RED TEAM

VS

BLUE TEAM

Whoami

- Thiago Cunha
- 30 anos
- Red Team e Threat Intel Tech lead
- LinkedIn: thiagocunhasilva
- Github: Blu3B3ard
- Hobbies:
  - CTF
  - Livros
  - Quebrar coisas

Threat Actor

- Podem ser mas não limitados há
  - Pessoas
  - Empresas
  - Governos
  - Grupos
  - Entre outros
- Qual o objetivo deles?
  - Sujar reputações
  - Causas políticas
  - Lucro
  - Entre outros

Técnicas, Táticas e Procedimentos - TTPs

- **Tática** – Descreve o jeito que um atacante realiza o ataque do início ao fim.
- **Técnica** – Os métodos que são usados pelos atacantes para atingir os objetivos durante o ataque.
- **Procedimentos** – Definição de como o Threat Actor vai iniciar o ataque e a quantidade de ações dependendo do objetivo.

Historia

- 1964 – Criado o termo para o Programa de Gerenciamento de Design e Desenvolvimento de aeronaves espaciais.
- 1970 – Utilizado um Tiger Team na missão APOLLO 13.
- 197X – Utilizado pelos militares para resolução de problemas críticos

Qual o intuito de um Tiger Team?

- Criado para resolução de 1 ou mais problemas extremamente complexos.
- Grupo de especialistas com diversas origens e áreas de atuação separadas

Tiger Team em Cyber Security

- Modelo extraído dos militares:
  - 1 grupo de defesa
  - 1 grupo de ataque
- Equipes divididas em cores:
  - Blue Team – Defesa
  - Red Team – Ataque

Blue Team

- Responsabilidades:
  - Defender a empresa
  - Realizar resposta a incidentes
  - Controlar possíveis dados
  - Caçar ameaças cibernéticas
  - Realizar forense computacional
  - Conscientização de colaboradores
  - Operar e orquestrar ferramentas de segurança:
    - Firewall
    - IPS/IDS
    - SIEM
    - Antivírus
    - Outras Soluções

Red Team

- Responsabilidades:
  - Atacar a empresa (teste de invasão)
  - Realizar ataques de Engenharia Social
  - Explorar vulnerabilidades
  - Simulação de ataques reais (Black Box)
  - Scans de vulnerabilidades
  - Criar report com as vulnerabilidades encontradas
  - Analisar sistemas, escritórios, dispositivos, códigos, etc.
  - Campanhas de phishing
  - Monitoramento de vulnerabilidades, técnicas e táticas atuais utilizadas por hacktivistas

Quem faz parte do Red?

- Breakers - Quebradores
- Engenheiros Sociais
- Hacker Éticos
- Programadores
- Analistas de Marketing
- Analistas de Segurança da informação

