



A UTILIZAÇÃO DE PENTEST COMO FERRAMENTA DE SEGURANÇA OFENSIVA PARA ANÁLISE DE VULNERABILIDADES EM ORGANIZAÇÕES

DAVI VENTURA CARDOSO PERDIGÃO
EDMILSON LINO CORDEIRO
ERIC HENRIQUE DE CASTRO CHAVES

INTRODUÇÃO

**CONTEXTUALIZAÇÃO,
JUSTIFICATIVA,
OBJETIVOS,
HIPÓTESES**

01

REFERENCIAL TEÓRICO

**ETAPAS DO PENTEST,
BACKTRACK**

03

CONCEITOS E FUNDAMENTOS

**TIPOS DE ATAQUES,
TIPOS DE PENTEST**

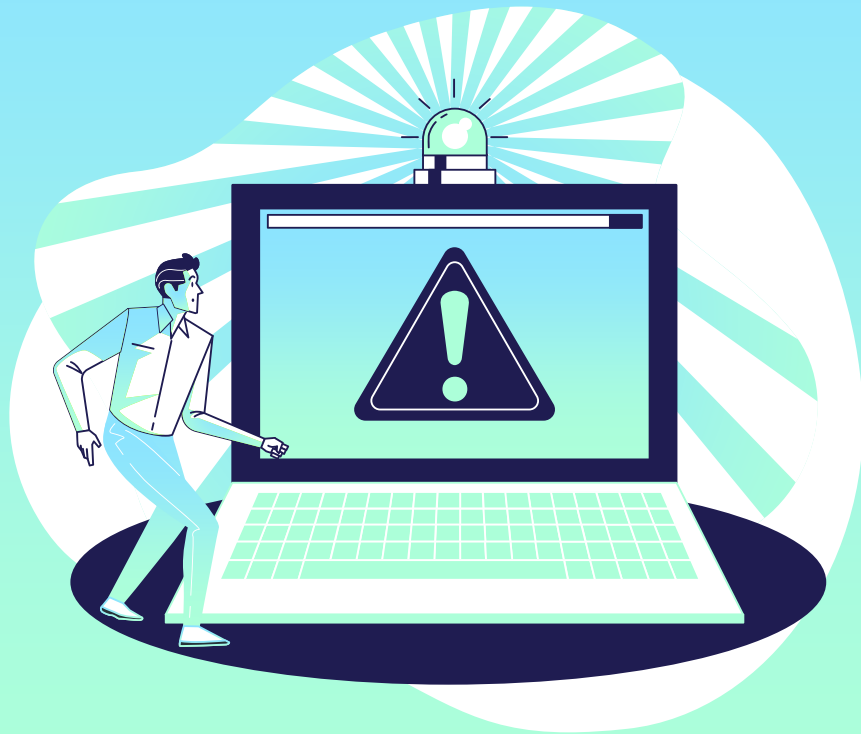
02

CONCLUSÃO

04

01

Introdução



• CONTEXTUALIZAÇÃO

- O Pentest é uma técnica que simula ataques cibernéticos para avaliar a segurança dos sistemas e infraestrutura de tecnologia da informação;
- Realizado por profissionais especializados que utilizam ferramentas e técnicas para identificar vulnerabilidades que possam ser exploradas por hackers;
- O resultado é um relatório que descreve as vulnerabilidades encontradas e as recomendações para corrigi-las;
- O Pentest é importante para aumentar a segurança e demonstrar a efetividade das medidas de proteção implementadas pela empresa.

JUSTIFICATIVA

- Segundo um relatório da *Verizon (2020)*, os ataques cibernéticos são responsáveis por mais de 40% dos incidentes de segurança em empresas de todo o mundo;
- Os Pentests são essenciais para prevenir e mitigar essas ameaças, identificando vulnerabilidades em sistemas de informação antes que possam ser exploradas;
- Além disso, a realização de Pentests é importante para garantir a conformidade com regulamentações de segurança da informação, como a GDPR (General Data Protection Regulation) na Europa e a LGPD (Lei Geral de Proteção de Dados) no Brasil;
- É fundamental que profissionais de TI e segurança estejam capacitados para realizar Pentests eficientes e eficazes, garantindo a segurança e proteção dos sistemas de informação das empresas.

OBJETIVOS

O objetivo deste artigo é destacar a importância dos Pentests como uma ferramenta de segurança ofensiva eficaz para identificar vulnerabilidades em sistemas de informação. Abordaremos os seguintes temas:

1. Definição do Pentest, seus tipos e etapas;
2. Como os Pentests ajudam as organizações a identificar e corrigir falhas de segurança em seus sistemas;
3. A importância da realização de Pentests para demonstrar a eficácia das medidas de segurança implementadas;
4. Principais desafios e limitações encontrados na realização de Pentests e como superá-los;
5. Contribuição para a disseminação do conhecimento sobre a importância dos Pentests como ferramenta de segurança ofensiva.

