CENTRO UNIVERSITÁRIO BRASILEIRO – UNIBRA

CURSO DE GRADUAÇÃO TECNÓLOGO EM REDES DE COMPUTADORES

KLEYBSON FERREIRA DE CASTRO BATISTA

ROBERTO FRANCISCO MINZÉ FILHO

PEDRO IGOR ARAÚJO CAETANO DA SILVA

ANÁLISE DE VULNERABILIDADE COM FERRAMENTAS AUTOMATIZADAS

RECIFE/2021

KLEYBSON FERREIRA DE CASTRO BATISTA

ROBERTO FRANCISCO MINZÉ FILHO

PEDRO IGOR ARAÚJO CAETANO DA SILVA

ANÁLISE DE VULNERABILIDADE COM FERRAMENTAS AUTOMATIZADAS

Artigo apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professor Orientador: Msc Ameliara Freire Santos de Miranda

RECIFE/2021

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 2338/ O.

B333a Batista, Kleybson Ferreira de Castro

Análise de vulnerabilidade com ferramentas automatizadas. / Kleybson Ferreira de Castro Batista, Pedro Igor Araújo Caetano da Silva, Roberto Francisco Minzé Filho. - Recife: O Autor, 2021.

24 p.

Orientador(a): Ameliara Freire Santos de Miranda.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de Computadores, 2021.

Inclui Referências.

1. Análise de vulnerabilidade. 2. Ferramentas automatizadas. 3. Nmap. 4. Metasploit. 5. Segurança. I. Silva, Pedro Igor Araújo Caetano da. II. Minzé Filho, Roberto Francisco. III. Centro Universitário Brasileiro - UNIBRA. IV. Título.

CDU: 004

Dedicamos esse trabalho aos nossos pais, aos nossos professores e todos que nos permitiram chegar até aqui.

AGRADECIMENTOS

Agradecemos aos nossos pais, que nos incentivaram e apoiaram até o término do curso.

Aos professores, pelas correções e conhecimentos que nos permitiram apresentar este trabalho.

Aos nossos amigos que conhecemos durante a formação do curso.

“O homem é bom por natureza.

É a sociedade que o corrompe.”

Jean-Jacques Rousseau

TABELAS DE SIGLAS

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

IP - Internet protocol

CHS - Community Health System

VS - Versus

Sumário

ANÁLISE DE VULNERABILIDADE COM FERRAMENTAS AUTOMATIZADAS

Kleybson Ferreira de Castro Batista

Roberto Francisco Minzé Filho

Pedro Igor Araújo Caetano da Silva

Resumo: Com os avanços tecnológicos e com o aumento de cibercrimes, as empresas tornam-se alvos de ataques dos cibercriminosos, por armazenar dados sensíveis de usuários ou por ter grande parte de seu funcionamento pela rede mundial de computadores (internet). Esses ataques normalmente são executados através de alguma vulnerabilidade no sistema utilizado pela empresa, para evitar isso é preciso uma avaliação completa do sistema que é chamado de análise de vulnerabilidade. Análise de vulnerabilidade é o processo de identificação e avaliação de vulnerabilidades que comprometem a segurança do sistema. A partir desse processo, o administrador toma conhecimento dos pontos fracos de seu sistema. Assim, pode efetuar uma correção da vulnerabilidade de todo o sistema. Esse processo pode ser automatizado por ferramentas específicas, que têm a capacidade de obter muitas informações úteis em pouco tempo e disponibilizando uma avaliação completa do sistema alvo. O Nmap e o Metasploit são ferramentas especializadas em análise de vulnerabilidade, disponibilizando muitos recursos para o administrador.

Palavras-Chaves: Análise de vulnerabilidade, Ferramentas automatizadas, Nmap, Metasploit, Segurança.

Abstract: Technological advances and with the increase of cybercriminals, companies become targets of attacks from these cybercriminals, by storing sensitive user data or by having a large part of its operation through the worldwide network of computers (internet). These attacks are usually executed through some vulnerability in the system used by the company, to avoid this it is necessary a complete evaluation of the system that is called vulnerability analysis. Vulnerability analysis is the process of identifying and assessing vulnerabilities that compromise system security. From this process, the administrator becomes aware of the weaknesses of his system. Thus, it can perform a system-wide vulnerability fix. This process can be automated by specific tools, which have the ability to obtain a lot of useful information in a short time and provide a complete assessment of the target system. Nmap and Metasploit are specialized tools in vulnerability analysis, providing many resources for the administrator.

