eBook

OSINT

O Jogo Avançado

Investigações Digitais de Verdade

📚 Sumário

✍️ Apresentação

Bem-vindo(a) ao Volume 1 do eBook **OSINT – O Jogo Avançado**, uma eletrizante jornada investigativa pelo mundo da inteligência de código aberto e do hacking ético. Neste volume, mergulhamos em casos mais complexos, reais e desafiadores, com uma pegada CSI digital, onde suas habilidades como investigador(a) e hacker serão testadas ao limite.

Aqui, você não vai apenas aprender sobre ferramentas: vai usar cada uma delas para resolver mistérios digitais reais, passo a passo, com linguagem acessível, descontraída e técnica ao mesmo tempo.

🔎 Introdução

Se você chegou até aqui, é porque o universo da investigação digital já despertou algo em você. Talvez tenha percebido o quanto dados são poderosos. Ou quem sabe, esteja buscando usar seus conhecimentos para o bem, ajudando pessoas, empresas e até colaborando com a justiça.

Este livro não é apenas um manual técnico. Ele é um desafio interativo. A cada capítulo, você enfrentará situações reais — como recuperar contas invadidas, rastrear pessoas desaparecidas, desmascarar golpistas e muito mais.

Você vai colocar a mão na massa com:

Ferramentas como Maltego, Sherlock, Have I Been Pwned, Google Dorks, Whois, EtherScan, Chainalysis, entre outras;
Técnicas de rastreamento digital, engenharia reversa, inteligência artificial aplicada e até blockchain forensics;

E, acima de tudo, uma abordagem ética e legal, pois o objetivo aqui é proteger, descobrir e resolver, nunca invadir ou expor.
Prepare-se: o jogo ficou sério.

🗒️ Capítulo 1 – A Recuperação do Instagram: O Caso da Conta Hackeada

---

🎬 CENA 1: A Ligação Desesperada

Você está curtindo um café tranquilo quando recebe uma ligação. Do outro lado da linha, uma voz tremida:

— *"Pelo amor de Deus, me ajuda! Alguém invadiu meu Instagram. Eu trabalho com ele, é meu ganha-pão. Trocou a senha, o e-mail... tudo!"*

A pessoa é uma influenciadora digital com mais de **150 mil seguidores**. Ela usa a conta para fechar parcerias, divulgar marcas e principalmente: pagar as contas. Agora, sem acesso, ela está à beira de um colapso.
Sua missão? Agir como um hacker ético e especialista em OSINT para ajudar a recuperar o acesso à conta dela. Pronta(o)?

🧠 Missão: Recuperar a Conta com Inteligência Digital

Você não tem acesso ao e-mail antigo, nem ao número de telefone. Só tem o **@username** da conta.

Vamos lá, detetive digital. A estratégia será dividida em etapas, como um verdadeiro **CSI cibernético**:

🔍 Etapa 1 – Identificando o Campo de Batalha com o Sherlock

Ferramenta utilizada: Sherlock

O que é?
Sherlock é uma ferramenta de OSINT que permite procurar nomes de usuários em diversas redes sociais.
Objetivo:
Descobrir se o invasor está usando o mesmo nome de usuário em outras plataformas. Hackers amadores cometem erros bobos — como usar o mesmo username para mais de uma coisa.

```
git clone https://github.com/sherlock-project/sherlock.git
cd sherlock
python3 sherlock nome_de_usuario
```

Se encontrar esse mesmo usuário em outras redes como Twitter, TikTok ou Reddit, pode haver pistas valiosas por lá.

🕵️ Etapa 2 – Rastreando o E-mail de Recuperação com Have I Been Pwned

Ferramenta utilizada: Have I Been Pwned

O que é?
Um banco de dados gigantesco com milhões de vazamentos. Se o e-mail da influenciadora (ou possíveis e-mails associados à conta) estiverem nesse site, você pode descobrir senhas vazadas, vazamentos anteriores e outras informações.

Como usar:
Basta digitar o e-mail conhecido dela (ou variações que ela costumava usar).
Dica de ouro: Se ela usava o mesmo e-mail para o PayPal ou outras plataformas, você pode tentar esses e-mails também.
Se descobrir uma senha vazada, anote — pode ser a que o hacker está usando agora (eles raramente mudam todas as senhas de forma inteligente).

🧩 Etapa 3 – Google Dorking na Veia

O que é?
Uma técnica ninja para pesquisar com precisão no Google.

Exemplos úteis:

- site:instagram.com "usuário123" → Vê perfis ou menções arquivadas do usuário.
- "usuário123@gmail.com" → Pode mostrar onde o e-mail foi publicado antes.
- "usuário123" password → Sim, você ficaria surpreso onde senhas vazadas aparecem.

Com sorte, você encontrará perfis secundários, antigos ou até fóruns com relatos de atividades suspeitas.

🖼️ Etapa 4 – Análise de Imagens e Metadados

Peça prints, fotos ou vídeos antigos da conta. Use ferramentas como:

- FotoForensics
- EXIF.tools
- Image Edited?

Objetivo: Ver se há metadados (dados escondidos na imagem) como IP, geolocalização ou até nome do arquivo original que possam indicar o dispositivo usado.

🧠 Etapa 5 – Engenharia Social com Inteligência

Se o invasor ainda está usando a conta, é hora de entrar no jogo.

- Crie um perfil fake (sim, de forma ética e controlada), siga o invasor e tente puxar assunto. Pergunte sobre “serviços de crescimento de Instagram” ou diga que quer comprar a conta. Veja como ele responde.

Ferramenta extra:
Use o **Instagram Web Inspector** (modo desenvolvedor do navegador) para observar como os dados fluem.
Se for muito técnico, você pode usar plugins como o **DataMiner** para extrair informações públicas da conta.

🛡️ Etapa 6 – Contato com o Suporte do Instagram

Depois de reunir prints, e-mails alternativos, evidências de identidade (RG, contratos com marcas, etc.), oriente a vítima a preencher este formulário:

🔗 Formulário de Ajuda do Facebook/Instagram

Ou diretamente:
🔗 Ajuda do Instagram para Contas Hackeadas
Se ela tiver contrato com uma empresa ou for verificada, pode acionar suporte especializado.

🔚 Fechamento do Caso

Com todas essas informações, o suporte do Instagram terá material suficiente para comprovar que a conta foi hackeada. Mas além disso, você já mapeou possíveis rastros deixados pelo invasor, reforçando seu trabalho como hacker ético.

Final feliz? Com sorte, sim.
Mas o que importa mesmo é o conhecimento adquirido no processo.

