Insper

# Tecnologias Hackers

Aula inaugural

**Professor Dr. Rodolfo Avelino**

# Quando o assunto é Segurança o que você pensa?

# Segurança da Informação

(Fundamentos)


| | |
|---|---|
| Confidencialidade | • Assegurar que a informação é acessível somente por aqueles devidamente autorizados |
| Integridade | • Salvaguardar a veracidade e complementariedade da informação bem como os seus métodos de processamento |
| Disponibilidade | • Assegurar que quem devidamente autorizado tem acesso á informação e bens associados sempre que necessário |

# Ementa

- Princípios básicos da Segurança da Informação.
- Metodologias de Pentest.
- Testes de penetração de redes e aplicações web.
- Fases de um Pentest.
- Teste de Vulnerabilidade.
- Fundamentos da criptografia computacional: Criptografia Simétrica e Assimétrica, criptografia de via única (Hash), codificação com Base64 e complexidade computacional de decriptar pacotes.

# Ementa

- Serviços de segurança em rede de computadores.
- Protocolos de segurança de rede.
- Ética na informática.
- Engenharia social e aspectos humanos de segurança.
- Pesquisa bibliográfica e normas técnicas para citações e referências.

# Ao final da disciplina o aluno será capaz:

- Propor controles de segurança da informação para mitigar os riscos em projetos e ambientes computacionais;
- Identificar possíveis ameaças, vulnerabilidades e riscos associados a ativos de informação;
- Identificar fraquezas de um sistema, como injeção arquivos, de comandos SQL ou Cross Site Scripting;
- Realizar testes de penetração e avaliações de vulnerabilidade;

# Ainda.....

- Implementar e usar chaves públicas e algoritmos de criptografia de chave simétrica;
- Entender a complexidade computacional envolvida em decriptar dados;
- Aplicar conceitos de segurança de rede e gerenciamento de rede;
- Usar protocolos que garantam a segurança de dados em redes contemporâneas;
- Identificar potenciais conflitos entre aplicações de informática e considerações legais ou éticas, e exercitar o julgamento profissional para resolver esses tipos de conflitos.

# METODOLOGIA

**Avaliação**

- Avaliação continuada em grupo e individual, por meio de tarefas (roteiros), desafios registrados em diário de bordo e CTFs;
- Avaliação Intermediária – Relatório de Testes.
- APS.
- Projeto Final

**Aulas práticas**

- Por meio de exercícios em laboratórios, simulações e desafios.

# Os CTFs


CTFd

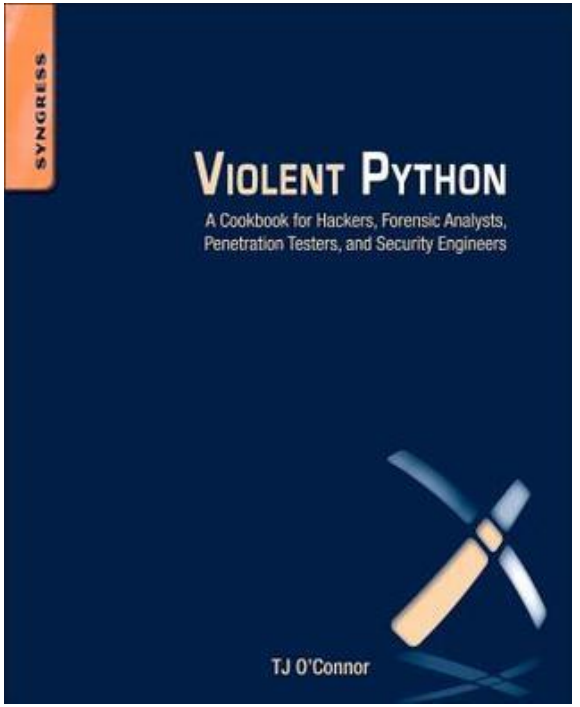
A cool CTF platform from ctfd.io

# Resumo do programa

| | Objetivo |
|---|---|
| Camada de Aplicação | Análise comunicação cliente servidor |
| | Coleta de Informações e reconhecimento (Footprinting e Fingerprinting) |
| | Exploração em Aplicação WEB |
| | Exploração de banco de dados |
| | Exploração de usuários web |
| Camada de Rede | Introdução |
| | Análise de tráfego de rede e Forense Computacional |
| | Reconhecimento do alvo |
| | Criptografia |
| | Exploração |
| | Engenharia Social e OSINT |

