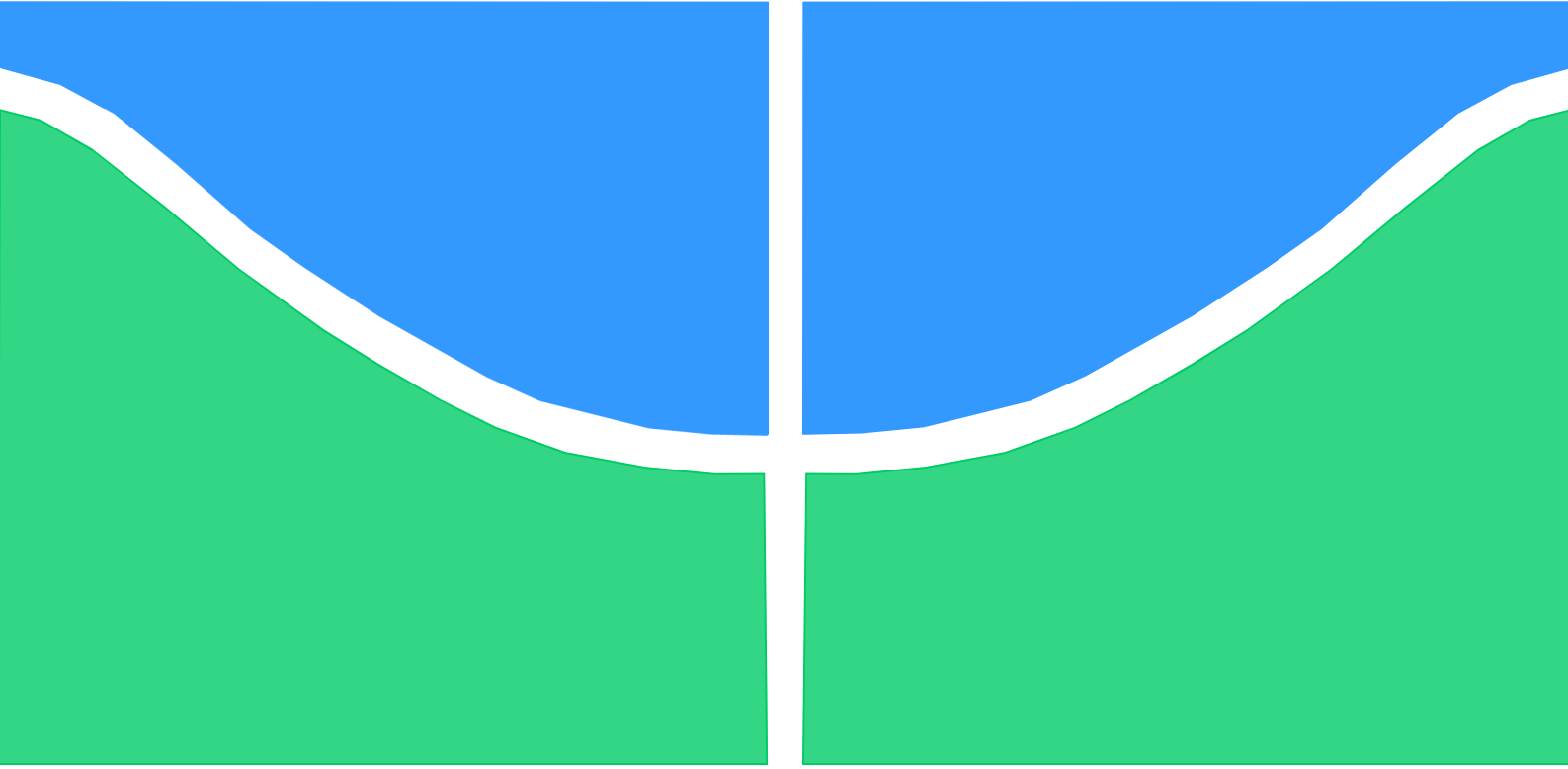

UMA SOLUÇÃO PARA GESTÃO DE VULNERABILIDADES DE SEGURANÇA DA INFORMAÇÃO

LUCAS VINICIUS ANDRADE FERREIRA

ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UMA SOLUÇÃO PARA GESTÃO DE VULNERABILIDADES DE SEGURANÇA DA INFORMAÇÃO

LUCAS VINICIUS ANDRADE FERREIRA

ORIENTADOR: LAERTE PEOTTA DE MELLO

ESPECIALIZAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

PUBLICAÇÃO:

BRASÍLIA, DF: 31 DE MAIO / 2017.

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

UMA SOLUÇÃO PARA GESTÃO DE VULNERABILIDADES DE SEGURANÇA DA INFORMAÇÃO

LUCAS VINICIUS ANDRADE FERREIRA

MONOGRAFIA SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS PARA OBTENÇÃO DO GRAU DE ESPECIALISTA EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO.

APROVADO POR:

_____
LAERTE PEOTTA DE MELO
DOUTOR (ORIENTADOR)

_____
NOME
GRAU

_____
NOME
GRAU

BRASÍLIA, DF, 31 DE MAIO DE 2017.

FICHA CATALOGRÁFICA

Ferreira, Lucas Vinicius Andrade.
Uma Solução para Gestão de Vulnerabilidades de Segurança da Informação [Distrito Federal], 2017.
xi, 43p., 210 x 297 mm (ENE/FT/UnB, Especialista, Engenharia Elétrica, 2017).
Monografia de Especialização – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Segurança da Informação
2. Gestão de Vulnerabilidades
3. Gestão de Ativos
4. Disponibilidade/Continuidade
I. ENE/FT/UnB
II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

Ferreira, Lucas Vinicius A. (2017). Uma Solução para Gestão de Vulnerabilidades de Segurança da Informação. Monografia de Especialização, publicação: UNB 2017. Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, (43)p.

CESSÃO DE DIREITOS

AUTOR: Lucas Vinicius Andrade Ferreira

TITULO DA DISSERTAÇÃO: Uma Solução para Gestão de Vulnerabilidades de Segurança da Informação

GRAU/ANO: Especialista/2017

_____

Lucas Vinicius Andrade Ferreira
QD 101 LT 05 APTO 1907 – Águas Claras
CEP: 71907-180 – Brasília/DF
Tel. +55 61 99918-5842 / lucas.vinicius@live.com

AGRADECIMENTOS

Primeiramente a Deus por ter me concedido toda a sabedoria, paciência, motivação e energia necessárias para concluir esta jornada.

A meu filho Pedro e minha esposa Juliana por entenderem minhas ausências, suportar minhas inúmeras atividades acadêmicas e também profissionais, as várias horas de estudos, mas, acima de tudo por acreditarem em mim e por sempre me incentivar a permanecer nesta longa caminhada que é minha carreira profissional.

Aos meus Pais Celso e Edina, por todo o amor, incentivo e carinho.

A direção e a coordenação do LabRedes e da renomada Universidade de Brasília por proporcionar toda a infraestrutura necessária.

Aos Doutores, mestres e professores do curso de Gestão de Segurança da Informação, em especial ao respeitado Professor Laerte Peotta, por sua dedicação e por compartilhar seu tempo, conhecimento e experiência orientando este trabalho.

Ao Banco do Brasil, instituição ao qual dedico mais de 6 anos da minha vida profissional, por apoiar, financiar e proporcionar a oportunidade de aprimorar meus conhecimentos através desta especialização.

RESUMO

UMA SOLUÇÃO PARA GESTÃO DE VULNERABILIDADES DE SEGURANÇA DA INFORMAÇÃO
Autor: Lucas Vinicius Andrade Ferreira
Orientador: Professor Dr. Laerte Peotta de Mello
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 31 de maio de 2017.

Em uma realidade em que o mundo está cada vez mais automatizado e conectado à internet, segurança da informação é uma área essencial para as organizações pois a exposição de dados sigilosos podem causar prejuízos financeiros e de imagem da empresa perante a sociedade. A gestão de segurança da informação já é uma realidade para as grandes organizações que investem muito dinheiro com políticas de segurança, planos de continuidade, combate a ataques cibernéticos, sistemas e dispositivos de segurança. Além disso, precisam manter toda essa estrutura funcionando e organizada. Porém, já é sabido que os ataques cibernéticos são procedentes basicamente da exploração de vulnerabilidades que indivíduos maliciosos têm conhecimento com o objetivo de obter alguma vantagem ou cometer algum ilícito. Estas vulnerabilidades podem ser em hardwares, softwares ou nas pessoas que não tomam devidas precauções com os ativos da empresa. Este trabalho faz um estudo profundo do tema de gestão de vulnerabilidades, explorando seus fundamentos, conceitos, características, procedimentos bem como técnicas e ferramentas que podem auxiliar as organizações de forma geral a efetuar uma eficiente gestão de vulnerabilidade. Além disso, ao final é realizada uma abordagem pratica que tem a finalidade de implantar um sistema que tenha a capacidade de percorrer todos as etapas da gestão de vulnerabilidades que possa efetuar varreduras, emitir relatórios, gerar gráficos e ainda realizar a abertura automatizada de bilhetes para o devido tratamento das vulnerabilidades encontradas.

ABSTRACT

A SOLUTION FOR THE MANAGEMENT OF INFORMATION SECURITY VULNERABILITIES
Author: Lucas Vinicius Andrade Ferreira
Supervisor: Professor Dr. Laerte Peotta de Mello
Programa de Pós-graduação em Engenharia Elétrica
Brasília, 31 de maio de 2017.

In a reality where the world is increasingly automated and connected to the internet, information security is an essential area for organizations because the exposure of sensitive data can cause financial losses and image of the company before society. Information security management is already a reality for large organizations that invest a lot of money with security policies, continuity plans, against cyber-attacks, systems, and security devices. In addition, they need to keep this whole structure up and running. However, it is already known that cyber-attacks are basically derived from exploiting vulnerabilities that malicious individuals are aware of in order to gain some advantage or commit some illicit. These vulnerabilities can be in hardware, software, or people who do not take proper precautions with company assets. This work makes a deep study of the topic of vulnerability management, exploring its fundamentals, concepts, characteristics, procedures as well as techniques and tools that can help organizations in general to perform an efficient vulnerability management. In addition, at the end of the day a practical approach is executed to implement a system that has the ability to go through all the steps of vulnerability management that can scan, issue reports, generate graphs, and perform automated ticket opening for the due treatment of the vulnerabilities are founded.

SUMÁRIO

LISTA DE TABELAS

LISTA DE ILUSTRAÇÕES

LISTA DE SIMBOLOS, NOMENCLATURA E ABREVIAÇÕES

ABNT	*Associação Brasileira de Normas Técnicas*
CERT	*Computer Emergency Response Team*
CERT.br	*Centro de Estudos, Respostas e Tratamento de Incidentes do Brasil*
CGI	*Common Gateway Interface*
CNA	*CVE Numbering Authority*
CVE	*Common Vulnerabilities and Exposures*
CVSS	*Common Vulnerability Scoring System*
FEBRABRAN	*Federação Brasileira de Bancos*
GPL	*General Public License*
ICMP	*Internet Control Message Protocol*
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Comission*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
ISO	*Internacional Organization for Standardization*
NBR	*Norma Brasileira Regulamentadora*
NVD	*Nacional Vulnerability Database*
RFC	*Requests for Comments*
RFID	*Radio Frequency Identification*
S.O	*Sistema Operacional*
SLA	*Service Level Agreement*
T.I	*Tecnologia da Informação*
SIEM	*Security Information and Event Management*

1 INTRODUÇÃO

Atualmente, a humanidade dispõe de inúmeros serviços via computadores, celulares e na internet. Serviços esses que até pouco tempo atrás eram inimagináveis. Seria difícil, por exemplo, imaginar ou garantir de alguma forma que, seria possível efetuar qualquer transação bancária em um computador ou celular. Operações como: verificar saldo ou extratos ou muito menos: transferências, pagamentos e recentemente deposito de cheques e envio de mensagens aos gerentes de contas diretamente pelo aplicativo do banco pareciam utópicos.

Mas tudo isso atualmente tornou-se comum. E os usuários estão cada dia mais ávidos por um aumento no valor no limite de transações financeiras via internet ou mobile banking, bem como pelo acesso a serviços exclusivos nestas plataforma e maiores comodidades para tornar mais raras a idas as agências bancarias ou até mesmo simplesmente exterminar essas visitas de vez. Conforme dados presentes na pesquisa FEBRABAN de tecnologia bancária de 2017, encomendada pela FEBRABAN à Deloitte Auditoria e Consultoria Empresarial:

Conforme a figura 1-1, o volume de transações via canais digitais quadruplicou nos últimos três anos e cresceram aproximadamente 27% em 2016, indo de 28,37 bilhões para 36,7 bilhões de transações bancarias no período. Com destaque para o canal *mobile banking* que acumulou uma alta de 96% em relação a 2015. Indo de 11,2 bilhões em 2015 para 21,9 bilhões de transações bancárias em 2016 superando assim o canal *internet banking*.

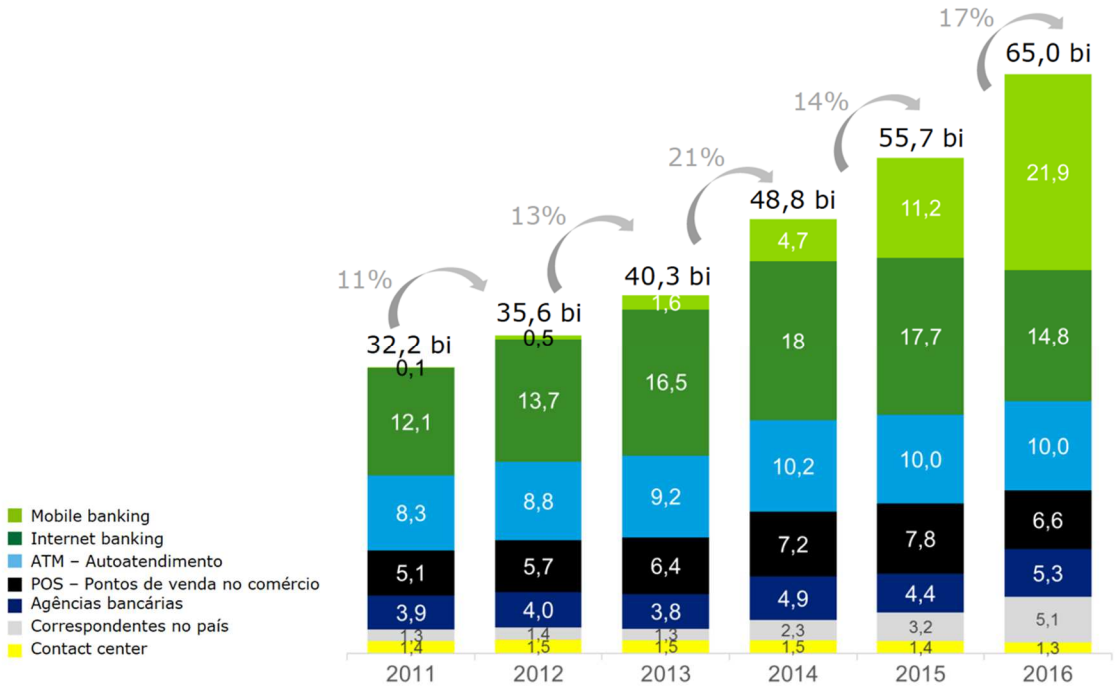

Figura 1-1 - Comparativo do volume de transações bancárias nos últimos seis anos

As transações realizadas via canais digitais (*Internet* e *mobile banking*) já representam mais da metade de todas as transações financeiras. Ainda de acordo com a mesma pesquisa, os investimentos em tecnologia continuarão com tendência de alta. Os dados e os números desta pesquisa são extremamente expressivos e comprovam a preferência dos clientes no uso de canais digitais.

A comodidade de usar dispositivos portáteis e pessoais para realizar transações financeiras é incontestável, porém, toda esta comodidade traz consigo muito desafios no que concerne a segurança da informação, a autenticidade, confiabilidade, integridade e disponibilidade dos dados das transações e principalmente dos dados pessoais, financeiro e bancários dos clientes. Consequentemente pesquisas e a implementação de dispositivos e ferramentas de segurança com o intuito de diminuir e principalmente acabar com as indisponibilidades ou exposição de seus serviços a exploração de terceiros mal-intencionados são indispensáveis pois tudo isso implica em prejuízos financeiros e de imagem. Mas somente a implantação destes dispositivos por si não garantem a segurança dos ativos de uma organização visto que existem vários pontos passiveis de exploração de vulnerabilidades de segurança tais como: pessoas, processos, serviços e etc...