🧠 Bônus: Lições que Aprendemos

- Nunca usar o mesmo e-mail para tudo.
- Ativar autenticação de dois fatores (2FA) **SEMPRE**.
- Monitorar senhas em vazamentos com **Have I Been Pwned**.
- Usar ferramentas de OSINT para além da investigação criminal: elas são instrumentos de defesa digital.

No próximo capítulo, vamos usar suas habilidades para encontrar uma pessoa desaparecida apenas com informações mínimas. Prepare o **Maltego** e a mente analítica — o jogo só começou.

Capítulo 2 – Desaparecida: O Mistério da Garota do Story

🎬 CENA 2: Um Pedido Inesperado no Direct

Você está scrollando o feed quando recebe uma mensagem direta de um perfil anônimo no Instagram:

— *"Ei, você é bom com essas coisas... preciso de ajuda. Uma amiga minha desapareceu. Ela postou um story estranho e depois sumiu. A polícia disse que ainda é cedo pra investigar. Mas eu tô desesperado..."*

Você não é policial. Mas você é bom com OSINT. E com as ferramentas certas, talvez consiga rastrear algo antes que seja tarde demais.
A única pista que o rapaz tem: o story que ela postou antes de sumir. Uma selfie com a legenda:

"Última parada antes do tédio"
Local: marcado como "Café 34"

Nada mais. Nenhuma resposta. Nenhuma atualização. Sumiu do WhatsApp. Instagram em silêncio.

🧠 Missão: Rastrear a garota com base em evidências digitais

Seu trabalho agora é usar análise de imagem, dados públicos e um pouco de intuição hacker pra montar o quebra-cabeça.

🖼️ Etapa 1 – Análise do Story (Imagem/Vídeo)

Ferramentas utilizadas:

- FotoForensics
- EXIF.tools
- Google Reverse Image Search
- Yandex Imagens

Objetivo:
Descobrir qualquer informação escondida na foto. Às vezes, uma simples selfie revela mais do que parece:
Identifique reflexos em vidros, placas, detalhes do local (menu, logo, uniforme de atendente).

- Faça upload no Google Imagens ou Yandex pra identificar se essa cafeteria aparece online.
- Use EXIF.tools para tentar extrair geolocalização (se o story original for enviado e não uma captura de tela).

🗺️ Etapa 2 – Localização via Google Maps e OpenStreetMap

O que temos: O nome do local: “Café 34”

Ferramentas:

- Google Maps
- OpenStreetMap
- Street View

Procure por todas as unidades ou estabelecimentos com esse nome na cidade dela (que você pode descobrir pelo perfil). Se encontrar o café, use o Street View para ver se bate com o fundo da imagem.
Dica ninja: Combine com a dica visual da foto. Uma placa vermelha? Um banco azul? Um grafite?

📲 Etapa 3 – Pegadas Digitais: Últimas atividades da garota

Acesse o perfil dela e analise:

- Últimos seguidores adicionados.
- Quem comentou ou reagiu recentemente.

- Se ela repostou algum conteúdo de terceiros.

Use ferramentas como:

- Webstagram
- Plugins como **IG Export Tool** pra coletar os dados públicos da conta.

Organize tudo em uma planilha e analise padrões de horário, frequência e interações.

🧠 Etapa 4 – Entra em cena o Maltego

Ferramenta profissional de OSINT.

Objetivo: Montar um grafo de conexões a partir do nome da garota, e-mails públicos, possíveis domínios, ou nomes de usuários em outras redes.
No Maltego:

- Crie uma nova entidade do tipo **Person**.
- Insira nome, nickname ou e-mail (se tiver).
- Execute transformações como:
  - "To Social Media Profiles".
  - "To Domains".
  - "To Email Addresses".

Você pode encontrar domínios registrados, sites pessoais ou links esquecidos no passado.

Etapa 5 – Monitoramento em Tempo Real com Alerts e Bots

Ferramentas:

- Google Alerts (crie alertas com nome dela ou possíveis apelidos).
- TweetDeck (monitore palavras-chave no Twitter).
- Instagram Searcher Bots (monitoramento de stories, seguidores, alterações no perfil).

Exemplo: Crie um alerta com "Camila Desaparecida" ou "Viu Camila Café 34" — se alguém postar algo, você recebe instantaneamente.

🛑 Importante: Contato com autoridades

Assim que qualquer evidência concreta for encontrada (geolocalização, print com horário, conversa suspeita), oriente quem pediu ajuda a levar tudo à delegacia.

Você pode auxiliar. Mas não substitui o trabalho oficial de investigação.

🔚 Conclusão: OSINT salva vidas?

Sim. Em muitos casos, a inteligência de fontes abertas consegue antecipar pistas, reforçar linhas de investigação, e até mesmo salvar pessoas.

Mas precisa ser usada com responsabilidade, respeito à privacidade e foco no bem.

🧠 Bônus de Aprendizado:

- Stories podem conter muito mais do que aparentam — zoom neles! O Yandex é um dos
- melhores buscadores visuais do mundo. Às vezes supera o Google. OSINT não é só
- sobre encontrar coisas — é sobre ligar pontos que ninguém percebeu.

No próximo capítulo, você será contratado para descobrir se uma empresa está cometendo fraude financeira... usando apenas o site dela, redes sociais e dados públicos.
Vamos descobrir os segredos de uma startup com cara de golpe?

💰 Capítulo 3 – A Startup Fantasma: Fraude Disfarçada de Inovação

---

🎬 CENA 3: Um e-mail anônimo, um convite tentador

— "Ei, tenho uma proposta. Não posso te dizer quem sou. Mas essa empresa que apareceu no Shark Tank está enganando investidores. Preciso que você descubra a verdade."

O link: www.bluxr.ai
Uma startup de “inteligência artificial descentralizada” que promete “democratizar algoritmos com propósito ESG”. Soa bonito. Até demais.

Você entra no site. É limpo, elegante. Equipe sorridente, gráficos falsamente impressionantes. Só que algo não bate. E você decide cavar fundo.

🎯 Missão: Confirmar se a empresa é real ou apenas uma casca de marketing para lavagem de dinheiro ou golpe financeiro

---

🔍 Etapa 1 – Investigação de domínio

Ferramentas:

- WHOIS.domaintools.com
- URLVoid
- crt.sh – Para certificados SSL
- ViewDNS.info

Objetivo: Descobrir:

- Quando o domínio foi registrado.
- Por quem foi registrado (pode estar sob proxy — suspeito).
- Histórico de domínios antigos com o mesmo IP (há clones?).

- Se foi usado para phishing ou spam antes.

Dica: Se o domínio foi registrado há menos de 6 meses e a empresa diz ter anos de operação, acenda o alerta vermelho.