• HIPÓTESES

- O Pentest é uma técnica de segurança ofensiva altamente eficaz para identificar vulnerabilidades em sistemas de informação;
- A realização de Pentests pode ajudar as organizações a reduzir o risco de ataques cibernéticos, fornecendo informações valiosas sobre as falhas de segurança;
- Medidas de segurança eficazes, incluindo a realização de Pentests, podem contribuir para a proteção da informação e para a confiança dos stakeholders;
- É importante interpretar e tratar adequadamente os resultados gerados pelo Pentest, a fim de garantir que as vulnerabilidades sejam corrigidas e a segurança da organização seja mantida.

02

Conceitos e Fundamentos



TIPOS DE ATAQUES

Captura e Análise de Pacotes



Utiliza ferramentas como o **Wireshark** para verificar se a rede está segura e se os dados são transmitidos de forma criptografada. As informações sensíveis podem ser capturadas em texto simples, o que pode ser uma vulnerabilidade. É uma técnica comum para identificar vulnerabilidades e proteger os dados da organização.

Falsificação de Pacotes



Ataque em diferentes níveis da pilha de protocolos de rede. Permite que o atacante envie pacotes maliciosos que pareçam ter sido enviados por um dispositivo legítimo, enganando o destinatário. Um exemplo é **spoofing** de endereço IP, utilizado para interceptar informações sensíveis ou realizar ataques de negação de serviço.

Negação de serviço (DoS)



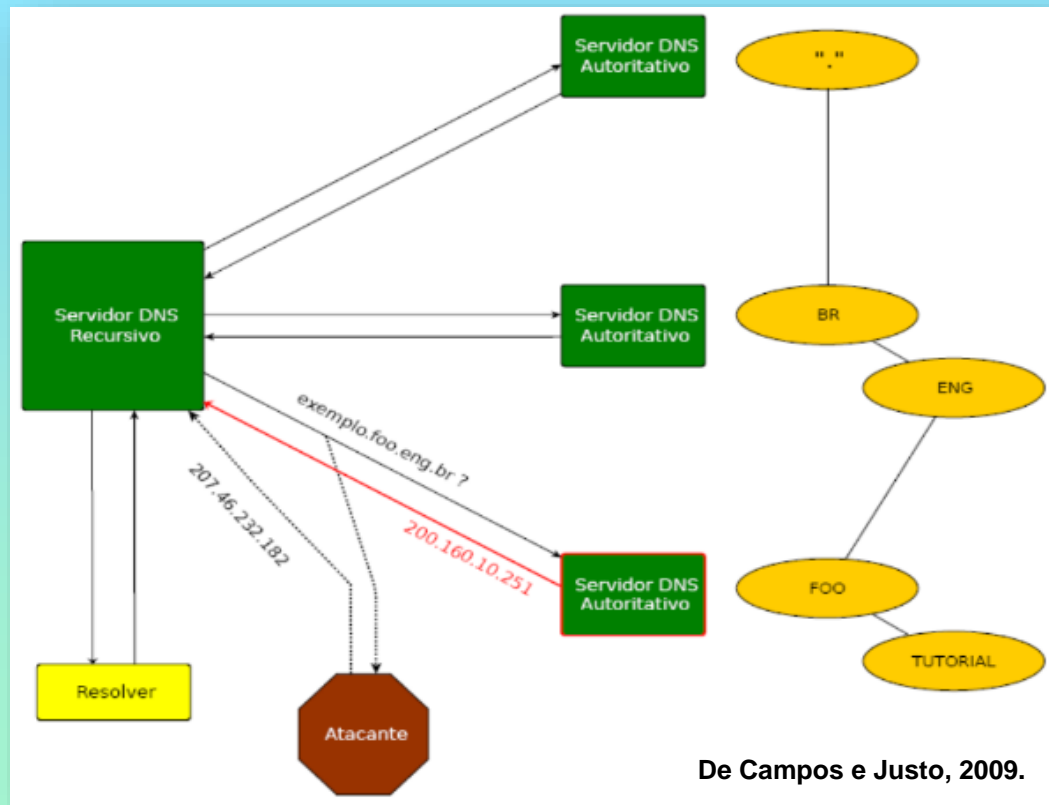
O objetivo é tornar serviços ou recursos inacessíveis para usuários legítimos. Para isso, realiza o envio de grande quantidade de tráfego, **flooding** de requisições HTTP/HTTPS, exploração de vulnerabilidades em protocolos de rede. Isso pode ocasionar perda de dados, interrupção de serviços, queda na produtividade, etc.