# Bibliografia básica

O’CONNOR, T. J. Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers, 2012, ISBN-13: 978-1597499576

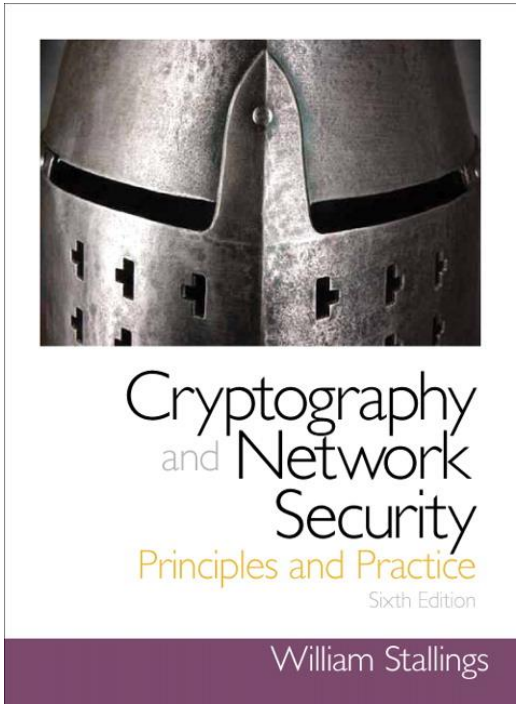



# Bibliografia básica

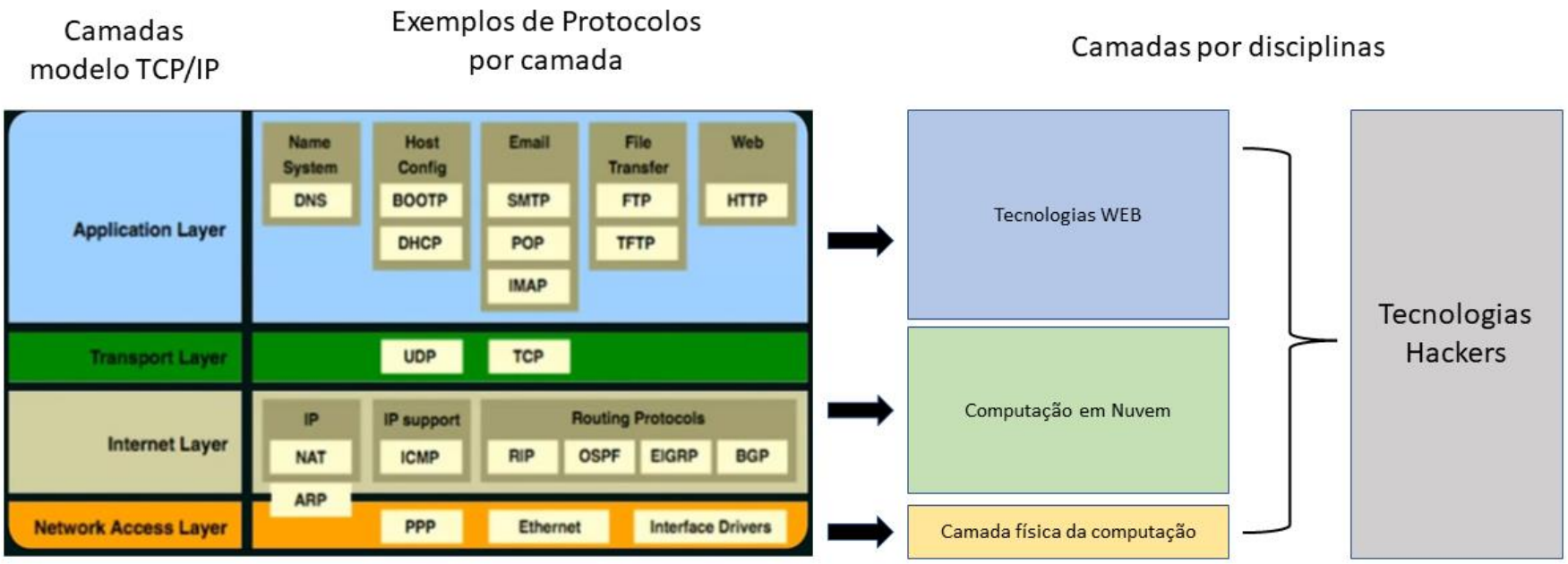
DUFFY, Christopher. Aprendendo Pentest com Python. Novatec, 2015, ISBN: 978-85-7522-505-9