Keywords: Vulnerability analysis, Automated tools,Nmap, Metasploit, Security

1. Introdução

A segurança da informação é sem dúvida um dos temas mais discutidos na atualidade e de maior relevância no ambiente corporativo, e por essa razão, merece toda atenção e cuidado por parte dos gestores e administradores de uma empresa. Por causa da necessidade de se obter dados e informações sensíveis, para as organizações é crucial implantar procedimentos de segurança, com o intuito de prevenir ameaças. Atualmente, ações maliciosas voltadas a invadir sistemas, causar vazamento de dados e ataques cibernéticos são populares, e as ações dos cibercriminosos são sempre prejudiciais, tanto para imagem da empresa, quanto para clientes e funcionários (TOTVS,2021).

Caso, uma empresa sofra um vazamento de dados, ela pode sofrer multa equivalente a 2% do faturamento bruto que pode ser aplicada a cada instância com irregularidade. Penalidades podem ser aplicadas a empresas a qual impossibilita ela de fazer tratamento de dados (COMPUGRAF,2020). A chance de sofrer vazamentos de dados pode ser reduzida através de uma análise de vulnerabilidade.

Uma análise de vulnerabilidade fornece a uma organização informações sobre vulnerabilidades de segurança em seu sistema . Também fornece orientação sobre como avaliar os riscos associados a essas vulnerabilidades, por meio disso, a organização consegue ter uma melhor compreensão de seus ativos, falhas de segurança e risco geral, reduzindo a chance de um cibercriminoso comprometer seu sistema. A análise de vulnerabilidade pode ser automatizada por meio de ferramentas (COSTA,2021).

As ferramentas de análise de vulnerabilidade fazem a maior parte do trabalho para o administrador, de modo que ele não precisa verificar manualmente cada possível ameaça, algumas ações que a automação pode fazer é detectar ameaças no sistema, fazer a triagem de ameaças em potencial e determinar se deve corrigir. Tudo isso pode ocorrer em segundos sem consumir tempo do administrador, que pode ser melhor aproveitado em outras atividades durante a varredura da ferramenta (SPLUNK, 2021).

1.1 Motivação

Em 2012, foram vazados 214 milhões de contas de usuários entre Facebook, Instagram, Linkedin e outras redes sociais. Ao todo, foram detectados 11.651.162 de perfis de usuário do instagram, 66.117.839 do Linkedin, 81.551.567 do Facebook vazados, além disso empresas como eBay ou Yahoo! também foram invadidas por meio de um ataque, em 2015, outras indústrias também foram afetadas, como é o caso da Community Health System (CHS), nos Estados Unidos, que foi vítima do vazamento de 4.5 milhões de registros médicos. (FELIX, 2021).

A escolha do tema foi devido ao crescente número de vazamentos e invasões por cibercriminosos, que exploram vulnerabilidades no sistema das empresas.

Sendo de interesse geral comparar ferramentas automatizadas com o processo manual, e como as ferramentas automatizadas podem auxiliar na segurança da empresa.

1.2 Problema

De acordo com os autores do tema proposto, será comparado ferramentas automatizadas com os processos manuais executados pelos administradores do sistema e o porquê deve usufruir de ferramentas automatizadas na análise de vulnerabilidades.

- Com o avanço da tecnologia, os ataques a sistemas empresariais vêm aumentando
- A ausência de uma execução de análise de vulnerabilidade pode acarretar complicações com a segurança do sistema da empresa.
- O tempo necessário para a execução de uma análise de vulnerabilidade manual efetiva pelo administrador, é demasiadamente longo.

1.3 Objetivos gerais

Realizar uma comparação entre análise de vulnerabilidade manual com ferramentas automatizada, sua praticidade e a economia de tempo que o administrador ganha ao executar uma análise automatizada, verificar sua efetividade na procura de vulnerabilidade.

1.3.1 Objetivos específicos

Para alcançar nossa finalidade foi definido os seguintes objetivos específicos:

- Analisar e fazer estudo sobre ferramentas automatizadas;
- Comparar ferramentas automatizadas com o processo de análise manual;
- Apresentar a efetividade das ferramentas automatizadas;
- Apresentar as vantagens de utilização de ferramentas automatizadas no geral;

2 Metodologia

Este trabalho trata-se de uma pesquisa bibliográfica. A pesquisa bibliográfica é construída a partir de materiais já publicados, em especial, livros e artigos científicos (3ven3, 2020).