TIPOS DE ATAQUES

Envenenamento de cache DNS

Técnica em que um atacante envia respostas falsas para um servidor DNS, com informações adulteradas de resolução de nomes, que são armazenadas em cache.

Por exemplo, supondo que um usuário tente acessar o site "**www.banco.com.br**". O servidor DNS solicita informações de resolução de nomes ao servidor autoritativo do domínio "banco.com.br", que responde com o endereço IP correto do site. No entanto, um atacante pode interceptar essa resposta e enviar uma resposta falsa contendo um endereço IP diferente, correspondente a um servidor mal-intencionado. O servidor DNS armazena essa resposta falsa em seu cache e o atacante redireciona o tráfego de rede para o servidor mal-intencionado, interceptando as informações sensíveis.



De Campos e Justo, 2009.

TIPOS DE ATAQUES

Buffer Overflow



Comum em linguagens como C e C++. Isso ocorre quando um aplicativo tenta armazenar mais dados em um buffer do que ele pode suportar, levando a um estouro do buffer e uma sobrescrita da memória adjacente, permitindo que um atacante insira código malicioso no sistema.

Injeção de DLL



Ataque que se aproveita da capacidade do Windows de carregar bibliotecas dinâmicas em tempo de execução. O objetivo é inserir código malicioso em uma biblioteca dinâmica e, em seguida, injetá-la em um processo em execução para executar o código malicioso no contexto do processo.

Sequestro de sessão



Ataque em que um invasor rouba as informações de autenticação de um usuário já autenticado em uma aplicação. Isso pode ser feito através da captura de cookies de sessão enviados em cada solicitação ao servidor, por meio de um **sniffer** de rede. Para prevenir, é importante proteger as sessões com criptografia, e uso de tokens de autenticação de longa duração.

TIPOS DE ATAQUES

Quebra de senhas



Tipo comum de ataque utilizado por cibercriminosos para obter acesso a sistemas e dados protegidos por senha. As técnicas utilizadas incluem força bruta e análise de hashes de senha. Para se proteger contra esse tipo de ataque, é essencial utilizar senhas fortes e difíceis de serem adivinhadas ou descobertas.

Engenharia Social



A engenharia social é uma técnica de ataque que explora a vulnerabilidade humana para obter informações confidenciais ou realizar ações maliciosas. Durante um Pentest, a equipe de segurança pode usar técnicas de engenharia social para testar as políticas de segurança da informação da organização, por exemplo, enviando um e-mail phishing para os funcionários e verificar quantos deles clicam no link malicioso ou fornecem informações confidenciais. Essa ação pode ajudar a educar os funcionários sobre como evitar golpes de engenharia social.

TIPOS DE PENTEST

Antes de realizar um Pentest, o profissional deve conversar com os responsáveis da organização para entender as necessidades de verificação de vulnerabilidades, tanto internas quanto externas (BERTOGLIO; ZORZO, 2015).

- **Black Box:** tipo mais exigente para o Pentester, pois ele começa do zero sem nenhuma informação da empresa contratante. Por esse motivo, ele é mais caro e mais utilizado pelas empresas que desejam simular uma invasão externa e analisar a vulnerabilidade de sua rede;
- **Gray Box:** nesse tipo de teste, o Pentester tem um breve conhecimento e limites de teste liberados pela empresa contratante, definindo os limites dos ataques;
- **White Box:** muito utilizado e facilita bastante o trabalho do Pentester, pois ele já tem conhecimento sobre todas as informações do sistema antes de realizar o Pentest.

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

- Antes de realizar um Pentest, é fundamental formalizar um acordo de confidencialidade entre a empresa contratante e o Pentester. O acordo estabelece os termos e limites do teste de invasão e evita a divulgação indevida de informações confidenciais;
- O NDA (Non Disclosure Agreement) deve ser firmado antes do início dos testes para garantir a segurança e privacidade das informações da empresa;
- O escopo do Pentest, os limites do Pentest e o plano de comunicação são uma parte essencial do acordo.