A adoção de processos e uma gestão de segurança eficiente são aliados importantes para mitigar eventuais riscos de segurança, e dentro deste contexto a gestão de vulnerabilidades é uma ferramenta de controle interessante pois permite identificar rapidamente, classificar e priorizar quais ativos estão expostos e que devem ser corrigidos e quando devem corrigidos.

Os incidentes de segurança estão frequentemente relacionados a exploração de vulnerabilidades. O caso mais emblemático visto recentemente foi o caso do *ransomware* "*Wannacry*". Ele explorou uma vulnerabilidade em um sistema operacional popular e gerou prejuízos muito difíceis de serem calculados a vários hospitais, fábricas, órgãos públicos, entre outros.

Conforme pode ser verificado na figura 1-2, o número de vulnerabilidades divulgadas e catalogadas tiveram um crescimento significativo na última década, especialmente no ano corrente que não se encontra nem na metade ainda e já foram reportadas mais vulnerabilidades que todo o ano de 2013.

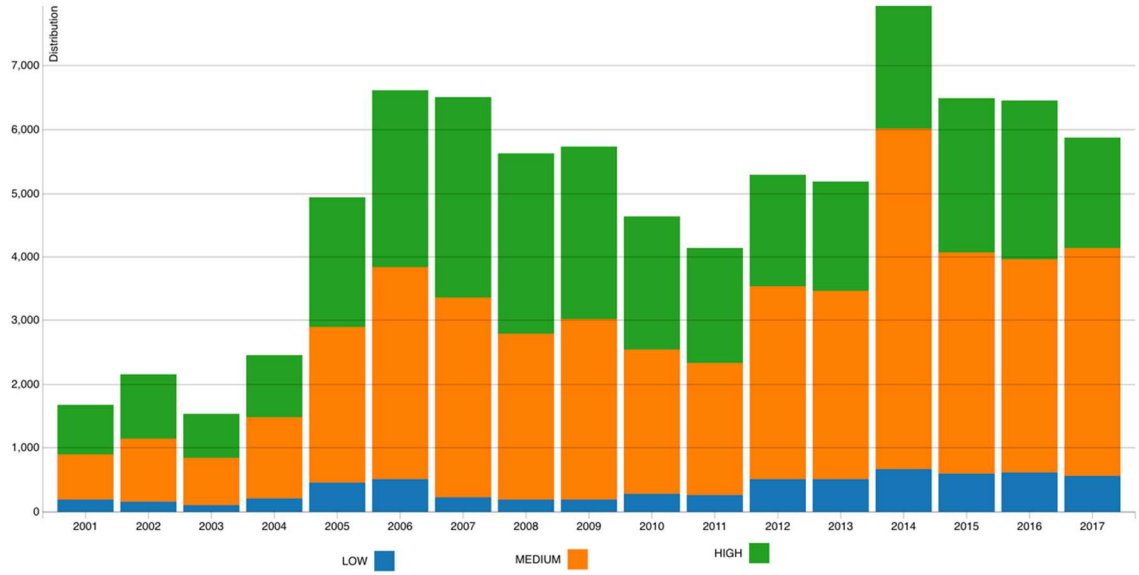

Figura 1-2 - Distribuição de vulnerabilidades por gravidade ao longo do tempo (NIST U.S, 2017)

1.1 OBJETIVOS

Este trabalho tem o objetivo de elaborar uma solução que integre ferramentas de monitoração de segurança com uma ferramenta de registro e controle de bilhetes para documentar, organizar e emitir relatórios sobre as vulnerabilidades.

1.2 OBJETIVOS ESPECÍFICOS

Os objetivos deste trabalho serão focados nas vulnerabilidades de segurança da informação e são respectivamente:

a. Discorrer sobre o tema de gerenciamento de vulnerabilidades de segurança da informação e suas relações com o negócio;
b. Analisar e propor processos no gerenciamento de vulnerabilidades de segurança da informação;
c. Analise dos alarmes gerados nas ferramentas de monitoração e nos dispositivos da rede;
d. Integração de ferramentas de monitoração com ferramentas de registros de vulnerabilidade;
e. Elaboração de matrizes de urgência x impacto para definir a gravidade das vulnerabilidades;
f. Registro automático de bilhetes em formulário padrão com todas informações pertinentes apontando inclusive a causa raiz.

1.3 JUSTIFICATIVA

Em face do crescente número de incidentes de segurança da informação e a sua complexidade, é consenso entre as instituições que se tratando de segurança da informação apenas uma boa gestão de incidentes de segurança não é suficiente para se garantir a confidencialidade, integridade e disponibilidade das informações em frente as ameaças.

Em consonância com a gestão de incidentes, uma gestão de vulnerabilidades eficaz e bem estruturada tem a capacidade de diminuir consideravelmente a exposição dos ativos de TI da empresa.

À vista disso, a implementação de uma ferramenta capaz de identificar com clareza a causa raiz, classificar com exatidão a exposição do ativo, registrar em um formulário todas as informações pertinentes e possivelmente efetuar uma investigação preliminar e sugerir ações corretivas para mitigação ou extinção da vulnerabilidade, colaboraria de forma muito efetiva no processo e pouparia tempo precioso do analista que poderia envolver-se mais no processo de análise de incidentes ou cuidando de outros processos referentes a gestão de segurança da informação.

1.4 ORGANIZAÇÃO DESTE TRABALHO

A fim de garantir um melhor entendimento dos objetivos e das propostas apresentadas neste trabalho, foi definida a seguinte organização:

No capítulo 2 serão apresentados os fundamentos e conceitos técnicos relacionados com o tema.

O capitulo 3 comtempla as referências teóricas que sustentarão o desenvolvimento pratico do trabalho.

No capítulo 4 além da aplicação dos conhecimentos apresentados no capítulo 2 e 3, será o modelo proposto de solução e serão efetuados os ensaios para a efetiva integração das ferramentas para a implementação da proposta de gestão de vulnerabilidades de segurança da informação.

E finalmente no capitulo 5 serão realizadas as análises críticas dos resultados obtidos bem como da eficiência dos procedimentos adotados na gestão de vulnerabilidades de segurança da informação e tem-se a conclusão do trabalho com os panoramas possíveis futuros bem como avaliações de performance e os possíveis ganhos obtidos nas instituições com a implementação da ferramenta.

2 FUNDAMENTOS E CONCEITOS

A segurança da informação tem como princípio básico a manutenção da confidencialidade, da integridade e da disponibilidade das informações, qualquer uma destas três propriedades não deve ser violada de maneira alguma. A segurança da informação, pode ser conceituada como a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre o investimento e as oportunidades de negócio. Ainda existe outras propriedades tão importantes quanto a confidencialidade, a integridade e a disponibilidade que também devem ser consideradas no processo de segurança: a autenticidade, responsabilidade, o não repúdio e a confiabilidade. (NBR ISO/IEC 27002:2005)

Deste modo, pode-se afirmar que qualquer evento que termine por violar um destes princípios deve ser classificado como um incidente de segurança e deve ser remediado com a maior brevidade possível a fim de minimizar a exposição dos ativos.

A exploração de vulnerabilidade é uma técnica muito difundida e bastante explorada por indivíduos maliciosos. Existem ainda inúmeros portais, sites e sistemas especializados em procurar e divulgar estas vulnerabilidades.

Sendo assim, a gestão de vulnerabilidade tornou-se uma necessidade no processo de gestão de segurança da informação.

2.1 VULNERABILIDADE

Vulnerabilidade é a fragilidade de um ativo ou grupos de ativos que pode ser explorada por uma ou mais ameaças. Ou ainda, um ponto fraco que pode ser explorado por uma ameaça, por exemplo, uma porta de firewall aberta, uma senha que nunca foi alterada. Um controle que não é executado também é considerado como sendo uma vulnerabilidade. (NBR ISO/IEC 27002, 2013)

Como pode ser verificado, as vulnerabilidades estão relacionadas diretamente com as fragilidades. Essas fragilidades podem estar nos processos, políticas, equipamentos e nos recursos humanos. Por si só, elas não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou de condição favorável, já que se trata de ameaças.

A fragilidade ou o ponto fraco referido no parágrafo anterior, pode ser qualquer um dos vários ativos que uma empresa possui, seja ele tangível, ou intangível, por exemplo: num dispositivo, uma política, um processo ou um funcionário.

A vulnerabilidade por si só não pode ser considerada um incidente pois trata-se de um elemento passivo, necessitando para tanto de um agente causador ou de condição favorável, para tornar-se uma ameaça.

2.2 AMEAÇAS

Conforme informado anteriormente, quando uma vulnerabilidade é explorada de forma intencional ou mesmo acidental por um elemento interno ou estranho, temos uma ameaça.

Uma ameaça tem o potencial de comprometer ativos (tais como: informações, processos e sistemas) e, por isso também as organizações. As ameaças podem ser origem natural ou humana e podem ser acidentais e intencionais. (NBR ISO/IEC 27005 , 2008)

As ameaças intencionais são provocadas por invasões, fraudes e roubo de informações.

As ameaças involuntárias são causadas por erros de desconhecimento no uso do ativo, onde aparecem erros inconscientes de funcionários que não foram devidamente treinados, infecções por vírus ou até mesmo os acessos indevidos. As ameaças exploram os pontos fracos afetando assim a segurança da informação.

Tem-se ainda as ameaças decorrentes de fenômenos da natureza, tais como, fogo, enchentes e terremotos, que também podem provocar danos aos ativos.

2.3 EXPLOIT

Um *exploit* geralmente é uma sequência de comandos, dados ou uma parte de um software elaborados por indivíduos que tem o propósito de tirar vantagem ou explorar vulnerabilidades de sistemas. O objetivo, neste caso, é causar um comportamento acidental ou imprevisto na execução de um software ou hardware, tanto em computadores quanto em outros aparelhos eletrônicos.

Existem diversos sistemas e páginas na internet que são dedicados a estudo e análise deste tipo de conteúdo. Dentre eles pode-se mencionar o programa *Metaexploit* e a página na internet chamada *exploit-database*.

2.4 ATAQUE

Ataque é uma ação inteligente que ameaça a segurança através da violação da política de segurança de um sistema ou com intuito de invadir serviços de segurança (RFC 2828, 2010).

Existem três categorias de ataque:

- Ataques internos são aquelas ocorrências que ocorrem dentro de organizações e são praticados por funcionários.
- Ataques externos são os ataques com origem externa a organização e da rede, quando, por meio da internet um indivíduo não autorizado ou ilegítimo tem acesso ao sistema.
- Ataques físicos ocorrem quando o invasor tem acesso físico às organizações, ou seja, são roubados equipamentos, software ou dispositivos de armazenamento. Além do roubo é possível executar uma série de ações maliciosas ou destrutivas, tais como, copiar documentos confidencias, obter informações privilegiadas, modificar arquivos importantes ou alterar privilégios de usuários.

Os ataques geralmente são baseados ou direcionados pelo *exploits* divulgados em fóruns ou em ferramentas próprias semelhantes as mencionadas anteriormente no capítulo anterior.

2.5 CICLO DE VIDA DA VULNERABILIDADE

Na figura 2-1 é possível visualizar o ciclo de vida das vulnerabilidades.

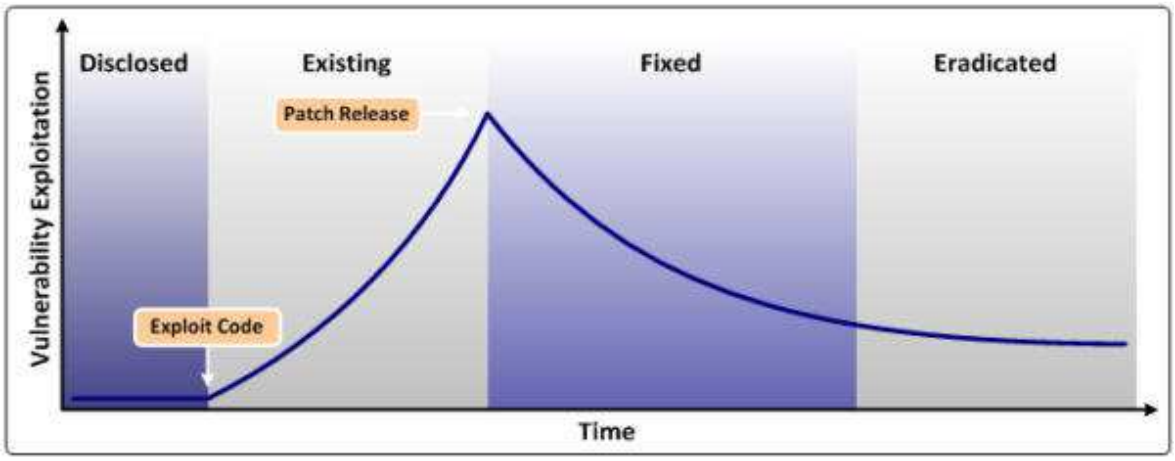

Figura 2-1 - Ciclo de Vida de uma Vulnerabilidade (OLLMAN, s.d.)

O gráfico mostra uma abordagem do volume de exploração de uma vulnerabilidade versus o tempo. Na figura pode-se identificar um pico no volume de explorações que cresce conforme o seu código de exploração se populariza.

As fases do ciclo de vida da vulnerabilidade incluem:

Divulgação (*Disclosed*) - quando a vulnerabilidade é divulgada, mas não explorada porque o código de exploração não está normalmente disponível.

Existência (*Existing*) - uma prova de conceito ou código de exploração aparece e há um aumento na taxa de exploração.

Conserto (*Fixed*) - nesta fase os patches de fornecedores são desenvolvidos e aplicados gradualmente. Os sistemas vulneráveis são corrigidos paulatinamente e as taxas de exploração começam a decrescer.

Erradicação (*Eradicated*) - a vulnerabilidade e suas correspondentes explorações deixam de ser uma ameaça prática pois seu agente explorador foi neutralizado através de um novo código de sistema ou através de um controle compensatório.

Mesmo quando uma vulnerabilidade ela entra na fase de erradicação, ela não deve jamais sair do radar dos gestores de vulnerabilidade, pois, embora uma vulnerabilidade possa ser "erradicada", ela não significa que todas as infecções foram removidas ou que a ameaça deixa de existir. Em vez disso, assume que as tecnologias de detecção, proteção e remoção estão cientes do código de exploração e suficientemente implantadas para evitar que a ameaça volte a exibir as mesmas taxas de exploração.

2.6 GESTÃO DE ATIVOS / INVENTÁRIO

Ativo é qualquer coisa que tenha valor para a organização. (NBR ISO/IEC 27001, 2006). Ou seja, qualquer elemento (hardware, software, pessoas) que armazene, processe ou imprima as informações que tem valor para o negócio da organização.

Os ativos ainda podem ser classificados como tangíveis, quando são físicos, como dispositivos de informática, ou prédios. E como ativos intangíveis quando não são físicos como sistemas, o conhecimento ou uma informação.

Uma gestão de ativos eficaz deve comtemplar de formar organizada os seguintes tópicos:

- Itens de Software e Hardware;
- Contratos administrativos e técnicos;
- Informações sobre o suporte, garantia e licenciamento dos ativos;
- Quais as regras, frequência e como se dá as atualizações das informações do inventário;
- Serviços suportados ou que rodam em determinado ativo ou grupo de ativos.

Todas estas informações organizadas e bem controladas servem de base para confecção do inventário de T.I. O inventario de T.I é fundamental para qualquer tipo de organização, uma vez que, os recursos tecnológicos são responsáveis por suportar o negócio fim das organizações.

Baseado nas informações contidas no inventario de *hardware* e *software* é possível dimensionar os investimentos necessários na área de infraestrutura de T.I para ampliação dos negócios da organização, acompanhar a situação dos contratos de suporte e manutenção, verificar os limites das garantias de dispositivos, verificar o processo de renovações de licenças e suporte e ainda controlar os responsáveis pelos ativos.

Para catalogar, controlar e manter atualizado centenas ou muitas vezes milhares de ativos de um inventário, a organização pode se servir de simples planilhas à complexas ferramentas ou sistemas de computacionais com controle de RFID para ter de forma exata e atualizada as movimentações de ativos dentro da organização. Tudo isso a depender muito do número de ativos a serem controlados.

Independentemente do número de ativos ou do tamanho da organização, uma instituição que deseja implementar uma gestão de vulnerabilidades eficiente é não pode prescindir-se de um inventário atualizado e bem controlado pois ele é um pré-requisito importante na fase de planejamento das varreduras de vulnerabilidades.