Etapa 2 – Verificando a equipe da empresa

Ferramentas:

- LinkedIn (modo anônimo ativado).
- Hunter.io – Para verificar e-mails corporativos válidos.
- Namechk / Sherlock – Para procurar os mesmos nomes de usuário em outras redes.

Objetivo:

- Encontrar os fundadores e validar a existência deles.
- Verificar se trabalham em outras empresas ao mesmo tempo (conflito?).
- Ver se os perfis são fantasmas (poucos seguidores, sem interações, só fotos profissionais e frases genéricas).

💰 Etapa 3 – Rastreamento de investidores

A empresa diz ter "captado 3 milhões em seed money".

Verificações:

- Sites como Crunchbase e PitchBook – Veja se há registros formais.
- Pesquise os nomes dos investidores no Google + [fraude, processo, scam].
- Verifique se já investiram em outras empresas problemáticas.
- Use combinações como: nome do investidor + processo + SEC + fraude + alerta CVM.

📄 Etapa 4 – Auditoria pública e dados financeiros

Fontes abertas importantes:

- Receita Federal (busque o CNPJ se for brasileiro).
- Radar Empresarial.
- Glassdoor – Veja se há denúncias de funcionários.
- Sites de Diários Oficiais.

Objetivo:

- Ver se a empresa está ativa, tem capital declarado.
- Comparar o número de funcionários no site com o número real (pode ter 2 pessoas fingindo ser 50).
- Procurar reclamações trabalhistas ou pedidos de falência.

📸 Etapa 5 – Engenharia reversa de imagens e vídeos

Toda imagem no site foi feita por IA?

Ferramentas:

- Google Reverse Image Search e Yandex Imagens – Para verificar se as imagens do time são roubadas.
- Plugins como **Fake Profile Detector** – Para analisar imagens de perfil.
- Vídeos institucionais podem ser feitos com atores de bancos de vídeo como:
  - Artgrid
  - Pexels
  - Fiverr (atores freelancers).

🧠 Dica avançada: Analyze This!

Use o Wayback Machine para ver como o site era meses atrás.

- Se em janeiro o site vendia criptomoeda e hoje vende IA, temos um pivô forçado (ou fingido).
- Compare os textos e descubra incoerências no discurso da marca.

🚨 Alerta Vermelho: Quando uma empresa é suspeita?

- Equipe com rostos IA (ou sem redes sociais reais).
- Endereço físico é uma caixa postal ou coworking de fachada.
- Nenhum case concreto de cliente.
- Investidores misteriosos, estrangeiros e sem histórico conhecido.
- Rebranding constante (troca de nome e domínio).

Conclusão: Fraude corporativa pode estar a um clique de distância

O OSINT é o fio da navalha entre o “parece legítimo” e o “golpe institucionalizado”.

Você pode proteger investidores, usuários e até órgãos públicos se dominar essa arte.

E neste caso, você descobriu que a tal Bluxr.ai foi criada há 2 meses, com equipe falsa, site clonado de outra startup canadense, e investidores que nem existem no LinkedIn.
Você salvou milhares de reais de serem injetados em um buraco negro de promessas vazias.

No **Capítulo 4**, um pedido especial da Interpol: rastrear um fugitivo internacional que está usando perfis falsos em redes sociais para se esconder no Brasil.

Tá pronta(o) pra seguir o rastro de alguém que apagou todos os vestígios digitais?

🕵️ Capítulo 4 – O Fantasma Digital: Caçando um Fugitivo nas Redes

---

🎬 CENA 4: Um pedido incomum da Interpol

— *"Temos razões pra acreditar que um homem procurado por tráfico internacional está se escondendo no Brasil usando identidade falsa. A última pista? Uma conta no Instagram com localização em Campina Grande."*

Você recebe a foto de um homem chamado **Lucien Vargaz**, procurado na Europa. Mas o nome do perfil no Instagram é **@bruno.freitas.photography**. O conteúdo? Fotos de café, paisagens, frases de Clarice Lispector. Muito pacato... talvez demais.

🎯 Missão: Confirmar se 'Bruno Freitas' é o fugitivo Lucien Vargaz, e ajudar a Interpol a localizá-lo

---

🧾 Etapa 1 – Coleta de metadados das postagens

Ferramentas:

- Exif.tools
- PhotoForensics
- Jimpl (Image Metadata Viewer)

Objetivo:

- Ver dados embutidos em fotos (data, GPS, modelo do celular).
- Comparar horários e locais das postagens com dados públicos.

Exemplo:
Uma foto de uma xícara de café em **2024-02-03 às 06:24** com GPS de João Pessoa, postada só no dia 10, sugere tentativa de mascarar movimento.

🕵️ Etapa 2 – Reconhecimento facial reverso

Ferramentas:

- PimEyes (ferramenta poderosa, paga, mas há testes grátis).
- Betaface (extrai pontos do rosto e compara com bases).
- Yandex Reverse Image Search

Objetivo:

- Enviar a foto do Bruno e tentar achar correspondências com fotos antigas de Lucien ou de perfis antigos deletados.
- Mapear se a imagem já foi usada em outros contextos.

Resultado:
Bruno Freitas usava outro perfil em 2022 chamado **@luccafreire_**, hoje excluído, mas ainda com cache no Yandex.

📍 Etapa 3 – Geolocalização via imagens

Ferramentas:

- GeoSpy
- Google Earth Pro
- StreetComplete (OpenStreetMap)
- Suncalc.org (análise da luz solar)

Objetivo:

- Ver se é possível identificar lugares exatos das fotos.
- Confirmar se os lugares são compatíveis com a região em que ele supostamente está.

Técnica:
Uma das fotos mostra um outdoor parcialmente visível com um número de telefone com DDD **83**. Usando **Google Street View**, você percorre Campina Grande até achar o mesmo ângulo.

💡 **Localização confirmada:** Bairro do Catolé, nas proximidades de um coworking de fotografia.

📡 Etapa 4 – Inteligência de rede social

Ferramentas:

- Maltego (plugin de redes sociais).
- Social Links Pro (ou buscadores OSINT como Whopostedwhat.com).
- SpiderFoot – Para varredura de dados cruzados.

Você mapeia os seguidores, os perfis com quem ele mais interage, e encontra:

- Um perfil com quem ele conversa quase todos os dias: **@mariax_xx**.
- Ela postou um vídeo em que o “Bruno” aparece ao fundo. E o rosto... é **Lucien**, com cabelo tingido.

📱 Etapa 5 – Número de telefone e pegadas digitais

Ele colocou um número de WhatsApp nos destaques: “contato para ensaios”.