# Bibliografia básica

STALLINGS, W. Cryptography and Network Security: Principles and Practice. 6th Edition. Pearson Prentice Hall, 2013



# Fundamentos de rede dentro da formação da Engenharia de Computação



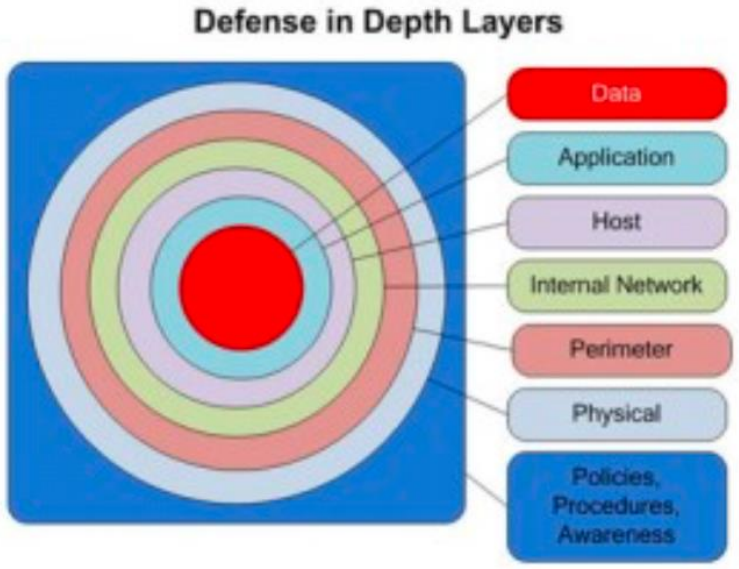

Fonte imagem: https://analyticsindiamag.com/difference-between-cybersecurity-information-security/

# Basicamente….

Cyber Security está mais voltado para a proteção de sistemas e redes digitais contra ameaças cibernéticas.

Information Security tem uma abordagem mais abrangente, incluindo proteção contra uma variedade de ameaças, não apenas digitais, e envolvendo medidas de proteção organizacionais e físicas, além das tecnológicas.

