Comunidade LIFE 4 SEC
WWW.LIFE4SEC.COM.BR

Campus Party™

EPU
Engineers and Programmers United

COMO GERENCIAR UM RED TEAM

WWW.LIFE4SEC.COM.BR

Comunidade LIFE 4 SEC
WWW.LIFE4SEC.COM.BR

Campus Party™

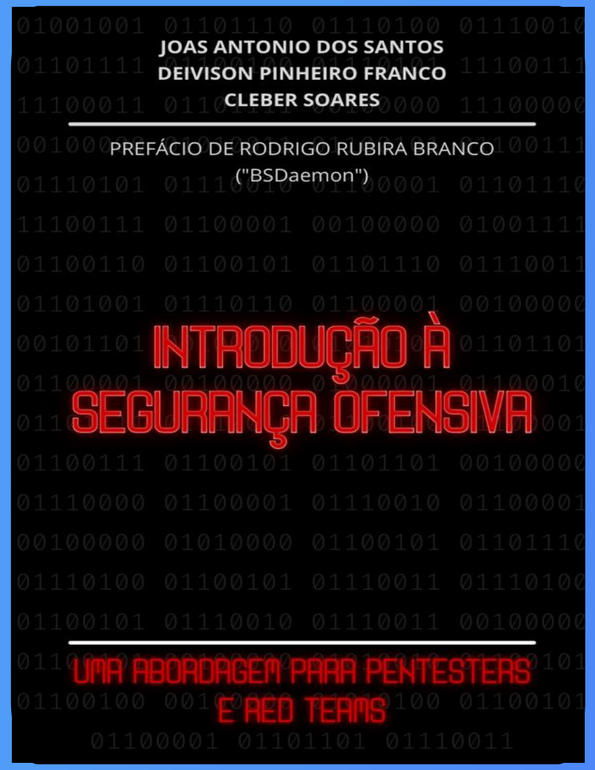
EPU
Engineers and Programmers United

- Red Team Leader, PenTester, Instrutor;
- Possuo algumas CVE's publicadas;
- Contribuidor do Mitre Att&ck;
- +90 Certificações internacionais;
- Synack Red Team Member;
- Autor e Palestrante;

WWW.LIFE4SEC.COM.BR

Comunidade LIFE 4 SEC
WWW.LIFE4SEC.COM.BR

Campus Party™



Spoiler

Joas Santos

Deivison Franco

Cleber Soares

WWW.LIFE4SEC.COM.BR

Comunidade LIFE 4 SEC
WWW.LIFE4SEC.COM.BR

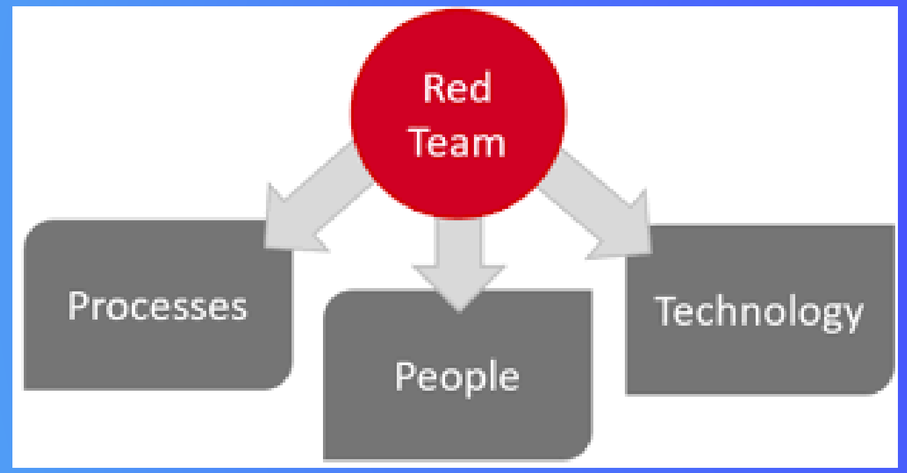
Campus Party™

EFU Engineers and Programmers United

O que é Red Team?