2.1 Construção da pesquisa

O trabalho foi iniciado buscando a definição do tema e sua relevância para segurança da empresa, seguido da coleta de informações onde foram pesquisados artigos e livros temas que dessem embasamento para a construção deste trabalho, filtrando por autores que têm um conhecimento aprofundado na área pesquisada.

2.2 Ferramentas utilizadas

Foram utilizadas nesta pesquisa duas ferramentas automatizadas, que foram escolhidas a partir de uma pesquisa Hackersec. destacam o Nmap e Metasploit como duas ferramentas que fazem parte das melhores e mais usadas ferramentas de análise de vulnerabilidade (HackerSec, 2020). como os autores desta pesquisa já tinham um conhecimento prévio das ferramentas elas foram adotadas na construção da pesquisa.

2.3 Comparações

Foram feitas comparações entre o processo manual de análise de vulnerabilidade e a ferramenta automatizadas, destacando o ponto forte de cada utilização e sua importância para garantir um sistema seguro na empresa. por último foi feito uma comparação entre Nmap e Metasploit destacando o ponto forte de cada uma e sua importância para a segurança.

3 Referencial teórico

Neste capítulo é apresentada a fundamentação teórica sobre análise de vulnerabilidade, ferramentas automatizadas, conceito de ferramentas automatizadas para análise de vulnerabilidade.

3.1 Análise de vulnerabilidade

Uma vulnerabilidade de segurança é qualquer meio que possa contribuir para uma invasão, vazamento de dados ou acesso não autorizado ao sistema. Fatores que podem contribuir para a ocorrência de uma vulnerabilidade de softwares mal configurados, sistemas desatualizados e arquivos sensíveis expostos publicamente. (ITEAM, 2020) Para identificar as vulnerabilidades no sistema e corrigir é preciso fazer uma análise de vulnerabilidade em todo sistema.

A análise de vulnerabilidade é o processo de identificação e análise das vulnerabilidades encontradas na infraestrutura de tecnologia da empresa, por meio dessa análise, o profissional responsável pode corrigir falhas, aumentar o desempenho e a segurança. Como consequência, a análise de vulnerabilidade garante a melhoria contínua do sistema da empresa (FLOWTI, 2020).

3.2 Importância das portas de rede

De acordo com Loik (2020), as portas são utilizadas como ponto finais de comunicação em rede, quando uma porta está aberta quer dizer que possivelmente contém algum serviço utilizando-a para se comunicar, é importante fazer o monitoramento de todos os serviços que estão sendo executados e dispositivos que se conectaram a esses serviços. Uma porta aberta pode trazer um risco a segurança, principalmente se o serviço que está utilizando essa porta está desatualizado ou com alguma vulnerabilidade existente.

3.3 Ferramentas automatizadas

Ferramentas automatizadas são soluções de software para reproduzir interações humanas com o sistema, trabalhando dentro dos limites das instruções que lhe foram programadas. Ao adotar essas ferramentas é possível eliminar processos repetitivos e manuais que consomem tempo do administrador, permitindo que o administrador seja mais produtivo em áreas mais específicas (Red Hat, 2020).

As ferramentas automatizadas de segurança podem ser usadas para identificar vulnerabilidades e executar proteções mais rapidamente, podendo auxiliar na prevenção de ataques de cibercriminosos (ALLEASY, 2019). dois exemplos de ferramentas automatizadas de segurança são Nmap e Metasploit.

3.3.1 Nmap

Nmap é uma ferramenta de código aberto utilizado para análise de rede, construída com o propósito de analisar redes amplas, embora funcione para hosts individuais, a sua varredura pode determinar quais hosts estão ativos na rede, quais serviços eles executam, qual o sistema operacional está executando e se os hosts utilizam alguma regra de firewall (Nmap, 2019).

3.3.2 Metasploit

Segundo Martins, (2016), o metasploit é uma ferramenta de segurança da informação, usado para investigar a vulnerabilidade em sistemas operacionais e servidores. Sendo assim, é possível realizar testes de invasões, fazendo um scan mais simples até uma análise ou invasão completa, fazendo com que seja explorado as vulnerabilidades do sistema vulnerável.

