

INTRODUÇÃO A SEGURANÇA OFENSIVA

LEONARDO FERREIRA



HACKERMAN

AGENDA

- Segurança da Informação (Conceito)
- Áreas de Segurança da Informação
- Segurança Ofensiva
- Análise de Vulnerabilidades
- Pentest
- Red Team
 - Cenário de um Red Team real
- Perfil de Profissional de Segurança Ofensiva
- Treinamento
- Livros
- Certificações
- Canais no Youtube

#WHOAMI

- Leonardo Ferreira
- Eng Comp (UFES), ex-aluno ~~CEFETES~~-IFES
- Líder técnico do Red Team da iSecurity Inc. 🇨🇦 (a Calian company)
- +5 anos trabalhando diariamente com Pentest, Red/Purple Team, simulações adversariais, etc etc...
- Certificações na área: OSWE, OSCP, CRTE, CTO, CARTP, Pentest+, DCPT
- Já reportei bugs pra Microsoft, Facebook, BMC, Cisco, DoD-EUA
- *Sou péssimo em falar em público, mas amo compartilhar conhecimento, me chama aí 😊*
 - Estou quase o dia todo no telegram: [at]frr3ir4s6



SEGURANÇA DA INFORMAÇÃO

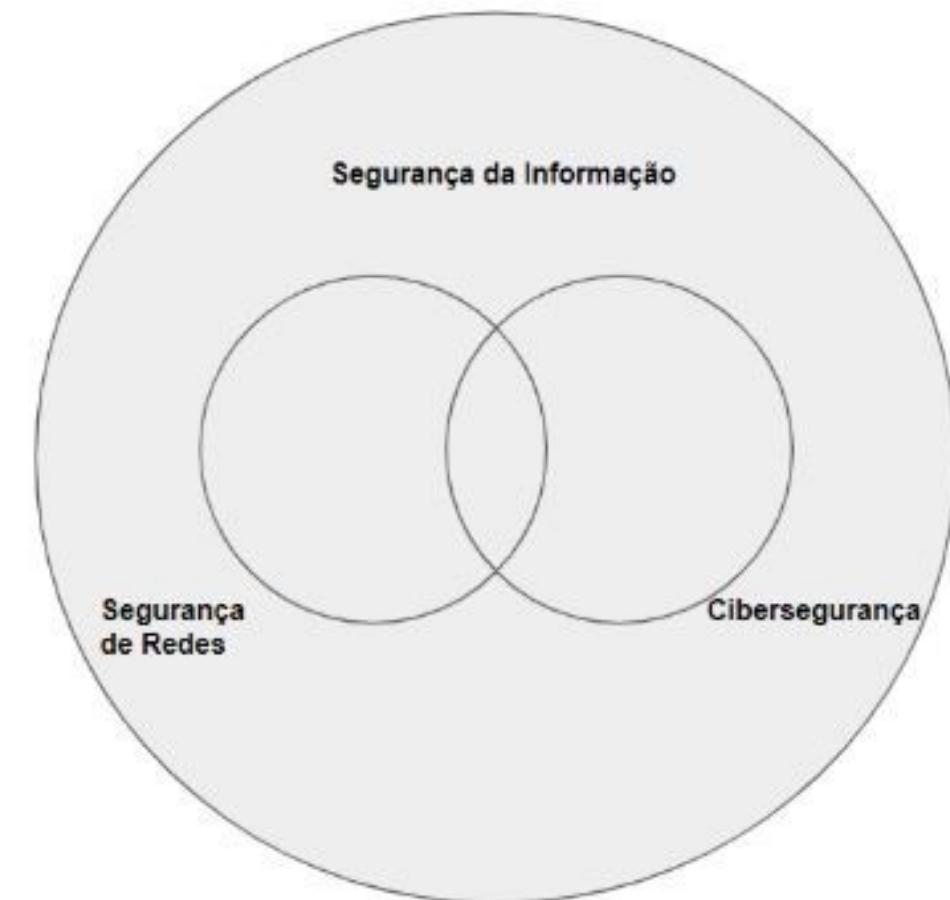
- Segurança da informação é o processo de proteger a informação de diversos tipos de ameaças externas e internas para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio. Segurança se faz protegendo todos os elos da corrente, ou seja, todos os ativos (físicos, tecnológicos e humanos) que compõem seu negócio.
- “Uma corrente é tão forte quanto seu elo mais fraco”.
- “The weakest link in the security chain is the human element.” – Kevin Mitnick

