Análise de Vulnerabilidade utilizando a ferramenta OpenVAS

Luiz F. F. Irineu, Lucas S. Vaz, Matheus B. Teixeira, Evandro C. Vilas Boas, Francisco A. S. do Carmo
Laboratório de Cyber Segurança e Internet das Coisas (CS&I Lab.), Instituto Nacional de Telecomunicações - Inatel
luizirineu@get.inatel.br, lucas.vaz@get.inatel.br, matheus.braga@get.inatel.br, evandro.cesar@inatel.br, francisco.assis@inatel.br

***Abstract*—This work presents a brief tutorial for using the OpenVAS tool to search and analyze vulnerabilities in telecommunications systems and networks. It demonstrates how to create a new analysis by configuring the tool, includes a specific target, performs the analysis, and extract the results report. It also discusses some important points of the report. The tutorial represents a summary of an experiment prepared for the discipline of Network Management and Security at Inatel (National Telecommunications Institute), whose objective is to provide the reader's understanding of issues related to criticality and risk of the vulnerabilities present in computer systems and telecommunications networks.**

***Index Terms*—Cyber security, OpenVAS, Vulnerability assessment.**

***Resumo*—Esse trabalho apresenta um breve tutorial para uso da ferramenta OpenVAS na busca e análise de vulnerabilidades em sistemas ou redes de telecomunicações. Demonstra-se como configurar a ferramenta para criar uma nova análise, incluir um determinado alvo, executar a análise e extrair o relatório com resultados. Assim como, analisam-se alguns pontos importantes do relatório. O tutorial representa um resumo de um caderno elaborado para a disciplina de Gerência e Segurança de Redes do Inatel (Instituto Nacional de Telecomunicações), cujo objetivo é proporcionar a compreensão do leitor às questões relacionadas à criticidade e ao risco da presença de vulnerabilidades nos sistemas computacionais e nas redes de telecomunicações.**

***Palavras chave*—Análise de vulnerabilidades, OpenVAS, segurança cibernética.**

I. Introdução

A digitalização da informação e o seu acesso via redes de computadores ou Internet abriu precedentes para o uso indevido de dados e práticas maliciosas que levam a inoperabilidade de sistemas. Dessa forma, surgiu no âmbito da segurança da informação a segurança cibernética. Esse ramo dedica-se a análise e adequação dos sistemas de telecomunicações para a proteção de ativos de empresas e dados pessoais [1]. Nesse contexto, desenvolveram-se ferramentas para auxílio na análise de vulnerabilidades de sistemas e redes de telecomunicações.

Define-se a vulnerabilidade de um sistema ou rede de telecomunicações como a incapacidade de responder de forma adequada à uma ameaça ou tentativa de invasão [1]. No âmbito da segurança cibernética, uma vulnerabilidade permite que atacantes realizem algum dano ao meio tecnológico em questão, inclusive ao operador ou consumidor desse meio. A vulnerabilidade se relaciona diretamente à falta de proteção, à exposição ou à crença de segurança tanto nos operadores quanto nos dispositivos de um sistema ou rede de telecomunicações [1, 2]. A análise de vulnerabilidades identifica, quantifica e prioriza a fragilidade desses sistemas e redes com o objetivo de tornar sua segurança mais robusta, sendo uma prática em ambientes de TIC (Tecnologia da Informação e Comunicação).

A análise de vulnerabilidade difere-se de outras práticas como os testes de intrusão/penetração em sistemas (Pentest) [1, 3]. O Pentest explora táticas específicas de invasão e estabelece um conjunto de etapas (reconhecimento, varredura, enumeração, exploração, elevação de privilégios e eliminação de rastros) para explorar um sistema ou rede de telecomunicações. Enquanto a análise de vulnerabilidades realiza um mapeamento e um cruzamento de informações encontradas com as bases de vulnerabilidades mundialmente conhecidas, identificando brechas existentes em um determinado sistema. Dentre as ferramentas desenvolvidas para a análise de vulnerabilidades, citam-se a OpenVAS, Tripwire IP360, Nessus Vulnerability Scanner, Comodo HackerProof, Nexpose community e Nikto [4, 5, 6, 7].