- Processo importante para validar os controles de segurança interno e externo
- Criar e melhorar o gerenciamento de vulnerabilidades
- Aprimorar um plano de testes de segurança e simulação de ataques

WWW.LIFE4SEC.COM.BR



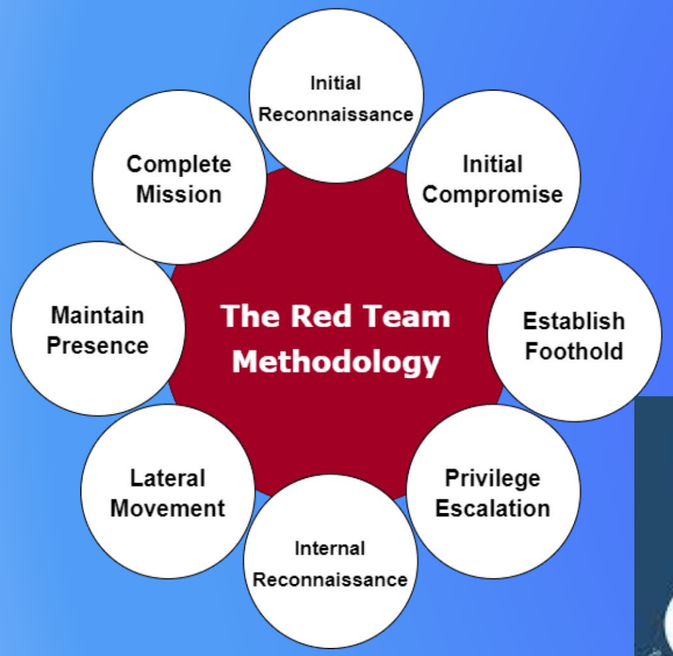
- Processos: Métodos e procedimentos que vão ser utilizados
- Pessoas: Conhecimento, motivação e com ambiente propicio para atuação
- Tecnologia: Ferramentas que vão ser utilizadas para o objetivo

Comunidade LIFE 4 SEC
WWW.LIFE4SEC.COM.BR

Campus Party™

EPU Engineers and Programmers United

Processos



MITRE ATT&CK™

- Implementar programas de gestão de vulnerabilidades, patchs e riscos
- Criar cronogramas de campanhas de Red Team (PenTest, Engenharia Social, Conscientização, Testes de controles de segurança e etc
- Implementar frameworks e metodologias de mercado

Comunidade LIFE 4 SEC
WWW.LIFE4SEC.COM.BR

Campus Party™

EPU Engineers and Programmers United

Pessoas

- Investir em capacitação de profissionais nas tecnologias utilizadas internamente
- Prover certificações para aumentar as Skills técnicas
- Criar um meio de comunicação efetivo entre os times de segurança
- Gerar engajamento através de eventos e ações internas

Comunidade LIFE 4 SEC
WWW.LIFE4SEC.COM.BR

Campus Party™

EPU Engineers and Programmers United

Tecnologia

- Implementar soluções de cibersegurança para gestão e analise de vulnerabilidades
- Orquestrar tecnologias com soluções de Blue Team
- Operacionalizar ferramentas para testes de segurança e simulação de adversários