Você joga no:

- Sync.me
- TrueCaller
- Google direto com aspas (“+5583xxxxxxxxx”)

Resultado:

- O número já foi registrado em 2021 em um grupo de Telegram sobre “Turismo na Espanha”.
- Depois, usado em um grupo chamado “Tech Nomads BR-Europa”.
- E adivinha o nome do criador do grupo? **Lucien V.**

🚨 Conclusão: A falsa vida do fotógrafo

Você envia todas as provas para a Interpol:

- Reconhecimento facial batendo com o rosto de Lucien.
- Localização rastreada.
- Número vinculado a atividades antigas dele na Espanha.
- Perfil com nome falso, mas com os mesmos contatos de antes.

Três dias depois, ele é detido pela PF no bairro que você identificou.

Você não só usou OSINT para pegar um criminoso. Você salvou vidas. Porque **Lucien era perigoso**.

No próximo capítulo? Um desafio ético: Uma garota está sendo stalkeada e alguém está vazando suas fotos

pessoais em fóruns obscuros. Ela quer
saber quem é o responsável. Você consegue montar esse quebra-cabeça sem ultrapassar os limites legais?

👥 Capítulo 5 – A Sombra no Espelho: Rastreamento de um Vazar de Intimidade

---

🎬 CENA 5: Um pedido pessoal e delicado

— "Alguém está divulgando minhas fotos privadas em fóruns fechados. Eu não faço ideia de quem seja... Já troquei senha, saí de todos os grupos. Mas continua. Por favor, você pode me ajudar?"

Você sente o peso da missão. Não é só uma investigação. É sobre privacidade, confiança e dignidade.

🎯 Missão: Descobrir quem está vazando o conteúdo íntimo de uma jovem sem ultrapassar os limites legais

---

🛑 Nota de Ética:

Você não vai invadir sistemas, nem usar engenharia social agressiva. Vai jogar limpo, dentro da legalidade, porque ética é o escudo de quem lida com OSINT real.

🧩 Etapa 1 – Identificação da origem das fotos

Ela te manda três imagens que foram vazadas:

- Uma selfie deitada na cama, feita com iPhone.
- Uma imagem tirada no espelho do banheiro.
- Uma que ela diz “nunca mandei pra ninguém, só salvei na galeria por 1 dia”.

Ferramentas:

- Exif.tools ou Photo Forensics.
- HashMyFiles (gera hash das imagens para busca reversa).

- Google Lens + Yandex Reverse Image Search.

Descober tas:
A imagem do espelho aparece em um fórum obscuro, com a marca d'água **"uploaded by user2023_b4"**.

Etapa 2 – Busca pelo nome de usuário 'user2023_b4'

Ferramentas:

- NameCheckr.
- WhatsMyName.app.
- Holehe (para verificar quais e-mails estão atrelados a redes sociais).

Descober tas:

- O nome de usuário aparece em um fórum russo, mas também vinculado a um perfil em um grupo de WhatsApp sobre trading.
- O mesmo nome é usado em um Twitter suspenso, mas o cache mostra a bio: **"BR - Manaus / gamer de coração / adm no canal XYZ"**.

🔍 Etapa 3 – Investigação de canais onde ele é ADM

Você procura pelo tal "canal XYZ" no Telegram.

Ferramentas:

- Telegram Open Search Bot.
- TGStat.
- Scraper manual em grupos públicos.

Descober tas:
Aparecem dois canais: um de memes e um grupo fechado chamado **"Só pros chegados 🔞"**.
Ao verificar, você encontra uma imagem de divulgação com o nome da vítima borrado, mas a silhueta é idêntica à selfie dela.
Alguém do círculo próximo pegou, editou e soltou ali.

👥 Etapa 4 – Investigando quem tinha acesso às fotos

Você pede que ela refaça a linha do tempo:

- Para quem enviou a imagem da cama?
- Quem já viu a do espelho?
- Quem sabia que ela tinha salvo aquela que "nunca mandou pra ninguém"?

Resultado:
A única pessoa em comum entre os três casos é um ex-namorado, **Lucas**. Ele trabalha com TI, sabe como esconder rastros e já foi tóxico no passado.

🧠 Etapa 5 – Engenharia OSINT e confirmação

Você busca perfis que Lucas possa estar usando.

Ferramentas:

- Sherlock (busca por usernames).
- HaveIBeenPwned (para ver e-mails vazados).
- Google Dorking com:

```
"lucas" AND "manaus" AND "trading"
site:telegram.me
```

Bingo.

Você encontra um perfil de Telegram de Lucas usando o mesmo nome da conta **“user2023_b4”** em 2022. O e-mail é similar a um usado por ele num fórum de TI.

⚖️ Encaminhamento ético: o momento de agir certo

Você coleta todas as provas:

- Prints das postagens.
- Rastros do username.
- Ligação direta com e-mail dele.
- Confirmação de que ele teve acesso a tudo.

Com consentimento da vítima, você monta um dossiê e encaminha para a **Delegacia de Crimes Cibernéticos**.
Dois dias depois, o canal é derrubado, e Lucas é intimado.

> *“Obrigada. Eu me sentia vazia e agora me sinto... de volta.”* – ela diz, com lágrimas nos olhos.

No próximo desafio? **OSINT de campo misturado com fake news:**

Uma cidadezinha no interior está entrando em pânico por conta de uma notícia falsa que envolve sumiço de crianças e supostos rituais. Você precisa descobrir quem criou essa desinformação, e por quê.

📰 Capítulo 6 – A Fábrica do Pânico: Investigando Fake News

🎬 CENA 6: “Sumiram três crianças. Disseram que foi um ritual...”

Você recebe uma mensagem no grupo do Telegram dos Investigadores Éticos Anônimos:

— "Galera, a cidade de Boa Esperança tá em caos. Pais com medo, escolas fechadas. Tá todo mundo falando de sequestro e ritual satânico. Mas nada disso tá confirmado. Podem ajudar?"

Esse tipo de histeria pode virar tragédia real. Você respira fundo. Hora de entender o que está por trás do medo.

🎯 Missão: Identificar a origem e os propagadores de uma fake news que espalhou pânico numa cidade pequena

---

🧭 Etapa 1 – Mapeamento da narrativa

Ferramentas:

- Google Trends (para verificar aumento de buscas).
- CrowdTangle (Meta) para rastrear postagens no Facebook.
- Twitter Advanced Search com:

```
"Boa Esperança" AND "ritual" OR "criança" since:2025-04-01
```

Descober tas:
Você percebe que a narrativa ganhou força no WhatsApp e no Facebook. Primeira aparição? Um post do tipo:

> *“⚠ ALERTA: Tia da escola falou que pegaram 3 crianças aqui perto da rodoviária. Dizem que é coisa de magia negra. Fiquem atentos!”*

Post anônimo, mas com **200 compartilhamentos em menos de 3h**.