# Pensando Segurança em camadas




**Dados-** Alvo final do invasor, incluindo seus bancos de dados, documentos e assim por diante.

**Aplicação -** O software que manipula os dados que é a meta final de ataque.

**Host** - Os computadores que estão executando as aplicações.

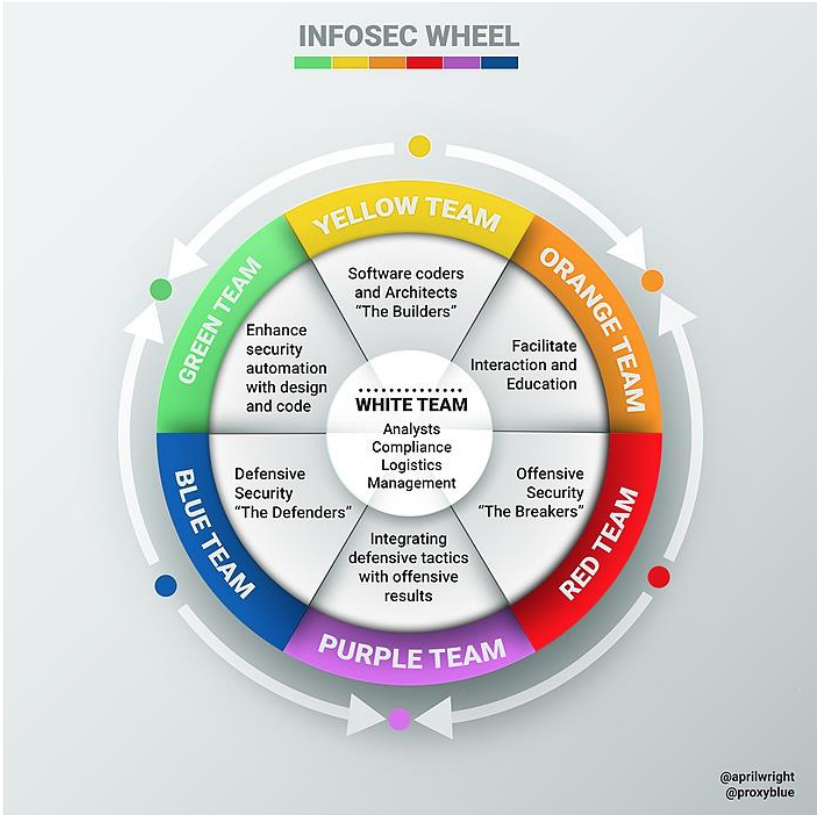
**Rede interna -** A rede na infraestrutura de TI da empresa.

**Perímetro -** A rede que conecta a infraestrutura de TI corporativa para outra rede, como a usuários externos, parceiros ou a Internet.

**Físicas** - Os aspectos tangíveis em computação: os servidores, discos rígidos, switches de rede, energia....

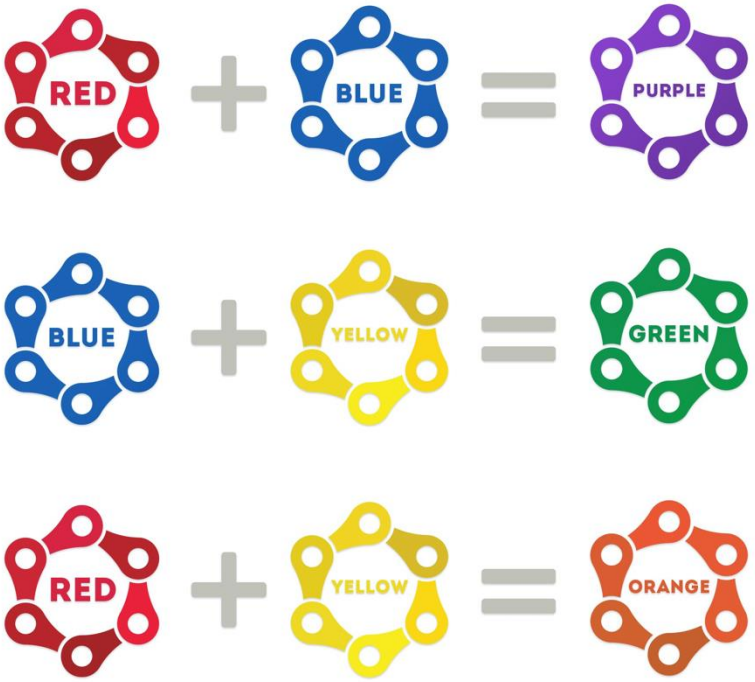
**Políticas, procedimentos, consciência -** Os princípios gerais que regem da estratégia de qualquer organização de segurança. Sem esta camada, toda a estratégia de falhar.

# A carreira na área




Fonte: https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700

# Misturando as carreiras primárias



Todos os ataques cibernéticos são realizados por hackers?

# O que é Hack?

O termo "hack" originalmente descrevia um software muito bem escrito ou "codificado".

Geralmente, esses tipos de software solucionavam um problema imediato ou complicado de maneira rápida e eficiente.