2.7 O PLANO DE GESTÃO DE VULNERABILIDADES

O inventario de ativos de T.I é pré-requisito quase que indispensável para elaboração do plano de gestão de vulnerabilidades. Não que não seja possível efetuar uma gestão de vulnerabilidades sem o inventario, porém, sem dúvida alguma, em um ambiente de infraestrutura complexa como o de organizações muito imensas como bancos e empresas globais, as informações organizadas conforme capitulo anterior serão de extrema importância para montagem do plano de gestão de vulnerabilidades.

Abaixo seguem transcrevidas as diretrizes indicadas pela norma ABNT NBR ISO/IEC 27002:2013 para Gestão de Vulnerabilidades:

a) Convém que a organização defina e estabeleça as funções e responsabilidades associadas na gestão de vulnerabilidades técnicas, incluindo o monitoramento de vulnerabilidades, a avaliação de risco de vulnerabilidades, correções, acompanhamento dos ativos e qualquer responsabilidade de coordenação requerida;

b) Convém que os recursos de informação a serem usados para identificar vulnerabilidades técnicas relevantes e para manter a conscientização sobre os mesmos, sejam identificados, para *softwares* e outras tecnologias (baseado na lista de inventário dos ativos, convém que esses recursos de informação sejam mantidos atualizados com base nas mudanças no inventário de ativos, ou quando outros recursos novos ou úteis sejam encontrados;

c) Convém que seja definido um prazo para a reação a notificações de potenciais vulnerabilidades técnicas relevantes;

d) Uma vez que uma vulnerabilidade técnica potencial tenha sido identificada, convém que a organização avalie os riscos associados e as ações a serem tomadas; tais ações podem requerer o uso de emendas de correções (*patches*) nos sistemas vulneráveis e/ou a aplicação de outros controles;

e) Dependendo da urgência exigida para tratar uma vulnerabilidade técnica, convém que a ação a ser tomada esteja em acordo com os controles relacionados com a gestão de mudanças ou que sejam seguidos os procedimentos de resposta a incidentes de segurança da informação.

f) Se uma correção é disponibilizada, convém que sejam avaliados os riscos associados à sua instalação (convém que os riscos associados à vulnerabilidade sejam comparados com os riscos de instalação da correção);

g) Convém que as emendas (*patches*) sejam testadas e avaliadas antes de serem instaladas para assegurar a efetividade e que não tragam efeitos que não possam ser tolerados; quando não existir a disponibilidade de uma emenda de correção, convém considerar o uso de outros controles, como:

1) A desativação de serviços ou potencialidades relacionadas à vulnerabilidade;
2) A adaptação ou a agregação de controles de acesso, por exemplo *firewalls* nas fronteiras da rede;
3) O aumento do monitoramento para detectar ou prevenir ataques reais;
4) O aumento da conscientização sobre a vulnerabilidade.

h) Convém que seja mantido um registro de auditoria de todos os procedimentos realizados;

i) Com a finalidade de assegurar a eficácia e a eficiência, convém que processo de gestão de vulnerabilidades técnicas seja monitorado e avaliado regularmente;

j) Recomenda-se contemplar em primeiro lugar os sistemas com altos riscos;

k) Convém que um processo de gestão de vulnerabilidade técnica eficaz esteja alinhado com as atividades de gestão de incidentes, para comunicar dados sobre as vulnerabilidades, às funções de resposta a incidentes e fornecer procedimentos técnicos no caso em que ocorra um incidente.

l) Convém que seja definido um procedimento para contemplar a situação onde uma vulnerabilidade tenha sido identificada e não existam controles adequados. Nesta situação,

convém que a organização avalie os riscos relativos à vulnerabilidade conhecida e defina correções e ações corretivas apropriadas.

A gestão de vulnerabilidades técnicas pode ser vista como uma subfunção da gestão de mudanças e, como tal, pode aproveitar os procedimentos e processos da gestão de mudanças.

Fornecedores estão frequentemente sob grande pressão para liberar correções o mais breve possível. Portanto, existe a possibilidade de uma correção não resolver o problema adequadamente e causar efeitos colaterais negativos. Também, em alguns casos, a desinstalação de uma correção pode não ser facilmente obtida após sua instalação.

Quando testes adequados de correção não forem possíveis, por exemplo, devido a custos ou falta de recursos, um atraso na aplicação da correção pode ser considerado para avaliar os riscos associados, baseados nas experiências relatadas por outros usuários.

A gestão de vulnerabilidades é um processo contínuo e retroalimentado. Desta maneira, deve-se existir métricas bem definidas e um modelo pré-estabelecido para direcionar o fluxo das atividades relacionadas a esta gestão.

Sendo assim, com posse das informações relevantes constantes no inventario de T.I, é possível se iniciar o processo de implantação da gestão de vulnerabilidade. Nesta fase deve se atentar aos termos dos acordos para a efetiva gestão. Deve-se atentar ao também ao fato que gestão de vulnerabilidade não é gestão de risco, embora seja um dos processos da gestão de risco seu escopo é mais limitado.

Abaixo estão destacados alguns pontos importantes que devem ser priorizados na fase de planejamento, pois, são tópicos de referência para execução de um plano de gestão de vulnerabilidade eficaz. São regras que servirão de guia para manutenção do sistema cíclico que é a gestão de vulnerabilidades.

- Definição dos métodos e ferramentas utilizados no ciclo de vida dos processos para a gestão de ativos, varreduras, abertura de bilhetes e a gestão de fato das vulnerabilidades;
- Definição do escopo para varreduras;
- Definição da periodicidade das análises de vulnerabilidade segundo estudo prévio dos ativos ou das estruturas alvo da varredura;
- Processo de notificação de responsáveis pelos ativos vulneráveis.
- Definição de procedimentos para aplicação de mitigação;

- Definição clara do tempo de correção baseado na classificação das vulnerabilidades (tempo inversamente proporcional a criticidade);
- Definição de procedimentos para efetuar a validação da mitigação;
- Definição dos modelos e formatos dos relatórios emitidos após as varreduras de vulnerabilidade. Verificar se os relatórios emitidos pelas ferramentas são suficientes ou se precisam de alguma forma serem analisados.

2.8 CICLO DE VIDA DOS PROCESSOS

Após a organização definir as regras regais do plano de gestão de vulnerabilidades, pode iniciar de fato a aplicar os processos.

Conforme pode-se observar na imagem 2-2, existe um ciclo de vida bem definido para os processos de gestão de vulnerabilidades que são basicamente as etapas de um sistema que é cíclico e em muitas oportunidades, é alimentado com os resultados obtidos nas etapas anteriores. Sendo assim, tem-se a etapa de descobrimento, priorização, avaliação, elaboração de relatórios, remediação e verificação.

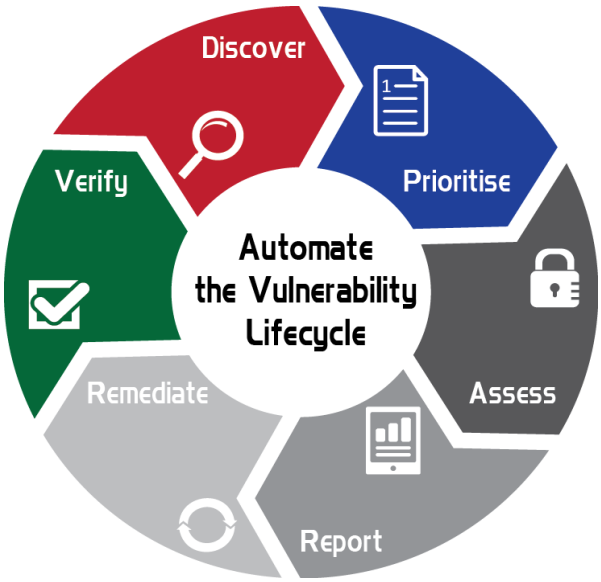

Figura 2-2 - Ciclo de Vida dos Processos de Gestão de Vulnerabilidade (COG SECURITY, 2016)

Como estes processos são periódicos e o resultado de um processo, em várias oportunidades retroalimenta o próximo processo, um plano de ação bem estruturado e devidamente preparado e elaborado conforme as características da organização, tem uma função importante na regulamentação da execução dos procedimentos inerentes a cada uma das etapas.

A seguir serão detalhados cada um dos processos e seus procedimentos.

I. Descoberta (*Discovery*): Não é possível medir um risco se a organização não conhece o que existe em sua rede. A descoberta dos recursos ajuda a determinar as áreas mais sensíveis a ataques e o mapeamento de rede detecta automaticamente todos os dispositivos em rede. As Vulnerabilidades geralmente são encontrada em serviços e podem ser originadas por falhas de *Software* ou má configuração. Estas falhas podem ser descobertas por testes manuais ou ferramentas específicas além de ser realizado remotamente ou em redes locais.

II. Priorização (*Prioritise*): É essencial a previsão de priorização de ativos ou estruturas para antes de iniciar a análise das vulnerabilidades. Esta priorização pode ser realizada por segmentos de rede, por serviço, superfície de ataque ou a exposição da rede, levando-se em conta o custo de operação dos ativos ou ainda os benefícios que o devido tratamento tempestivo da vulnerabilidade pode trazer a organização. Em linhas gerais, as organizações tendem a priorizar os serviços mais expostos as ameaças externas como servidores web por exemplo. Inclusive, recomenda-se fortemente o estabelecimento de uma frequência pré-determinada para as varreduras de vulnerabilidade baseado na criticidade conforme determinado pela organização no plano da de gestão.

III. Avaliação (*Assess*): Neste processo, executar exames detalhados e precisos nos ativos, começando com os mais importantes, fará com que o gestor responsável pelas varreduras tenha maior visibilidade do nível de exposição associado aos ativos. As varreduras detectam de formar eficaz vulnerabilidades nas estruturas de rede de forma automática ou sob demanda. É possível efetuar o *scan* de um número menor de ativos com frequência diferentes dependendo da criticidade e dos acordos previamente realizados entre os intervenientes. Ao longo da realização das varreduras, eventualmente, pode ser observado uma lentidão nos sistemas ou um congestionamento no tráfego da rede, logo, tudo isso deve ser levado em conta no momento de determinar a frequência e definição dos horários de execução das varreduras.

IV. Elaboração de Relatórios (*Report*): Existem algumas questões importantes que merecem atenção no momento de confecção dos relatórios, tão importante quanto a produção do documento em si, é de extremamente

pertinente a ponderação das informações que serão descritas nele. Uma política para verificação e validação das informações relatadas é essencial para evitar falsos alarmes positivos e perca de tempo das equipes intervenientes. Outro ponto primordial é a natureza do relatório. A profundidade das informações muda conforme o perfil dos profissionais que receberão o documento: por exemplos relatórios gerenciais, técnicos e para auditoria. Em alguns casos apenas os relatórios emitidos pelas ferramentas com as devidas ponderações são suficientes. É salutar contextualizar os dados dos relatórios gerados pelas ferramentas, adicionando informações completas sobre os ativos afetados e a descrição das vulnerabilidades encontradas inclusive constando a severidade de acordo com o CVSS ou classificação interna da organização e o CVE da cada vulnerabilidade encontrada.

Informações sobre processos de mitigação: Listar os patches disponíveis e/ou configurações alternativas e controles compensatórios pode direcionar as ações dos responsáveis, as informações dos desenvolvedores do software e/ou mantenedores do sistema sobre a vulnerabilidade podem auxiliar no processo de mitigação.

V. Remediação (*Remediate*): Para efetuar a mitigação é importante planejar o momento da intervenção no ativo. Conforme a criticidade da vulnerabilidade o processo de mitigação pode aguardar uma janela de manutenção ou será necessária uma parada emergencial. Além disso, deve ser considerado o tipo de medida que será adotado nesta mitigação: se será implementando na estrutura um controle compensatório, aplicado um *patche*, executada uma reconfiguração ou o responsável pelo ativo irá simplesmente assumir o risco de ameaça da vulnerabilidade mapeada.

Independente da ação que será adotada é conveniente realizar ensaios no ambiente de testes e homologar a ação escolhida para evitar surpresas no momento da aplicação da mitigação. Os fabricantes executam testes antes da liberação de patches ou atualizações de segurança, porém, seu escopo é limitado e não consegue jamais reproduzir em totalidade a complexidade das infraestruturas das mais diversas organizações. Mesmo com todo planejamento e prudência, ainda assim é possível que algo não saia conforme planejado e neste momento ter um plano de recuperação ou *rollback* é fundamental para continuidade dos negócios.

VI. Verificação (*Verify*): Alinhada com a fase final/posterior da mitigação, no processo de verificação são aplicadas as mesmas regras e premissas de

notificação citadas anteriormente. Deverão ser utilizadas as mesmas ferramentas e deve-se tentar reproduzir com fidelidade o mesmo cenário, contexto e a ordem de execução das ações dos processos anteriores com a finalidade de testar se de fato uma vulnerabilidade foi devidamente mitigada.

Elaborar um relatório final e receber aceite sobre a estrutura. Deixar claro o que foi executado para evitar que problemas futuros sejam atribuídos as atividades de mitigação das vulnerabilidades. Os casos em que as vulnerabilidades sejam assumidas deve existir um termo claro com os riscos e as informações pertinentes a este fato. Os termos devem ser assinados por todos os gestores e intervenientes.

Retroalimentar o processo. Deve ser executado de forma transversal a todos os processos. Este processo basicamente estrutura a validação das mitigações verificando se todos os pontos do processo respeitaram devidamente o plano de gestão previamente acordado. Deste modo, revisar todos os processos, cuidar do inventário de ativos, definir frequência de revisão, os responsáveis e atualizar todas as informações dos serviços e ativos é atividade constante e paralela aos processos. Entre os pontos de reflexão que comtemplam este processo, tem-se:

- O escopo das varreduras: importante saber se o escopo inicial foi completamente coberto, se o escopo precisa mudar, se a periodicidade é ideal ou se tem de ser revista de alguma forma.
- Os relatórios: verificar se foram compreensíveis aos interlocutores, se os responsáveis foram claramente notificados e se atingiram os resultados esperados.
- As mitigações: constatar se foram aplicadas dentro dos tempos previstos no acordado de nível de serviço.

3 REFERENCIAL TEÓRICO

Quando existe a suspeita que eventualmente exista um agente explorando uma vulnerabilidade ou falha de segurança, existe uma prática que pode ajudar a moderar a exposição dos ativos a ameaças denominada *Baseline Reporting*. Esta técnica consiste basicamente em monitorar e detectar o que ocorre na rede da organização em seu funcionamento típico, ou seja, quando não há atividades maliciosas em andamento, e criar uma base de dados com estas informações para uso como referência, e quando haver alguma atividade maliciosa na rede, o sistema será capaz de identificar ameaças pois com suporte da base de dados ele pode inferir que esta atividade é maliciosa ou não. O maior desafio na

utilização destes sistemas reside na atualização iterada desta base de dados, pois a própria rede ou o comportamento de tráfego da organização podem sofrer mutações ao longo do tempo. A gestão de vulnerabilidades tem o objetivo de evitar que a vulnerabilidade evolua a ponto de tornar-se uma ameaça e seja necessária a atuação de ferramentas semelhantes a esta descrita acima, porém, é importante a utilização de vários tipos de ferramentas pois elas se completam entre si e assim diminui a exposição dos ativos e abaixa a probabilidade de ataques bem-sucedidos.

3.1 TÉCNICAS PARA ANÁLISE DE VULNERABILIDADES

A frente será relatada as técnicas que podem ser utilizadas para efetuar a identificação e análises das vulnerabilidades dentro das organizações. Estas técnicas são as mais notáveis existentes atualmente e são geralmente utilizadas em conjunto para investigar com maior profundidade um determinado evento de segurança. Seu uso é intenso em diversas etapas dos processos de gestão de vulnerabilidades.

3.1.1 Honeypots/Honeynets

Honeypots (potes de mel) é um recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido que tem o objetivo de atrair ameaças que são direcionadas ao ambiente de produção. Em um *honeypot* podem ser instaladas ferramentas para emular sistemas operacionais e serviços com os quais os atacantes irão interagir ou existir sistemas operacionais, aplicações e serviços reais para exploração. (CERT.br, 2007)

Uma *honeynet* (rede de mel) é uma ferramenta de pesquisa, que consiste de uma rede projetada especificamente para ser comprometida, e que contém mecanismos de controle para prevenir que seja utilizada como base de ataques contra outras redes (CERT.br, 2007)

Uma vez comprometida, a *honeynet* é utilizada para observar o comportamento dos invasores, possibilitando análises detalhadas das ferramentas utilizadas, de suas motivações e das vulnerabilidades exploradas. (CERT.br, 2007)

Uma *honeynet* normalmente contém um segmento de rede com *honeypots* de diversos sistemas operacionais e que fornecem diversas aplicações e serviços. Também contém mecanismos de contenção robustos, com múltiplos níveis de controle, além de sistemas para captura e coleta de dados, e para geração de alertas. (CERT.br, 2007)

3.1.2 Analisadores de Protocolo

Um analisador de protocolo é uma ferramenta (*hardware* ou *software*) utilizado para capturar e analisar sinais e o tráfego de dados através de um canal de comunicação. Esse canal varia de um barramento de computador local para um link de satélite remoto, que fornece um meio de comunicação usando um protocolo de comunicação padrão (em rede ou ponto-a-ponto). Cada tipo de protocolo de comunicação tem uma ferramenta diferente para coletar e analisar sinais e dados.