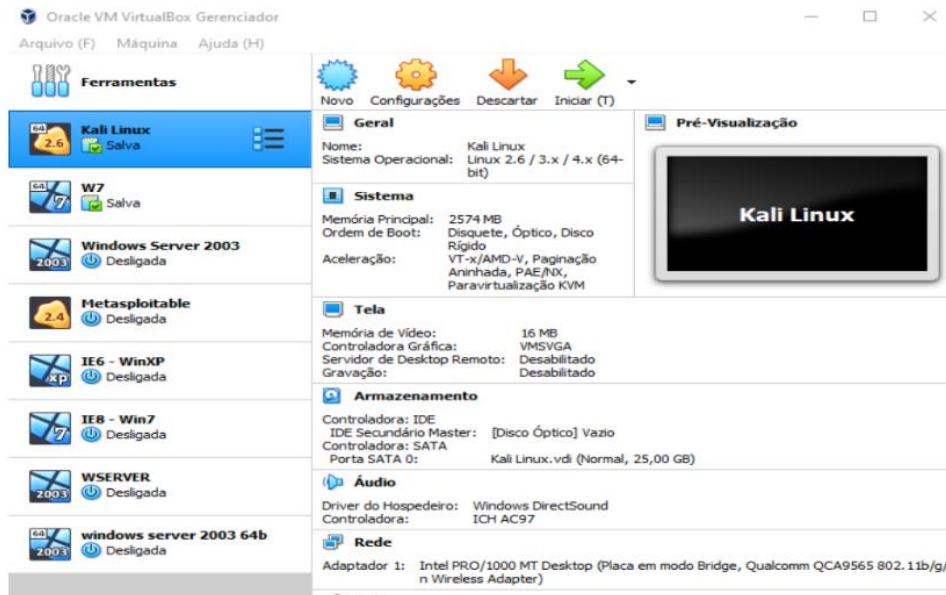
RELATÓRIO

- Para gerar relatórios detalhados é necessário um entendimento completo da empresa contratante;
- Existem dois tipos principais de relatórios: Sumário Executivo e Relatório Técnico;
- O **Sumário Executivo** é um resumo para os executivos da empresa apresentando os problemas encontrados e os possíveis danos que essas falhas podem causar, bem como o tempo necessário para resolvê-los;
- O **Relatório Técnico** é mais detalhado e apresenta uma descrição passo a passo das vulnerabilidades encontradas, incluindo capturas de tela e gravações de tela;
- É importante documentar todo o processo do Pentest para gerar relatórios detalhados com gráficos de análise de riscos;
- A documentação do processo de Pentest não se limita apenas aos relatórios finais e pode ser útil para a empresa contratante e o próprio Pentester;
- O relatório de Pentest é um documento técnico, mas deve ser apresentado de forma clara e objetiva para todos os envolvidos, evitando jargões técnicos que possam dificultar a compreensão dos resultados apresentados.

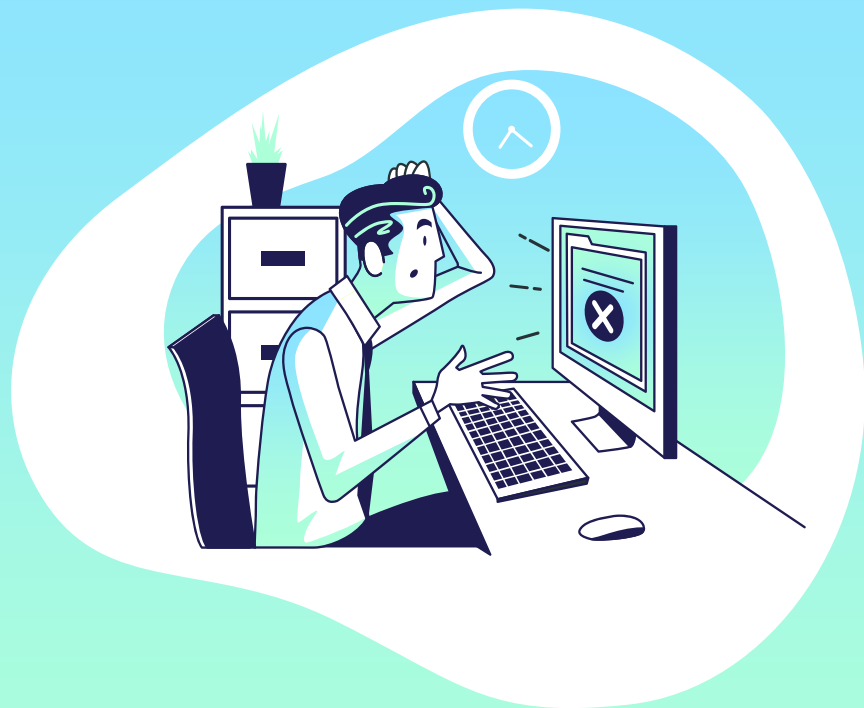
PREPARAÇÃO DO AMBIENTE DE TESTES

Para realizar testes de intrusão de forma segura e eficiente, é importante criar um ambiente virtualizado. Algumas etapas necessárias para isso são:

- Obter um software de virtualização, como o **VirtualBox**;
- Baixar um disco virtual (ISO) do Kali Linux;
- Configurar o Kali Linux com pelo menos 1024 MB de memória RAM, 30GB de espaço em disco e uma placa de rede em modo Bridge;
- Criar outras máquinas virtuais para representar o alvo do cliente (Ex: Windows 7 64 bits);
- Certificar-se de que as máquinas virtuais estejam na mesma faixa de endereço IP da rede local para permitir a comunicação entre elas.