Esse trabalho explora a ferramenta OpenVAS (Open Vulnerability Assessment System) para demonstrar a execução de uma análise de vulnerabilidade [4, 5, 7]. O OpenVAS é um sistema de código aberto e bibliotecas públicas destinado à verificação e varredura de protocolos, serviços e portas abertas em um *host* alvo (computador, *smartphone* ou outro dispositivo computacional). Essa ferramenta elenca um conjunto de informações por meio da varredura e identificação destes protocolos, portas e serviços. Em seguida, comparam-se esses resultados às bases mundiais de vulnerabilidades, que se encontram disponíveis e atualizadas na ferramenta. Dentre as bases, têm-se as CVEs (*Common Vulnerabilities Exposures*) que são vulnerabilidades identificadas por qualquer cidadão, em sua maioria pesquisadores, e validadas pelo Mitre, órgão associado à Agência Nacional de Segurança Cibernética dos Estados Unidos. Também estão presentes nas bases da ferramenta as NVDs (*National Vulnerabilities Databases*) que são informações de vulnerabilidades reportadas e identificadas pelo governo dos Estados Unidos em parceria com o NIST (*Natitonal Institute of Security Technology*). Ressalta-se que países, organizações e projetos de segurança cibernética de todo o mundo contribuem para a formação dessas bases mundialmente utilizadas.

Estruturou-se esse tutorial em quatro seções. Na Seção II, especificam-se os sistemas utilizados para instalar a ferramenta, exploram-se alguns aspectos da ferramenta e como incluir o alvo para análise. Na Seção III, avaliam-se os resultados contidos no relatório de vulnerabilidade. Dispõe-se as conclusões e principais comentários na Seção IV.

II. Análise de vulnerabilidades com OpenVAS

Nessa seção, demonstram-se os passos para configurar o alvo para análise, como executá-la e gerar o relatório.

A. *Configurações iniciais e inclusão de alvo*

Dispõe-se os passos para a inclusão de alvos de análise em uma rede de computadores e modelos de análises possíveis. Para ambientar o leitor, descreve-se as configurações do ambiente utilizado para a realização do experimento:

- Sistema Operacional VWMare Vsphere ESXi versão 7.0;
- Virtual Apliance da ferramenta OpenVAS (arquivo OVA);

Instalou-se o sistema operacional em um servidor Dell Power Edge R430 Series. O arquivo OVA é preparado exclusivamente para ser importado dentro do ambiente do sistema operacional compondo uma máquina virtual que já tenha a ferramenta OpenVAS previamente instalada [5]. Existe a possibilidade de instalação da ferramenta em sistemas operacionais Linux diversos com base em repositórios públicos disponíveis no Github.com. No entanto, esta não é uma boa prática de segurança. A distribuição oficial da ferramenta OpenVAS pode ser encontrada no site (https://www.greenbone.net/en/testnow/), sendo utilizada nesse trabalho. Após a importação do arquivo OVA no ambiente, inicia-se a máquina virtual que contém o OpenVAS. Utiliza-se o endereço IP dessa máquina virtual para acessar o OpenVAS em uma segunda máquina via navegador web. Na Figura 1, visualiza-se a página de *login* da ferramenta.

Fig. 1. Tela de *login* do OpenVAS.

As credencias de *login* são padrão para o sistema (usuário = admin e senha = newpassword). Após o primeiro acesso, recomenda-se alterá-las para maior segurança do usuário. Após efetuado o *login*, tem-se uma tela de configurações do sistema, conforme visto na Figura 2. Identificam-se quatro gráficos indicados com as setas vermelhas: gráficos de atualizações de CVEs e NVDs e os serviços de tarefas de busca e identificação de vulnerabilidades.