Os analisadores de rede não se destinam a substituir *firewalls*, antivírus, ou programas de detecção de *spyware*. No entanto, o uso de um analisador de rede além de outras contramedidas pode minimizar a probabilidade de um ataque ocorrer e pode facilitar a resposta rápida no caso de um ataque começar.

Estes analisadores são usados para analisar o comportamento típico de uma rede, facilitando assim a detecção de qualquer comportamento de tráfego anômalo que possa eventualmente configurar uma ameaça. Com o uso de uma ferramenta dessa em alguns casos é possível visualizar dados críticos e privados dos usuários como senhas de acesso e conversas de alguns tipos de programas de bate-papo caso estas não utilizem algoritmos criptográficos e naveguem em texto claro.

3.1.3 Escaneamento de Portas

Escaneamento de Portas (*Port Scanning*) é o nome da técnica utilizada para identificar portas abertas e serviços disponíveis em um host de rede. Ele permite que os auditores e administradores de rede examinem a segurança da rede enquanto atacantes e hackers a usam para identificar portas abertas para explorar e / ou executar serviços mal-intencionados em um computador host ou servidor.

Os scanners de portas são usados principalmente por administradores de segurança de rede para verificar e monitorar portas de rede em um sistema, servidor ou ambiente de TI buscando vulnerabilidades.

3.1.4 Varredura de Vulnerabilidade

Um scanner de vulnerabilidades (*Vulnerability Scanning*) é um aplicativo de software que avalia vulnerabilidades de segurança em redes, sistemas e dispositivos informáticos e produz um relatório com um conjunto de resultados de verificação. No entanto, como os administradores e os invasores podem usar a mesma ferramenta para corrigir ou explorar um sistema, os administradores precisam realizar uma varredura e

corrigir problemas antes que um invasor possa utilizar a mesma técnica e explore as vulnerabilidades encontradas. (WEIDMAN, 2014)

Um scanner de vulnerabilidades pode avaliar uma serie de vulnerabilidades em sistemas de informação (incluindo computadores, sistemas de rede, sistemas operacionais e aplicativos de software, versões de software, serviços e banco de dados) que possam ter sido originadas por um fornecedor, por atividades de administração do sistema ou ainda por atividades gerais de usuários no dia-a-dia.

Essas ferramentas são alimentadas por informações coletadas por base de dados de colaboração na internet e também pelas informações divulgadas por fabricantes de hardwares e softwares, assim permitindo que os sistemas das organizações sejam sempre verificados pelas vulnerabilidades mais recentes divulgadas pela comunidade.

3.1.5 Teste de Penetração

O teste de penetração, ou *pentest*, envolve a simulação de ataques reais para avaliar o risco associado a possíveis violações de segurança. Em um *pentest* (em oposição a uma avaliação de vulnerabilidade), os testadores ou *pentesters* não só descobrem vulnerabilidades que podem ser usadas por invasores, mas também exploram essas vulnerabilidades, sempre que possível, para avaliar o que os invasores podem obter após uma exploração bem-sucedida. (WEIDMAN, 2014)

Quando um teste de penetração é conduzido em uma organização, consequentemente também é realizada uma varredura de vulnerabilidades. Isso ocorre porque a fase inicial de testes de penetração requer que uma avaliação completa de vulnerabilidade seja conduzida para que os analistas responsáveis pela condução do *pentest* possam aprender os endereços IP, tipos de dispositivos, sistemas operacionais e quaisquer vulnerabilidades apresentadas pelos sistemas.

A partir daí o analista tenta explorar as vulnerabilidades das mais variadas maneiras possíveis e conhecidas por ele. Isso pode incluir a utilização de ferramentas automatizadas para explorar vulnerabilidades em servidores, firewalls e roteadores ou explorar aplicativos da Web para vulnerabilidades comuns e também incluir engenharia social na tentativa de extrair informações ou obter acesso físico a um local através do usuário final. Também pode-se explorar manualmente o sistema, o que às vezes pode expor vulnerabilidades que um scanner de vulnerabilidades não seria capaz de identificar. Isso inclui escrever scripts de exploração personalizados, introdução de sequência de comandos e *scripts*.

O teste de intrusão aprofunda e complementa a análise de vulnerabilidades. De forma geral, é um serviço realizado por empresas externas e especializadas a organização e ao final da atividade é confeccionado e entregue a organização um relatório detalhando todos as vulnerabilidades encontradas

Existem essencialmente três tipos de teste de penetração:

- *Black box*: O responsável pela realização dos testes de não tem nenhum conhecimento prévio da rede, infraestrutura ou serviços da organização, desta forma o teste fica muito semelhante a um ataque originado de forma externa a organização como se fosse gerado por *crackers* ou *hackers blackhats*.
- *Grey box*: É apresentado algum conhecimento preliminar sobre a infraestrutura ou serviços da organização ao analista responsável pelo teste. Este teste é indicado para simular acesso de colaboradores, empregados terceirizados, ou prestadores de serviço que tem acesso limitados e por alguma razão estejam mal-intencionados.
- *White box*: Os analistas responsáveis pelo teste têm pleno conhecimento da infraestrutura da organização, inclusive as informações mais sensíveis como códigos fontes, os endereços IP dos dispositivos, diagramas das redes, estrutura de serviços e credenciais de acesso. Este teste é o mais arrojado e tem a finalidade de simular um ataque interno, por um funcionário com privilégios e conhecimento técnico como os funcionários que trabalham diretamente com tecnologia.

Uma análise de vulnerabilidade procura vulnerabilidades conhecidas nos sistemas e relatar possíveis exposições. Um teste de penetração é projetado para realmente explorar falhas na arquitetura dos sistemas. Onde uma varredura de vulnerabilidade pode ser automatizada, um teste de penetração requer vários níveis de especialização dentro de seu escopo de sistemas.

As verificações de vulnerabilidade devem ser executadas continuamente enquanto os testes de penetração podem ser eventuais. Os exames de vulnerabilidade devem ser executados pelo próprio corpo técnico da organização, para que seja possível construir uma base de conhecimento do que é normal para o programa de segurança de informações daquela instituição. Testes de penetração devem ser executados por uma consultoria externa para que o teste tenha o benefício da independência e os "olhos de fora" possam fornecer uma visão diferente das diversas situações eventualmente exploradas. Juntos, o teste de

penetração e a varredura de vulnerabilidades são poderosas ferramentas usadas para monitorar e aperfeiçoar os planos e políticas de segurança da informação.

Na tabela 3-1, é possível visualizar um quadro comparativo entre as análises de vulnerabilidades e os testes de penetração.

Tabela 3-1 - Comparativo Análise de Vulnerabilidade e Teste de Intrusão (AVYAAN LABS, 2014)

Diferenças	Análise de Vulnerabilidades	Teste de Penetração
Características	Orientado a base de dados	Orientado a um objetivo
Tipo de relatório	Lista priorizada de Vulnerabilidades	Informações específicas sobre a vulnerabilidade explorada e suas consequências.
Propósito	Identificação de Vulnerabilidades de Segurança.	Determinar se um sistema pode resistir a uma tentativa de intrusão.

3.2 FERRAMENTAS PARA GESTÃO DE VULNERABILIDADES

Para auxiliar o processo de gestão de vulnerabilidades, a automatização e adoção de sistemas de apoio é fundamental. Processos enxutos e maduros, requerem um nível de organização muito grande, e somente com a adoção de ferramentas é possível efetuar o controle de grandes estruturas. Deste modo, grandes organizações não podem de maneira alguma se furtar de utilizar e customizar as melhores ferramentas do mercado para suportar seus negócios.

A seguir serão apresentadas algumas alternativas de ferramentas para suporte nos processos de gestão de vulnerabilidades.

3.2.1 Ferramentas de Apoio na Gestão de Inventário

Conforme já reiterado outras vezes, para uma gestão de vulnerabilidade eficaz é interessante um inventario bem controlado e organizado.

Um inventário pode ser controlado manualmente quando os dados dos ativos são informados pelo analista responsável, ou de forma automática quando os dados são coletados através de agente ou SNMP. Existem algumas técnicas e ferramentas que podem ajudar a manter este controle atualizado:

- FPING: é um programa para enviar pacotes ICMP para hosts de rede, semelhante ao comando *ping*, mas com um desempenho muito melhor que o *ping* para efetuar testes de conectividade em vários hosts. Ferramenta útil para controle de endereçamento IP em uso na rede.

- Zabbix Discovery Rules: ferramenta que faz a descoberta automática da rede, descobre IPs e faz mapeamento FQDN. Mapeia serviços ativos e mantém um histórico de eventos.
- Zabbix Host Inventory: Ferramenta focada em *hosts*, descobre dispositivos baseados em agentes instalados nas máquinas. Controla o tipo e função do ativo, nome, informações sobre sistema operacional, aplicativos e detalhes de *hardware*.
- Rack Tables: Agrega diversas funções em somente um sistema. Gerencia um catálogo completo com informações de *software* e *hardware* dos ativos. Controla acomodações de racks e utilização de espaços em *racks*. Realiza o gerenciamento de endereços, faz mapeamento entre portas de *patch-panel*, cabos, *switches* e também executa mapeamento de *Vlans*.
- PRADS (*Passive Real-time Asset Detection System):* É um Sistema Passivo de Detecção de Ativos em Tempo Real. Ele escuta passivamente o tráfego de rede e reúne informações sobre hosts e serviços que vê na rede. Essas informações podem ser usadas para mapear sua rede, permitindo que você saiba quais serviços e hosts estão ativos. E como ele funciona de forma passiva, ele faz a varredura de sistemas sem enviar um único pacote. Para isso o PRADS captura o tráfego silenciosamente através de uma interface em modo promíscuo. Deste modo, ele é muito mais furtivo do que um *scanner* clássico, que geralmente gera muitas entradas de log em firewalls ou IDS. O PRADS funciona em várias camadas e é baseado em todos os protocolos comuns, como: TCP, UDP, ICMP, ARP, o que o torna extremamente eficiente e rápido.

3.2.2 Ferramentas para Análise de Vulnerabilidade

As análises de vulnerabilidades são basicamente efetuadas por *softwares* que integram uma ou mais ferramentas de segurança e atuam em diversas camadas, inclusive na camada 7, de aplicação. A seguir serão apresentados técnicas e exemplos de ferramentas que podem sem usadas para auxiliar as varreduras de vulnerabilidades.

- Nmap: O Nmap ("Network Mapper") é um utilitário de código aberto e licença gratuita para exploração de rede ou auditoria de segurança. O Nmap usa pacotes IP para determinar quais hosts estão disponíveis na rede, quais serviços (nome e versão do aplicativo) esses hosts estão oferecendo,

que sistemas operacionais (e versões do S.O) eles estão executando, entre outras coisas. Ele foi projetado para digitalizar rapidamente grandes redes. O *Nmap Scripting Engine* (NSE) é um dos recursos mais poderosos e flexíveis do Nmap. Ele permite aos usuários escrever (e compartilhar) scripts simples (usando a linguagem de programação Lua) para automatizar uma ampla variedade de tarefas de rede. Esses scripts são executados em paralelo com a velocidade e eficiência do Nmap. Os técnicos podem utilizar os scripts distribuídos com o Nmap, ou escrever os próprios *scripts* para atender às necessidades individuais de cada organização.

- Nessus: Líder mundial em scanners ativos, com detecção de alta velocidade, auditoria de configuração, criação de perfis de ativos, descoberta de dados confidenciais e análise de vulnerabilidades. O Nessus é um scanner de vulnerabilidades de rede completo que inclui verificações de alta velocidade para milhares das vulnerabilidades mais atualizadas, uma ampla variedade de opções de verificação, uma interface fácil de usar e relatórios eficazes. Sua Base de dados é atualizada frequentemente, porém esta ferramenta para uso comercial cobra pela licença e torna se assim uma opção apenas para organizações com os processos maduros e bem implantados que sentem de alguma forma que pode dispor de mais recursos financeiros para investir com gerenciamento de vulnerabilidades.
- Lynis: É uma ferramenta de auditoria para Unix. Ele verifica o sistema e o software disponível, para detectar problemas de segurança. Além das informações relacionadas à segurança, também irá procurar informações gerais do sistema, pacotes instalados e erros de configuração. Este software tem como objetivo auxiliar a auditoria automatizada, gerenciamento de patches de software, vulnerabilidade e varredura de malware de sistemas baseados em Unix. A Lynis é altamente recomendada para os auditores atuar nas verificações de conformidade.
- Nikto: É um scanner de servidor Web de código aberto (GPL) que realiza testes abrangentes contra servidores web para vários itens, incluindo mais de 6700 arquivos / programas potencialmente perigosos, verifica versões desatualizadas de mais de 1250 servidores e problemas específicos de versão em mais de 270 servidores. Ele também verifica se há itens de

configuração do servidor, como a presença de vários arquivos de índice, opções de servidor HTTP e tentará identificar servidores e software da Web instalados. Os itens de digitalização e os *plugins* são atualizados com frequência e podem ser atualizados automaticamente. O Nikto não é projetado como uma ferramenta furtiva. Ele irá testar um servidor web no menor tempo possível, e é óbvio em arquivos de log ou para um IPS / IDS. No entanto, há suporte para os métodos anti-IDS do LibWhisker no caso de você querer experimentá-lo (ou testar seu sistema IDS).

- OpenVAS (Open Vulnerability Assessment System): É uma estrutura de vários serviços e ferramentas que oferecem uma solução abrangente de varredura e gerenciamento de vulnerabilidades. É uma ferramenta descendente do Nessus e seu scanner pode detectar problemas de segurança em todos os tipos de servidores e dispositivos de rede. O núcleo desta arquitetura orientada a serviços com SSL é o OpenVAS Scanner. O scanner executa de forma muito eficiente os Testes de Vulnerabilidade de Rede (NVTs) reais que são veiculados através do OpenVAS NVT Feed ou através de um outro serviço da escolha da organização. Uma das vantagens é o fato da ferramenta ser código aberto, e desta maneira se a ferramenta gerar um alarme falso positivo; é possível analisar o plug-in para determinar por que a vulnerabilidade foi sinalizada. OpenVAS tem uma forte comunidade de profissionais de segurança e divulgar qualquer falso positivo para a lista de discussão OpenVAS muitas vezes resulta em feedback imediato. Consequentemente, o falso positivo reportado pode ser consertado rapidamente beneficiando toda a comunidade de usuários.

3.2.3 Avaliação e Classificação de Criticidade

As vulnerabilidades de software, hardware e firmware representam um risco crítico para qualquer organização e podem ser difíceis de categorizar e mitigar.

Regras claras e bem definidas são imprescindíveis para a efetuar a devida classificação das vulnerabilidades encontradas nas varreduras pelas ferramentas e para a tempestiva atuação na correção e mitigação das mesmas. As organizações têm liberdade para definir os critérios que julgue mais relevantes no momento de classificar as vulnerabilidades encontradas, porém, já existe o CVSS, que é sistema de metrificação já maduro e conceituado desenvolvido pela FIRST. A FIRST é uma confederação internacional de

equipes de resposta a incidentes de computadores. Ela lida cooperativamente com incidentes de segurança de computadores e promovem programas de prevenção de incidentes.

As organizações podem utilizar as pontuações ou *scores* CVSS para determinar a gravidade dos eventos gerados nas varreduras e priorizar as mitigações e correções das vulnerabilidades encontradas. A pontuação CVSS reflete o impacto de segurança geral de uma vulnerabilidade

- CVSS (*Common Vulnerability Scoring System)*: É uma estrutura aberta para comunicar as características e a gravidade das vulnerabilidades do software. O Sistema de Pontuação de Vulnerabilidade Comum (CVSS) fornece uma maneira de capturar as principais características de uma vulnerabilidade e produzir uma pontuação numérica refletindo sua gravidade, bem como uma representação textual dessa pontuação. A pontuação numérica pode então ser traduzida em uma representação qualitativa (como baixa, média, alta e crítica) para ajudar as organizações a avaliar adequadamente e priorizar seus processos de gerenciamento de vulnerabilidade. (THE MITRE CORP., 2017)

O CVSS consiste em três grupos métricos: Base, Temporal e Ambiental. O grupo Base representa as qualidades intrínsecas de uma vulnerabilidade, o grupo Temporal reflete as características de uma vulnerabilidade que muda ao longo do tempo e o grupo ambiental representa as características de uma vulnerabilidade que são exclusivas do ambiente de um usuário. As métricas Base produzem uma pontuação que varia de 0,0 a 10,0, que pode então ser modificada pontuando as métricas Temporais e Ambientais. Uma pontuação CVSS também é representada como uma sequência vetorial, uma representação textual compactada dos valores usados para derivar a pontuação. (THE MITRE CORP., 2017)

Na figura 3-1, pode-se observar como os três grupos compõem a pontuação CVSS.

