNU/LINUX

Trabalho de conclusão apresentado ao Núcleo de Pós-Graduação e Extensão da Faculdade de Tecnologia Ibratec como requisito para a obtenção do título de Especialista em segurança da informação.

Orientador: Prof. Dailson Fernandes

RECIFE

2017

Sumário

1 INTRODUÇÃO

Um dos grandes desafios dos administradores de ambientes GNU/Linux é a aplicação de atualizações críticas em ambientes de produção. Esta atividade exige maturidade e conhecimento para evitar que operações de atualização se tornem catástrofes, comprometendo ambientes e causando prejuízos. Um conjunto de boas práticas, utilizando processos alinhados e ferramentas podem auxiliar os gestores nesta árdua tarefa.

Neste artigo, será apresentada a ferramenta *apt-sec* cujo o objetivo é auxiliar os gestores na realização de atualização de *patches* de segurança em ambientes GNU/Linux Debian.

Dentre suas funcionalidades, o *apt-sec* pode auxiliar nas seguintes atividades:

1. Identificação de todas as atualizações disponíveis para o ambiente;
2. Identificação e instalação de atualizações que possuem *Common Vulnerabilities and Exposures* (CVE) associado;
3. Visualização/seleção de severidade da atualização e detalhamento do CVE;
4. Consulta sobre histórico de atualizações;
5. Realização de *rollback* de atualizações que podem ter comprometido ambiente;
6. Envio de *e-mail* para gestor comunicando sobre atualização relevante no ambiente.
7. Identificação de necessidade de reinicialização (*reboot*) de ambiente após atualização para aplicação de atualizações;

O *apt-sec* foi desenvolvido para automatizar algumas atividades de gestão de atualização de *patches*. Originalmente escrito em *bash script*, utiliza como base as próprias ferramentas das *suites apt, apt-get* e *aptitude* para criar um mecanismo que

permite a rastreabilidade de atualizações e identificar problemas de forma mais controlável e eficiente para os gestores.

O *apt-sec* pretende oferecer em modo texto, um suporte semelhante ao *yum history* presente em distribuições derivadas do *Redhat Entreprise Linux* (RHEL) que possui a funcionalidade de realização de *undo* e *redo* de ações utilizando o *yum*. Inicialmente o *apt-sec* pretende ser uma aplicação *standalone*, para gerenciamento de apenas o servidor local.

2 JUSTIFICATIVA

Equipes de segurança estão cada vez mais emprenhadas em identificar vulnerabilidades em sistemas e essa velocidade de identificação e liberação de atualizações são importantes para garantir a integridade, confidencialidade e disponibilidade de serviços. Por outro lado, a velocidade com que essas liberações são publicadas pode causar sérios problemas quando os testes não cobrem situações específicas. Os problemas se confirmam quando estas atualizações são inadvertidamente aplicadas em ambientes de produção.

Com a evolução desta problemática, processos foram amadurecidos para que a aplicação de *patchs* de atualização causassem menos impactos as organizações. Diversos *frameworks* como o ITIL propuseram a construção de uma gerência de mudança e dentre suas atividades, a elaboração de um mecanismo de restauração ao estado anterior de ambientes que sofrem as mudanças, comumente conhecido como *rollback*.

Atualmente as distribuições GNU/Linux estão bem servidas de ferramentas de gerenciamento de pacotes (*yum, dnf, apt, apt-get, apititude, zypper entre outros*) que fazem a verificação de pacotes instalados, desatualizados e auxiliam a instalação e atualização de pacotes e dependências, reduzindo significativamente o esforço manual. Um problema que foi solucionado com bastante praticidade pela equipe da Red Hat foi a necessidade de realização de *rollback* em atualizações que não foram bem sucedidas fazendo uso do recurso do *yum history.*

Outra característica importante é a apresentação de informações sobre os pacotes de forma semelhante ao *yum security* que permite identificar os pacotes por urgência/severidade da atualização dentre outras possibilidades de filtros.

3 OBJETIVOS

3.1 OBJETIVO GERAL

Apresentar ferramenta customizada que foi desenvolvida pelo autor para auxiliar as atividades de atualização de pacotes e oferecer mais recursos informativos para auxiliar o administrador na tomada de decisão.

3.2 OBJETIVOS ESPECÍFICOS

- Conceituar todo referencial teórico do trabalho;
- Conceituar a coletar informações da base de dados *UDD* do Debian para obtenção de informações sobre os pacotes que estão disponibilizadas;
- Conceituar e apresentar a concepção e modelagem do *apt-sec*, licenciamento e acesso para download do código fonte;
- Apresentar testes e resultados alcançados;

4 HIPÓTESES

- **Ferramenta oferece informação para tomada de decisão**.
  - Confirmar a capacidade de avaliação de atualização de pacotes que são críticos em sua proposta de correção
  - Confirmar a capacidade de rastreabilidade de atualizações;
- **Atualização seletiva de pacotes**
  - Confirmar a capacidade de atualização seletiva de pacotes com base em informação coletada sobre urgência/severidade e existência de CVEs associados
- **Aumento de produtividade na aplicação de *patchs* de atualização.**
  - Confirmar a capacidade de reversão (*rollback* de pacotes) ou sinalização para o administrador que determinada atualização não poderá ter seu *rollback* gerenciado pelo *apt-sec.*

5 METODOLOGIA

A pesquisa foi fundamentada em estudo de funcionalidades presentes nas ferramentas de gestão de pacotes existentes e presentes no Debian, de forma que fosse possível automatizar ações específicas que aumentam a produtividade e assertividade de ações de atualização segura de ambientes críticos.

Este estudo tem como base de comparação alguns comportamentos já existentes em ferramentas que não estão presentes no ambiente Debian, como as soluções propostas pelo *yum history* e *yum security,* presentes em distribuições baseadas em *Red Hat Enterprise Linux* (RHEL). O estudo pretende incorporar parte das funcionalidades presentes nas ferramentas citadas a ambientes Debian.

Como resultado deste trabalho de pesquisa foi desenvolvida uma ferramenta chamada *apt-sec* que serve como um *framework,* sendo esta produção disponibilizada para comunidade de software livre. A produção deste trabalho visa comprovação de melhoria de aspectos informativos, atualização seletiva e capacidade de resiliência de ambientes críticos com o aprimoramento de restauração.

As informações coletadas neste trabalho serão obtidas por meio de pesquisa bibliográfica discorrida no desenvolvimento do referencial teórico.

6 CRONOGRAMA

Atividades	Set 2017	Out 2017	Nov 2017	Dez 2017	Jan 2018	Fev 2018	Mar 2018	Abr 2018	Mai 2018
Pesquisa do tema.	☑								
Definição do tema.		☑							
Pesquisa bibliográfica.		☑	☑						
Desenvolvimento de ferramenta.			☑	☑					
Apresentação e discussão dos resultado obtidos.				☑	☑				
Elaboração do projeto.					☑	☑			
Entrega do projeto.						☑	☑		

REFERÊNCIAS

RHEL DEPLOYMENT GUIDE. **Working with Transaction History.** Disponível em: <https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sec-Yum-Transaction_History.html>. Acesso em 23 de setembro de 2017.

RHEL DEPLOYMENT GUIDE. **Yum security plugin.** Disponível em: <https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sec-Plugin_Descriptions.html>. Acesso em 23 de setembro de 2017.

EXIN. **ITIL.** Disponível em: <https://www.exin.com/br/pt/qualification-program/itilr >. Acesso em 23 de setembro de 2017.

https://access.redhat.com/solutions/10021

https://access.redhat.com/solutions/258973