Para incluir um ou mais alvos, seleciona-se o item ”Task”e cria-se uma nova ”Task”por meio da tela mostrada na Figura 3(a). Para isso configuram-se alguns campos dessa tela conforme especificado:

- *Name* = criar um nome sugestivo para a tarefa;
- *Scan Targets* = será o alvo propriamente dito, um endereço IP ou uma URL;
- *Scanner* = mantém-se o modo ”OpenVAS Default”;
- *Scan Config* = opta-se pelo modo ”Full and Very Deep”;

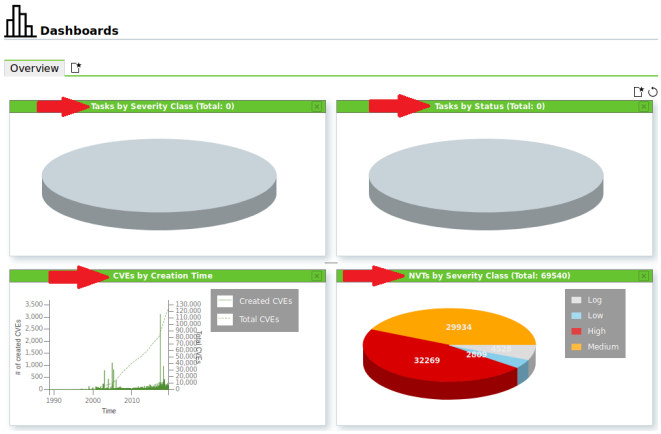
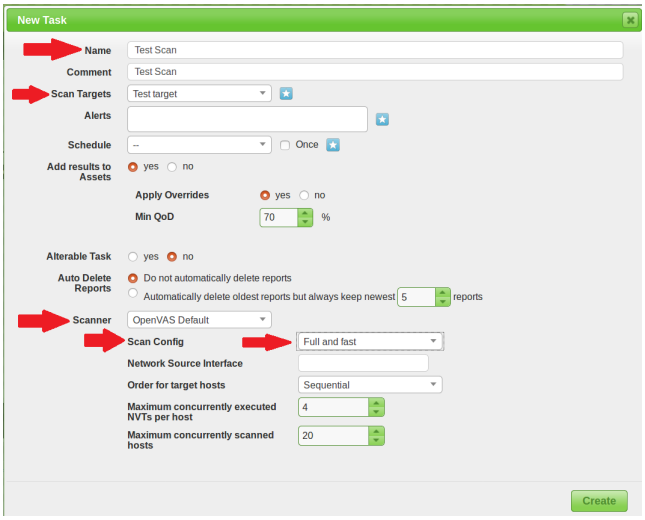
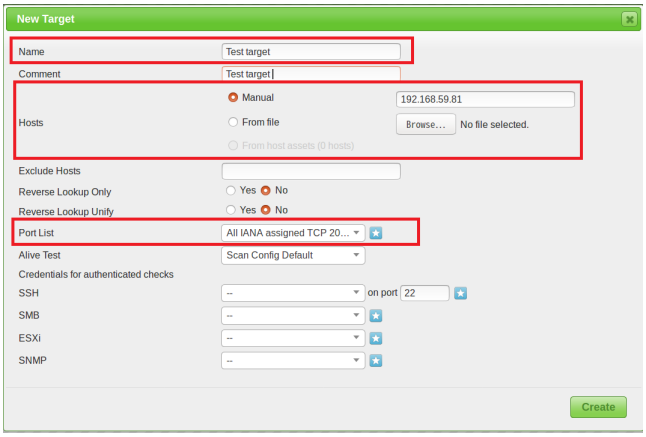


Fig. 2. Tela inicial do sistema OpenVAS.

Para incluir o IP ou URL do alvo para a análise de vulnerabilidades, deve-se clicar no ícone em estrela localizado à frente do campo *Scan Targets* para habilitar uma segunda janela de diálogo como visto na Figura 3(b).



(a)



(b)

Fig. 3. Configurando uma nova análise de vulnerabilidade (a) Tela para criação de uma nova ”Task”e (b) Tela para inclusão do IP ou URL alvo.