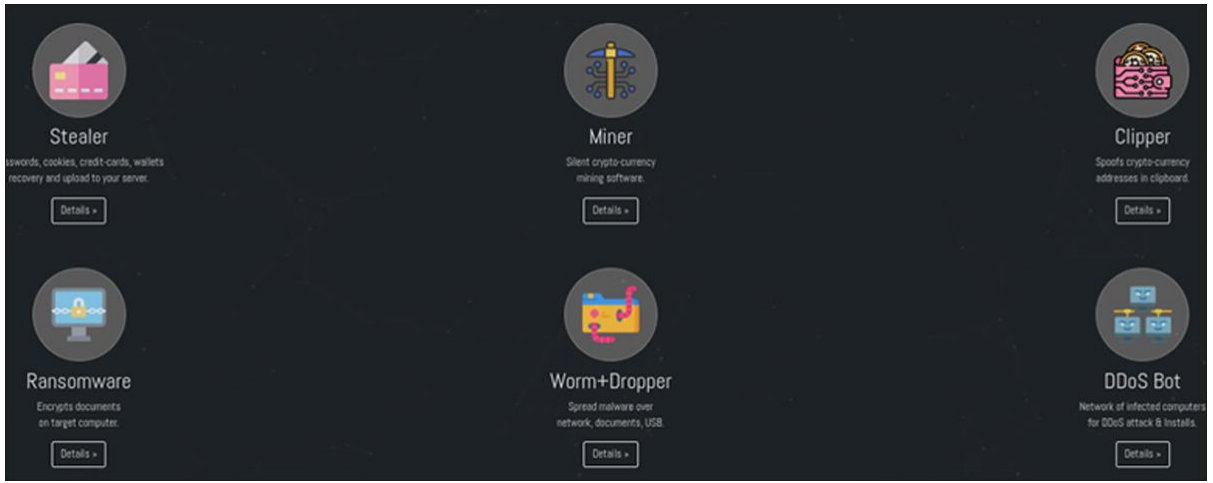
Fonte: https://www.icann.org/ru/blogs/details/is-this-a-hack-or-an-attack-15-9-2015-pt

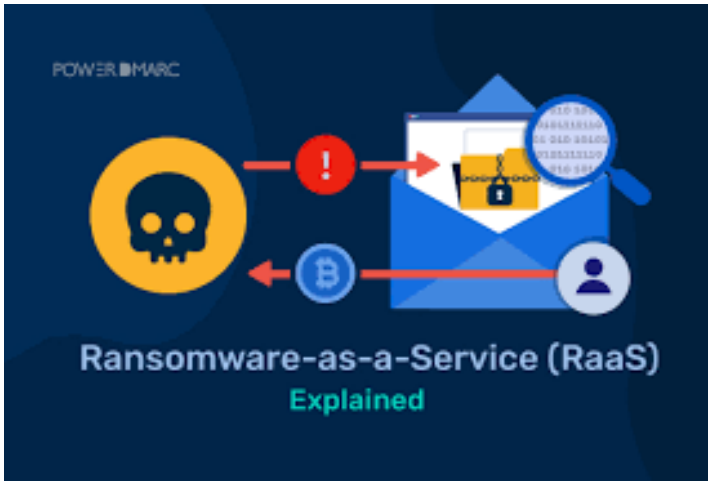
# A resposta é não!

- Hoje existe um mercado em expansão que disponibilizam **poderosas suítes** para a execução de ataques.
- Nem todos os tipo de ataque envolvem hacking! Ataques de engenharia social e sequestro de redes sociais por exemplo não usam hack!