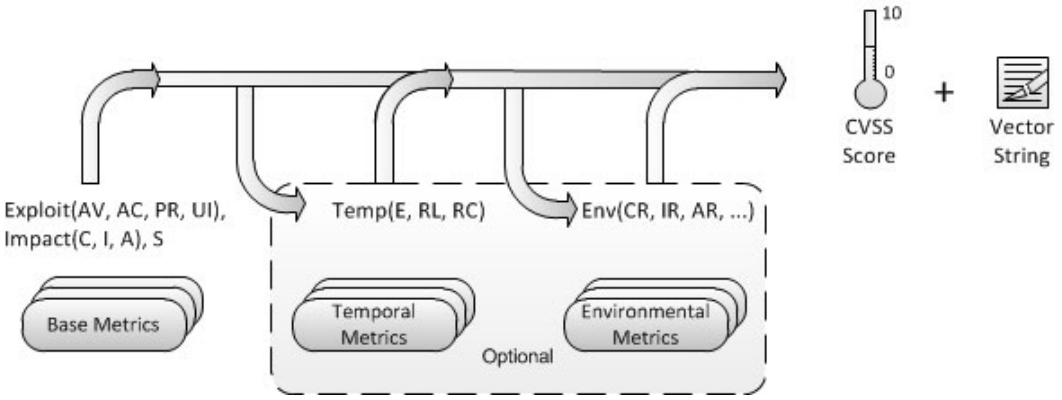

Figura 3-1 - Métricas e Equações CVSS (ALIENVAULT INC, 2017)

Atualmente o CVSS encontra-se na terceira versão e suas avaliação são atribuídas conforme a graduação abaixo:

- As vulnerabilidades são rotuladas com gravidade "baixa" se tiverem um índice base CVSS de 0,0 - 3,9.
- As vulnerabilidades serão rotuladas de gravidade "média" se tiverem uma pontuação CVSS de base de 4,0 - 6,9.
- As vulnerabilidades serão rotuladas de gravidade "alta" se tiverem um índice base CVSS de 7.0 - 8.9.
- As vulnerabilidades serão rotuladas de gravidade "crítica" se tiverem uma pontuação base CVSS de 9.0 - 10.0.

Durante a triagem de problemas, é possível alterar a gravidade de um problema substituindo manualmente a pontuação CVSS previamente calculada pelo valor da severidade para que seja possível priorizar a gravidade com relação a outros problemas. A modificação da gravidade ajuda a transmitir o grau de severidade de um problema ao desenvolvimento e ao gerenciamento para que as vulnerabilidades mais críticas sejam corrigidas primeiro. (THE MITRE CORP., 2017)

- CVE (*Common Vulnerabilities and Exposures*): é um dicionário de nomes comuns para vulnerabilidades de segurança cibernética publicamente conhecidas. Os identificadores comuns do CVE facilitam o compartilhamento de dados entre bancos de dados e ferramentas de segurança de rede e fornecem uma linha de base para avaliar a cobertura das ferramentas de segurança de uma organização. Se um relatório de uma ferramenta de segurança incorpora identificadores CVE, é possível, de forma rápida e precisa, acessar as informações de correção em um ou mais bancos de dados compatíveis com CVE para corrigir o problema. (THE MITRE CORP., 2017)

As CVE's são atribuídas por uma Autoridade de Numeração CVE (CNA). Existem três tipos principais de atribuições de números CVE:

I. A MITRE Corporation funciona como Editor e CNA Primário;
II. Várias empresas operam como CNA's e atribuem números CVE para seus próprios produtos (por exemplo: Microsoft, Oracle, HP, Red Hat, etc.)

III. Um centro de estudos e pesquisas como o CERT pode atribuir um CVE para vulnerabilidades que não foram descobertas ou analisadas por outros CNA's

Ao investigar uma vulnerabilidade ou vulnerabilidade em potencial, as CNA's ajudam a adquirir um número CVE logo no início.

4 DESENVOLVIMENTO

O Sistema escolhido para realização da abordagem prática deste trabalho foi o OSSIM em função de sua interface amigável, facilidade de instalação, capacidade de integração das diversas ferramentas e também por conta de sua eficácia para registro automático de eventos usando seu módulo de registro de bilhetes automatizado.

4.1 SOBRE SOLUÇÃO OSSIM

O nome OSSIM nada mais é que a abreviatura de *Open Source Security Information Management*. Ele foi desenvolvido pela AlienVault, e tem o objetivo de oferecer um SIEM de código aberto rico em recursos, com coleta de eventos, normalização e correlação. Lançado por engenheiros de segurança por causa da falta de produtos de código aberto disponíveis. Sendo assim, ele destina-se a fornecer aos analistas de segurança e administradores uma visão de todos os aspectos relacionados à segurança de seu sistema, combinando gerenciamento de log, gerenciamento de ativos, avaliação de vulnerabilidade, descoberta com informações de controles de segurança de informações e sistemas de detecção de intrusos dedicados. Esta informação é então correlacionada em conjunto para criar contextos para a informação não visível a partir de uma única ferramenta. (ALIENVAULT INC, 2017)

OSSIM executa essas funções usando outros conhecidos componentes de segurança de software de fonte aberta, unificando-os em uma única interface de usuário baseada em uma interface gráfica acessada via navegador. A interface fornece ferramentas de análise gráfica para informações coletadas do componente de software de código aberto subjacente (muitas das quais são apenas ferramentas de linha de comando que, de outra forma, serão registradas apenas em um arquivo de texto simples) e permitem gerenciamento centralizado de opções de configuração.

O software é distribuído livremente sob a GNU *General Public License*. Ao contrário dos componentes individuais que podem ser instalados em um sistema existente, o OSSIM

é distribuído como uma imagem ISO instalável projetada para ser implantada em um host físico ou virtual como o sistema operacional principal do host. OSSIM é construído usando a distribuição Debian GNU/Linux como seu sistema operacional subjacente.

Apesar da versatilidade e das diversas aplicações do OSSIM, este trabalho será focado apenas nas ferramentas que tem pertinência na gestão de ativos e análises de vulnerabilidades. Que são basicamente processadas pelo PRADS e o OpenVAS. Para enriquecer a abordagem prática, também serão aproveitados os recursos de geração de gráficos, geração de relatórios e de controle de bilhetes.

4.2 ARQUITETURA DA SOLUÇÃO

Conforme pode ser visualizado na figura 4-1, o OSSIM funciona como um sistema operacional em um servidor dedicado, que pode ser real ou virtual. O servidor é responsável por processar e armazenar as informações coletadas pelos sensores.

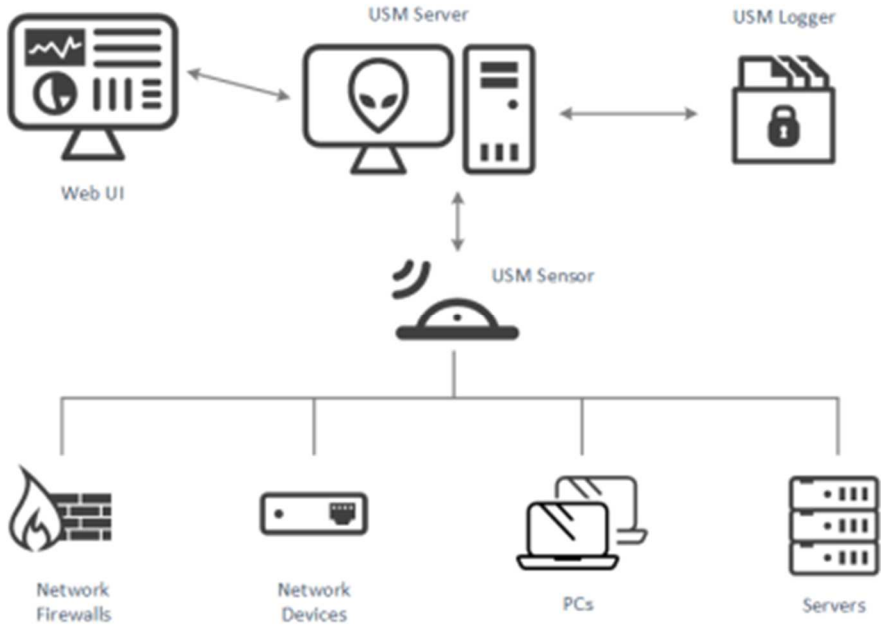

Figura 4-1 - Arquitetura do Sistema Ossim (ALIENVAULT INC, 2017)

Os sensores podem ser dispositivos de segurança que já se encontram na rede da organização como IPS, IDS, *firewalls*, entre outros dispositivos, ou pode ser as ferramentas fornecidas pelo próprio OSSIM. O servidor por padrão já é instalado com os sensores, de forma que se for do interesse da organização, na mesma imagem ISO de instalação do servidor da solução, também existe a opção de se instalar os sensores com as ferramentas que compõem o OSSIM em maquinas separadas, apenas configurando a integração entre servidor e sensor posteriormente. Esta instalação separada é interessante em estruturas grandes e complexas e tem a finalidade de descentralizar os processos com o objetivo de

desonerar os recursos do servidor que teria uma quantidade muito grande de informações para processar.

Nesta abordagem prática, por razões de limitação de recursos computacionais, o servidor e o sensor da solução foram instalados em uma única máquina virtual. Para tornar mais rica e plural o ensaio, foram configuradas diversas máquinas virtuais rodando vários sistemas operacionais diferentes e também serão realizadas análises em outros dispositivos tecnológicos conforme a tabela abaixo.

Na tabela 4-1, é possível visualizar os ativos em operação na rede analisada.

Tabela 4-1 - Relação dos ativos analisados

DISPOSITIVO	ENDEREÇO IP	SISTEMA OPERACIONAL
Roteador Wi-Fi	192.168.15.1	Linux
Notebook Macbook PRO	192.168.15.2	MacOS
Notebook Macbook PRO	192.168.15.3	MacOS
SmarTV Sony	192.168.15.4	Linux
Videogame PS4	192.168.15.5	FreeBSD
Notebook Lenovo Windows 10	192.168.15.7	Windows
Iphone 6S	192.168.15.8	IOS
Maquina Virtual Kali Linux	192.168.15.9	Kali Linux
Notebook Lenovo Windows 10	192.168.15.10	Windows
Iphone 7	192.168.15.11	IOS
Maquina Virtual Windows XP	192.168.15.12	Windows
Interface AlienVault Sensor	192.168.15.50	AlienVault OS
Máquina Virtual Windows XP	192.168.15.101	Windows
Máquina Virtual Ubuntu Mate	192.168.15.102	Linux
Interface Alienvault Servidor	192.168.15.150	AlienVault OS

4.3 IMPLANTAÇÃO DA SOLUÇÃO

A figura 4-2 exibe a tela do servidor. Todas as configurações da ferramentas e customizações podem ser realizadas desta maneira, porém, conforme pode ser observado no rodapé da tela, é possível o acesso via navegador com interface *web,* que pode ser acessado através da URL: https://192.168.15.150/ (este endereço foi configurado no ato de instalação do sistema na máquina).

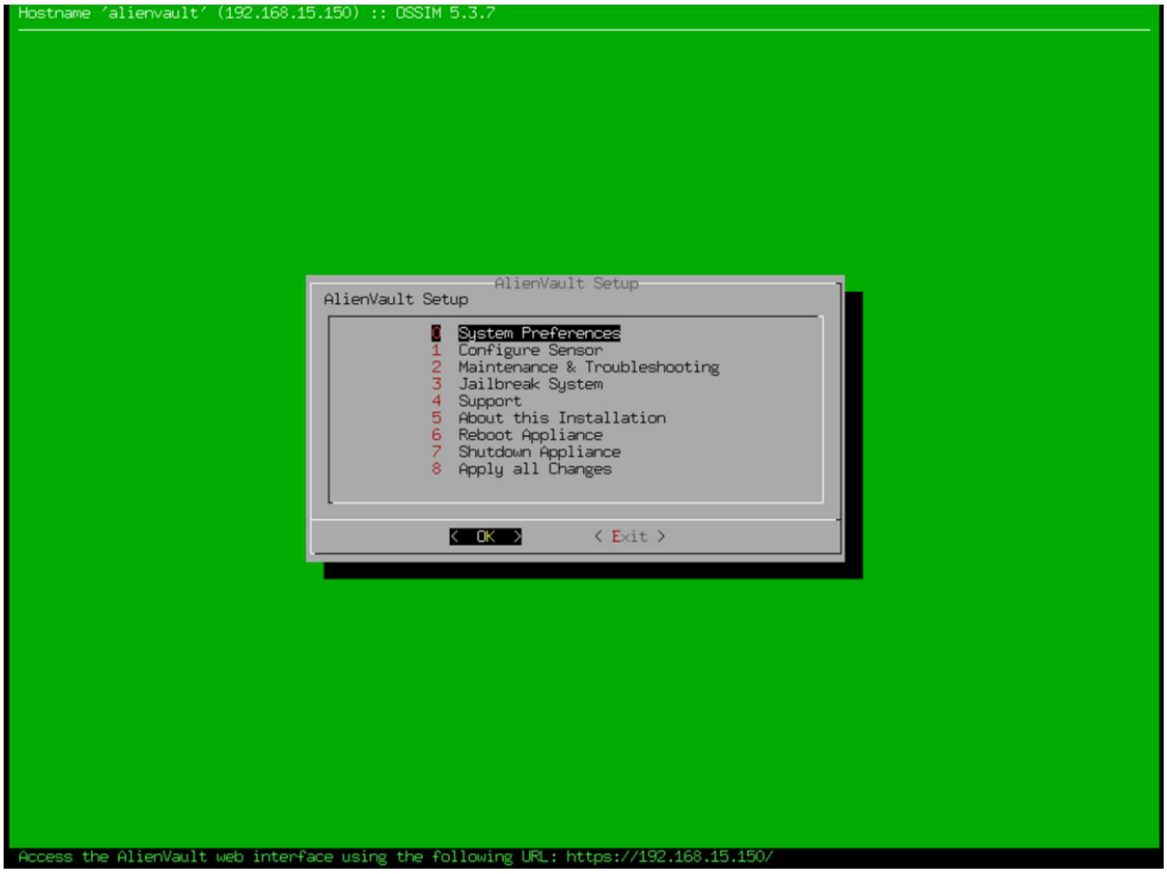

Figura 4-2 - Tela do Servidor

Acessando o servidor via navegador web, verifica-se como pode ser verificado na figura 4-3, que contém a tela com as configurações do servidor. Existe uma área dedicada a implantação do serviço que mostra um resumo da situação do servidor, inclusive com um panorama atualizado dos consumos de memória ram, *swap* e *cpu*. Como é possível visualizar, o consumo de recursos computacionais fica elevado, principalmente de memória.

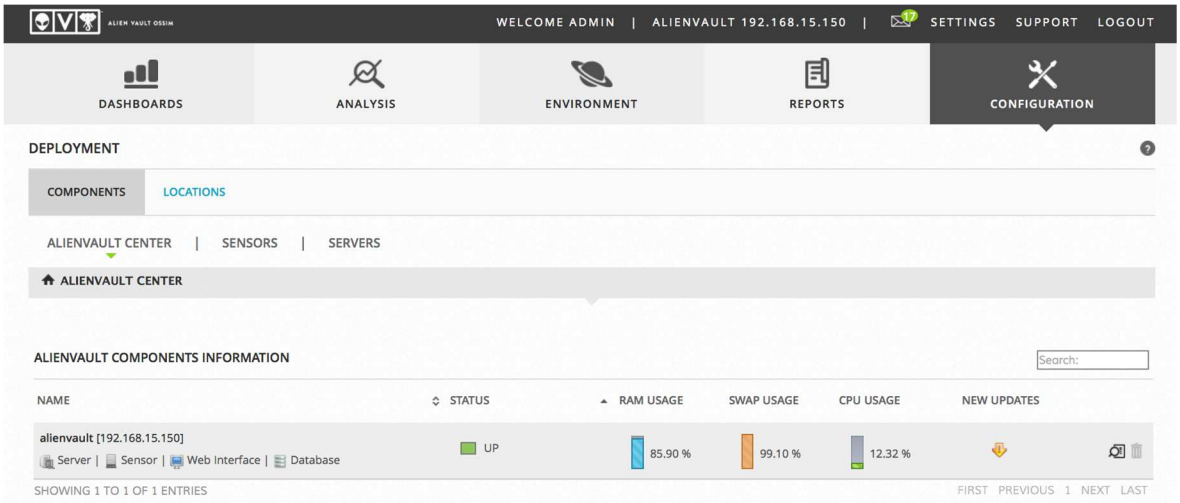

Figura 4-3 - Resumo dos componentes da solução

Ao clicar sobre o componente, abre-se uma a nova tela que está na figura 4-4, que mostra o status do geral do sistema.