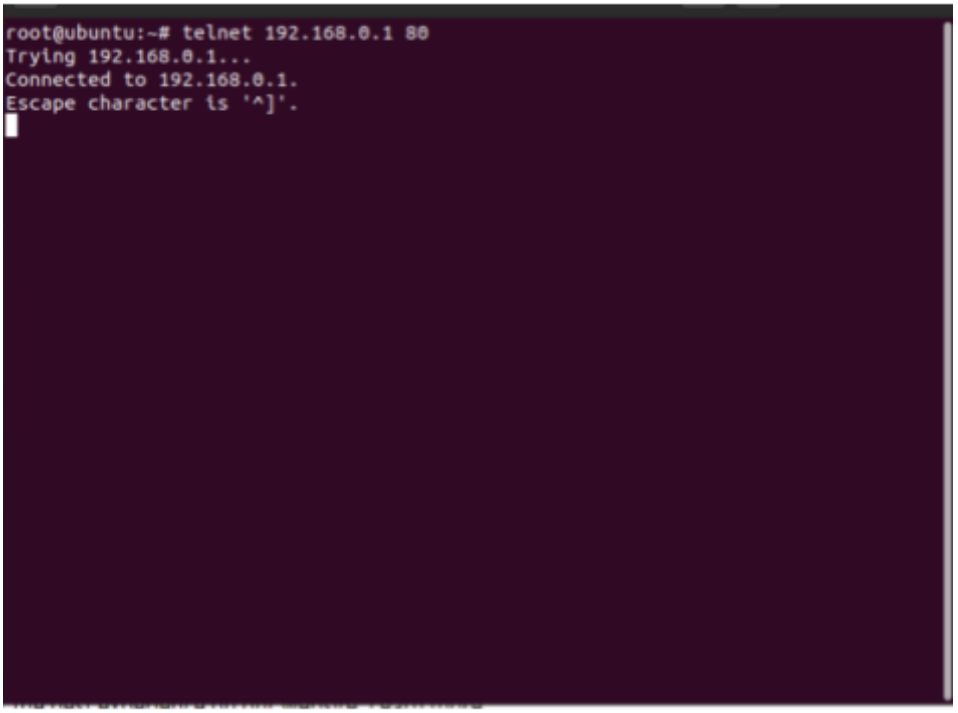
O metasploit, é programado em ruby, sendo organizado em módulos. Nesses módulos contém alguns programas construídos especificamente para tirar proveito de uma vulnerabilidade que existe no sistema (PPLWARE, 2011).

4 Resultados

4.1 Varredura manual de portas

Uma varredura manual de porta pode ser executada utilizando o utilitário telnet, que permite fazer conexão em um determinado host com uma porta específica, se o telnet efetuar a conexão, a porta está aberta, se não conseguir retornar que não foi possível a conexão. A execução da varredura se dá pelo comando, telnet endereço IP PORTA Para fazer uma varredura completa é necessário testar todas as 65.536 portas (Synology, 2021), A Figura 1 apresenta um exemplo de varredura de porta que identificou uma porta aberta usando o telnet em uma distribuição GNU/Linux. Já na figura 2 apresenta uma falha ao tentar se conectar;