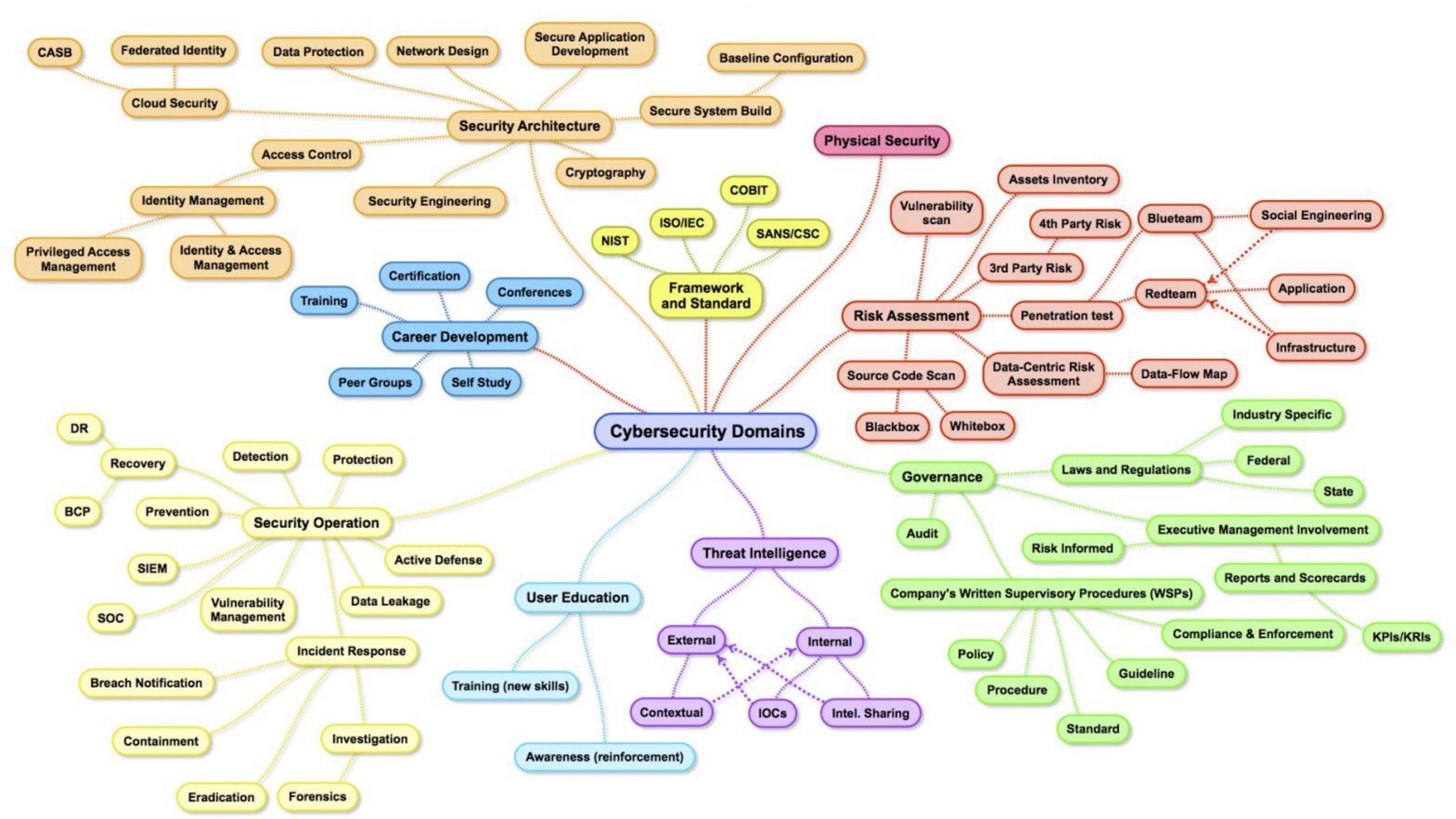
ÁREAS DE SEGURANÇA DA INFORMAÇÃO

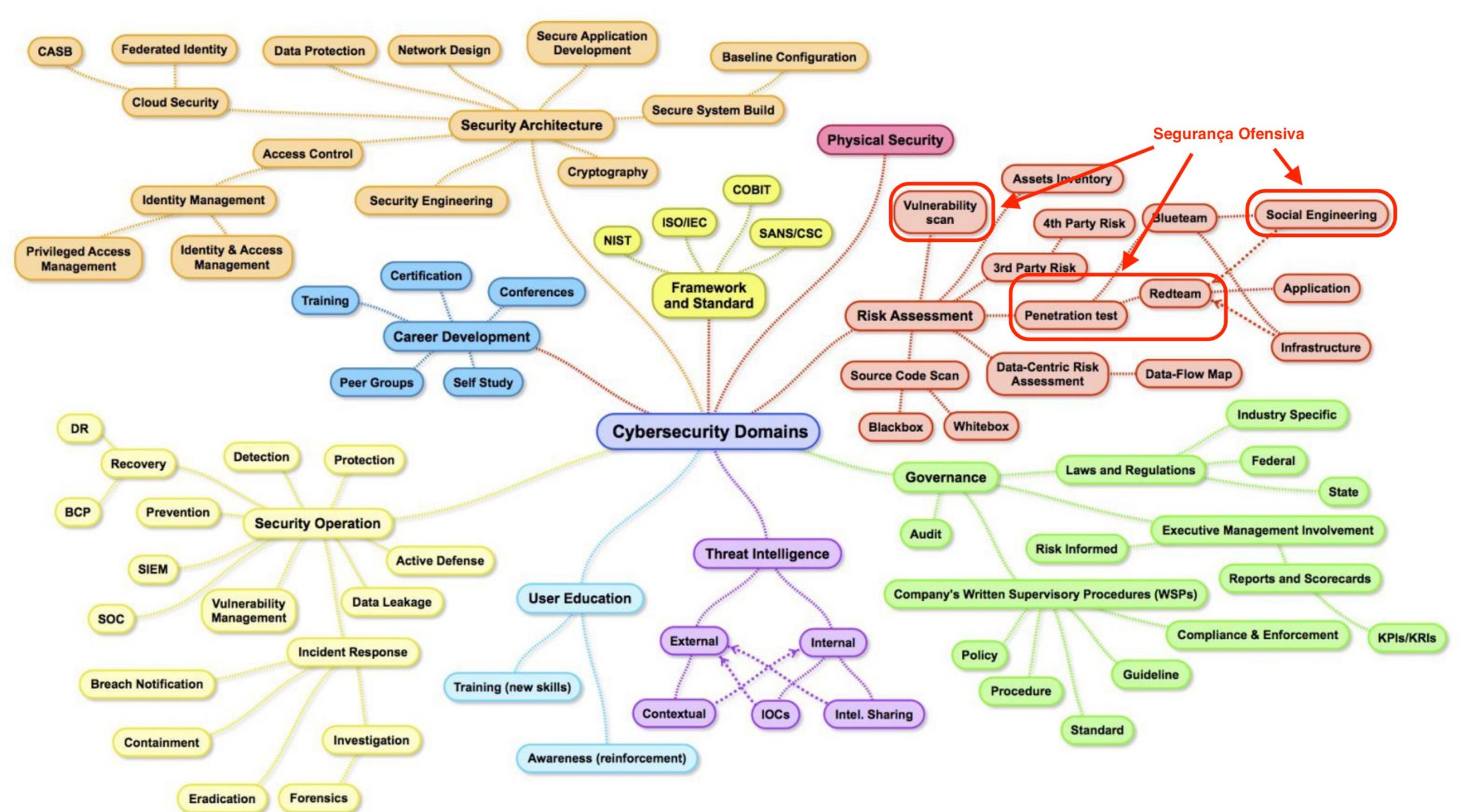
- Segurança da informação é uma área **MUITO** abrangente.
- **Ser um profissional de Segurança da Informação não quer dizer que você consegue fazer qualquer coisa dentro dessa área. Há muitos perfis totalmente diferentes um dos outros e todos podem carregar o mesmo nome, ex:Analista de Segurança da Informação.**

ÁREAS DE SEGURANÇA DA INFORMAÇÃO