Esta tela tem mais detalhes ainda sobre o sistema implementado. Aqui vê-se que existem duas interfaces de rede configuradas, onde uma é responsável pelo gerenciamento e a outra pelo gerenciamento da rede de fato. Existe uma terceira interface que se encontra desabilitada.

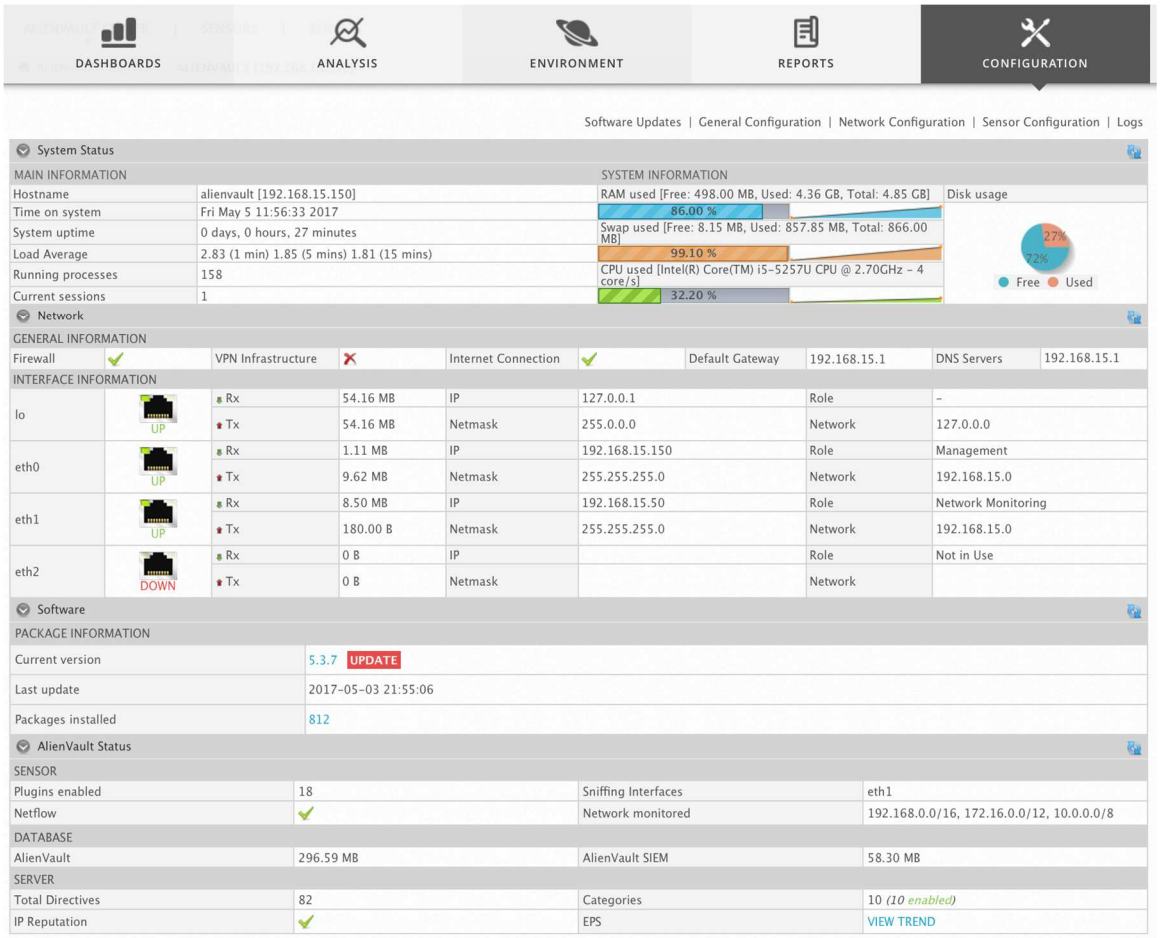

Figura 4-4 - Status do sistema

4.4 GERENCIAMENTO DOS ATIVOS

O OSSIM usa a ferramenta PRADS para efetuar descoberta de ativos na rede e usa recursos próprios para manter uma base de dados com todas estas informações. Nele também há opções de cadastrar manualmente os ativos ou criar grupos de ativos que podem ser úteis para organização de estruturas grandes e complexas.

Na figura 4-5, é possível identificar uma relação de ativos que foram descobertos na varredura da rede. Clicando sobre os ativos é possível customizar seus nomes e acrescentar diversas informações como os sistemas operacionais que estão rodando e outra informações dos serviços que eles eventualmente atendam.

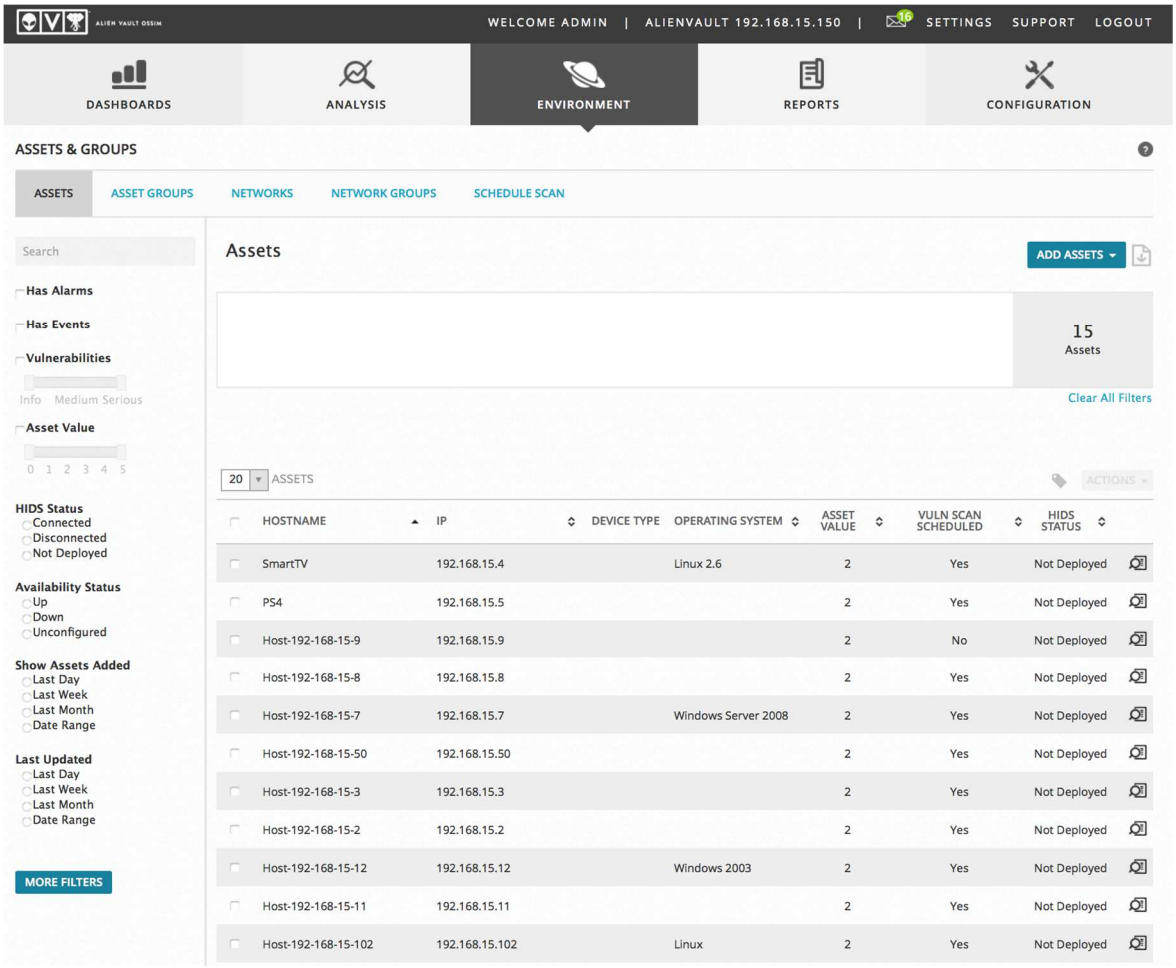

Figura 4-5 - Relação de ativos descorbertos

Com os ativos mapeados, organizados e dividido em grupos é possível programar e planejar varreduras de vulnerabilidades especificas para ativos específicos ou para um determinado grupo de ativos que compõem uma estrutura de um determinado serviço.

4.5 ANÁLISES DE VULNERABILIDADES

Para realizar as análises de vulnerabilidades o OSSIM utiliza a ferramenta OpenVAS, ela efetua as varreduras na rede conforme plano de ação acordado previamente com os intervenientes. Para isso, conforme explorado no tópico anterior, existem diversas opções de planejamento para as varreduras, inclusive há também a possibilidade de programar varreduras em horários e frequências específicas para cada ativo ou grupo de ativos automaticamente.

Na figura 4-6, é possível visualizar uma relação de vulnerabilidades realizadas no sistema. Algumas foram realizadas em apenas um ativo, outras em um grupo de ativos por isso foi retornado um número maior de vulnerabilidades e o tempo de varredura também foi mais extenso conforme pode ser verificado na relação que existe na figura.

A última coluna da relação que está na figura 4-6 acima, denominada '*actions*', é de extrema relevância para o processo pois, nela contém as opções de exportação dos relatórios preparados pelo sistema e a opção de reexecução da varredura com os mesmos parâmetros que foram utilizados da última vez.

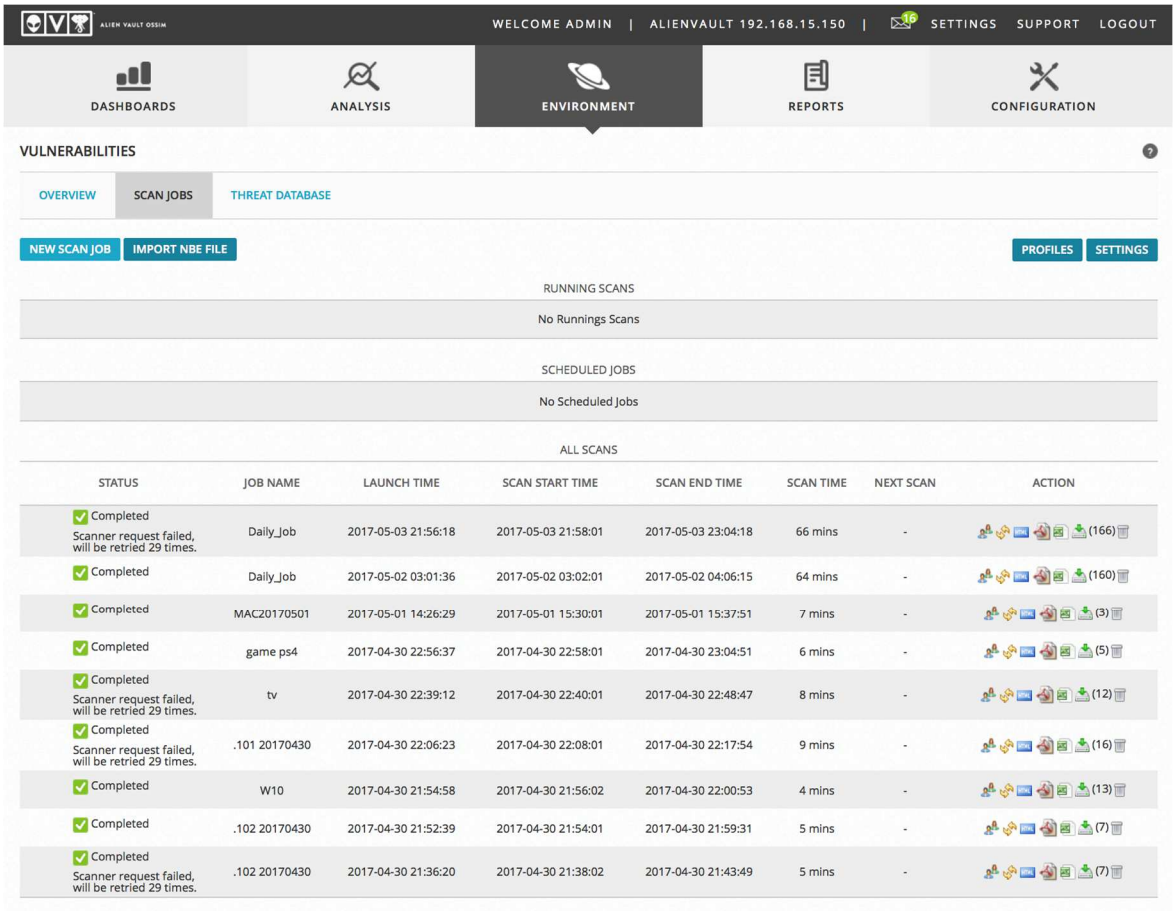

Figura 4-6 - Varreduras de vulnerabilidades realizadas

Estes relatórios produzidos pelo sistema frequentemente não são suficientes para apresentação pois, geram muitos alertas que são apenas informativos e por vezes alertas que são falsos positivos. Logo é imprescindível uma boa revisada nestes laboratórios antes de efetivamente apresenta-los aos intervenientes do processo.

Na figura 4-7, está a visão geral gerada pelo sistema para todas as varreduras executadas. Nota-se que existe um volume muito grande de alertas gerados para informação somente, estes alertas onde geralmente não requerem ações por parte dos intervenientes, em muitos casos não existe nem CVSS ou CVE associados a elas. Ainda assim o gestor de vulnerabilidades não pode se furtar de analisar caso a caso.

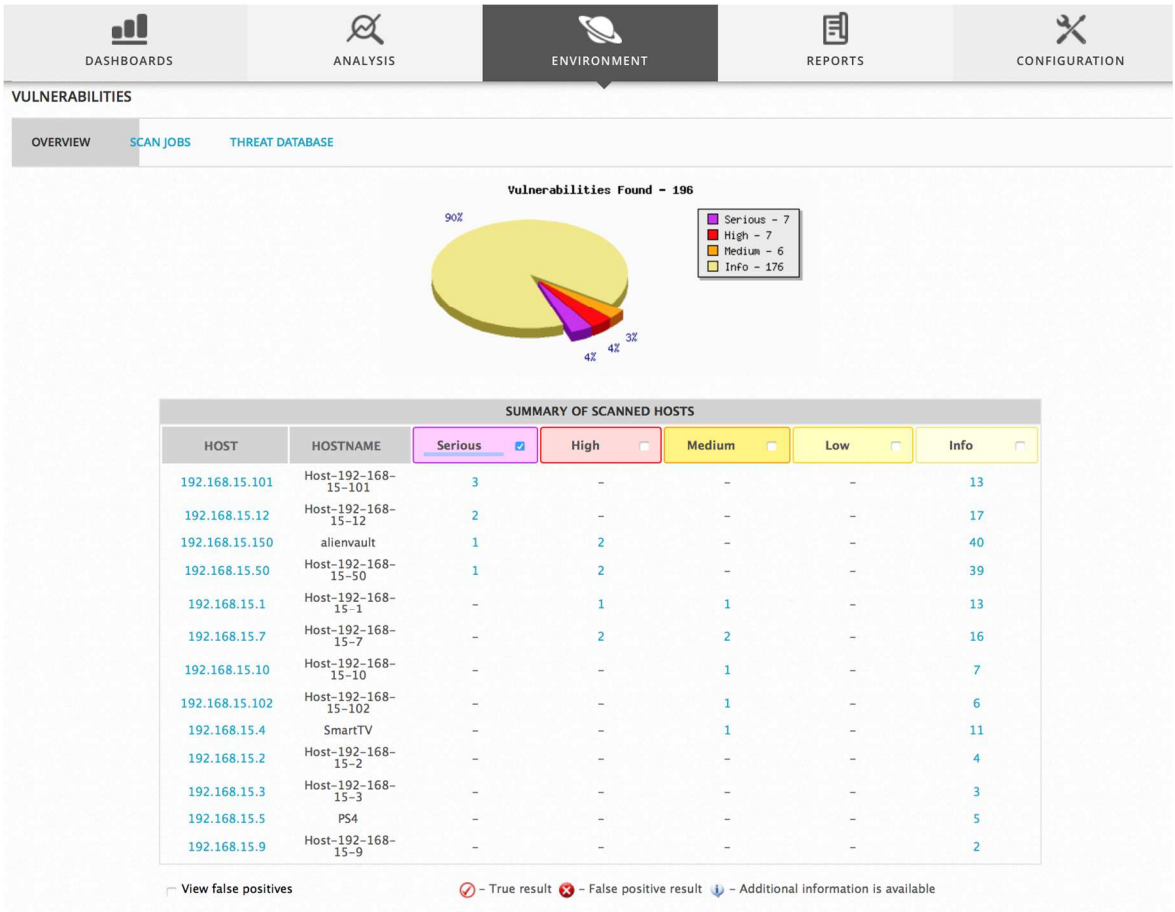

Figura 4-7 - Overview de todas as varreduras executadas

Nesta tela, que se encontra na figura 4-7, é possível verificar que há aderência nas varreduras executadas pelo sistema com os ativos levantados anteriormente. Nesta tela também há uma série de possibilidades de visualização dos relatórios. Há a possibilidade de se selecionar um host ou um nível de criticidade específicos para visualização das vulnerabilidades encontradas.