🧠 Etapa 2 – Engenharia reversa de narrativa

Você começa a puxar o fio da meada.

Ferramentas:

- InVID (análise de vídeos para verificar metadados, manipulações).
- Wayback Machine (salvou algumas postagens apagadas).
- Google Dorking:

```
site:facebook.com "Boa Esperança" AND "ritual" AND "sumiço"
```

Identifica o primeiro vídeo alarmista: Uma mulher tremendo com o celular dizendo que “a irmã da amiga da cunhada viu uma Kombi preta pegando crianças”.

Você investiga os metadados:

- Publicado por um perfil chamado **@AlertaPatriotaBR**, criado há 2 semanas.

- As fotos do perfil foram geradas por IA (**DeepFake Detectors confirmam**).

🧩 Etapa 3 – Ligando os pontos: quem está por trás da conta?

Você vai pro modo stalker avançado (ético, claro):

Ferramentas:

- FotoForensics nas imagens.
- Google Reverse Image Search.
- DataSploit e Maltego CE para criar relações entre domínios, perfis e nomes.

Descobre que:

- O perfil **@AlertaPatriotaBR** foi usado para espalhar fake news em três outras cidades pequenas do Brasil.
- O mesmo conteúdo tem padrão de formatação idêntico: emojis, letras maiúsculas, termos religiosos e tons conspiratórios.

Bingo: Há um padrão de desinformação programada. Isso não é um boato comum. É uma campanha de caos fabricado.

Etapa 4 – Encontrando o mandante da histeria

Você joga pesado (legalmente):

- Descobre que os posts sempre colocam links para um canal de notícias chamado **“Brasil Livre News”**.
- Quem administra esse domínio? Um CNPJ falso, mas o servidor de DNS aponta para um IP em São Paulo.

Com ajuda de colegas, você faz um cruzamento entre:

- IPs de comentários.
- Cookies vazados (em vazamentos anteriores).
- Contas do Twitter com mesmo e-mail base.

Um nome aparece: J. M. Oliveira, especialista em marketing político digital, já envolvido em investigações anteriores por manipulação de massa.

⚖️ Etapa 5 – Encaminhamento

Você coleta o dossiê:

- Prints dos posts.
- Metadados do vídeo.
- IPs associados.
- Relações com domínios.

Encaminha à **Polícia Federal** e ao **TSE**, porque percebe que isso vai além da cidade: é uma preparação para agitação pré-eleitoral.

> *"Depois da sua denúncia, as autoridades intervieram, o canal caiu e o pânico na cidade passou. Nunca mais acreditamos em qualquer corrente do WhatsApp."* – diz o delegado local, emocionado.

Missão cumprida. Mas... você está pronto para ir mais fundo?

No próximo capítulo: **investigando influenciadores que promovem esquemas de pirâmide com promessas de day trade e criptomoedas milagrosas.**

💰 Capítulo 7 – Caçando Golpistas de Criptomoeda: O Caso da Fraude de Investimentos

---

🎬 CENA 7: O Som da Verdade Oculta

— "Eu só queria fazer meu investimento crescer. Agora eu perdi tudo. Como posso confiar em alguém novamente?"

Você recebe uma ligação de um cliente que está devastado. Ele caiu em um golpe de criptomoedas, onde supostos "consultores financeiros" o convenceram a investir grandes quantias em uma plataforma de troca de cripto. Agora, não consegue mais acessar a conta, e o dinheiro sumiu.

🎯 Missão: Localizar os responsáveis por um golpe de criptomoedas e reverter o roubo.

🛑 Nota de Ética:

Em casos de fraudes digitais e golpes financeiros, a investigação deve ser conduzida com ética, respeitando a privacidade das vítimas e a legislação vigente. O objetivo aqui é localizar os criminosos sem comprometer a integridade dos dados.

🧩 Etapa 1 – Identificando a Plataforma Fraudulenta

A vítima está nervosa, mas fornece algumas informações. O nome da plataforma de criptomoedas era **CryptoFlex**. O site parecia legítimo, com todos os requisitos de uma corretora confiável — até que sumiram com o dinheiro. Sua primeira tarefa é investigar se o site realmente existe e se ele é confiável.

Ferramentas:

- Whois Lookup para verificar o domínio da plataforma e sua origem.
- Google Dorking para descobrir sites ou artigos relacionados a críticas ou golpes envolvendo a CryptoFlex.
- PhishTool para verificar se o site contém elementos de phishing ou páginas falsas.

Descober tas:
Ao investigar, você descobre que o domínio **cryptoflex.com** foi registrado recentemente, em um país conhecido por ser um ponto de atenção para fraudes financeiras. O servidor de e-mail está vinculado a um domínio genérico e a plataforma tem apenas alguns meses de operação.

Etapa 2 – Rastreamento das Transações de Criptomoeda

Agora que você sabe que a plataforma foi criada recentemente e parece ser falsa, sua próxima missão é rastrear as transações de criptomoeda feitas pela vítima.

Ferramentas:

- Blockchain Explorers como EtherScan e Blockchain.com Explorer para mapear transações de criptomoeda.
- Chainalysis para identificar padrões de movimentação de criptomoedas e endereços envolvidos.
- Whale Alert para monitorar grandes movimentações de criptomoedas.

Descober tas:
Usando o EtherScan, você consegue acessar o histórico de transações da carteira de criptomoeda fornecida pela vítima. A primeira transação foi feita para um endereço anonimizado, mas você observa que uma grande quantidade de criptomoeda foi transferida para uma segunda carteira, e de lá para múltiplas outras.

🔍 Etapa 3 – Descobrindo a Identidade dos Golpistas

Você agora tem várias transações e endereços de carteira para trabalhar. O próximo passo é identificar se esses endereços estão associados a alguma pessoa ou organização. Para isso, você vai precisar verificar em várias fontes.

Ferramentas:

- Whois para verificar os domínios associados às carteiras de criptomoedas.
- Google Dorking para buscar qualquer menção desses endereços em fóruns ou sites relacionados a golpes.
- Chainalysis para investigar os endereços de criptomoeda e suas relações com carteiras ou exchanges legítimas.

Descober tas:
Durante sua investigação, você descobre que um dos endereços de carteira está vinculado a uma exchange desconhecida, que foi listada em sites de fraude de criptomoedas. Outro endereço de carteira já foi vinculado a várias fraudes anteriores e está listado em um banco de dados de endereços de scam wallets.

🧠 Etapa 4 – Rastreando os Golpistas em Redes Sociais

Agora que você tem informações sobre os endereços de carteira envolvidos, seu próximo movimento é encontrar os responsáveis por trás dessa rede de golpistas. Muitos criminosos digitais deixam rastros em suas redes sociais.

