



# Workshop:

## Como encontrar Vulnerabilidades com Técnicas de OSINT

Com Filipe Cavalcante – Especialista em Segurança da Informação e Hacking

# QUEM SOU EU?

Analista de Segurança da Informação, especialista em Red Team e Inteligência Cibernética, com forte atuação em programas de Bug Bounty e pesquisa ofensiva.

Contribuí com a identificação de falhas de segurança reais em grandes empresas e instituições, incluindo:



Essas descobertas envolveram vulnerabilidades como:

- Exposição de dados sensíveis
- Acessos indevidos a sistemas e APIs
- Painéis administrativos públicos
- Tokens e credenciais vazadas
- XSS, má configuração de permissões, entre outras

Minha missão é reforçar a segurança digital, atuando de forma ética, colaborativa e educativa — através de treinamentos, palestras e workshops práticos em OSINT, hacking e investigação digital.



# O que é OSINT?

**OSINT (Open Source Intelligence)** é a prática de coletar informações públicas e acessíveis na internet, como sites, redes sociais, fóruns e bancos de dados.

## Importância:

Permite identificar falhas de exposição antes que sejam exploradas por Ciber Criminosos.



# Metodologia de OSINT

## Etapas da Metodologia OSINT

A metodologia de OSINT segue 6 passos bem definidos:

1. **Definir o objetivo** – o que você quer descobrir?
2. **Escolher as fontes** – onde você vai buscar?
3. **Coletar os dados** – manualmente ou com ferramentas.
4. **Processar os dados** – tirar duplicados, ruídos.
5. **Analisar** – descobrir padrões, conexões, falhas.
6. **Reportar** – documentar e comunicar os achados.