Selecionando apenas as vulnerabilidades categorizadas como '*Serious*', temos a imagem que se encontra a seguir na figura 4-8. Nela vemos uma vulnerabilidade considerada catalogada como critica conforme o CVSS, neste caso ela foi avaliada com a nota 10, que é a mais alta. Conforme pode ser observado no sumário do formulário há uma breve descrição sobre a vulnerabilidade encontrada, a solução prevista e o impacto e como esta vulnerabilidade pode ser explorada. Neste caso o sistema operacional está sem uma atualização de segurança crítica e a solução seria simplesmente proceder a atualização do sistema. Há inclusive os links com a descrição e as referências no site oficial do fornecedor. Rolando a página para baixo, o sistema vai mostrando as outras vulnerabilidades encontradas pela varredura.

Outra questão importante a ser ressaltada no formulário, são as identificações CVE associadas e esta vulnerabilidade. Conforme a figura 4-8, essas informações são mostradas quando o ponteiro do mouse fica repousado sobre a vulnerabilidade. Como já foi informado anteriormente, as identificações CVE ajudam a buscar informações sobre a vulnerabilidade e as suas correções.

Figura 4-8 – Relatório gerado pela ferramenta

Uma característica importante do sistema a ser destacada, é sobre a sua capacidade e a grande quantidade de gráficos que ela é capaz de gerar. Logo na tela de início do aplicativo já existe um painel de controle com alguns gráficos gerenciais conforme pode ser observado na figura 4-9. Estes gráficos não são especificamente de vulnerabilidades, porém, são interessantes para mostrar a capacidade de a ferramenta relacionar eventos, uma vez que, apenas com as funcionalidades de controle de ativos e de análises de vulnerabilidades configuradas ele já foi capaz de gerar alguns gráficos com informações relevantes.

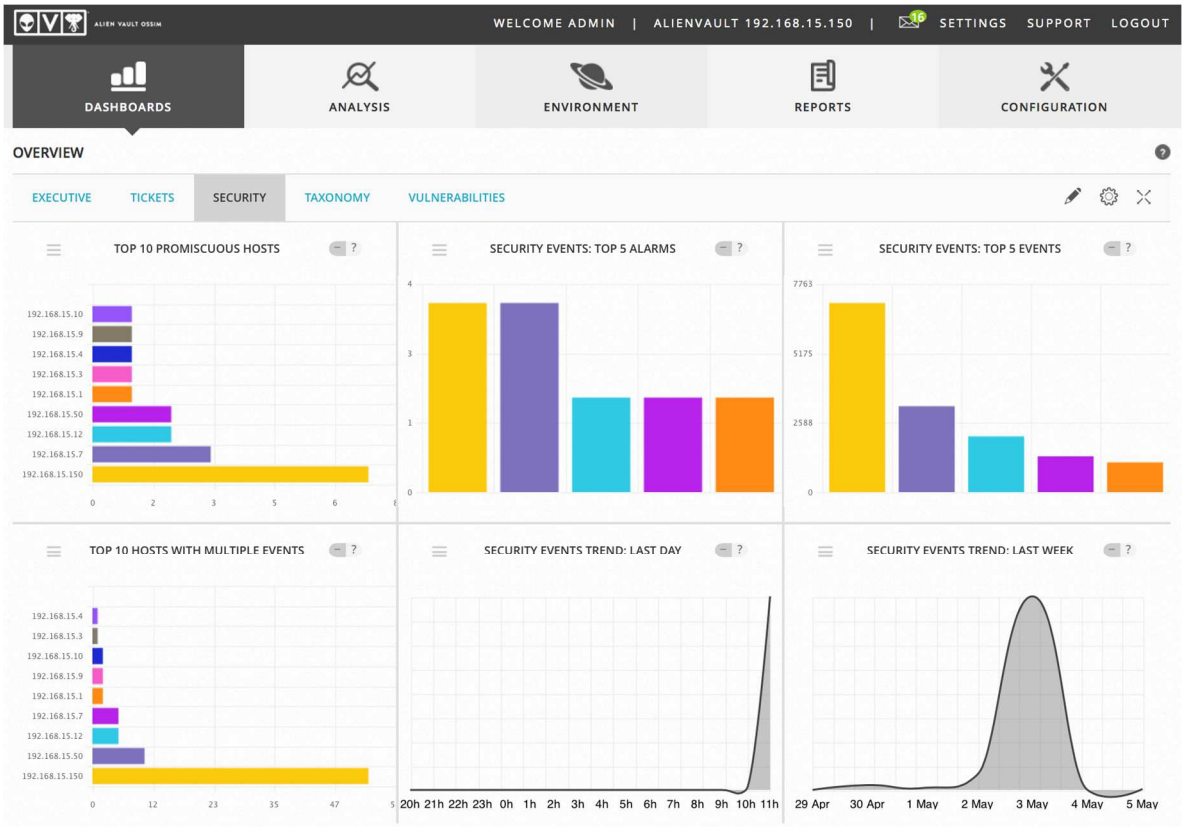

Figura 4-9 - Painel de controle com gráficos gerenciais de eventos de segurança

As informações em forma de gráficos são fundamentais para se ter um panorama atual sobre como esta toda a estrutura. Desta maneira é possível identificar pontos fortes, pontos fracos, oportunidade e ameaças e auxiliar o processo de tomada de decisões estratégicas pelas áreas gerenciais.

A próxima imagem na figura 4-10 estão os gráficos específicos sobre os bilhetes. Informando inclusive tempo de resolução e o volume de bilhetes fechado por mês.

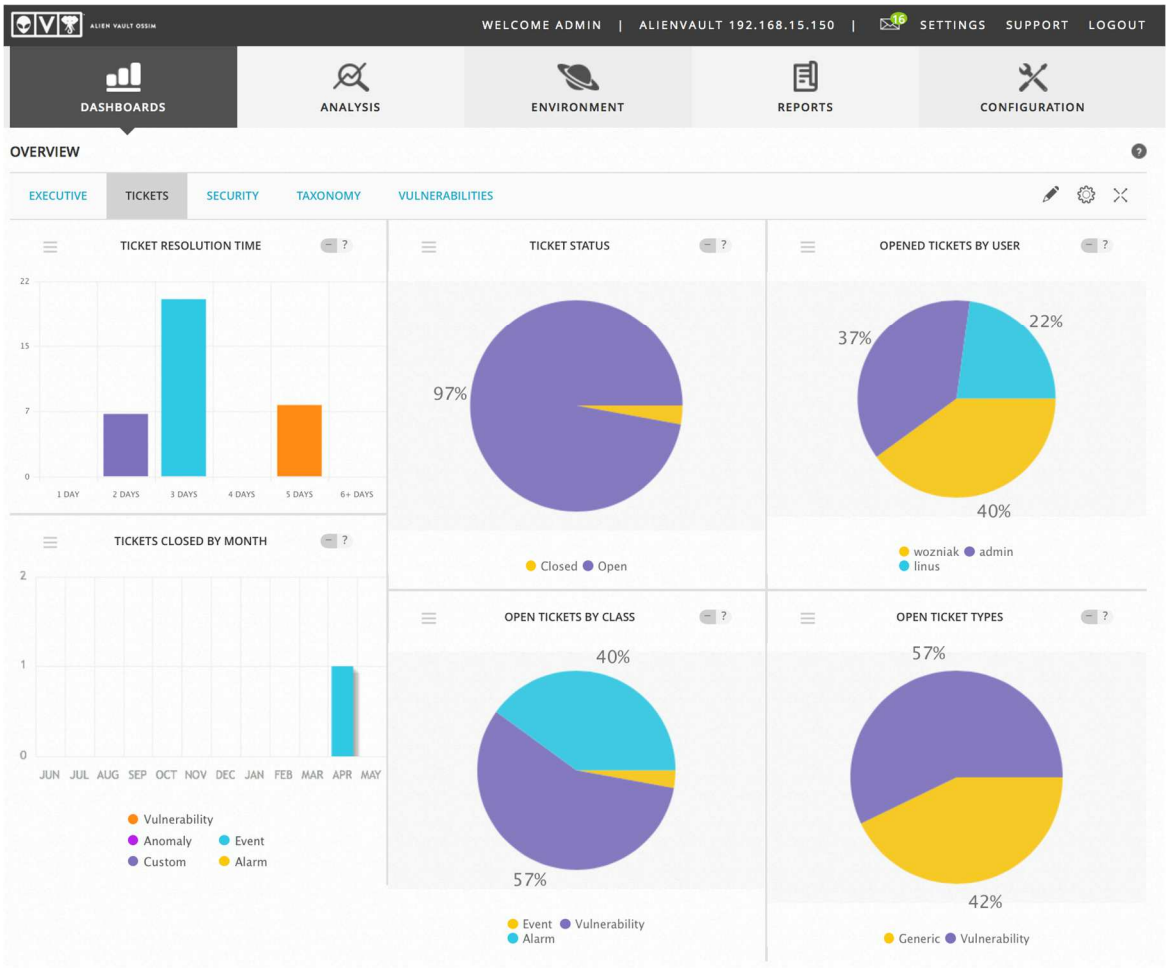

Figura 4-10 - Painel de controle especifico sobre bilhetes

Todos os recursos são notáveis, porém é importante não perder o foco deste trabalho que é a gestão de vulnerabilidades, e como seria de se esperar, a ferramenta tem a capacidade de gerar diversos gráficos a cerca deste tema. Na figura 4-11 é possível observar o gráfico que mostra as vulnerabilidades classificadas conforme sua severidade e uma classificação de maquinas maior número de vulnerabilidades. Estes controles são importantes para esclarecer e contextualizar a situação de algumas determinadas vulnerabilidades dentro do universo descoberto pelas varreduras. No caso especifico desta abordagem prática, nota-se que há muitos eventos de informação apenas, e os casos de severidade maior não representam uma porcentagem elevada das ocorrências. Desta maneira é possível concentrara a força de trabalho para atuar em eventos mais severos ou não dependendo da prioridade da organização e ainda programar o prazo para correções.

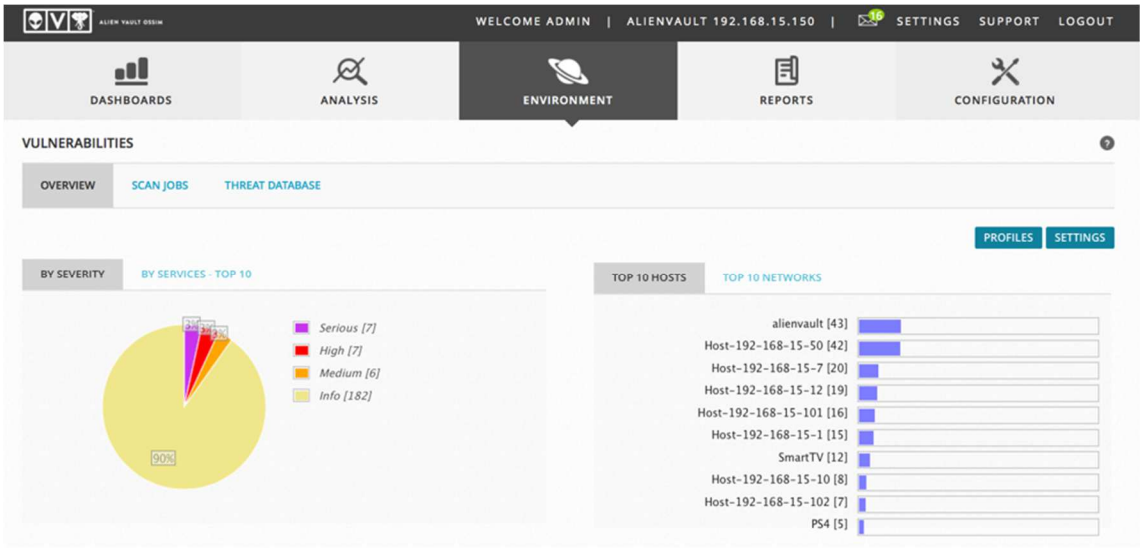

Figura 4-11 - Gráfico de vulnerabilidades por severidade

A figura 4-12 mostra o gráfico que expressa as vulnerabilidades por serviços afetados e pode ser útil para medir a vulnerabilidade de um determinado serviço e estudar maneiras de torná-lo menos vulnerável.

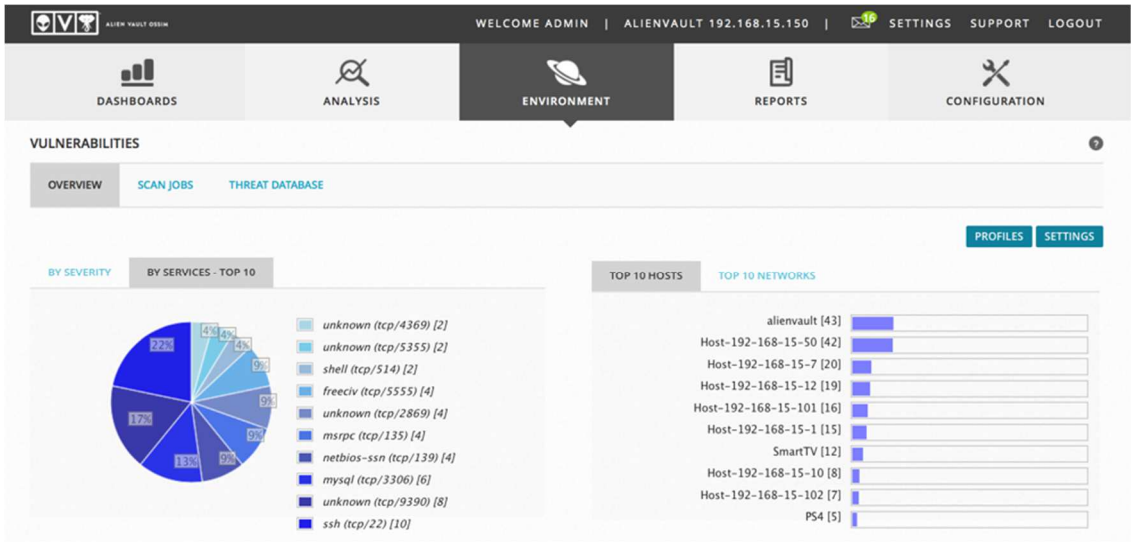

Figura 4-12 - Gráfico de vulnerabilidades por serviços

O último recurso do OSSIM utilizado para apoio da gestão de vulnerabilidades é o componente responsável por gerenciar os bilhetes de segurança. Desde que devidamente configurado, ele é capaz de abrir automaticamente bilhetes para os mais diversos eventos de segurança que ocorrem na estrutura. Inclusive para vulnerabilidades encontradas através das varreduras efetuadas pelo sistema.

A figura 4-13 tem a relação dos bilhetes abertos para alguns alarmes de segurança e também para as vulnerabilidades encontradas, é possível identificar os números associados a cada bilhete bem como sua prioridade conforme CVSS, data de abertura com contagem de tempo, o responsável, e a ferramenta que identificou o evento e o status atual.