Nessa tela, configuram-se alguns campos, conforme indicado:

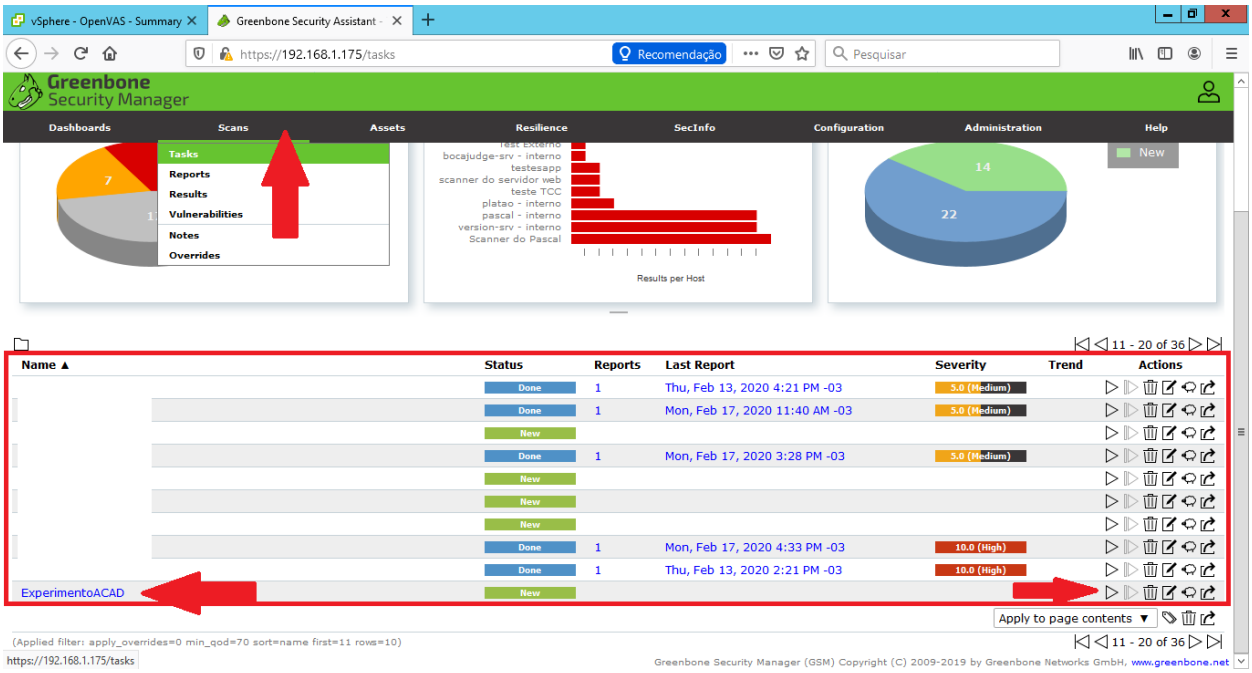


Fig. 4. Tela de *login* do OpenVAS.

- Name = criar um nome sugestivo para o host alvo;
- Hosts = será o alvo propriamente dito, um endereço IP ou uma URL a ser avaliado;
- Port List = por padrão vamos manter “All IANA assigned TCP 20...”

Em seguida, clica-se no botão “Create”para retornar para a tela de criação de uma nova tarefa, onde o nome do alvo já estará no campo “Scan Targets”. Finaliza-se a configuração da nova “Task”clicando no botão “Create”dessa tela.