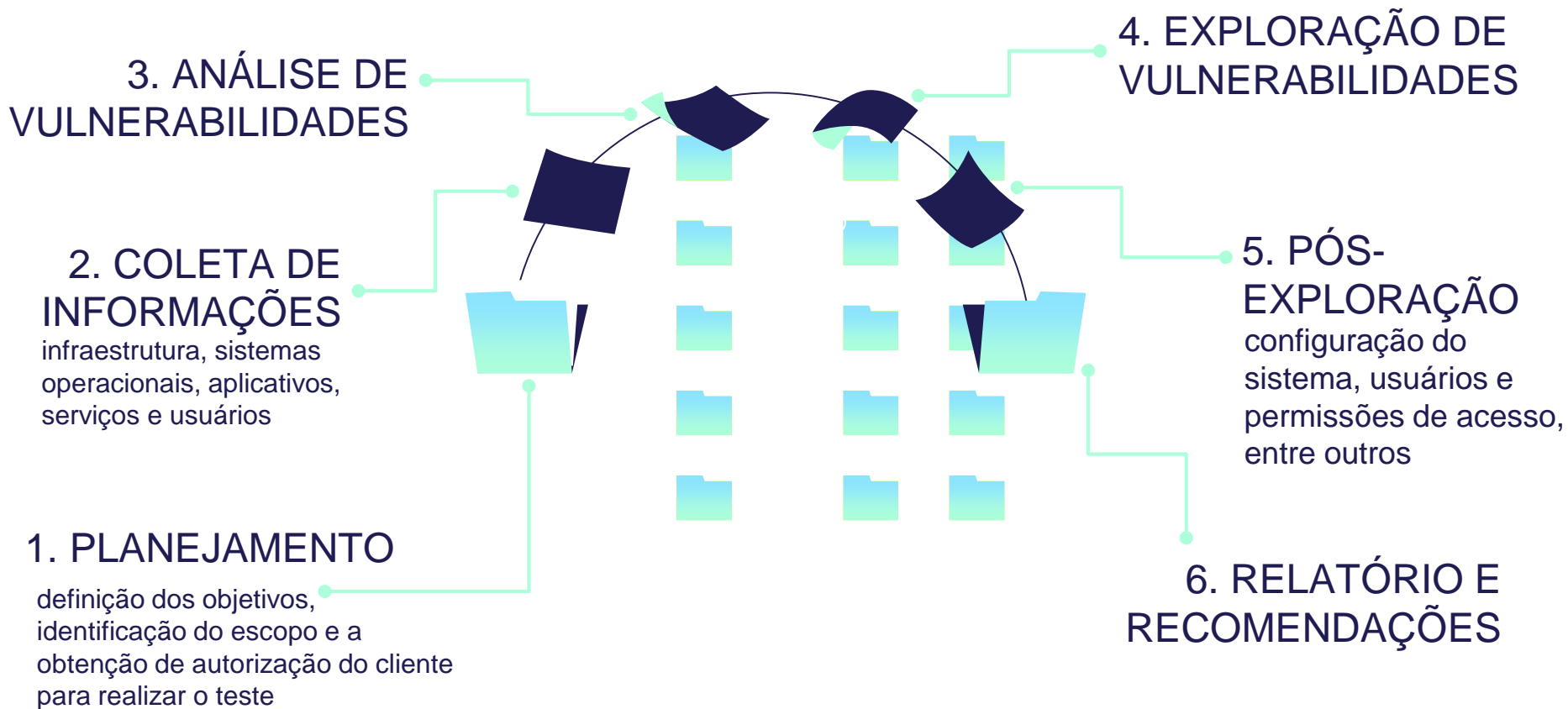


ASSUNÇÃO, 2017.