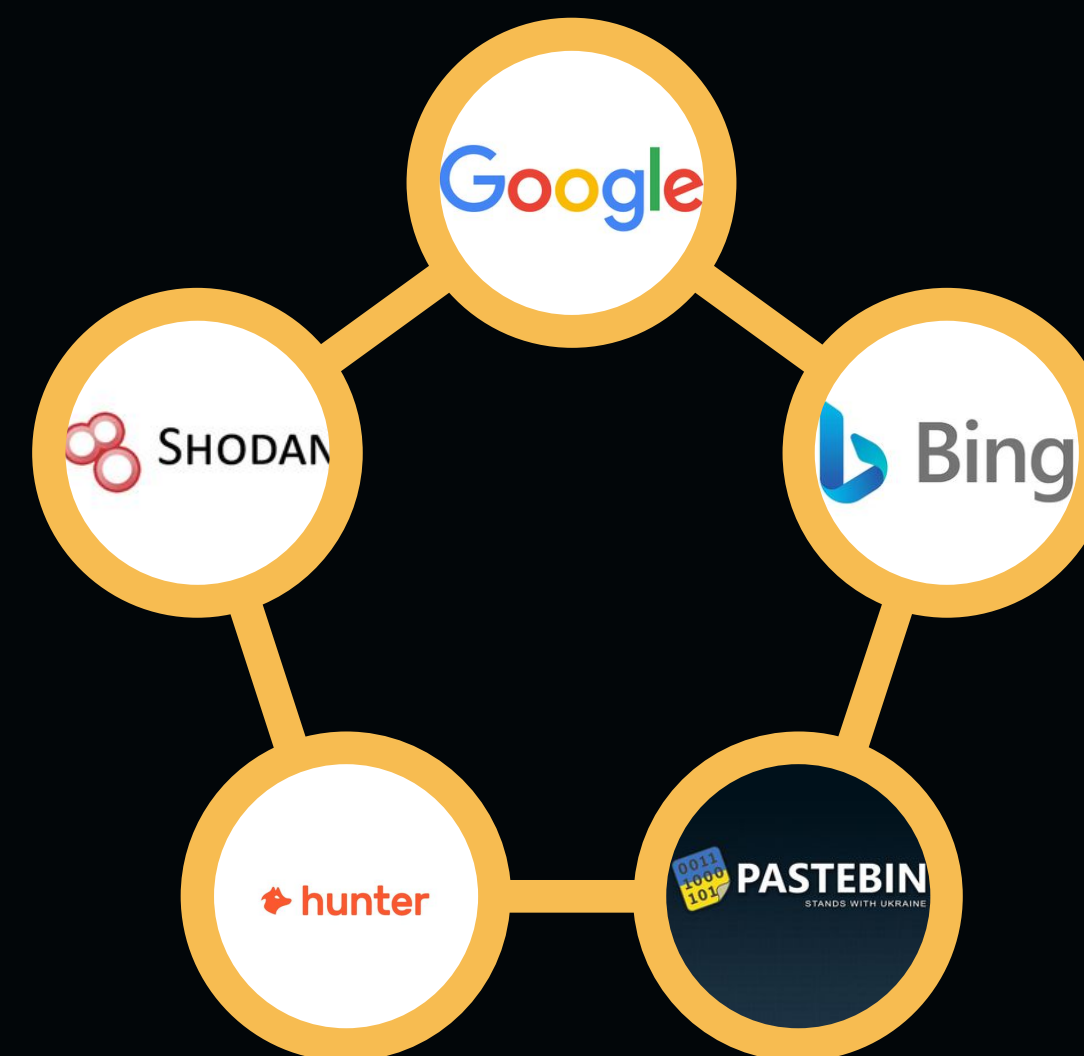


## Fontes comuns de OSINT:

- Motores de busca (Google, Bing)
- Bancos de dados públicos
- Redes sociais e fóruns
- Pastebins e vazamentos
- WHOIS, DNS e infraestrutura da web
- Documentos e arquivos indexados

### Por que é importante?

Informações públicas podem revelar vulnerabilidades, padrões de comportamento, estruturas organizacionais e superfícies de ataque exploráveis — sem a necessidade de exploração direta.



# SHODAN: O BUSCADOR MAIS PERIGOSO DO MUNDO!

O Shodan foi criado por **John Matherly**. Ele é um mecanismo de busca que permite encontrar dispositivos conectados à internet, como servidores, impressoras, roteadores e câmeras. A ferramenta foi lançada em 2009.

O criador do Shodan levou 5 horas para mapear todos os dispositivos na Internet.



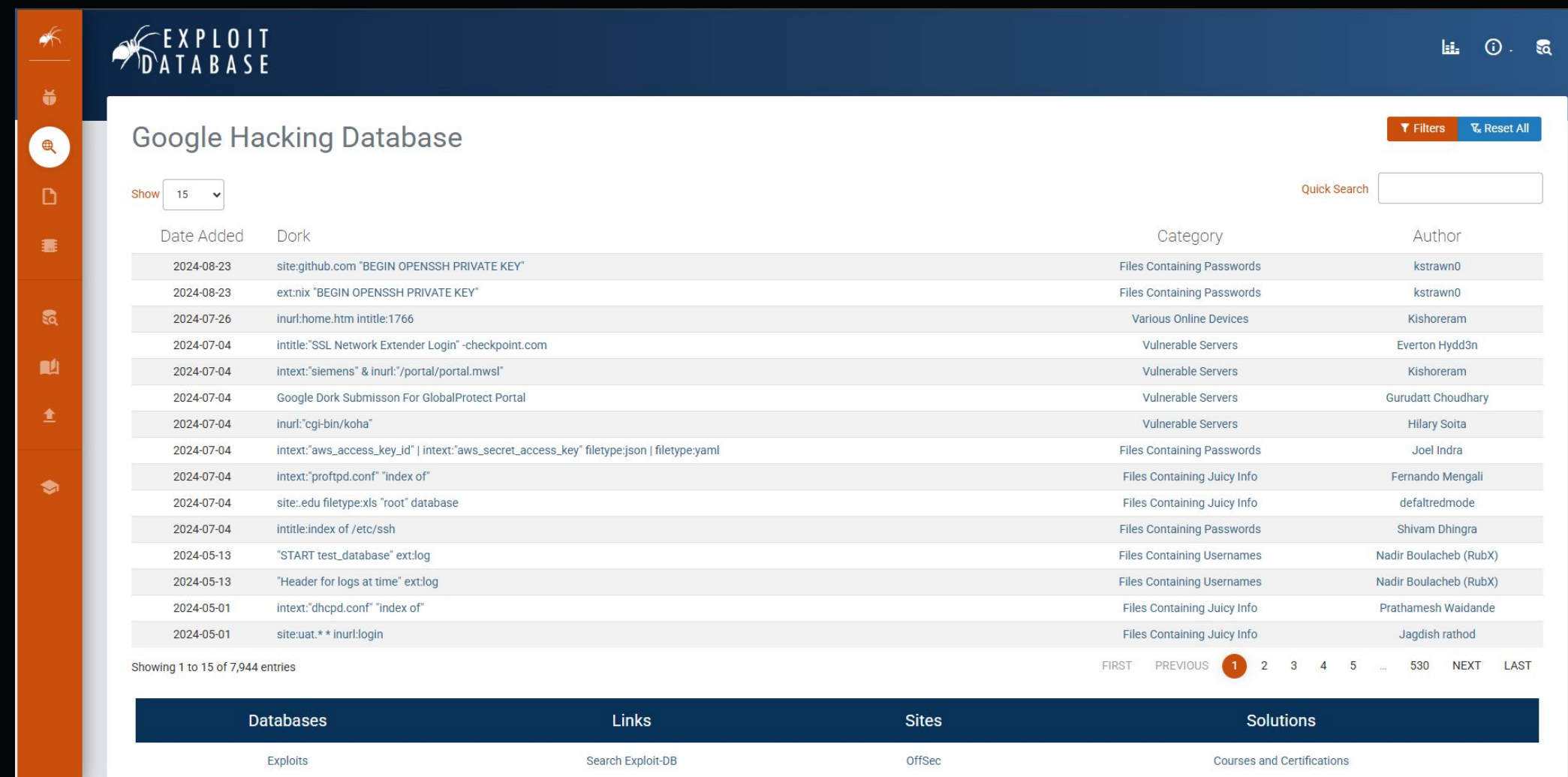
# Acessando dispositivos com **shodan.io**