Ferramentas:

- Sherlock para procurar o nome de usuário em várias redes sociais.
- Maltego para mapear a rede de contatos de golpistas que utilizam a mesma técnica de fraude.
- OSINT Framework para procurar informações relacionadas a pessoas e entidades que possam estar conectadas a esses golpistas.

Descober tas:
Ao fazer uma busca de username com Sherlock, você encontra um perfil de Instagram associado a um dos endereços de e-mail vinculados à plataforma fraudulenta. O perfil, que parece inofensivo, está cheio de posts sobre “consultoria de investimentos”, mas com algumas pistas inconsistentes. Você também encontra uma postagem antiga de um golpista usando o mesmo endereço de carteira em um fórum de criptomoedas.

🧩 Etapa 5 – Desmascarando o Golpe

Agora que você tem todas as informações necessárias, é hora de desmascarar o golpe e preparar um relatório detalhado para a vítima. Você reuniu informações sobre os endereços de criptomoeda, a plataforma fraudulenta e até mesmo os golpistas por trás disso. Seu trabalho agora é documentar tudo isso e entregar para as autoridades.

Ações:

- Relatar à polícia e autoridades de segurança cibernética, fornecendo todas as provas coletadas.
- Entrar em contato com a exchange para tentar congelar as transações ou identificar as movimentações ilícitas.
- Informar a vítima sobre os próximos passos para tentar recuperar parte do investimento perdido.

⚖️ Etapa 6 – A Responsabilidade do Hacker Ético

Agora, a responsabilidade de seguir as leis e práticas éticas de cibersegurança é crucial. O trabalho de um hacker ético não é apenas rastrear os criminosos, mas também garantir que a solução não envolva invasões ilegais ou ações que possam prejudicar a vítima.

Ações Legais:

- Consultar advogados especializados em fraude digital para garantir que todas as ações estão de acordo com as leis locais.
- Trabalhar com bancos de criptomoedas e exchanges para monitorar e prevenir futuras fraudes.
- Implementar ferramentas de segurança como autenticação de dois fatores (2FA) nas plataformas de criptomoeda para evitar novos golpes.

🧩 Resultado Final

Após semanas de investigação, você consegue rastrear a maioria dos golpistas. O relatório detalhado é entregue às autoridades competentes e, com a ajuda das exchanges de criptomoedas, algumas transações podem ser recuperadas.

Embora o dinheiro não seja 100% recuperado, sua investigação trouxe à tona uma rede de golpistas altamente organizada, que será desmantelada graças ao seu trabalho como hacker ético.

No próximo caso? **Agora, você enfrentará um novo desafio:** decifrar o mistério de um hacker invisível por trás de um sistema bancário comprometido. O uso de ferramentas de forense digital será essencial para pegar este criminoso.

⚖️ Capítulo 8: Ética e Legislação no Mundo do OSINT e Hacking Ético

---

Contexto:

Como hacker ético, é essencial entender os limites legais do que pode e não pode ser feito ao realizar investigações digitais e aplicar ferramentas de OSINT. Antes de usar qualquer técnica avançada, é necessário ter consciência de que o campo da cibersegurança não opera apenas com habilidades técnicas, mas também com respeito às leis e regulamentações que protegem a privacidade e os dados das pessoas.

Neste capítulo, vamos explorar as questões legais que você deve ter em mente ao realizar investigações, especialmente no contexto de hacking ético, como as regulamentações da **LGPD (Lei Geral de Proteção de Dados)** no Brasil e a **GDPR (Regulamento Geral sobre a Proteção de Dados)** da União Europeia. A ética na cibersegurança também será abordada, já que cada ação de um hacker ético deve ser pautada pela responsabilidade.

Passo 1: O Que é Hacking Ético?

Hacking ético, também conhecido como "hacking de chapéu branco", envolve a prática de explorar sistemas, redes e aplicativos em busca de falhas de segurança, **com a permissão do proprietário do sistema**, para corrigi-las antes que possam ser exploradas de forma maliciosa. O objetivo do hacking ético é melhorar a segurança cibernética, identificando vulnerabilidades que poderiam ser usadas por hackers "maliciosos" (chapéu preto).

Exemplo de Ação Ética:
Realizar uma análise de vulnerabilidade em uma empresa que contratou um hacker ético para testar a segurança de seu sistema. O hacker faz isso sem causar danos, sem roubar dados ou prejudicar o funcionamento do sistema.

Passo 2: Compreendendo a Legislação

O hacking ético não pode ultrapassar os limites do que é legal. Existem várias leis e regulamentos que os hackers éticos devem seguir para garantir que suas ações não infrinjam direitos e privacidade das pessoas. Vamos abordar as legislações mais relevantes que impactam as práticas de hacking ético.

Lei Geral de Proteção de Dados (LGPD):

Uma lei brasileira que regula a coleta, o armazenamento e o uso de dados pessoais. A LGPD é um dos regulamentos mais rigorosos do mundo, similar ao GDPR da União Europeia.

- **Aplicação da LGPD no OSINT:** Ao realizar investigações usando dados de fontes públicas, um hacker ético deve se atentar para não violar os direitos de privacidade de indivíduos. Isso significa que informações como dados pessoais, documentos e imagens não devem ser usadas sem o devido consentimento ou sem uma justificativa legal para sua coleta.

Regulamento Geral de Proteção de Dados (GDPR):

O GDPR é uma legislação da União Europeia que visa proteger os dados pessoais dos cidadãos da UE. Os hackers éticos que atuam em sistemas que operam na União Europeia precisam entender os direitos do titular dos dados e garantir que as investigações não violem o GDPR.

- **Aplicação do GDPR no OSINT:** Se você estiver investigando dados de pessoas ou coletando informações pessoais de indivíduos da UE, é importante garantir que sua investigação não infrinja o direito à privacidade e à proteção de dados. Isso inclui evitar o uso de ferramentas que possam acessar dados privados sem consentimento.

Passo 3: Principais Práticas e Ferramentas para Hacking Ético

O hacking ético é mais do que realizar ataques ou investigar falhas. A prática também envolve o uso de ferramentas de maneira legal e responsável. Existem diversas ferramentas no mundo do OSINT e hacking ético que são usadas para testar vulnerabilidades de forma controlada e sem violar leis.

Ferramentas de Teste de Penetração (Pen Testing):

- **Metasploit:** Um framework que permite a execução de testes de penetração e exploração de vulnerabilidades, sempre com a permissão do sistema alvo.
- **Wireshark:** Ferramenta de captura de pacotes de rede, útil para analisar tráfego e verificar falhas de segurança em redes. Seu uso deve ser restrito a sistemas onde a permissão foi concedida.