- **Segurança de Redes:** Tem por objetivo proteger os dados que estão percorrendo pela rede de computadores através dos ativos de rede. Para realizar essa proteção nos deparamos com uma infinidade de técnicas e controles que normalmente são executadas através de equipamentos ou tecnologias como: Firewall, WAF, Antivírus, IDS/IPS, Storages (backups)
- **Cibersegurança:** Tem por objetivo a proteção das informações que estão num formato digital e estão percorrendo por todo o ciberespaço.







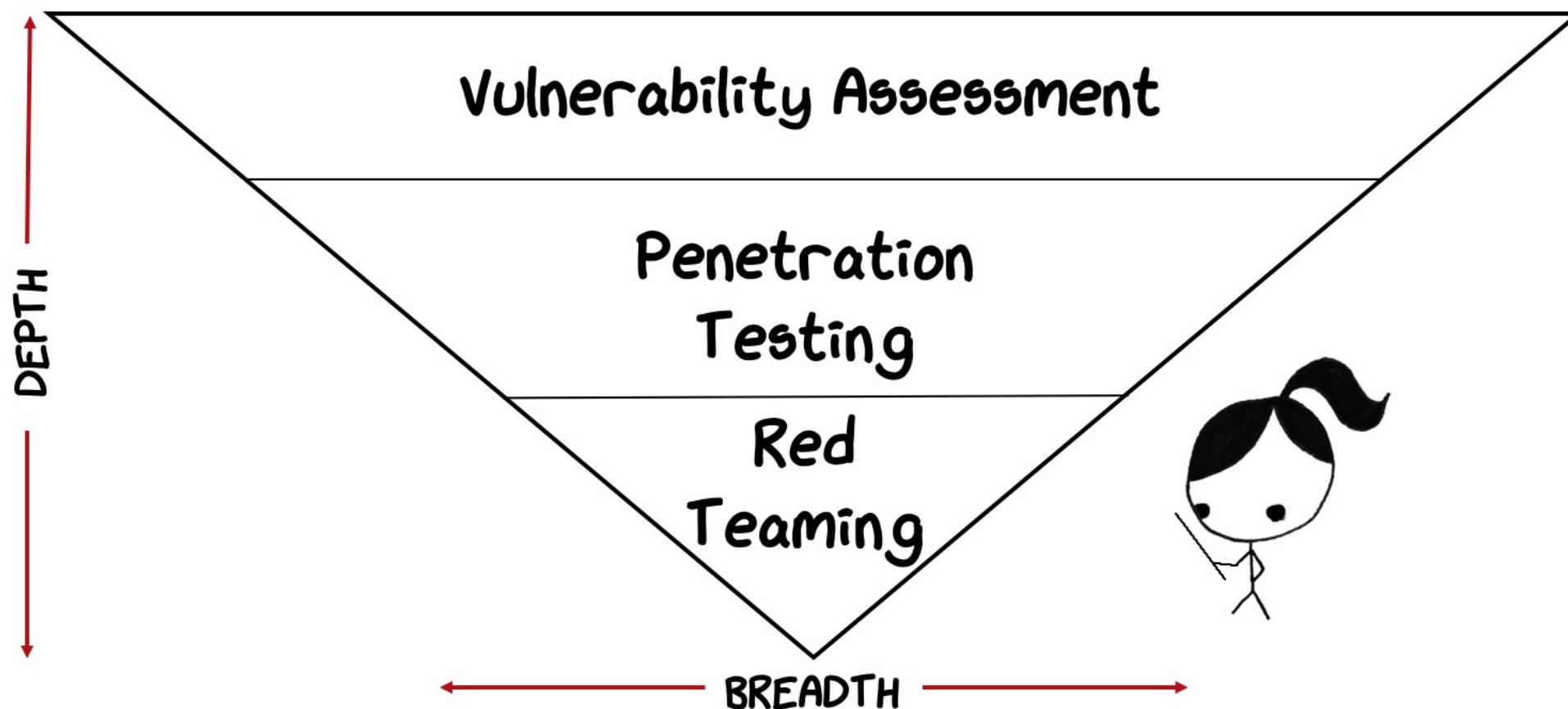
SEGURANÇA OFENSIVA (OFFENSIVE SECURITY)