03 REFERENCIAL TEÓRICO

ETAPAS DO PENTEST



BACKTRACK

BackTrack é um sistema operacional baseado no Ubuntu utilizado em testes de penetração e auditorias de segurança. Ele possui uma ampla variedade de ferramentas, tais como:

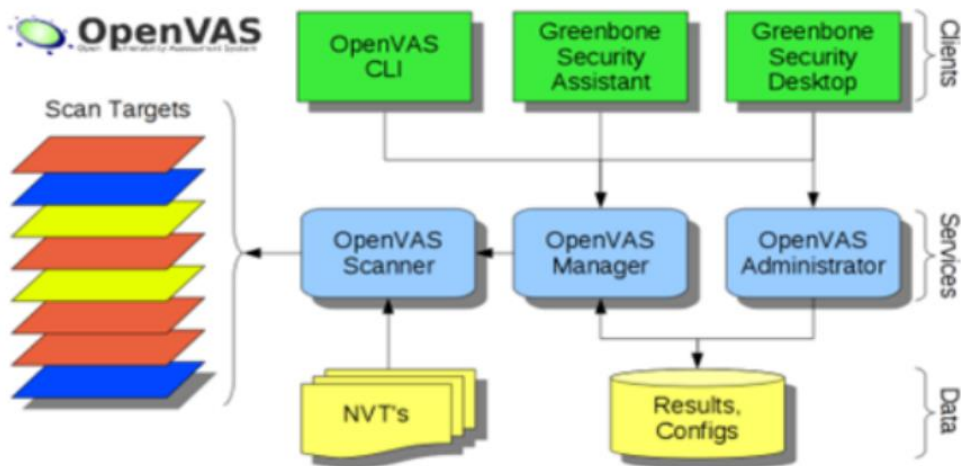
- Coleta de informações;
- Mapeamento de rede;
- Identificação de vulnerabilidades;
- Invasão;
- Elevação de privilégios;
- Manutenção de acesso;
- Eliminação de rastros;
- Analisadores de redes via rádio;
- Análise de VoIP e telefonia;
- Perícia forense digital;
- Ferramentas para engenharia reversa.

Diversas ferramentas do BackTrack podem ser utilizadas em um projeto, tais como o **OpenVAS**, **Metasploit Framework** e **SET** (Social Engineering Toolkit), durante as fases de identificação de vulnerabilidades e realização de ataques.

OPENVAS

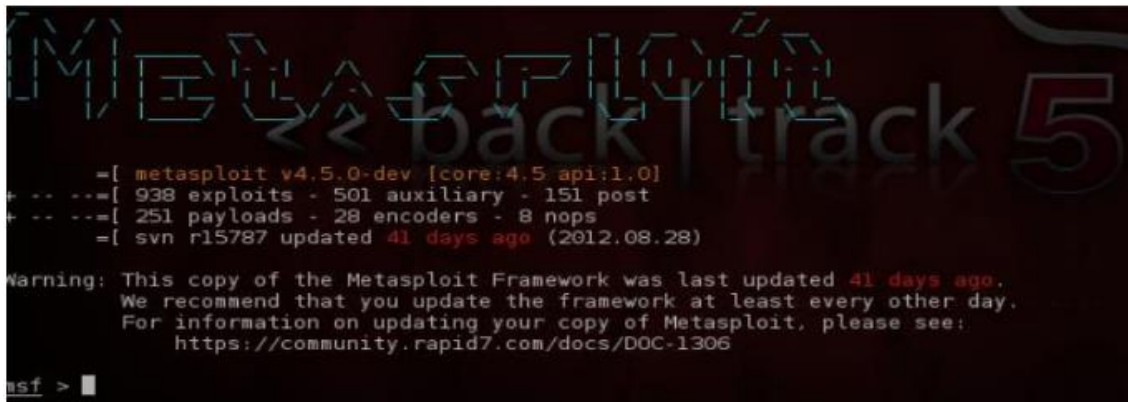
Plataforma de gerenciamento de vulnerabilidades, que opera em uma arquitetura cliente-servidor e permite a seleção de alvos na rede para testes de varreduras de vulnerabilidades. Possui vários componentes:

- **OpenVAS Scanner** gerencia a execução dos testes de vulnerabilidade de rede;
- **OpenVAS Client** controla a execução da varredura no sistema alvo;
- **OpenVAS Manager** armazena os resultados das varreduras e executa funções como agendamento de tarefas e geração de relatórios;
- **GSA** é uma interface web para configurar e gerenciar o processo de varredura;
- **OpenVAS Administrator** é responsável pela administração e logs dos usuários.