Ferramentas de Análise de OSINT:

- **Shodan:** Um motor de busca que permite descobrir dispositivos conectados à internet. Pode ser usado para encontrar dispositivos vulneráveis, mas é importante usá-lo com ética e responsabilidade.
- **Maltego:** Usada para análise de relacionamentos e grafos de pessoas e redes. Essa ferramenta pode mapear redes sociais e outros dados públicos, mas seu uso deve ser feito com cautela para não violar direitos de privacidade.

Passo 4: Limitações Legais ao Realizar Investigações de OSINT

Apesar de várias ferramentas poderem ser utilizadas para descobrir dados valiosos, há uma linha tênue entre a exploração legítima e a invasão de privacidade. Antes de realizar qualquer investigação, é importante ter certeza de que você está agindo dentro dos limites legais. Aqui estão algumas limitações importantes:

- **Não acessar sistemas sem permissão:** Mesmo se você tiver as habilidades técnicas para invadir um sistema, a menos que tenha permissão expressa do proprietário, você está violando a lei.
- **Respeitar as plataformas e os termos de serviço:** Muitas ferramentas de OSINT, como redes sociais, possuem termos de serviço que proíbem a coleta automatizada de dados. Ignorar essas regras pode

resultar em processos legais.
- **Evitar o uso de dados privados sem justificativa legal:** Mesmo que dados sejam encontrados publicamente, você precisa se atentar para sua utilização, evitando expô-los de maneira que possa prejudicar outras pessoas.

Passo 5: Consequências Legais do Hacking Ilegal

Realizar hacking ilegal pode ter sérias consequências, incluindo:

- **Prisão:** Dependendo da jurisdição, a invasão de sistemas sem permissão pode resultar em prisão, com penas que variam de acordo com a gravidade do ataque.
- **Processos Civis:** Empresas ou indivíduos afetados por ataques de hackers podem buscar compensação financeira por danos e perdas sofridas.
- **Danos à Reputação:** Além das consequências legais, um hacker que realiza atividades ilegais pode ter sua reputação destruída, o que impossibilita sua atuação no mercado de cibersegurança.

Passo 6: Ética em Cibersegurança

Finalmente, é importante lembrar que a ética não se resume apenas a seguir a lei. A ética em cibersegurança envolve agir com responsabilidade, transparência e respeito aos direitos dos outros. Aqui estão algumas diretrizes éticas que um hacker ético deve seguir:

- **Não causar danos:** Todo hacker ético deve agir de forma a não causar prejuízos ao sistema, dados ou usuários.
- **Transparência:** Sempre que possível, a pessoa ou organização que está sendo testada deve ser informada sobre a avaliação de segurança, especialmente se for um teste de penetração.
- **Confidencialidade:** Ao lidar com dados sensíveis, é essencial manter a confidencialidade das informações e não usar dados para fins pessoais.

Conclusão do Capítulo:

A ética e a legislação são pilares fundamentais para um hacker ético. Sem compreender as leis e atuar dentro de seus limites, suas habilidades podem ser usadas de forma prejudicial. Manter-se informado sobre as leis, praticar com responsabilidade e entender as implicações legais das ferramentas de hacking são passos essenciais para qualquer pessoa que deseje atuar no mundo da cibersegurança de forma legal e ética.

🎯 Capítulo 9: Casos Bônus – Desafios para Testar Seu Olhar Investigativo

Agora que você já teve uma boa dose de teoria e prática ao longo deste eBook, chegou a hora de testar suas habilidades em campo. Este capítulo traz **3 desafios bônus**, com diferentes níveis de dificuldade, que simulam situações reais para colocar em prática tudo que você aprendeu: coleta de dados, análise crítica, uso de ferramentas e, claro, sua criatividade investigativa.

Cada caso vem com pistas, fontes abertas e perguntas que você deve responder. Lembre-se: **não há uma única resposta certa**, e sim um raciocínio lógico e ético por trás de cada investigação. Pronto(a)? Que comecem os jogos!

🔍 Caso 1 – "O Influencer Misterioso" (nível fácil)

Contexto:
Um influenciador digital famoso desapareceu das redes sociais há semanas. Você foi contratada para descobrir se ele está ativo em outras contas secretas e se a ausência tem relação com um vazamento recente de dados pessoais.

Pistas:

- Nome artístico: **@EduWanderlust**
- Último post público foi no Instagram, com a legenda: *"É hora de sumir nas montanhas"*.
- Há rumores de que ele usa um perfil alternativo no Twitter para interações anônimas.
- Já deu entrevistas dizendo que ama montanhismo e trilhas fora do Brasil.
- Possui uma tatuagem exclusiva de um triângulo azul no antebraço esquerdo.

Tarefas:

1. Pesquise se existem outros perfis em redes sociais que possam ser dele (use técnicas de username reverse e reconhecimento facial, se possível).
2. Identifique se a localização da última imagem postada pode ser triangulada.
3. Analise possíveis vazamentos de dados recentes com esse nome artístico.
4. Hipotetize qual seria a motivação para ele sumir da rede.

🕵️ Caso 2 – "O Golpe do Pix Premiado" (nível médio)

Contexto:
Várias pessoas denunciaram um perfil no TikTok que promove sorteios falsos com o nome de empresas conhecidas. O sorteio exige um *"Pix de verificação"* para liberar o prêmio. Você foi chamada para identificar a real identidade da pessoa por trás da conta e coletar provas.

Pistas:

- Perfil: **@promooficial2025**
- Usam sempre os mesmos templates de vídeo.
- No áudio, uma voz masculina jovem e distorcida.
- Todos os sorteios pedem um Pix no valor de R$ 9,99 para uma chave aleatória.
- A conta marca falsamente empresas conhecidas como Nubank, PicPay, iFood.
- Comentários negativos são rapidamente apagados.

Tarefas:

1. Coletar prints e URLs dos vídeos postados.
2. Analisar metadados das imagens e vídeos (dica: ferramentas como Exiftool ou Forensically).
3. Tentar descobrir quem está por trás da chave Pix (verificando padrões, CPF/CNPJ se houver).
4. Mapear se o golpe se repete em outras redes com o mesmo conteúdo.

🧠 Caso 3 – "O Arquivista do Submundo" (nível difícil)

Contexto:
Um grupo de jornalistas investigativos recebeu um pendrive anônimo contendo PDFs e imagens de arquivos secretos. Alguns documentos estão criptografados. Um deles tem como nome **“DDOS-CORP – Lista Classificada”**. Você foi acionada para descobrir se esse material é legítimo, quem pode ter vazado e quais são os riscos atrelados.