Figura 1. sucesso na conexão



Fonte. autores

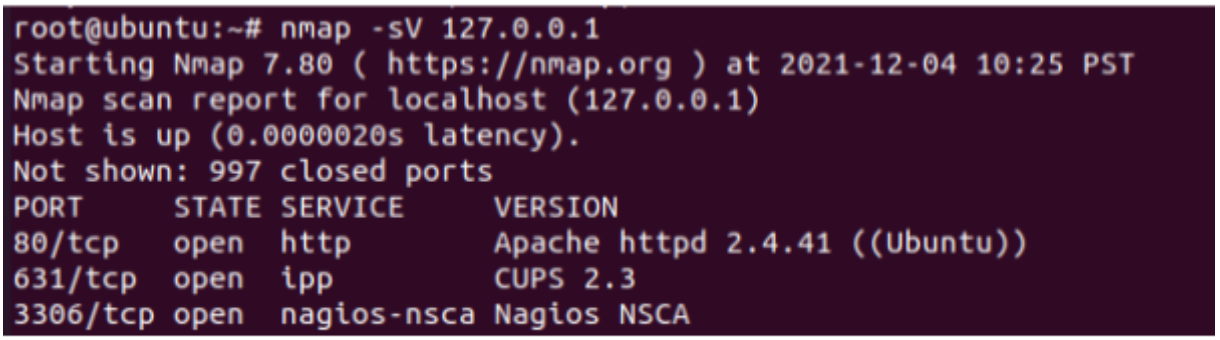
Figura 2. falha na

Fonte.
autores

4.2 Varredura de portas com Nmap

O nmap é capaz de fazer uma varredura automatizada de porta de forma rápida e eficiente, disponibilizando vários métodos para auxiliar na descoberta de portas disponíveis. Detectando serviços e suas versões, sistema operacional em execução na máquina alvo e verificando os filtros do firewall. O nmap pode executar uma varredura em todas as 65.536 portas, as portas que ele classifica como mais utilizadas ou em uma porta específica, sendo de escolha do usuário qual método utilizar. também sendo possível a varredura em uma lista de endereços ips alvos, tornando-se uma ferramenta ideal para uma varredura com muitos alvos (Seginfo,2012). a Figura 3 apresenta uma varredura simples do nmap;

figura 3. Varredura do Nmap



Fonte. autores

4.3 Varredura de portas manual vs automatizadas

De acordo com Loik, (2020) Uma varredura de porta manual é um processo extremamente lento, principalmente quando se trata de verificar a situação de todas as portas e agravando-se quando tem muitos alvos para fazer a verificação. Esse processo é bastante útil quando precisa-se verificar em um alvo a situação de um ou duas portas. Já utilizando uma ferramenta automatizada o processo torna-se mais rápido e se destaca-se em verificar todas as portas de vários alvos, apresentando para o administrador uma boa quantidade de informações úteis, como: serviços, versões de sistemas, sistema operacional e portas que sofrem algum tipo de filtro pelo firewall. Todas essas informações vêm sendo apresentadas de fácil entendimento para um administrador da rede.

Foram identificados alguns benefícios das ferramentas automatizadas que podem ser aplicadas a ferramentas de varredura, dois deles são: economia de tempo do administrador e qualidade na varredura. A economia de tempo é crucial, porque quanto mais rápido a identificação da vulnerabilidade menor é o tempo de exposição na rede. A qualidade na varredura também é importante, por que os resultados que são apresentados pela ferramenta necessitam ser corretos para uma possível correção (Kankaria, 2016).

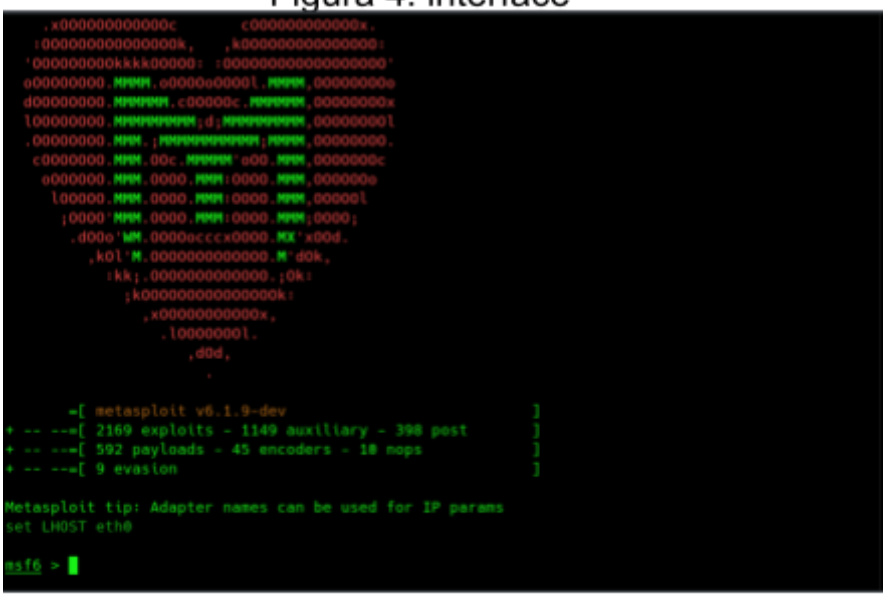
4.4 Exploração manual

Segundo Weidman, (2014) na exploração manual o administrador precisa identificar a vulnerabilidade, pesquisar sobre ela e manualmente fazer a exploração, este tipo de exploração pode utilizar muito tempo do administrador. já que é necessário seguir um passo-a-passo de como explorar determinada vulnerabilidade e as vezes pode se tratar de um falso positivo (quando o administrador classifica equivocadamente como vulnerabilidade). A exploração manual pode ser útil quando determinada vulnerabilidade ainda não foi descoberta ou não existe código disponível na ferramenta automatizada.