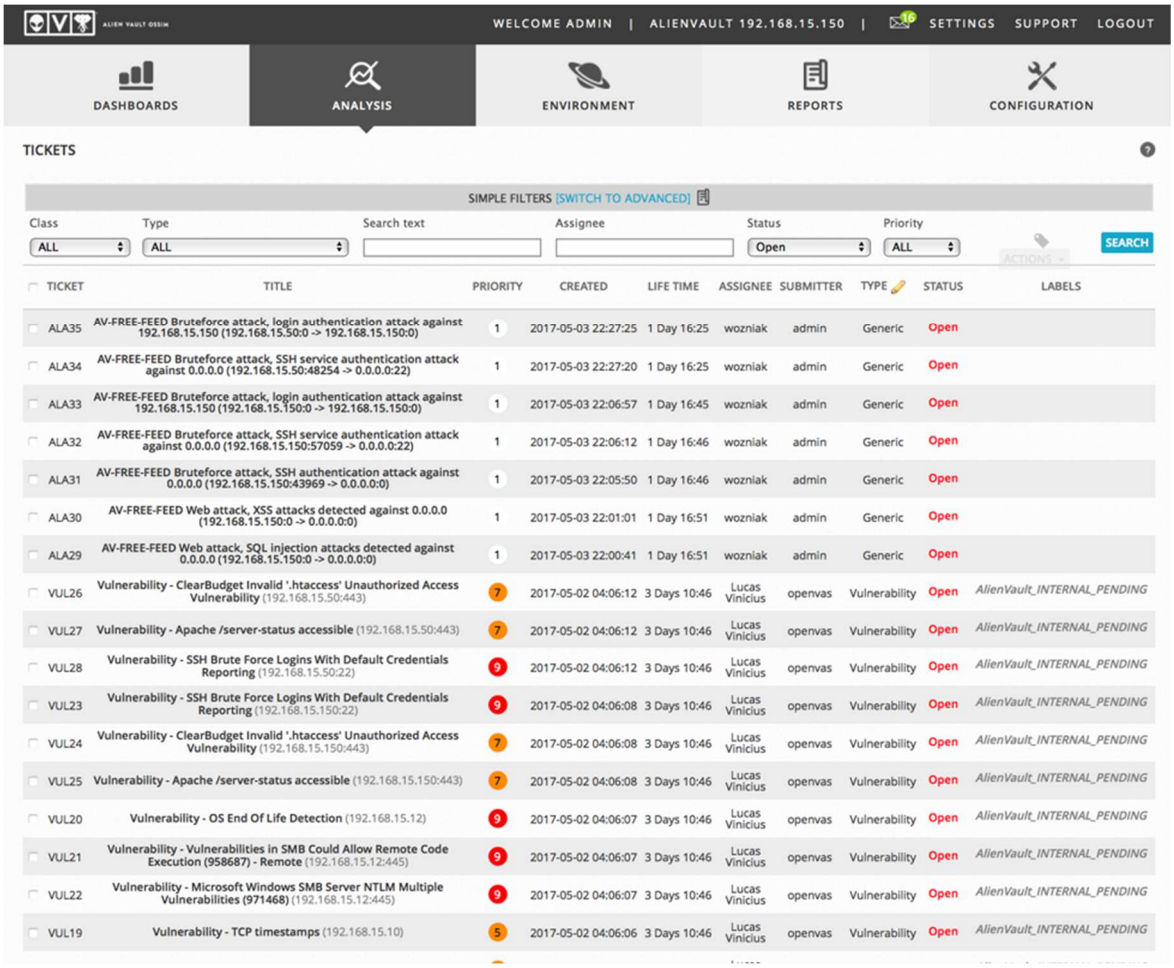

Figura 4-13 - Relação de bilhetes abertos no sistema

A figura 4-14 mostra os detalhes da vulnerabilidade ‘VUL21’. Esta vulnerabilidade é a mesma mostrada na figura 4-8 onde é mostrado o relatório produzido pelo sistema, então contêm basicamente as mesmas informações, sendo que este bilhete aberto tem um campo especifico e ele pode ser alimentado com informações adicionais para o tratamento e registro do ciclo de vida da vulnerabilidade desde a sua descoberta até a sua mitigação.

Os bilhetes ainda podem formar uma base de dados para consultas posteriores e formar uma base de conhecimento para futuras análises.

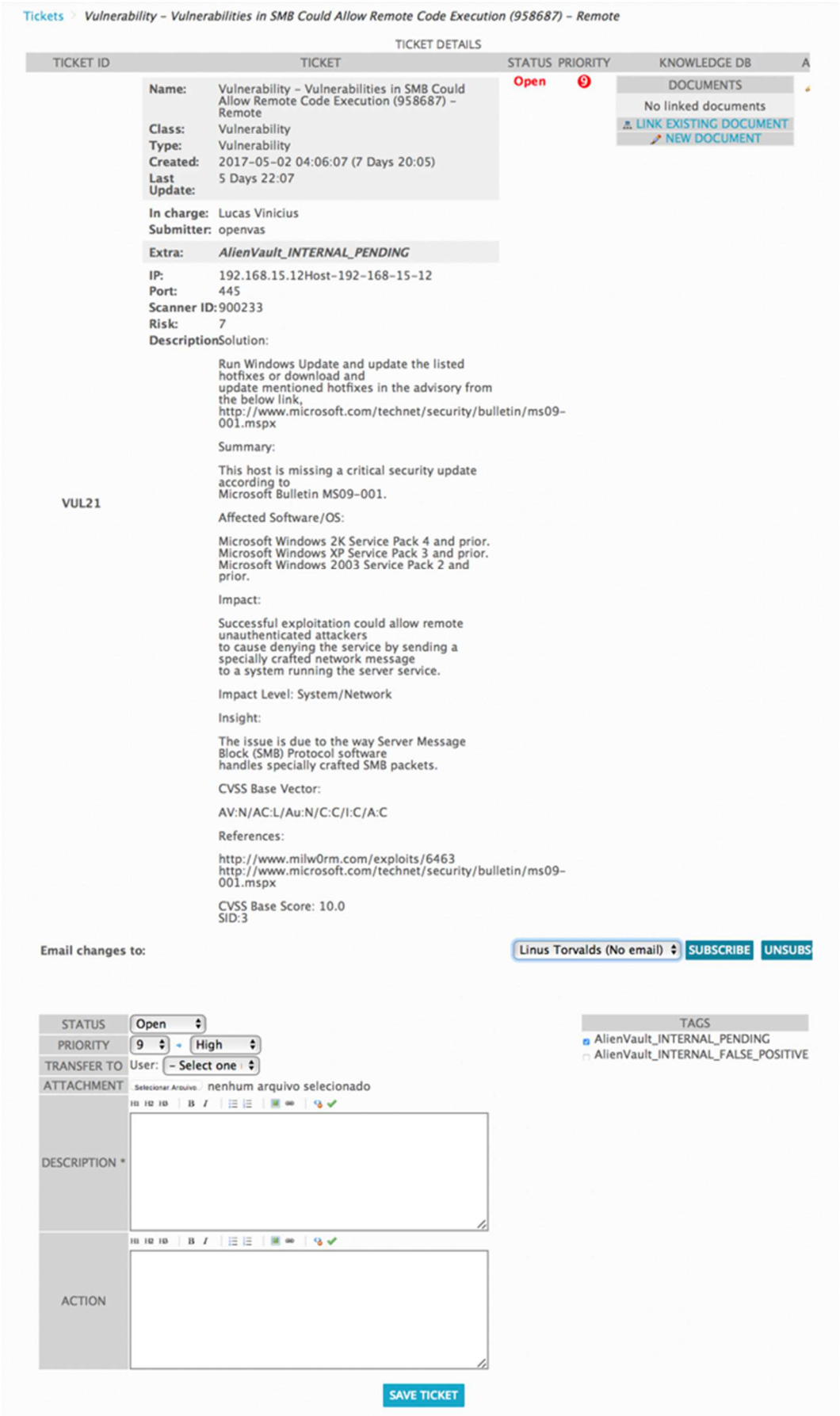

Figura 4-14 - Bilhete aberto automaticamente para tratamento da vulnerabilidade

5 CONCLUSÃO

O crescente uso dos meios digitais para realização de diversas tarefas profissionais e também os pessoais terminou por estimular uma crescente demanda por novos dispositivos, novas tecnologias e novas plataformas que pudessem suportar essa crescente exigência por recursos. Consoante a esta massificação do uso das tecnologias, houve a migração de algumas adversidades da vida concreta para o ambiente virtual. Problemas como furtos, estelionatos e extorsão podem ocorrer através da internet e causar inúmeros prejuízos as organizações. Desta maneira, a segurança da informação ganhou destaque e virou um tema imprescindível na gestão corporativa. Dentro deste contexto a gestão de vulnerabilidade acabou se destacando pois torna-se cada vez mais importante tentar se antecipar a eventuais falhas de segurança oriundas de exploração de vulnerabilidades em softwares e dispositivos de terceiros.

A gestão de vulnerabilidades é a prática cíclica de identificar, classificar, remediar e mitigar vulnerabilidades. O gerenciamento de vulnerabilidade é essencial para a segurança das organizações e de seus ativos.

De forma que; percebendo que este assunto é fundamental para manter as organizações seguras de uma forma cautelar, este trabalhou se dedicou a explorar o tema e todos os seus aspectos de maneira profunda para entender quais sãos suas particularidades, características e propor uma solução integrada para realizar a gestão de vulnerabilidades de sistemas e de infraestruturas atravessando todas as etapas dos ciclos de vida dos processos estudados.

Para propor esta solução foi essencial estudar, fundamentar e consolidar alguns conceitos, elaborar um plano de gestão, definir o ciclo de vida dos processos, analisar as técnicas existentes para controle de vulnerabilidades, e conhecer as ferramentas disponíveis no mercado e suas características para aferir quais seriam as mais eficientes trabalhando de forma integradas.

Ao longo dos estudos e do desenvolvimento do projeto, foi descoberta o *framework* OSSIM. Ele é classificado como um *SIEM* de código aberto que trabalha com a integração de diversas ferramentas de segurança e tem um potencial de gestão de segurança muito grande e promissor pois emite diversos relatórios e gera muitas informações visuais que auxiliam e facilitam a gestão de diversos aspecto da segurança da informação inclusive a gestão de vulnerabilidades que foi o foco.

Foi implantado a parte do sistema que faz a gestão de vulnerabilidades e de ativos. Foi possível efetuar varreduras buscando por ativos e vulnerabilidades em uma rede, classificar sua severidade baseada em um sistema de avaliação e pontuação CVSS, foi permitida a emissão de relatórios preliminares e geração de bilhetes para tratamento e mitigação das vulnerabilidades de forma automática.

Em função de problemas relacionados aos recursos computacionais disponíveis para implementação do sistema não possível implantar os outros disponíveis no sistema OSSIM, desta maneira, uma sugestão para trabalho futuro seria a implementação do sistema completo em uma infraestrutura mais robusta para analisar melhor a capacidade dele de correlacionar eventos de segurança e quais seriam os eventuais ganhos que este processo poderia agregar as organizações.

Outra questão relacionada as vulnerabilidades com potencial para investigação em um trabalho futuro seria a busca por técnicas de identificação e mitigação de vulnerabilidades *zeroday*, que são as vulnerabilidades com código de exploração extremamente pouco divulgado ou que ainda não tem nenhum código de exploração mas tem potencial devastador. Esta temática seria pertinente pois, a medida que a gestão de vulnerabilidade é difundida, os indivíduos maliciosos buscarão explorar vulnerabilidades cada vez mais exclusivas, que sejam recém descobertas, e foram pouco divulgadas.

6 REFERÊNCIAS

ALIENVAULT INC. (2017). *About USM Appliance System Architecture and Components*. Acesso em 16 de Maio de 2017, disponível em https://www.alienvault.com/documentation/usm-appliance/system-overview/about-usm-architecture-components.htm

ALIENVAULT INC. (2017). *OSSIM: The Open Source SIEM.* Acesso em 15 de Maio de 2017, disponível em https://www.alienvault.com/products/ossim

AVYAAN LABS. (10 de Setembro de 2014). *Vulnerability Assesment vs Penetration Testing - A Comparative Study.* Acesso em 17 de Maio de 2017, disponível em Avyaan Labs Infosec: https://pt.slideshare.net/Avyaansecurity/avyaan-vulnerabilityassessmentpentesting

BUZZATTE, P. M. (s.d.). Análise de Vulnerabilidades através de scanners detectores. *Dissertação para obtenção do grau de Tecnólogo em Redes de Computadores*. Santa Maria, RS, Brasil.

CERT.br. (10 de Outubro de 2007). *Honeypots e Honeynets: Definições e Aplicações*. Acesso em 16 de Maio de 2017, disponível em https://www.cert.br/docs/whitepapers/honeypots-honeynets/

COG SECURITY. (2016). Acesso em 29 de Abril de 2017, disponível em Cog Security – Experienced Consultancy: https://www.cog-security.com/wp-content/uploads/2016/05/process2.png

DANTAS, M. L. (2011). *Segurança da informação: uma abordagem focada em gestão de riscos*. Olinda, PE, Brasil: Livro Rápido – Elógica.

ESR RNP. (19 de Outubro de 2015). *Workshop Gestão de Vulnerabilidades de Segurança.* Acesso em 05 de Maio de 2017, disponível em 21º Seminário RNP de Capacitação e Inovação: https://esr.rnp.br/sci38/rnp-201510.1618

FEBRABAN. (2017). *Pesquisa FEBRABAN de Tecnologia Bancária 2017.* Acesso em 31 de Maio de 2017, disponível em https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20FEBRABAN%20de%20Tecnologia%20Banc%C3%A1ria%202017.pdf

FIRST. (1995). *Common Vulnerability Scoring System.* Acesso em 13 de Maio de 2017, disponível em https://www.first.org/cvss

FOREMAN, P. (2010). *Vulnerability Management.* Boca Raton, FL, Estados unidos: Taylor and Francis Group, LLC.

GATFORD, C., GOLD, A., & MANZUIK, S. (2007). *Network Security Assessment: From Vulnerability to Patch.* Rockland, MA, Estados Unidos: Syngress Publishing, Inc.

GHEORGHE, A. V. (2005). *Integrated Risks and Vulnerability Managment Assisted by Decision Support Systems.* Dordrecht, Holanda: Springer.

KANDEK, W. (2015). *Vulnerability Management For Dummies.* West Sussex, Inglaterra: John Wiley & Sons, Ltd.

NBR ISO/IEC 27001. (2006). *Sistemas de gestão de segurança da informação.*

NBR ISO/IEC 27002. (2013). *Código de Prática para Controles de Segurança da Informação.*

NBR ISO/IEC 27005 . (2008). *Gestão de Riscos de Segunrança da Informação.*

NIST U.S. (2017). *CVSS Severity Distribution Over Time*. Acesso em 31 de Maio de 2017, disponível em https://nvd.nist.gov/vuln-metrics/visualizations/cvss-severity-distribution-over-time

OLLMAN, G. (s.d.). *Old Threats*. Acesso em 01 de Maio de 2017, disponível em Technical Info - Making Sense of Security: http://www.technicalinfo.net/papers/OldThreats.html

PELTIER, T. R., JUSTIN, P., & A., B. (2003). *Managing a Network Vulnerability Assessment.* Boca Raton, FL, EUA: CRC Press.

RFC 2828. (2010). *Glossário de Segurança de Internet.* (Internet Engineer Task Force (IETF)) Acesso em 09 de Maio de 2017, disponível em http://www.ietf.org/rfc/rfc2828.txt

ROSA, R. V. (2011). Análise de técnicas de correlação e visualização de informações através de um estudo de caso da ferramenta OSSIM. *Dissertação para obtenção do grau de Engenheiro de Redes de Computadores*. Brasilia, DF, Brasil.

SILVA, P. T., CARVALHO, H., & TORRES, C. B. (2003). *Segurança dos Sistemas de Informação – Gestão Estratégica da Segurança Empresarial.* Lisboa: Centro Atlântico Ltda.

SYMANTEC. (2017). Internet Security Threat Report - ISTR 2017. Moutain View, CA, Estados Unidos.

TAVARES, L. A. (2015). Análise de eventos de segurança: baseado no OSSIM. *Dissertação para obtenção do grau de Mestre em Engenharia da Computação*. Braga, Portugal.

TCU (Tribunal de Contas da União). (2012). *Boas Práticas de Segurança da Informação 4. ed.* Brasília, DF, Brasil: TCU - Secretaria de Fiscalização de Tecnologia da Informação.

THE MITRE CORP. (2017). *Common Vulnerabilities and Exposures*. Acesso em 14 de Maio de 2017, disponível em https://cve.mitre.org/

WEIDMAN, G. (2014). *Penetration Testing - A Hands-On Introduction to Hacking*. San Francisco, CA: No Starch Press, Inc.

WILLIAMS, S. (2011). *Network Security Essentials: Applications and Standards 4. Ed.* Estados Unidos: Prentice Hall.