METASPLOIT FRAMEWORK

- Plataforma open source para desenvolvimento, teste e exploração de vulnerabilidades. Ajuda a "camuflar" a invasão e dificultar a detecção.;
- **Exploits** são softwares que exploram bugs ou vulnerabilidades presentes em um sistema;
- Possui três interfaces de uso: MSFCLI, MSFWeb e MSFConsole (mais eficiente e poderosa);
- Escolha do exploit e do alvo, seleção do payload e configuração das opções;
- Execução do exploit e possível fase de pós-exploração;
- **Meterpreter** é uma plataforma de exploração que permite elevação de privilégios, keylogging, criação de backdoor persistente e migração de processos;



```
Metasploit >> back | track 5

=[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- ==[ 938 exploits - 501 auxiliary - 151 post
+ -- ==[ 251 payloads - 28 encoders - 8 nops
=[ svn r15787 updated 41 days ago (2012.08.28)

Warning: This copy of the Metasploit Framework was last updated 41 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

msf > |
```

SET - Social Engineer Toolkit

Ferramenta para ataques de engenharia social que exploram fraquezas humanas. Os ataques do SET usam vetores para fornecer acesso ou informação do sistema.

- O **SphearPhishing Attack Vector** é um dos principais ataques e envolve o envio de um arquivo de exploit em formato de arquivo por e-mail para a vítima.
- Os **ataques web** são os mais completos e incluem o Java Applet, Metasploit Browser Exploit e Credentials Harvesting;
- O **Java Applet** adapta-se ao browser da vítima e entrega um payload disfarçado como serviço autêntico;
- O **Metasploit Browser Exploit** usa vulnerabilidades específicas do browser;
- O **Credentials Harvesting** clona um site como o Gmail para obter as credenciais de login do usuário.

```
The Spearphishing module allows you to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF flag to SENDMAIL=ON.
```

```
There are two options, one is getting your feet wet and letting SET do everything for you (option 1), the second is to create your own FileFormat payload and use it in your own attack. Either way, good luck and enjoy!
```

- 1) Perform a Mass Email Attack
 - 2) Create a FileFormat Payload
 - 3) Create a Social-Engineering Template
- 99) Return to Main Menu

- 1) Java Applet Attack Method
- 2) Metasploit Browser Exploit Method
- 3) Credential Harvester Attack Method
- 4) Tabnabbing Attack Method
- 5) Man Left in the Middle Attack Method
- 6) Web Jacking Attack Method
- 7) Multi-Attack Web Method
- 8) Victim Web Profiler
- 9) Create or import a CodeSigning Certificate

04

CONCLUSÃO



CONCLUSÃO

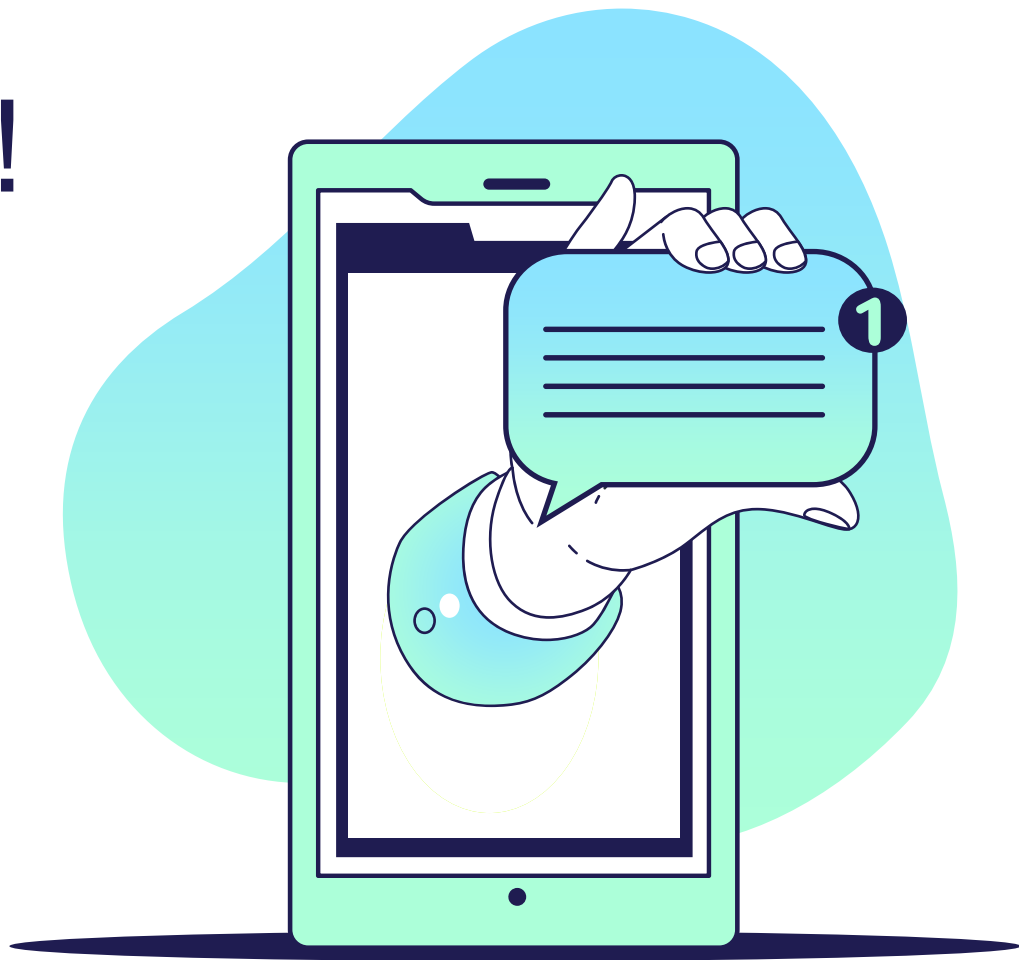
O Pentest é uma técnica preventiva de segurança da informação que identifica vulnerabilidades em sistemas e redes antes que sejam exploradas por invasores mal-intencionados. É necessário contar com profissionais qualificados e especializados, que realizem testes de forma ética e responsável, seguindo as normas e regulamentações vigentes, e ferramentas especializadas.