- Também conhecida como *Ethical Hacking*.
- Trata-se de uma abordagem **proativa**, que visa testar a segurança de máquinas/redes por meio de **testes de intrusão** (*Penetration Tests, Red Team, exercícios de “Escalação de Privilégios”, etc*).
- Parte do princípio que você não precisa esperar por uma tentativa de invasão e violação de dados para entender como se proteger de uma ameaça.
- “**A melhor defesa é o ataque**”... e vice-versa!

SEGURANÇA OFENSIVA (OFFENSIVE SECURITY)

- É uma abordagem que olha pra diferença entre “o que se pensa/sabe sobre a segurança de um sistema/rede” e o que **de fato** ela é.
- Para efetivamente testar a segurança de ativos, serão replicadas TTPs (táticas, técnicas e procedimentos) utilizadas por atacantes reais.
 - **Análise de Vulnerabilidades**
 - **Testes de Intrusão (*Penetration Test*)**
 - **Red Team**
 - E outros: *Purple Team (Red Team + Blue Team), Adversary Simulation, Ransomware Simulation...*

SEGURANÇA OFENSIVA (OFFENSIVE SECURITY)



ANÁLISE DE VULNERABILIDADES

- A análise de vulnerabilidades pode ser definida como o processo de avaliação e identificação de falhas e potenciais ameaças à segurança de ativos (computadores, aplicações web, aplicações móveis, etc). Ou seja, são brechas na segurança que podem facilitar o ataque de agentes maliciosos.
- Na maioria das vezes, é utilizado um “scanner” de vulnerabilidades
 - Nessus (Tenable), OpenVAS -> Foco em infraestrutura.
 - Acunetix, NetSparker, IBM AppScan -> Foco em aplicações web/APIs.

ANÁLISE DE VULNERABILIDADES

- Scanners utilizam-se de “plugins”/módulos para identificar vulnerabilidades já conhecidas. Como?
 - Análises baseadas em assinaturas (“Log4j 2.3.1”, “Drupal 7”, “Windows XP”)
 - Análises baseadas em comportamento (*behavior-based*).
 - Exemplo: Quando um scan web encontra um campo de entrada, ele ativamente envia cargas (“payloads”) que podem ser inesperadas à aplicação e analisa como a aplicação reage à elas.
 - Scanners de rede são quase sempre baseados em assinaturas.
 - Scanners web são quase sempre baseados em comportamento.

FOLDERS

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Customized Reports

Basic network Scan

[◀ Back to My Scans](#)

Configure Audit Trail Report Export ▾

Hosts 112

Vulnerabilities 272

Remediations 500

VPR Top Threats 3

Filter ▾

Search Hosts

112 Hosts

Host	Vulnerabilities
192.168.1.46	147 Critical 278 High 59 Medium 189 Info
192.168.1.83	60 Critical 333 High 86 Medium 184 Info
192.168.1.10	42 Critical 320 High 81 Medium 186 Info
192.168.1.53	28 Critical 48 High 508 Info
192.168.1.44	39 Critical 293 High 78 Medium 169 Info
192.168.1.66	22 Critical 228 High 52 Medium 174 Info
192.168.1.55	113 Critical 172 High 29 Medium 130 Info
192.168.1.40	65 Critical 154 High 88 Medium 56 Info
192.168.1.56	48 Critical 166 High 41 Medium 66 Info
192.168.1.11	15 Critical 87 High 178 Info
192.168.1.12	15 Critical 87 High 177 Info
data.tehgeek.local	12 Critical 266 Info
sshsrv.tehgeek.local	26 Critical 16 High 225 Info

! Notice: This scan has been updated with Live Results. [Launch](#) a new scan to confirm these findings or [remove](#) them.