B. Iniciando a análise de vulnerabilidades

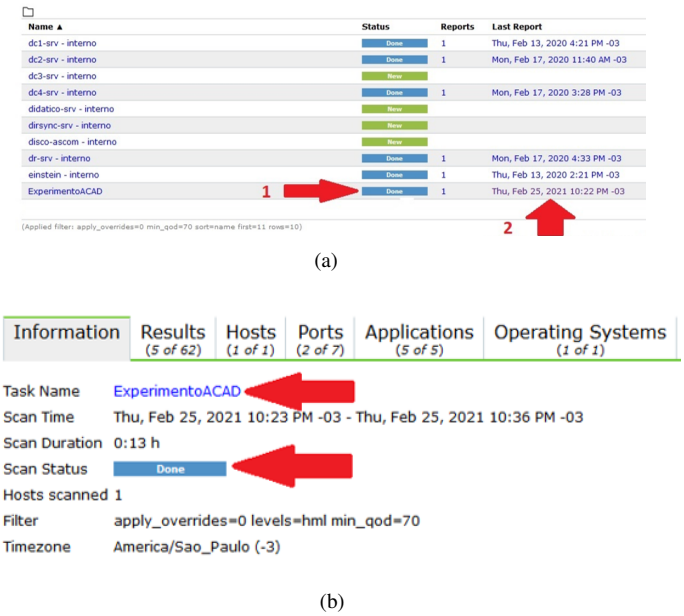
Para iniciar uma tarefa é necessário acessarmos a guia “Scans”na tela principal e o item “Tasks”, conforme inidicado na Figura 4. Essa ação lista todas as tarefas. Na Figura 4, verificam-se outras tarefas oriundas de análises posteriores. Para esse trabalho, utiliza-se o alvo denominado “ExperimentoACAD”. No caderno desenvolvido pelos autores, orientam-se os instrutores a direcionar os alunos para a criação de novas tarefas com novos alvos para exercício do aprendizado.

Para iniciar uma busca e análise de vulnerabilidade, seleciona-se o botão de “Play”, indicado na Figura 4, para ativar a atividade. Ressalta-se que a coluna “Name”descreve o nome da tarefa criada e não do alvo em si. Na tela de busca e análise de vulnerabilidades, tem-se a indicação de *status* que apresenta cinco possíveis estados:

- *New* = indica uma tarefa nova que ainda não foi inicializada;
- *Request* = indica que a tarefa foi inicializada e que ela está sendo estruturada junto aos serviços de busca e análise do OpenVAS. Esta tarefa também identifica se o alvo está ligado ou desligado;
- *Running* = indica uma tarefa em andamento;
- *Done* = indica que uma tarefa já foi totalmente finalizada e que os resultados já estão prontos;
- *Error* = indica uma anormalidade na tarefa ou em um dos serviços do OpenVAS responsáveis pela execução da tarefa.

C. Resultados e geração de relatório

Ao fim do teste de vulnerabilidades, a coluna “Status”, em relação ao alvo “ExperimentoACAD”, estará com o campo *status* configurado em “Done”(1) e a coluna “Last Report”estará preenchida com as informações de data e hora da geração dos resultados. Para analisar o resultado, basta clicar sobre esse campo (2), conforme indicando na Figura 5(a), e ter acesso à área de informações básicas, Figura 5(b).



(a)

(b)

Fig. 5. Acessando informações relacionada à análise de vulnerabilidade.

Na tela vista na Figura 5(b), pode-se realizar uma avaliação básica dos resultados clicando na guia “Results”. Nessa guia, tem-se a coluna “Severity”, onde existe uma classificação de 0 a 10 para os níveis de impacto possíveis das vulnerabilidades. Utiliza-se um código de cores para identificar a severidade das vulnerabilidades encontradas, como visto na Figura 6. Ressalta-se que a classificação por cores indica apenas a severidade da vulnerabilidade. Os valores dentro de cada campo correspondem ao número de vulnerabilidades identificadas. Os valores indicados na Figura 6 são fictícios. Exibem-se os valores reais e a classificação de 0 a 10 posteriormente à exportação do relatório completo da análise para o alvo “ExperimentoACAD”.

Fig. 6. Severidade em código de cores.

Para gerar o relatório de resultados da busca e análise de vulnerabilidades, seleciona-se o ícone indicado na Figura 7. Abre-se uma segunda janela para escolha do tipo de arquivo para exportação. Nesse trabalho, optou-se pelo formato PDF.