4.5 Exploração com metasploit

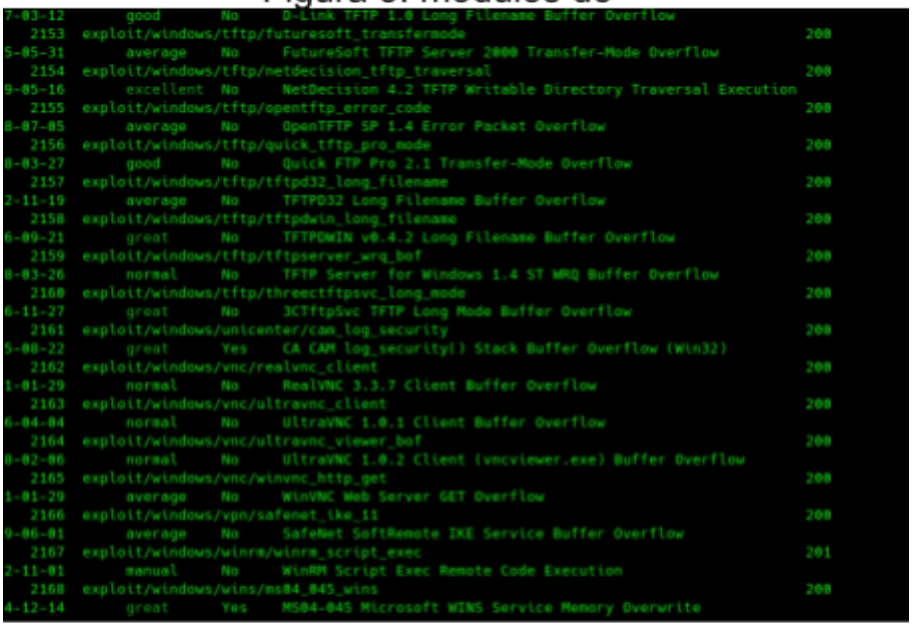
De acordo com Galossi (2018), o metasploit possui um banco de códigos para explorar várias vulnerabilidades de sistemas, caso o administrador identifique alguma vulnerabilidade no sistema, ele pode explorar a vulnerabilidade por meio dos códigos disponíveis na ferramenta para que seja confirmada a existência da vulnerabilidade para iniciar uma correção. O metasploit não se limita à parte de exploração, os seus módulos contêm códigos para auxiliar o administrador na configuração do código de exploração e de conexões com o sistema. Os códigos disponibilizados na ferramenta contêm classificações de acordo com sua efetividade, sendo excelente um código que não contém risco para o sistema e bom um código que pode causar uma perda de serviço no sistema. A figura 4 apresenta a interface gráfica do metasploit, já na figura 5 apresenta alguns módulos de exploração.

Figura 4. interface



Fonte.
autores

Figura 5. módulos do



Fonte.
autores

4.6 Exploração manual vs automatizada

Segundo Sampaio (2019), na utilização de exploração manual o administrador utiliza-se de bastante tempo para fazer a exploração, sendo pouco efetivo quando o objetivo é corrigir todas as vulnerabilidades o mais rápido possível. a exploração manual tem grande importância quando a vulnerabilidade é muito específica e não existe nenhuma ferramenta para sua exploração. já na utilização de ferramenta automatizada para exploração o administrador tem a sua disposição muitas funções e códigos de exploração tudo centralizado em uma ferramenta, assim corrigindo rapidamente a vulnerabilidade e diminuindo o tempo de exposição na rede. O metasploit é um exemplo desse tipo de ferramenta.