Scan Details

Policy: Basic Network Scan

Status: Imported

Severity Base: CVSS v3.0

Modified: April 1 at 1:00 PM (Live Results)

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info



Discovery

Targets

Scans

Scheduling

Reports

Vulnerabilities

Policies

Notifications

Integrations

Team

Activity

Agents

Settings

**4** User

2 user was active in the last week

20 Websites

3 Critical, 7 High

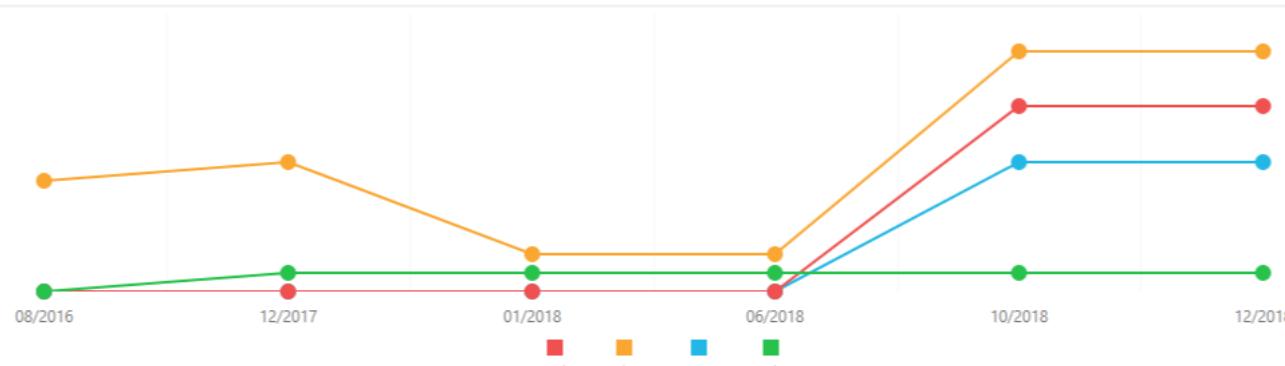
12 Completed Scan

Completed in 00:20:05 on average

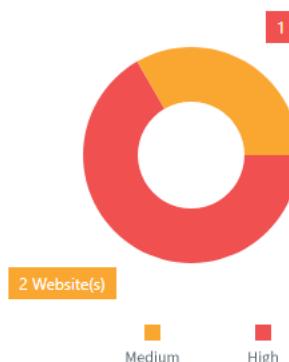
10 Act. Vulnerabilities

4 High, 6 Medium

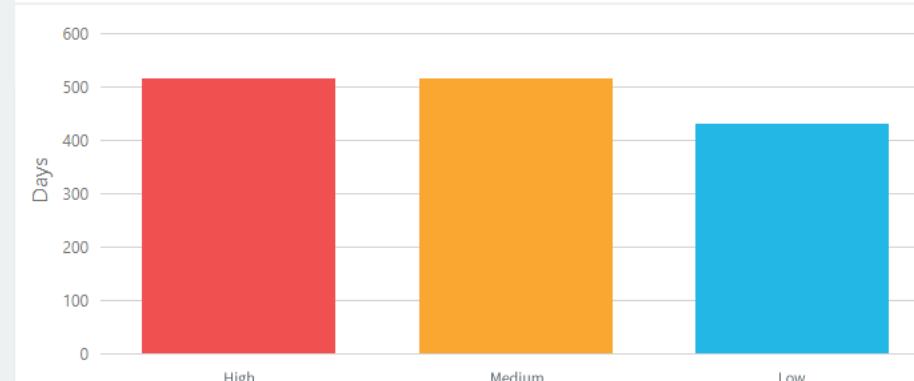
Open Vulnerabilities



Open Vulnerabilities



Average Time to Fix



Recent Scans

<http://testhtml5.vulnweb.com>

11 3

<http://testphp.vulnweb.com>

3 6

<http://testasp.vulnweb.com>

5 4

<http://testaspnet.vulnweb.com>

15 1

<http://test.vulnweb.com>

2 12

Top Vulnerabilities

Cross site scripting

3

Source code disclosure

6

Backup files

4

Blind SQL Injection

1

Directory listing

12

ANÁLISE DE VULNERABILIDADES

- Respeita-se o escopo dos testes (*Rules of Engagement*).
 - Janela de execução.
 - Data de início e término.
 - Ativos que serão avaliados.
 - **Exclusões!**
- O cliente está todo o tempo **ciente** da execução da análise de vulnerabilidades.

ANÁLISE DE VULNERABILIDADES

- O resultado de scans de vulnerabilidades podem conter **falsos positivos**.
- Falsos positivos: Vulnerabilidades que foram encontradas pelo scan mas que na verdade não existem.
- Exemplos:
 - Latência na rede fez com que um host demorasse muito a responder um teste de SQL Injection baseado em tempo. Scan poderia retornar falsos positivos do tipo “*Time-Based Blind SQL Injection*”.
 - Versão vulnerável, mas um patch foi aplicado para correção.
- É papel do analista tratar (sempre que possível) todos os falsos positivos de um resultado de scan.