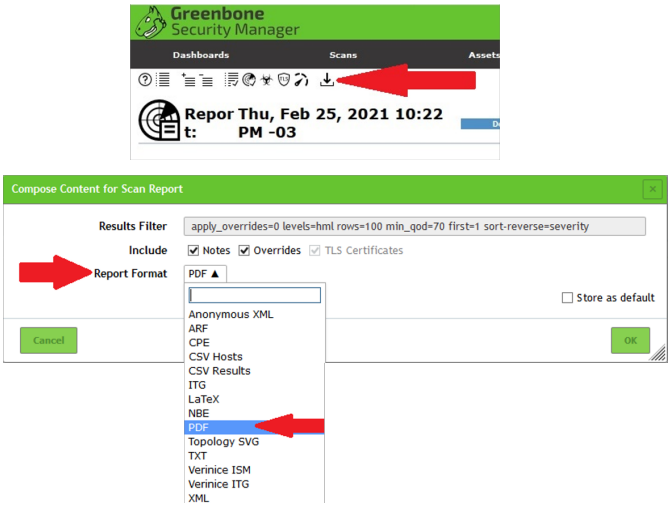


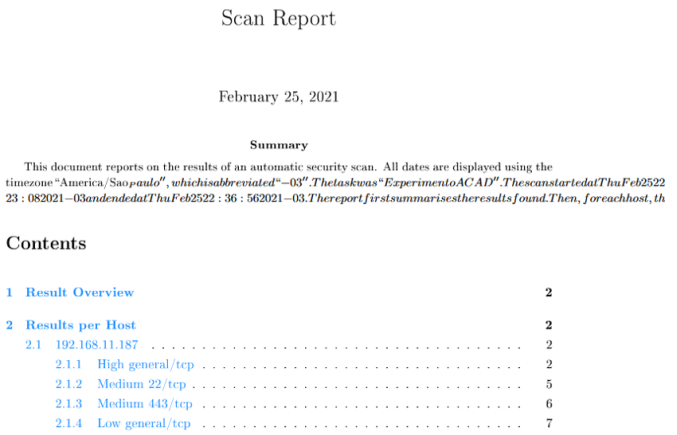
Fig. 7. Exportação do relatório de resultados.

Na Figura 8, visualiza-se a página inicial do arquivo PDF que contém os resultados da análise de vulnerabilidade. O idioma oficial do documento é inglês. Além disso, o documento inclui informações sobre a geolocalização, data e hora de execução dos testes.

III. Resultados sobre a análise de vulnerabilidade

Nessa seção, discutem-se alguns pontos da análise de vulnerabilidade efetuada na Seção II. Extraiu-se esses dados diretamente do relatório de resultados. Para o alvo analisado, identificaram-se um total de 05 vulnerabilidades classificadas em níveis de severidade conforme indicado na Tabela I. O *host* avaliado apresentou duas vulnerabilidades com nível de severidade elevado e outras duas com severidade média. Obteve-se também uma quinta vulnerabilidade de severidade baixa.

Por meio do relatório, pode-se obter uma relação de serviços ou portas relacionados as vulnerabilidades encontradas devido


Scan Report

February 25, 2021

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone “America/Sao Paulo”, which is abbreviated “-03”. The task was “Experimento ACAD”. The scan started at Thu Feb 25 22 23 : 08 2021 -03 and ended at Thu Feb 25 22 : 36 : 56 2021 -03. The report first summarises the results found. Then, for each host, th

Contents

Fig. 8. Página inicial do relatório de análise de vulnerabilidades.

TABELA I
CLASSIFICAÇÃO DAS VULNERABILIDADES ENCONTRADAS

Host	192.168.11.187 (ctic-srv.local.inatel.br)
Severidade	Numero de vulnerabilidades
Alta	2
Média	2
Baixa	1
Log	0
Falso Positivo	0

ou à má configuração ou à identificação de versões desatualizadas. Assim como, a classificação do nível de ameaça, conforme explicitado na Tabela II.

TABELA II
SERVIÇOS E PORTAS VULNERÁVEIS E NÍVEL DE AMEAÇA.