# MaaS (Malware as Service)

Eternity

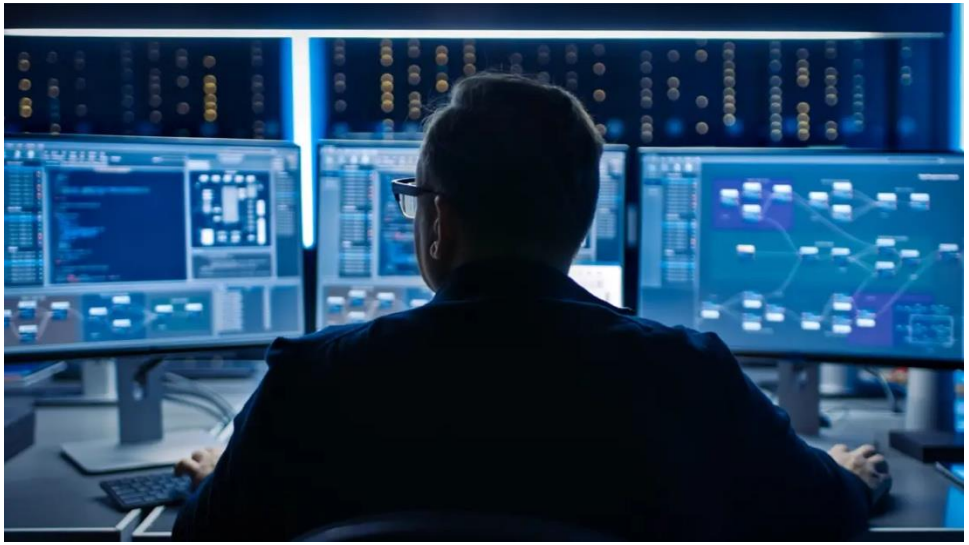



- Eternity Stealer - $260 annual subscription
- Eternity Miner - $90 annual subscription
- Eternity'Worm - $390
- Eternity Ransomware - $490
- Eternity Clipper - $110
- Eternity DDoS Bot - (Still in development)