TESTES DE INTRUSÃO (PENETRATION TEST)

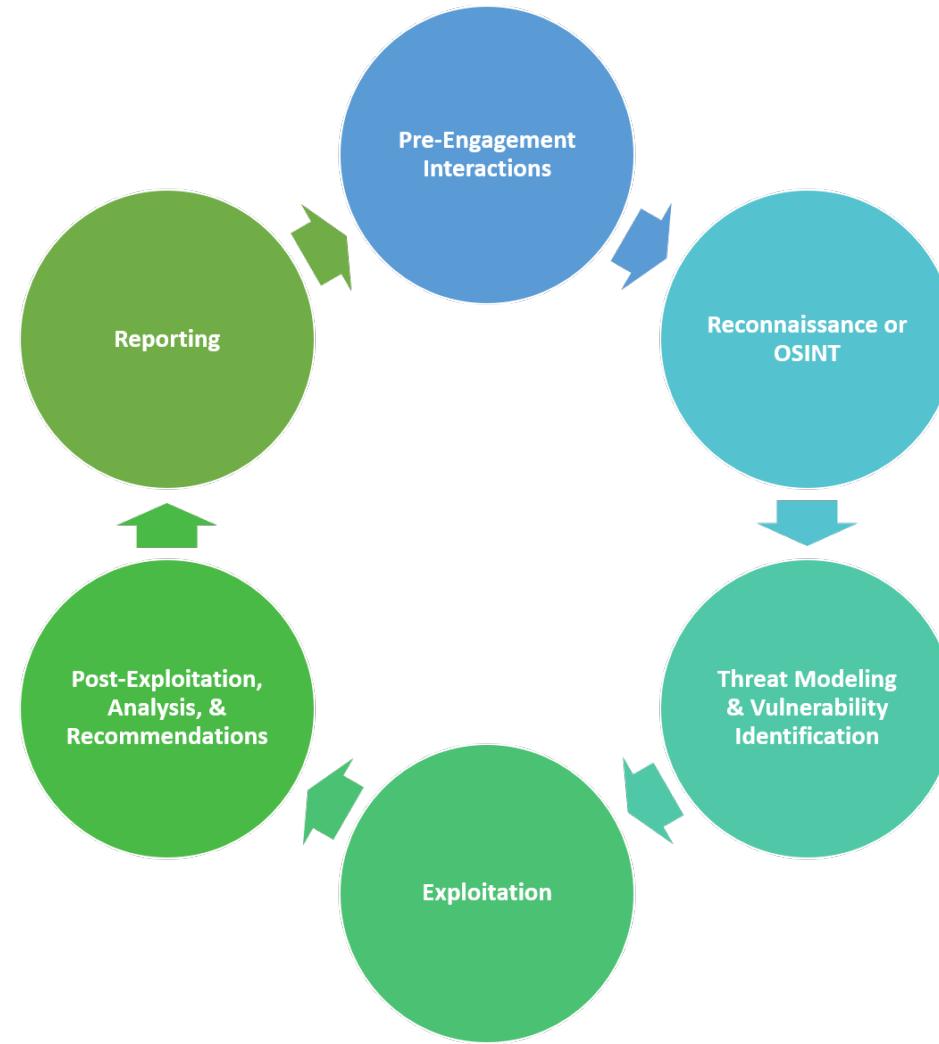
- Um teste de intrusão, *Pentest*, é uma avaliação de segurança que visa identificar e **explorar** pontos vulneráveis em uma organização a partir de um escopo definido entre as partes.
- Tem tempo limitado.
- Um *Pentester*, por vezes chamado de *Ethical Hacker*, tem a responsabilidade de conduzir o teste em questão utilizando metodologias e Frameworks.
- Pentest é feito combinando técnicas manuais e automatizadas.

TESTES DE INTRUSÃO (PENETRATION TEST)

- Respeita-se o escopo dos testes (*Rules of Engagement*).
 - Janela de execução.
 - Data de início e término.
 - Ativos que serão avaliados.
 - **Exclusões!**
- O cliente está todo o tempo **ciente** da execução do pentest.

TESTES DE INTRUSÃO (PENETRATION TEST)

- “Ciclo de vida” de um pentest



TESTES DE INTRUSÃO (PENETRATION TEST)

Pre-Engagement

- Definição do tipo de teste, escopo, expectativas, objetivos (*goals*).
- Existem vários tipos de pentest: Pentest em aplicações Web, pentest em redes internas, pentest em redes externas, pentest em aplicações móveis, etc.
- Cada um desses testes podem entregar mais ou menos informações para o analista.
 - *Black-Box*: Mínimo de informações, geralmente apenas informações de acesso ao ativo em escopo (Ex: URL da aplicação/IP)
 - *Gray-Box*: Informações regulares dos ativos em escopo (Ex: credenciais limitadas)
 - *White-box*: O máximo de informação dos ativos em escopo (Ex: Código-fonte, credenciais privilegiadas, diagramas da topologia de rede)

TESTES DE INTRUSÃO (PENETRATION TEST)

Pre-Engagement

- Trecho de um documento de “Rules of Engagement”