O BackTrack e o Social Engineer Toolkit (SET) são importantes ferramentas de Pentest, mas sua eficácia depende do conhecimento e habilidade do profissional que as utiliza.

O Pentest é fundamental para proteger os sistemas e redes de empresas e organizações, que devem investir em profissionais qualificados e em ferramentas especializadas para garantir a segurança de suas informações e dados sensíveis.

OBRIGADO!

Alguma pergunta?



REFERÊNCIAS BIBLIOGRÁFICAS

- ALI, R. M.; HERIYANTO, E. A. **Backtrack as a Penetration Testing Tool: An Overview**. 2011 International Conference on Electrical Engineering and Informatics, Bandung, Indonesia, 2011. Proceedings... Piscataway: IEEE, 2011. p. 1-4. Acesso em: 13 de abril de 2023.
- ALLSOPP, Will. **Advanced penetration testing: hacking the world 's most secure networks**. Indianapolis: Wiley, 2017. Acesso em: 30 de março de 2023.
- ASSUNÇÃO, Marcos Flávio Araújo. Segredos do Hacker Ético. 5. ed. Florianópolis: Editora Visual Books, 2014. Acesso em: 11 de abril de 2023.
- BERTOGLIO, Daniel Dalalana; ZORZO, Avelino Francisco. **Um Mapeamento Sistemático sobre Testes de Penetração**. 2015. 42 f. Monografia (Doutorado) - Curso de Pós-Graduação em Ciência da Computação, Pontifícia Universidade Católica do Rio Grande do Sul Faculdade de Informática, Porto Alegre, 2015. Acesso em: 11 de abril de 2023.
- BHARDWAJ, R., & SINGH, J. P. An approach to penetration testing of cloud computing infrastructure. In 2017 IEEE 7th International Advance Computing Conference (IACC) (pp. 145-150). IEEE. 2017. Acesso em: 12 de abril de 2023.
- CALDERÓN, J. M. **The penetration testing execution standard 2.0**. The SANS Institute, 2015. Acesso em: 12 de abril de 2023.
- KENNEDY, David et al. **Metasploit: The Penetration Tester 's Guide**. No Starch Press, 2011. Acesso em: 30 de março de 2023.
- PINTO, L. M.; FERNANDES, R. M. **Um estudo sobre as etapas do Pentest e a importância do relatório de testes**. Revista Brasileira de Computação Aplicada, v. 10, n. 1, p. 1-12, 2018. Acesso em: 12 de abril de 2023.
- SINGH, A., & ARORA, S. **A comprehensive study of penetration testing tools, techniques, and methodologies**. International Journal of Engineering Research & Technology, 10(3), 464-468. 2021. Acesso em: 12 de abril de 2023.
- SOOD, A. K., & ANAND, A. **Comprehensive approach to penetration testing**. 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICIC) (pp. 1-6). IEEE. Acesso em: 12 de abril de 2023.
- STUTTARD, Dafydd; PINTO, Marcus. **The Web Application Hacker 's Handbook: Finding and Exploiting Security Flaws**. 2nd ed. Indianapolis: Wiley Publishing, 2011. Acesso em: 29 de março de 2023.
- VERIZON. **Data Breach Investigations Report**. 2020. Acesso em: 29 de março de 2023. Disponível em: <<https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>>.
- WEIDMAN, Georgia. **Penetration Testing: A Hands-On Introduction to Hacking**. No Starch Press, 2014. Acesso em: 30 de março de 2023.
- ZOURIDAKI, C., & ANTONATOS, S. **A survey of penetration testing methodologies in cloud environments**. Future Internet, 8(4), 51. 2016. Acesso em: 12 de abril de 2023.