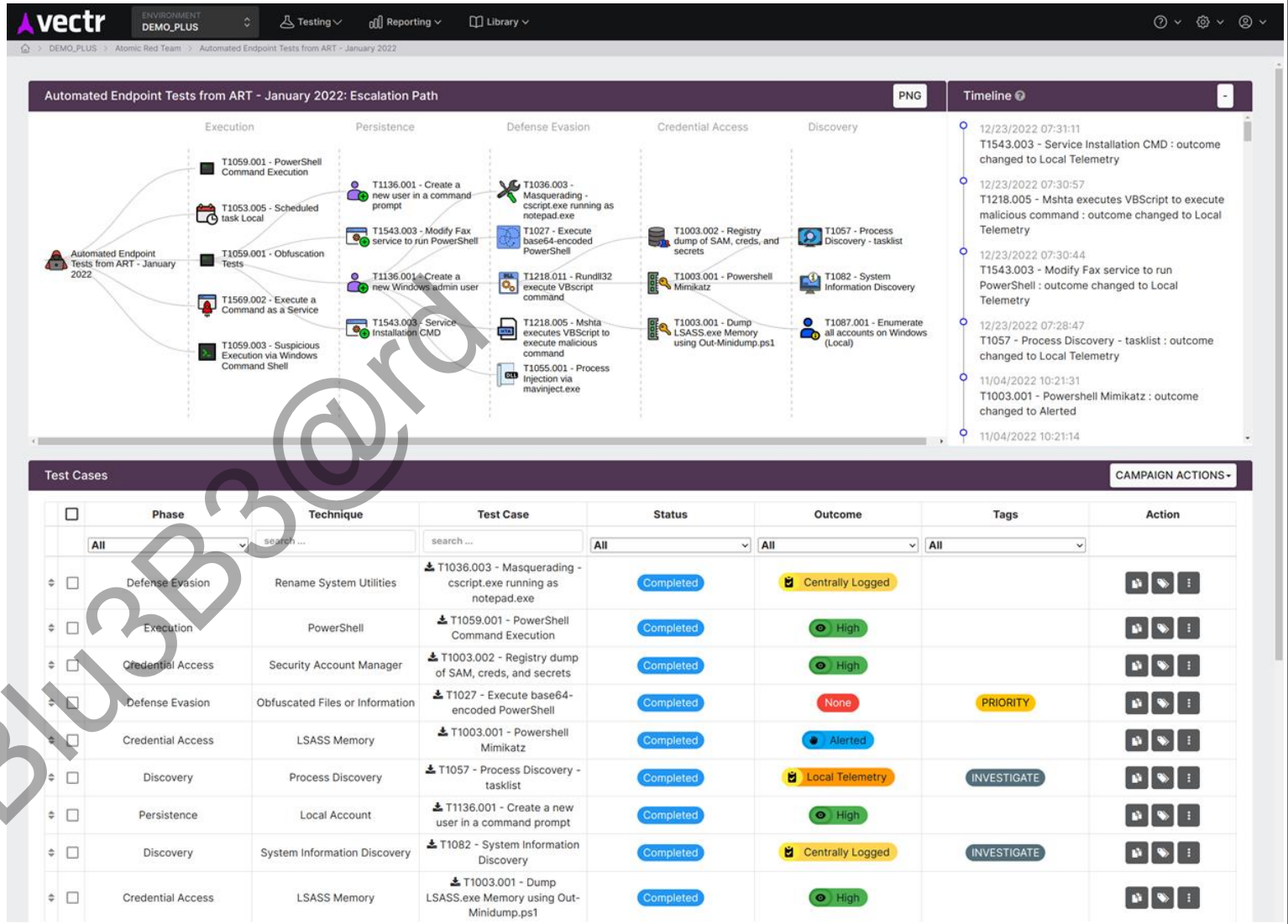
Operação de Red Team

- Ações de mimetismo podendo se passar mas não limitado a
  - APT
  - Fraudadores
  - Hacktivistas
  - Webscrappers
  - Scammers
  - Unicórnio? 

This guy taps into your girls mainframe, what do you do?

O que faço com o ataque?

- Registra tudo
- Mapeia os itens abaixo
  - Ataques realizados
  - Linha do Tempo
  - Nível de detecção (se houve)
  - Etapas do Ataque
  - Coleta e armazena evidências