Approach Type
<input checked="" type="checkbox"/> Penetration Test <input checked="" type="checkbox"/> Vulnerability Assessment (VA) <input type="checkbox"/> Red Team
Attack Perspective
<input type="checkbox"/> Black Box <input checked="" type="checkbox"/> Grey Box <input type="checkbox"/> White Box
Approach Position
<input type="checkbox"/> External Facing <input checked="" type="checkbox"/> Internal Facing <input type="checkbox"/> Whitelisting Required <input type="checkbox"/> SOC Monitored
Environment Type
<input checked="" type="checkbox"/> Production <input type="checkbox"/> Test <input type="checkbox"/> UAT <input type="checkbox"/> QA <input type="checkbox"/> Dev
Hosting Type
<input checked="" type="checkbox"/> On premise <input type="checkbox"/> AWS <input type="checkbox"/> Azure <input type="checkbox"/> Other: _____
Testing Type
<input checked="" type="checkbox"/> Network Infrastructure <input type="checkbox"/> Web Application <input type="checkbox"/> Web Services and APIs
<input type="checkbox"/> Network Segmentation <input type="checkbox"/> Leaked Credentials Search <input type="checkbox"/> Mobile Application

TESTES DE INTRUSÃO (PENETRATION TEST)

Reconnaissance e Open Source Intelligence (OSINT) Gathering

- Exemplos:
 - Consultas em engines de busca (Google, Bing, DuckDuckGo, etc)
 - Coletas de nomes de usuários e o padrão usado pela empresa (Linkedin)
 - Outros IPs associados a URL no passado (*Securitytrails.com*, útil pra bypass de WAF).
 - Internet Archive

TESTES DE INTRUSÃO (PENETRATION TEST)

Threat Modeling & Vulnerability Identification

- Modelagem dos ataques a serem realizados (fase de pré-ataque).
 - Antivirus nas máquinas? Versões de OS? Sistemas em escopo estão ativos?
- Análise de vulnerabilidades
- Além do uso de scanners automatizados, um pentester pode identificar outros tipos de vulnerabilidades por meio de testes manuais.
 - Vulnerabilidades Técnicas x Vulnerabilidades Lógicas

TESTES DE INTRUSÃO (PENETRATION TEST)

Threat Modeling & Vulnerability Identification

```
discovered open port 445/tcp on 192.168.0.63
Discovered open port 21/tcp on 192.168.0.63
Discovered open port 54045/tcp on 192.168.0.63
Discovered open port 2049/tcp on 192.168.0.63
Completed SYN Stealth Scan at 16:30, 1.23s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.0.63
Nmap scan report for 192.168.0.63
Host is up (0.00027s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nfs
54045/tcp open  unknown
MAC Address: 00:1E:4F:9F:DF:7F (Dell)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Uptime guess: 0.324 days (since Sun Apr 23 08:43:32 2017)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: All zeros
```



TESTES DE INTRUSÃO (PENETRATION TEST)

Exploitation

- Fase onde se dá a exploração das vulnerabilidades. O termo “**exploit**” é frequentemente utilizado nesta fase.
- **Exploit = Código utilizado para explorar uma falha.**
- Nem toda vulnerabilidade é imediatamente explorável. (Ex: “Versão de PHP não suportada”).
- Toda exploração possui um risco associado, mas a exploração de algumas vulnerabilidades certamente irá “crashar” a máquina (DoS).
- É **dever** do tester saber exatamente o que está executando.

TESTES DE INTRUSÃO (PENETRATION TEST)

Exploitation

- Lab Time (boot2root VM)

TESTES DE INTRUSÃO (PENETRATION TEST)

Post-Exploitation

- Após a exploração de uma vulnerabilidade, inicia-se a fase de pós-exploração. Alguns exemplos de pós-exploração:
 - Persistência.
 - Movimentação Lateral.
 - Escalação de privilégios (horizontal/vertical).
 - Extração de senhas em memória.
 - Extração de senhas em disco.
 - Exfiltração de dados.

TESTES DE INTRUSÃO (PENETRATION TEST)

Post-Exploitation

- Lab Time (boot2root VM)

RED TEAM

- Um Red Team Assessment é uma abordagem muito mais ampla em comparação a um Pentest. A ideia por trás deste tipo de abordagem não é evidenciar o máximo de vulnerabilidades possíveis, mas sim encontrar e explorar as vulnerabilidades que tenham relação com um **objetivo (goal)** específico, por exemplo, exfiltração de dados confidenciais ou financeiros.
- Geralmente o escopo a ser considerado é simplesmente o “nome da empresa”. Muito mais abrangente.
- Este tipo de teste busca avaliar os controles de segurança de uma organização, testar a equipe de segurança defensiva (Blue Team) e pôr à prova os procedimentos de resposta a incidentes adotados pela organização alvo.

RED TEAM

- Em um Red Team utiliza-se qualquer técnica necessária, ou quase qualquer técnica necessária, para atingir o objetivo previamente estipulado simulando um atacante real.
- Trabalhos tendem a ser mais longos comparados a um pentest.
- Mais “stealth”, isto é, o blue team do cliente **não está ciente** dos testes.

RED TEAM

- Em resumo:
 - Red Team é mais furtivo (*stealth*).
 - Escopo muito mais abrangente.
 - É o que mais se aproxima de um ataque real.
 - Pode envolver **engenharia social**.
 - Geralmente baseado em um objetivo específico (*goal*).
 - Visão muito mais em profundidade do que em “largura”.
 - Espera-se maturidade maior do cliente para um Red Team (*Tem ao menos um blue team?* ☺)

RED TEAM

Engenharia Social

- A engenharia social, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou para a divulgação de informações confidenciais.
- Pode ser uma ligação telefônica (*vishing*), um e-mail (*phishing*), um pendrive “esquecido” no estacionamento (*baiting*) e por aí vai...