# Google Hacking

É o uso avançado do Google para encontrar **informações sensíveis** ou **mal configuradas** na web.

Ele utiliza operadores especiais (Dorks) para localizar arquivos, painéis de login, diretórios abertos e até vazamentos de dados.



EXPLOIT DATABASE

## Google Hacking Database

Filters Reset All

Quick Search

Date Added	Dork	Category	Author
2024-08-23	site:github.com "BEGIN OPENSSE PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-08-23	ext:nix "BEGIN OPENSSE PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoreram
2024-07-04	intitle:"SSL Network Extender Login" -checkpoint.com	Vulnerable Servers	Everton Hydd3n
2024-07-04	intext:"siemens" & inurl:"/portal/portal.mwsl"	Vulnerable Servers	Kishoreram
2024-07-04	Google Dork Submission For GlobalProtect Portal	Vulnerable Servers	Gurudatt Choudhary
2024-07-04	inurl:"cgi-bin/koha"	Vulnerable Servers	Hilary Soita
2024-07-04	intext:"aws_access_key_id"   intext:"aws_secret_access_key" filetype:json   filetype:yaml	Files Containing Passwords	Joel Indra
2024-07-04	intext:"proftpd.conf" "index of"	Files Containing Juicy Info	Fernando Mengali
2024-07-04	site:.edu filetype:xls "root" database	Files Containing Juicy Info	defaultredmode
2024-07-04	intitle:index of /etc/ssh	Files Containing Passwords	Shivam Dhingra
2024-05-13	"START test_database" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)
2024-05-13	"Header for logs at time" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)
2024-05-01	intext:"dhcpd.conf" "index of"	Files Containing Juicy Info	Prathamesh Waidande
2024-05-01	site:uat.* * inurl:login	Files Containing Juicy Info	Jagdish rathod

Showing 1 to 15 of 7,944 entries

FIRST PREVIOUS 1 2 3 4 5 ... 530 NEXT LAST

Databases

Exploits

Links

Search Exploit-DB

Sites

OffSec

Solutions

Courses and Certifications






# Falha no Departamento de Defesa dos Estados Unidos

## Usando a Técnica de Google Hacking

### Exposição de Web Service no SharePoint


Um serviço web (lists.asmx?WSDL) do Microsoft SharePoint foi encontrado acessível publicamente e sem autenticação.

 **Impacto:**  
Permite que qualquer pessoa veja detalhes técnicos sobre o sistema, como estruturas de listas e métodos internos. Isso facilita ataques mais direcionados e exploração de falhas.

 **Correção:**  
Restringir o acesso anônimo ao serviço web no IIS ou na Central de Administração do SharePoint.

[ADICIONAR RESUMO DO HACKER](#)

[LINHA DO TEMPO](#) · [EXPORTAR](#)

 **filipecav** enviou um relatório ao **Departamento de Defesa dos EUA**.15 de junho de 2023, 19h46 UTC

**Descrição:**

O Microsoft SharePoint é uma plataforma de aplicativos web desenvolvida pela Microsoft. Devido a uma configuração incorreta, um usuário anônimo tem acesso aos Serviços Web do SharePoint.

`https://[redacted].education.nih.gov/[redacted]`

O impacto desta vulnerabilidade

Os Serviços Web do SharePoint podem divulgar informações confidenciais. Essas informações podem ser usadas para lançar novos ataques.

Como corrigir esta vulnerabilidade

Restringir o acesso a esta página.

**Referências**

**Impacto**

Um adversário pode utilizar as informações expostas sobre os serviços web para montar ataques específicos contra este site do SharePoint. Isso pode permitir que o invasor se comunique com o serviço web para identificar possíveis vulnerabilidades e comprometer ainda mais o sistema.