4.7 Metasploit vs Nmap

Segundo Sen (2021), tanto o Nmap quanto o Metasploit são excelentes ferramentas, o Nmap se destaca por ser uma ótima ferramenta para descoberta e mapeamento de rede, enquanto Metasploit se destaca por ser uma ótima ferramenta de exploração. Ambas as ferramentas requerem que o administrador tenha conhecimento na execução de análise de vulnerabilidade, contudo o Metasploit torna-se mais perigoso no momento de executar os códigos que ele contém, porque um administrador sem o conhecimento necessário pode causar uma negação de serviço pelo fato do metasploit disponibilizar códigos que utilizam muita da capacidade do alvo. Na questão de agilidade, as duas ferramentas conseguem obter informações e explorar o alvo rapidamente, porém quando houver muitos alvos a execução torna-se lenta, mas continua a ser mais rápida que a execução de vulnerabilidade manual.

De acordo com Hamdan (2020), mesmo que o Nmap e o Metasploit possam executar a mesma função de descoberta e exploração, o administrador não precisa escolher entre uma das duas, é possível utilizar as duas em conjunto para uma análise de vulnerabilidade mais rápida e completa.

5 Conclusão

A análise de vulnerabilidade é o processo de obter informações sobre serviços e aplicações, é através desse processo que o administrador fica ciente das vulnerabilidades presentes em seu sistema e posteriormente aplica uma correção para tornar o sistema mais seguro. É de grande importância a execução de uma análise de vulnerabilidade no ambiente tecnológico da empresa, com o objetivo de evitar prejuízos relacionados a ataques de cibercriminosos e disponibilizar um sistema seguro para seus clientes.O processo manual de uma análise de vulnerabilidade é efetiva quando o administrador procura por uma vulnerabilidade específica, mas torna-se lenta quando se trata de analisar muitos sistemas. Por isso, existem ferramentas automatizadas com o objetivo de fazer uma análise de vários sistemas rapidamente,Assim o administrador pode fazer a correção de vulnerabilidades em todos os sistemas mais rapidamente, diminuindo a exposição de sistemas vulneráveis para os clientes da empresa. Diante disso, neste trabalho foram apresentados o Nmap e o Metasploit, duas ferramentas que são popularmente conhecidas e utilizadas pelos administradores para efetuar uma análise de vulnerabilidade, sendo utilizados em conjunto com intuito de identificar o máximo de vulnerabilidades possíveis, ambas as ferramentas apresentam uma grande quantidade de funções disponibilizada para o administrador. O Nmap é mais utilizado na análise de redes, apresentando serviços e suas versões, portas abertas ou alteradas por firewall, mas também disponibiliza códigos de exploração de serviços vulneráveis. Já no caso do Metasploit é mais utilizado na parte de exploração, com intuito de comprovar que o sistema ou serviço está vulnerável, mas também disponibiliza módulos para reconhecimento de rede. Durante a busca por artigos científicos, foram encontradas uma gama de ferramentas de análise de vulnerabilidades. Diante disto, recomenda-se mais estudos sobre a utilização e efetividade das demais ferramentas de análise de vulnerabilidade.

REFERÊNCIAS

ALLEASY – Automação de segurança da informação: quais os benefícios?, 2019, Brasil.
Disponível em https://www.alleasy.com.br/2019/09/24/automacao-de-seguranca-da-informacao-quais-os-beneficios/. Acesso em 03/12/2021

COSTA, Edson. Saiba como fazer uma análise de vulnerabilidade eficiente. Huawei Cloud, 08 de jan. de 2021. Disponível em: <https://huaweibra.com.br/blog/seguranca/analise-de-vulnerabilidade/>. Acesso em: 02 de dez. de 2021.

COMPUGRAF. – Segurança da informação, 2020, Brasil.
Disponível em https://www.compugraf.com.br/impacto-da-lgpd/. Acesso em 02/12/2021

3EVEN3 -- Metodologia Científica: guia simplificado para escrever a sua, 2020. Disponível em: <https://blog.even3.com.br/metodologia-cientifica-como-fazer//>. Acesso em: 07 de dez. de 2021

FELIX, Bruno. Mais de 400 GB: vazamento expõe milhões de usuários de Facebook, Instagrame LinkedIn. Olhar digital, 2021. Disponível em: <https://olhardigital.com.br/2021/01/12/noticias/vazamento-de-mais-de-400-gb-expoe-milhoes-de-usuarios-de-facebook-instagram-e-linkedin/>. Acesso em: 05, 06 e 2021.