RED TEAM

- Exemplo de um Red Team real!
- Cenário:
 - **Empresa:** Seguradora (*insurance*)
 - **Escopo:** “O nome da empresa”. Qualquer coisa que envolve a empresa está no escopo.
 - **Empresa internacional** (North America, Europa, Asia).
 - **1 mês de trabalho.**
 - **Ataques de negação de serviço (DoS) estão fora do escopo.**
 - **Objetivo:** Comprometer o perímetro externo e alcançar a rede interna.

PERFIL DE UM PROFESSIONAL DE SEGURANÇA OFENSIVA

- Esteja em dia com os **fundamentos básicos** (conceitos de S.O, redes, arquitetura), a base.
- **Estude vulnerabilidades.** Estude reports públicos de bug bounty (*hackerone-reports* no github).
 - Como descrever, como identificar, como explorar, como **corrigir**, como prevenir.
- **Tenha curiosidade em entender como as coisas funcionam.** Vá além da “sala de aula”.
- **Estude inglês (!!!).**
- Compre livros.
- Tire certificações.
- **Pratique!**

TREINAMENTO

- Temos atualmente inúmeras plataformas pra treinamento, do básico ao avançado.
- São **free** (embora algumas VPNs dedicadas são pagas - *usualmente mensalidade*)
- Algumas que recomendo:
 - Tryhackme.com (tem MUITA coisa pra iniciante – recomendo!)
 - PortSwigger - Web Security Academy (O melhor conteúdo gratuito de web appsec)
 - Hackthebox.eu (boot2root e CTF)
 - Vulnhub.com (boot2root e CTF)
 - Ringzer0team.com (CTF)
 - W3challs.com (CTF)
 - SmashTheStack.IO, pwnable.kr, pwnable.eu (pra binary exploitation – mais pesado)

LIVROS

- **Redes:** TCP/IP Illustrated (Vol I), Análise de Tráfego em redes TCP/IP (João Eriberto)
- **Arquitetura:** O da capa vermelha do Tanenbaum
- **OS:** Operating System Concepts 8th (o livro com dinossauro na capa), Descobrindo o Linux (João Eriberto), Windows Internals (do Pavel... é um livro pesado, mas sempre foi e continua sendo a referência)
- **Programação:** Alguma coisa que te ensine a programar ao menos uma linguagem web e uma linguagem “desktop”. Aprender powershell e shell script vai te salvar também!

LIVROS

- **Segurança Ofensiva:**
- Penetration Testing “A Hand-On Introduction to Hacking” (Introdutório!)
- The Web Application Hacker’s Handbook
- The Hackers Playbook (1, 2 and 3)
- Red Team Development and Operations: A practical guide
- Advanced Penetration Testing: Hacking the World’s Most Secure Networks
- Advanced Persistent Threat Hacking: The Art and Science of Hacking Any Organization
- Android Hacker’s Handbook
- iOS Hacker’s Handbook
- The Art of Software Security Assessment
- Attacking Network Protocols: A Hacker’s Guide to Capture, Analysis, and Exploitation
- The Shellcoder’s Handbook: Discovering and Exploiting Security Holes

CERTIFICAÇÕES

- Em segurança ofensiva, eu geralmente opto por certificações **práticas**.
- Offensive Security Certified Professional (OSCP) abre portas. Cai no filtro dos recruiters.
- Depois da OSCP, siga a trilha que você curtir mais.
- Evasão? Cursos da Sektor7, OSEP
- AppSec? OSWE, eMAPT, eWPT, eWPTXv2, PortSwigger
- Infra? CRTP, CRTE, PACES, cursos da SpecterOps
- Foco em Red Team? CRTO e CRTL (da ZeroPointSecurity/Rastamouse)

CERTIFICAÇÕES

- Não é barato. Certificações da SANS (que eu nem citei) podem chegar a 20 mil reais. É prática no mercado que empregador cubra o custo delas pra você... mas não é regra.
- **Certificação não é atestado de conhecimento. (*Abre portas? Abre. Mas se na entrevista isso for pré-requisito... fuja*)**
- Se você não absorver o valor real de uma certificação (*conteúdo organizado e mastigado, laboratórios prontos – hoje em dia é caro e difícil manter um “lab pessoal”*)... ela se torna um mero pedaço de papel.

COMPETIÇÕES

- **Capture-The-Flag**
- CTF significa Capture the Flag. No âmbito da informática, são competições que envolvem diversas competências dos profissionais/estudantes/entusiastas para a resolução de desafios relacionados à infosec (segurança da informação), com o objetivo de capturar a bandeira (normalmente um código) e pontuar.
- A “CTF-BR” organiza eventos de CTF no BR (<https://ctf-br.org/sobre/>)
- <https://ctftime.org/> -> Lista de competições e os times.



CANAIS NO YOUTUBE

Muitos, mas recomendo demais:

- **John Hammond: @_JohnHammond**
- **IppSec (resolução de boxes do HTB... bem explicada!)**
- Fuzzing Labs (Patrick Ventuzelo)
- thecybermentor
- allh4zr3d
- HuskyHacks
- ElevateCyber
- HackerSploit
- Nahamsec
- Tib3rius