# O Cenário hacking

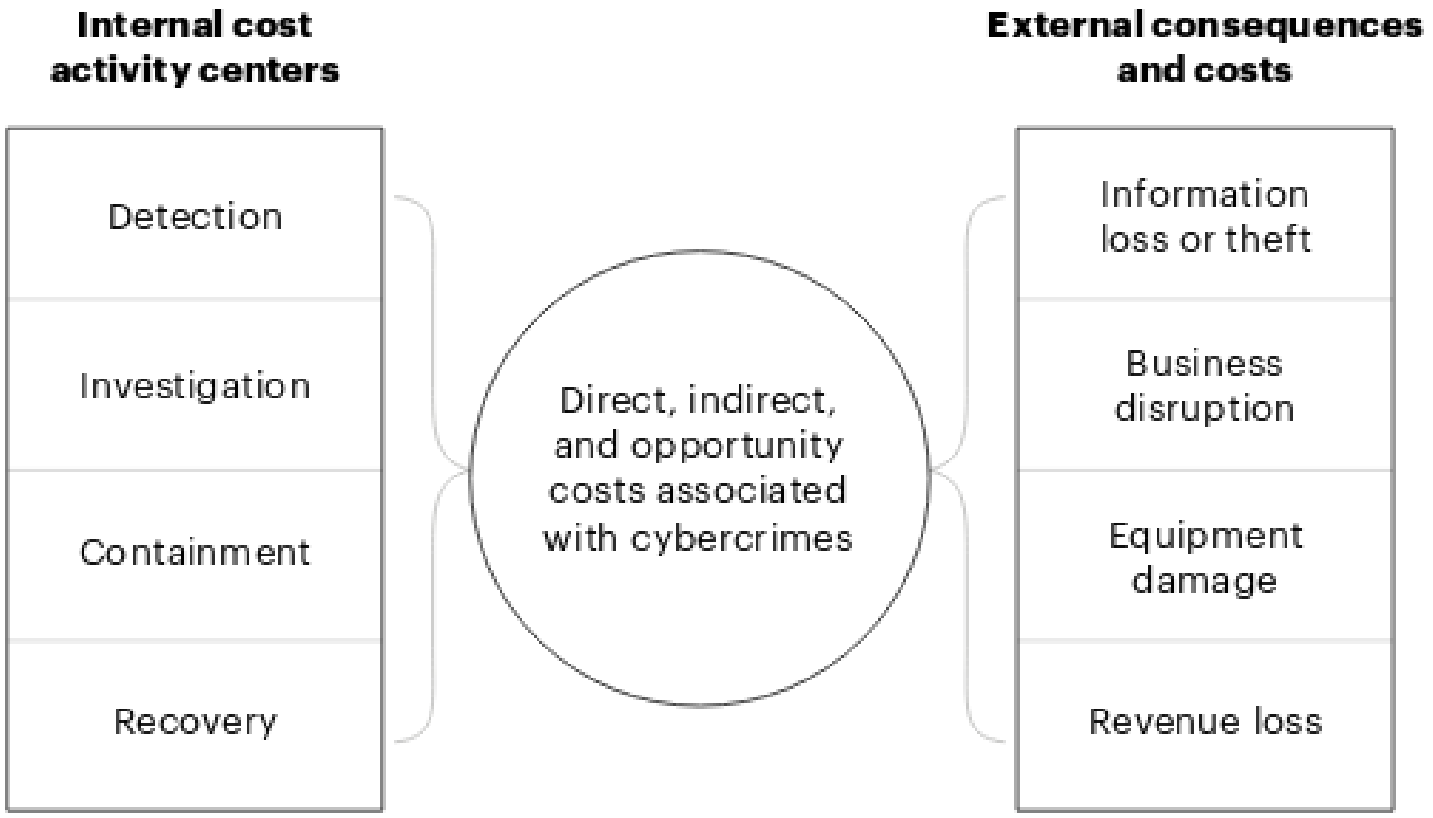
X



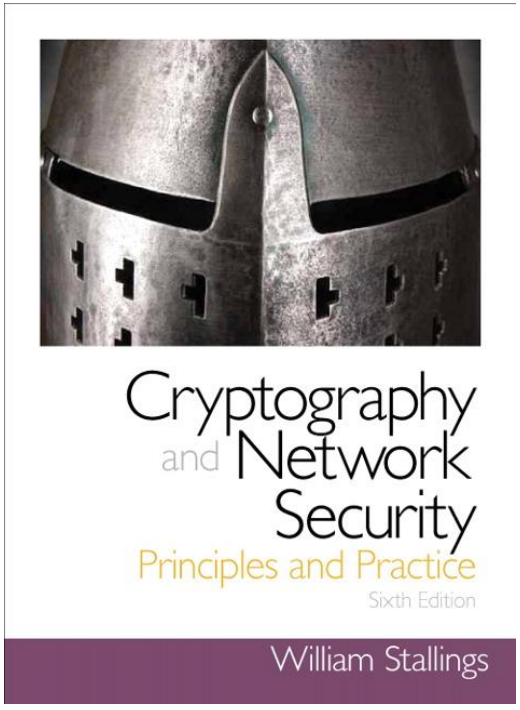
Underground
(criminosos/fraudadores)

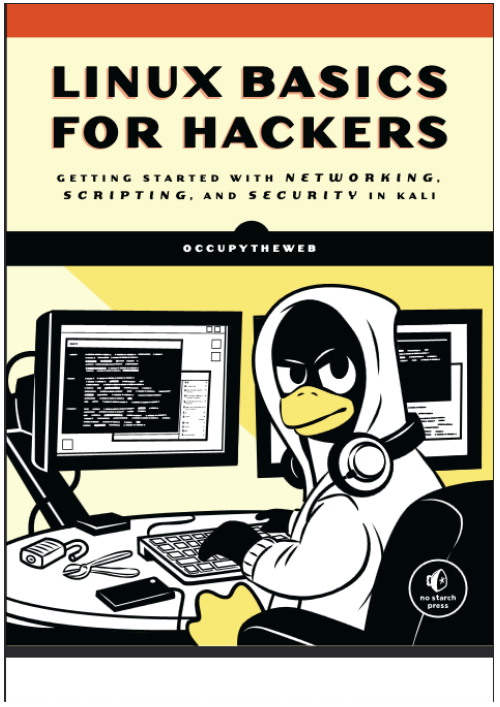
Corporativo
(as cores das carreiras)

# CUSTOS PARA O CIBERCRIME



# Próxima aula




Capítulo 1 (Material no Black Board)
Computer and Network Security Concepts

Capítulo 1 (Ler/exercitar)
Getting Started With the basics (pág 1 – 17)

Capítulo 2 (Ler/exercitar)
Text Manipulation (pág 19 – 27)

# Dúvidas e/ou comentários?