Pistas:

- Há uma imagem com um logotipo **“DDOS-CORP”** em baixa resolução.
- Um dos PDFs contém nomes, e-mails e senhas (parcialmente ofuscadas).
- Um arquivo de texto diz: *“hora de devolver o troco”*.
- Os metadados apontam edição feita no Kali Linux.
- Uma das fotos mostra uma tela de terminal com IPs suspeitos de servidores.

Tarefas:

1. Identificar se os dados são reais e se algum e-mail aparece em leaks públicos.
2. Verificar a origem dos IPs e se eles pertencem a servidores de empresas conhecidas.
3. Investigar a legitimidade da empresa **“DDOS-CORP”**.
4. Esboçar uma hipótese do porquê esse vazamento foi feito e quem pode estar por trás.

🎯 Dica final do capítulo:

Use tudo que você aprendeu até aqui: dorking, OSINT avançado, técnicas de fingerprinting, investigação de metadados, redes sociais, análise de fontes cruzadas... e mantenha sempre o senso crítico afiado. A resposta nem sempre está na primeira pista — às vezes, o melhor analista é aquele que sabe onde procurar, como buscar e, principalmente, quando parar.

🌐 Capítulo 10: Conclusão – O Futuro do OSINT e da Cibersegurança

---

Era quase 3 da manhã.

A tela do computador iluminava o quarto escuro. A investigação já estava finalizada, os dados organizados, e o último relatório enviado. Você respirou fundo e encostou na cadeira, olhando para o monitor como quem olha para um portal: o mundo digital. Um universo de informações escondidas em tweets esquecidos, perfis abandonados, endereços IP, fotos, domínios, blockchain e servidores ocultos. O que antes era apenas curiosidade, agora era habilidade.

Você não é mais um curioso. Agora você é **OSINT**.

Mas e agora?

🧠 A próxima fase: OSINT + IA

O jogo está mudando rápido. As ferramentas de OSINT do futuro já estão entre nós — e a maioria usa inteligência artificial. Modelos treinados para identificar padrões em vídeos, automatizar buscas por nomes e localizar rostos até em GIFs de baixa qualidade.

Imagine ter um bot que cruza dados de contas vazadas com perfis do LinkedIn e, com um clique, te entrega um dossiê. Isso já existe. Mas o poder vem com a responsabilidade: saber usar tudo isso sem ultrapassar a linha da ética será o verdadeiro diferencial entre profissionais e oportunistas.

🧪 OSINT como ciência investigativa

Sim, **ciência**.

Cada caso que você resolveu ao longo deste livro seguiu um método investigativo: coleta, análise, correlação e ação. Isso te coloca no mesmo patamar de jornalistas investigativos, policiais federais e analistas de inteligência de grandes agências. Não é exagero — é realidade.

A diferença é que agora você entende como pensar, como buscar, como montar uma teia de pistas digitais e, o mais importante: como não deixar rastros enquanto faz isso.

🛡️ A missão continua: defender e conscientizar

Você pode até não trabalhar na polícia, mas já entendeu que o **OSINT** é uma arma poderosa. Pode ser usado para o bem ou para o caos. O que diferencia você de um invasor é o propósito. E o seu, se chegou até aqui, é proteger.

Proteger sua família, seu trabalho, sua comunidade.

Compartilhar conhecimento.

E talvez... inspirar outras pessoas a também jogarem esse jogo — do lado certo da força.

👣 Seu próximo passo

Você já fez muito, mas ainda tem muito a explorar.

Aqui vão seus próximos desafios, caso queira continuar a trilha:

- 🧭 Criar sua própria ferramenta OSINT (com Python, claro).
- 🎯 Participar de **Capture The Flags (CTFs)** de inteligência.
- 📊 Publicar um relatório OSINT de um caso real (público ou fictício).
- 🔒 Ajudar ONGs ou vítimas reais com sua habilidade.
- 👨‍💻Se especializar em **Threat Intelligence**, **Blockchain Forensics** ou **OSINT para Red Team**.

Você não precisa fazer tudo. Só precisa continuar.

🚀 Finalizando

A internet é um campo minado. Mas agora você sabe onde pisar, como farejar pistas e quando parar.

No fundo, o **OSINT** não é sobre invadir coisas.

É sobre ver o que está bem na sua frente — e ninguém mais consegue enxergar.

Nos vemos na próxima missão.

E como sempre dizemos por aqui...

> *“Não é mágica. É método.”*

Fique curioso. Fique seguro.

💻

📖 Glossário Hacker

🥷 Para você nunca mais se perder no papo técnico (nem fingir que entendeu)

OSINT (Open Source Intelligence):

Inteligência de fontes abertas. Técnicas para encontrar, cruzar e analisar informações públicas disponíveis online.

Doxxing:

Ato de coletar e divulgar informações pessoais de alguém sem consentimento, geralmente com intenção maliciosa.

Metadata:

Dados sobre dados. Exemplo: uma foto tem como metadados a data em que foi tirada, o local, o modelo do celular etc.

CTF (Capture The Flag):

Competições hacker com desafios de segurança, investigação e análise de vulnerabilidades.

Footprinting:

Mapeamento de informações sobre um alvo antes de uma análise mais profunda.

Threat Intelligence:

Inteligência voltada à análise e previsão de ameaças digitais.

Dark Web:
Parte oculta da internet acessível apenas por softwares especiais como o Tor, onde muita coisa legal (e ilegal) acontece.

Hash:
Cadeia de caracteres gerada a partir de uma informação, usada para verificação de integridade ou anonimato.

Red Team / Blue Team:
Equipes que simulam ataques (Red) e defesas (Blue) em sistemas, geralmente em ambientes corporativos.

OSINT Tools:
Ferramentas como **Maltego**, **Spiderfoot**, **Sherlock**, **TheHarvester**, **Have I Been Pwned**, **ExifTool**, **Google Dorks Database** etc.

Referências

📚 As fontes que alimentaram esse eBook e te ajudam a ir ainda mais fundo.

Ferramentas

- Maltego
- SpiderFoot
- Sherlock
- TheHarvester
- Have I Been Pwned
- ExifTool
- Google Dorks Database

Sites e Comunidades

- OSINT Framework
- Bellingcat
- Intel Techniques
- Trace Labs

Livros e Leituras Recomendadas

- *Open Source Intelligence Techniques* – Michael Bazzell

- *Hacking for Beginners* – Kevin Beaver
- *The Cyber Effect* – Mary Aiken

Artigos e Casos Reais

- Casos adaptados de relatos da comunidade OSINT global (**Bellingcat**, **Reddit**, e **Trace Labs**)
- Estudos acadêmicos sobre **Cybercrime** e **Inteligência Digital**