FLOWTI, – Análise de vulnerabilidade: o que é e qual é a sua importância?, 2020. Disponível em <https://flowti.com.br/blog/analise-de-vulnerabilidade-o-que-e-e-qual-e-a-sua-importancia>. Acesso em: 03 de dez. de 2021

GALOSSI, Ricardo. Metasploit Framework de cabo a rabo, 2018. Disponível em: <https://www.guiadoti.com/2018/04/metasploit-framework-parte-1/>. Acesso em: 04 de dez. de 2021.

HackerSec --As melhores ferramentas hacker, 2020. Disponível em: <https://hackersec.com/melhores-ferramentas-hacker/>. Acesso em: 07 de dez. de 2021

Hamdan, Motasem .Using Metasploit and Nmap to scan for vulnerabilities, 2020. Disponível em: <https://www.cm-alliance.com/cybersecurity-blog/using-metasploit-and-nmap-to-scan-for-vulnerabilities>. Acesso em: 06 de dez. de 2021

ITEAM -- Análise de vulnerabilidade: o que é e qual é a sua importância?, 2020. Disponível em: <https://it-eam.com/entenda-o-que-e-vulnerabilidade-de-seguranca-e-quais-sao-as-mais-comuns/>. Acesso em: 03 de dez. de 2021

KANKARIA, Himani . Top 15 Benefits of Automated Testing Tools, 2016. Disponível em: <https://dzone.com/articles/top-15-benefits-of-automated-testing-tools>. Acesso em: 04 de dez. de 2021

LOIK, Nayla. Scanner de Porta: O que é e por que você deveria utilizá-lo, 2020. Disponível em: <https://blogs.manageengine.com/portugues/2020/12/29/scanner-de-porta-o-que-e-e-por-que-voce-deveria-utiliza-lo.html>. Acesso em: 04 de dez. de 2021.

MARTINS, Adriano. Saiba como funciona o Metasploit. Pmgacademy, 2016. Disponível em: < https://www.pmgacademy.com/blog/artigos/como-funciona-o-metasploit/>. Acesso em: 03 de dez. de 2021.

NMAP – Guia de referência do Nmap (página do manual), 2019. Disponível em: < https://nmap.org/man/pt_BR/index.html#man-description>. Acesso em: 03 de dez. de 2021

PPLWARE – Metasploit – Sabe o que é?, 2011, Brasil. Disponível em https://pplware.sapo.pt/internet/metasploit-sabe-o-que-e/. Acesso em 03/12/2021

RED HAT – Automação da infraestrutura de TI, 2020, Brasil. Disponível em https://www.redhat.com/pt-br/topics/automation/whats-it-automation. Acesso em 03/12/2021

SAMPAIO, Miguel. Metasploit desmistificado — Usar a MSFConsole, 2019. Disponível em: <https://medium.com/canivete-sui%C3%A7o-hacker/metasploit-desmistificado-ii-1-68ee353114d1>. Acesso em: 05 de dez. de 2021.

SEN, Kaushik . Metasploit vs Nmap for Ethical Hacking, 2021. Disponível em: <https://www.upguard.com/blog/metasploit-vs-nmap-for-ethical-hacking>. Acesso em: 06 de dez. de 2021

SEGINFO –Mapeamento de Redes com nmap, 2012, Brasil.
Disponível em
https://seginfo.com.br/2012/07/12/mapeamento-de-redes-com-nmap-ferramenta-de-codigo-aberto-com-diversas-funcionalidades-2/. Acesso em 04/12/2021

SPLUNK – What Is Security Automation, 2021, Brasil.
Disponível em
https://www.splunk.com/en_us/data-insider/what-is-security-automation.html. Acesso em 02/12/2021

SYNOLOGY. – How do I know if a TCP port is open or closed?, 2021, Brasil.
Disponível em
https://kb.synology.com/en-me/DSM/tutorial/Whether_TCP_port_is_open_or_closed#:~:text=On%20a%20Windows%20computer,-Press%20the%20Windows&text=Press%20the%20Windows%20key%20%2B%20R,test%20the%20TCP%20port%20status.. Acesso em 04/12/2021

TOTVS. – Segurança da informação, 2021, Brasil.
Disponível em https://www.totvs.com/blog/negocios/seguranca-da-informacao/.
Acesso em 02/12/2021

WEIDMAN, Georgia, et al. Título: Testes de invasão, Local de publicação: São paulo, SP, Editora: novatec, ano: 2014