Serviço (Porta)	Nível de ameaça
general/tcp	Alto
22/tcp	Médio
443/tcp	Médio
general/tcp	Baixo

O relatório também apresenta uma análise das vulnerabilidades elencando alguns pontos:

- *Summary* = apresenta um sumário básico sobre a vulnerabilidade;
- *Vulnerability Detection Result* = apresenta um resultado mais detalhado da vulnerabilidade detectada;
- *Solution* = faz sugestão à possíveis soluções para mitigar/eliminar uma ou mais vulnerabilidades;
- *Vulnerability Insight* = explica o pensamento e a motivação dos pesquisadores que aplicaram os testes relacionados à determinada vulnerabilidade detectada;
- *Vulnerability Detection Method* = apresenta detalhes de como a vulnerabilidade pode ser detectada e, se necessário, aponta a prova de conceito cabível;
- *References* = apresenta as CVEs e NVDs relacionadas ao registro e classificação das vulnerabilidades além de trazer direcionamentos para links externos onde possam conter mais informações sobre elas;

Na Figura 9, tem-se um fragmento do relatório referente a uma vulnerabilidade, onde indicifica-se um sumário com a cor da severidade relacionada à vulnerabilidade. Além disso, verifica-se a pontuação da vulnerabilidade dentro da faixa de

0 a 10, para o exemplo, a pontuação é 4,3. Essa pontuação é oriunda do CVSS(*Common Vulnerability Score System*) [8].

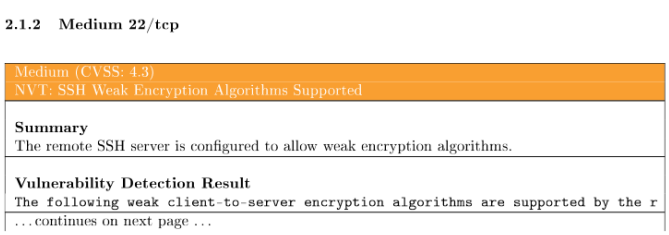


Fig. 9. Sumário de detalhamento de uma vulnerabilidade.

IV. Conclusão

Esse trabalho apresentou um breve tutorial para uso da ferramenta OpenVAS para busca e análise de vulnerabilidades em sistemas ou redes de telecomunicações. Demonstrou-se como configurar a ferramenta para criar uma nova análise, incluir um determinado alvo, executar a análise e extrair o relatório. Em seguida, demonstrou-se alguns resultados extraídos do relatório obtido. Esse breve tutorial representa um resumo de um caderno elaborado para a disciplina de Gerência e Segurança de Redes do Inatel (Instituto Nacional de Telecomunicações). Espera-se que o leitor seja capaz de replicar novos testes em alvos distintos e também compreender às questões relacionadas à criticidade e ao risco de vulnerabilidades presentes nos sistemas computacionais e nas redes de computadores e telecomunicações.

Referências

[1] W. Stallings. *Criptografia e Segurança de Redes*. 6th. Pearson, 2014.

[2] J. Hintzbergen, K. Hintzbergen, A. Smulders e H. Baars. *Fundamentos de Segurança da Informação: com Base na ISO 27001 e na ISO 27002*. 1th. Brasport, 2018.

[3] G. Weidman. *Penetration Testing : A Hands-On Introduction to Hacking*. 1th. No Starch Press, 2014.

[4] Greenbone. *Open System Vulnerabilities Analisys*. URL: https : / / community . greenbone . net / t / greenbone - community - edition - 6 - 0 - 10 - released / 6132 (acesso em 18/04/2020).

[5] Infosecurity. *OpenVAS Virtual Appliance*. URL: https://www.51sec.org/2018/05/09/openvas-virtual-appliance-greenbone-installation/ (acesso em 29/04/2020).

[6] Y. Wang e J. Yang. "Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool". Em: *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. 2017, pp. 110–113.

[7] Y. Wang, Y. Bai, L. Li, X. Chen e A. Chen. "Design of Network Vulnerability Scanning System Based on NVTs". Em: *2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC)*. 2020, pp. 1774–1777.

[8] FIRST. *Common Vulnerability Scoring System SIG*. URL: https://www.first.org/cvss/ (acesso em 27/02/2021).