CALDERA

KALI

ATOMIC RED TEAM

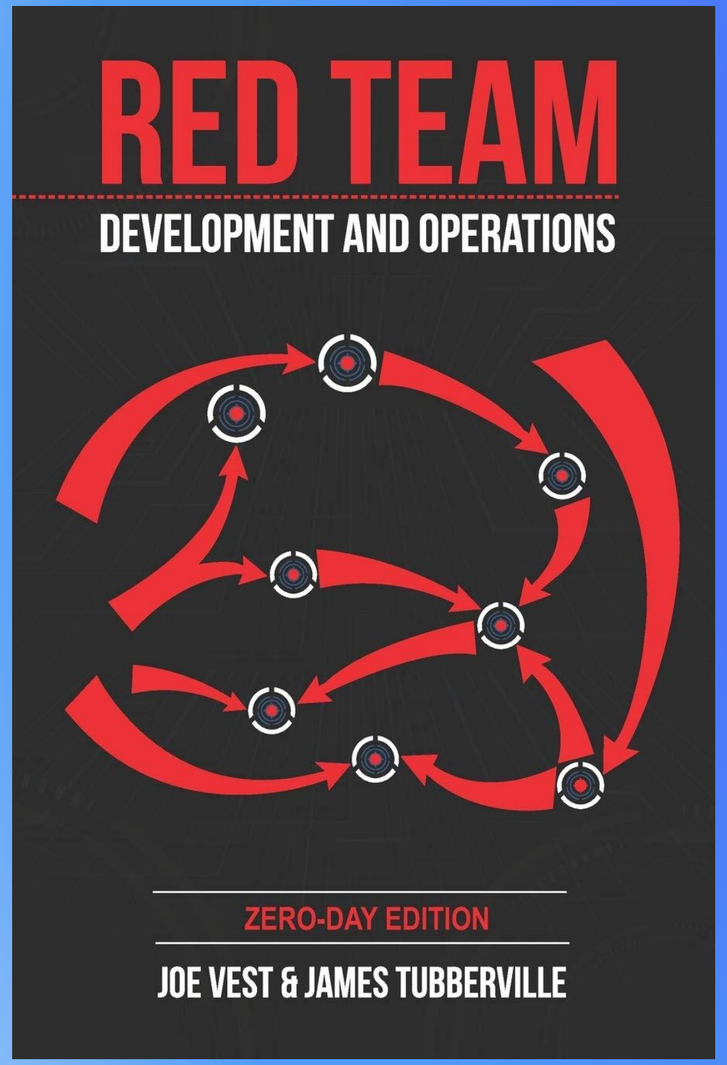
tenable

KnowBe4

HAK5

Comunidade LIFE 4 SEC
WWW.LIFE4SEC.COM.BR

Campus Party™



Como gerenciar o seu Red Team?

- Criar documentações para endereçar melhor a área internamente, exemplo: ROE para autorizar exercicios de Red Team dentro de um sistema
- Criar um perfil de ameaça com base no seu modelo de negócio (O mitre att&ck pode ajudar)
- Desenvolver guias e funções de responsabilidade
- Criar modelos de relatório de resumo técnico e totalmente técnico

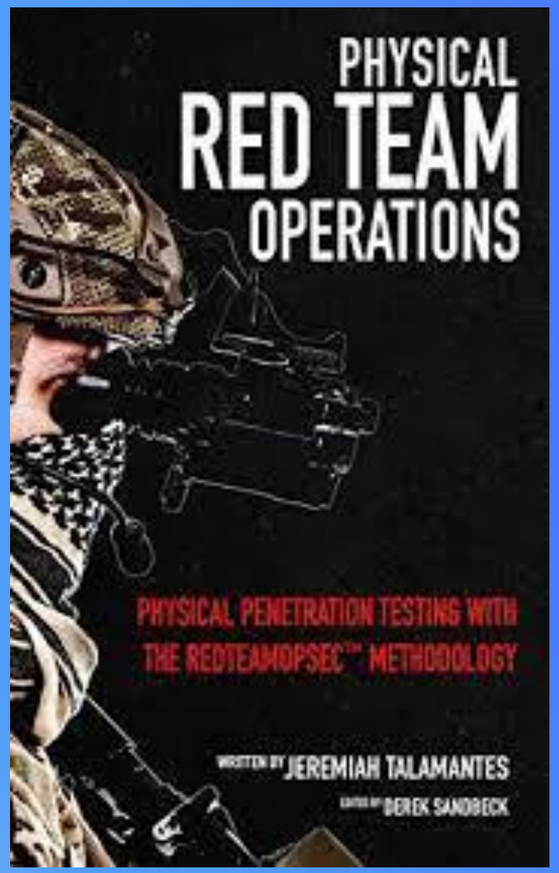
WWW.LIFE4SEC.COM.BR

Comunidade LIFE 4 SEC
WWW.LIFE4SEC.COM.BR

Campus Party™

EPU Engineers and Programmers United

Como gerenciar o seu Red Team?



- Criar um escopo em cima das tecnologias da empresa
- Planejar infraestrutura para a simulação de uma ameaça
- Desenvolver um repositório para coletar os engajamentos realizados
- Definir objetivos comuns dentro de um perfil de ameaça
- Brigar pelo Budget interno da área

WWW.LIFE4SEC.COM.BR

Comunidade LIFE 4 SEC
WWW.LIFE4SEC.COM.BR

Campus Party™

EPU
Engineers and Programmers United

OBRIGADO!

SCAN ME

WWW.LIFE4SEC.COM.BR