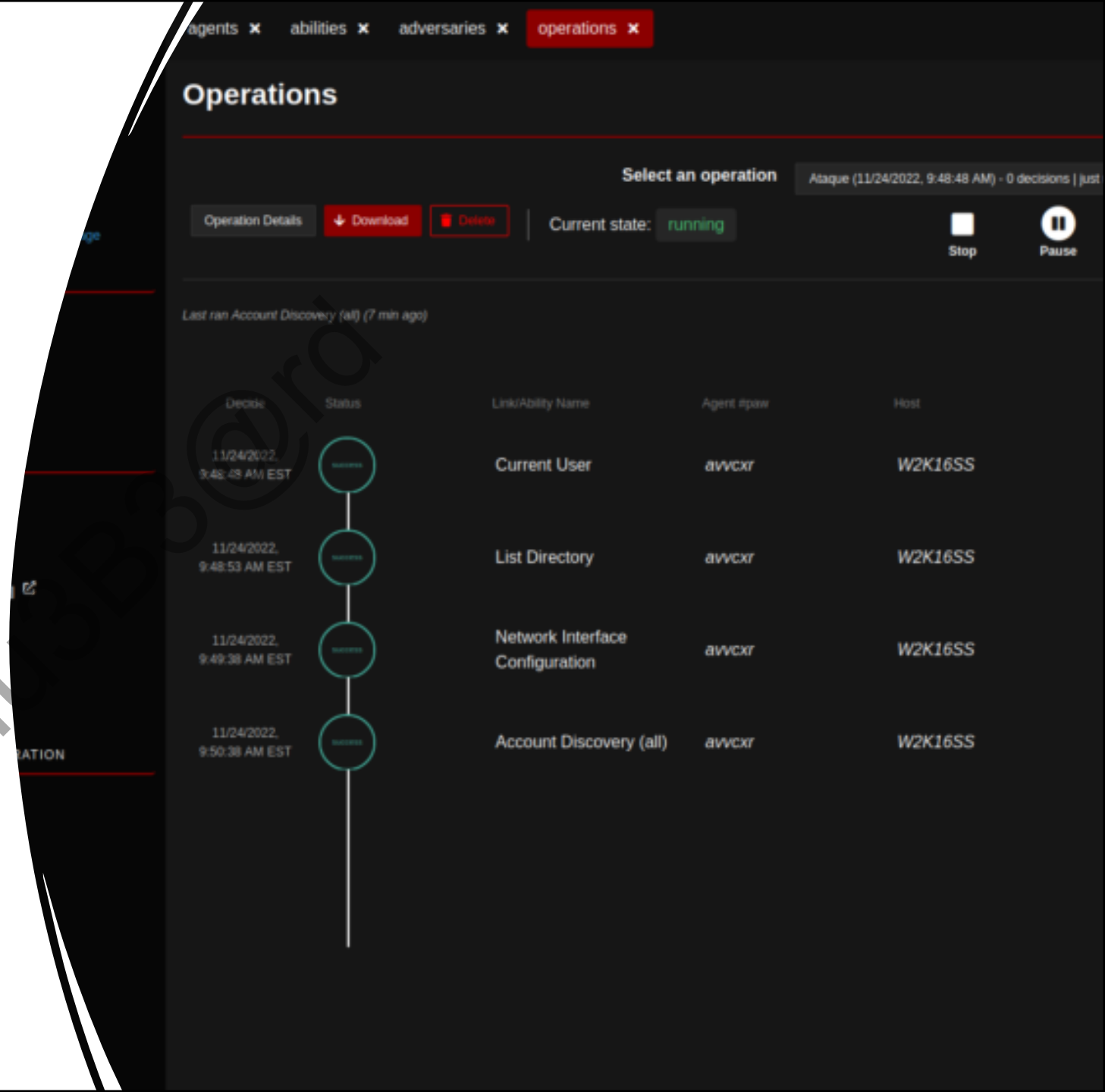


Finalizei a operação, e agora?

- Criação de report
- Apresentação dos resultados para
  - C-level
  - Áreas de defesa cibernética
  - Stakeholders

Automação é uma escolha?

- Sim, mas não pré requisito para execução
- Softwares que podem te auxiliar
  - Cobalt Strike
  - Cymulate
  - Caldera
  - Vectr
  - Entre outros



Blz, resume por favor?

- Longos períodos de trabalho em operação
- Trabalho em equipe
- Trabalhos mais elaborados
- Desenvolvimento de ferramentas
- Conhecimento e atuação 360º

Gostei, por onde começo?

- Os conhecimentos abaixo são requisitos base:
  - **Redes**
  - **Sistema Operacional**
  - **Cloud**
  - **Programação**
  - **Inglês**
  - Marketing
  - Engenharia Social
  - Criptografia
  - Costura
  - Eletrônica
  - Tudo

Fontes

- Frameworks
  - Mitre
  - NIST
  - ISO27001
- Cursos Oferecidos nas instituições
  - ACADTI
  - Academia de Forense Digital
  - Alura
  - Sec4us
  - Gohacking

Livros

- Red Team Development and Operations: A practical guide (English Edition)
- Manual de persuasão do FBI
- Como convencer alguém em 90 segundos
- Ghost in the Wires
- RFTM: Red Team Field Manual v2
- Hacking APIs
- Técnicas proibidas de Persuasão, manipulação e influência usando padrões de linguagem e de técnicas de PNL

Pratica é necessária?

- “Prática leva a perfeição” – Joemar Rios de Oliveira
- Fiz os cursos, estudei e agora?
- Existem plataformas para você praticar seu conhecimento:
  - Hack the box – inglês
  - Try Hack Me - inglês
  - Pentester Academy - Inglês
  - UHC labs - Português

Pessoas

- **Igor Rincon - rinconzeraa**
- **Rafael Sousa – Hackingnaweboficial**
- **Daiane Santos – wh0isdxk**
- **Marina Ciavatta – marinaciavatta**
- **Julio Dellaflora – juliodellaflora**
- **Davi Mikael – Penegui**
- **Sabrina Ramos – meninadecybersec**
- **Carlos Vieira - carlos.crowsec**
- **Thiago Cunha – blu.ebeard**

Eventos

- Boitatech – Online - Brasil
- MindSec – Online/Presencial - Brasil
- RoadSec – Online/Presencial - Brasil
- CryptoRave – Presencial – Brasil
- BlackHat – Online/Presencial – Estados Unidos
- DEFCON – Online/Presencial – Estados Unidos/China
- The Developer's Conference (TDC) – Online/Presencial - Brasil

Podcasts

- **Segurança Legal – PtBr**
- **Hipsters Ponto Tech – PtBr**
- **SecurityCast – PtBr**
- **The Privacy, Security & Osint – En**
- **Red Team Podcast – En**
- **Cyber Work – En**
- **Hackers Brasil - PtBr**


Duvidas?
Blu3B3@rd

Acabou?

Let the game beging