**Host(s) do sistema**

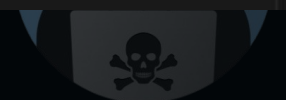
`[redacted].educação.nih.gov/[redacted]`

**Produto(s) e versão(ões) afetados(s)**

**Números CVE**

**Etapas para reproduzir**

`https://[redacted].e.education.nih.gov/[redacted]`



# Demonstrações Práticas: Hunter

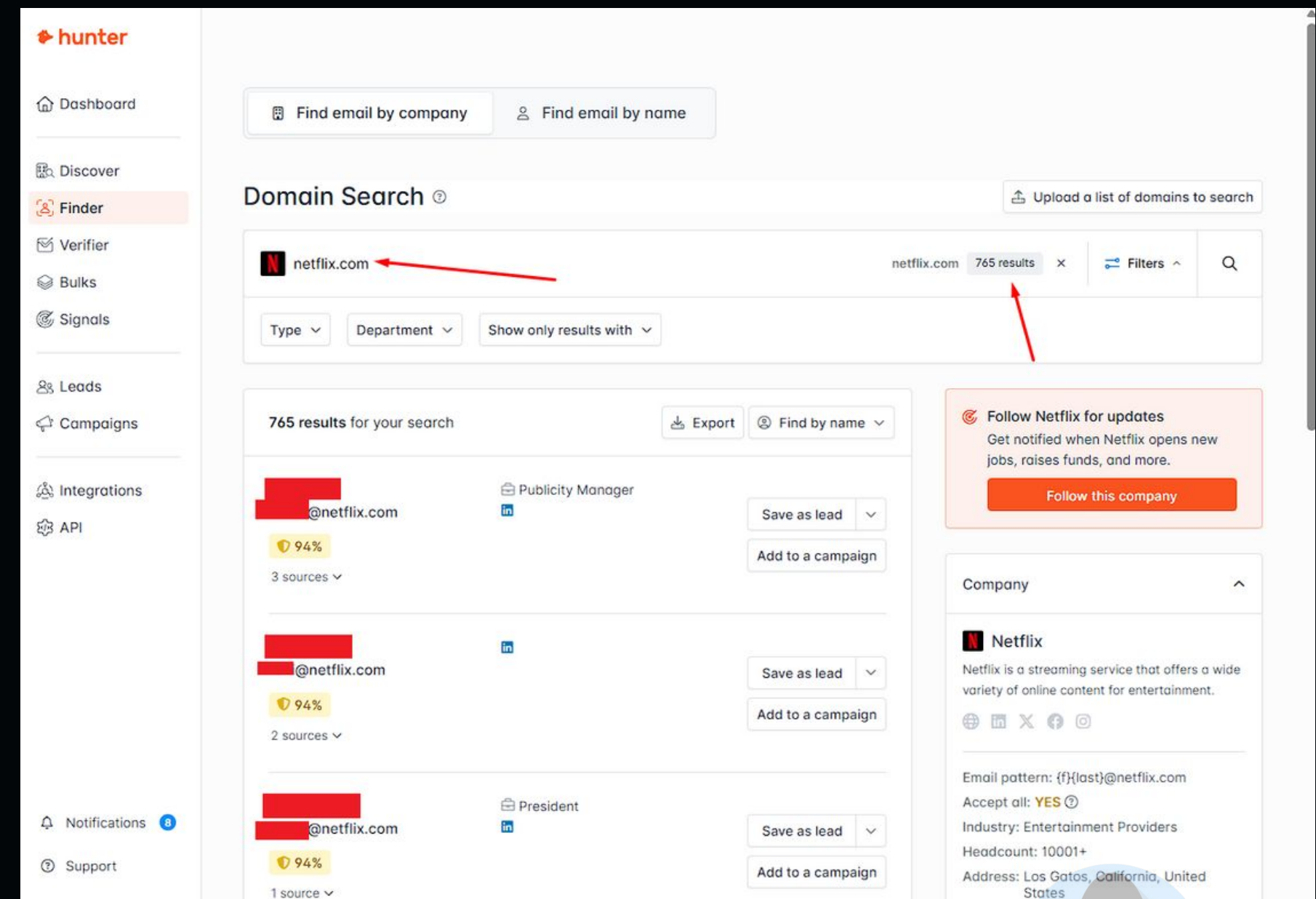
## O que é o Hunter.io??

É uma ferramenta de OSINT corporativo que permite encontrar e-mails associados a um domínio específico, analisando fontes públicas, registros DNS, redes sociais e páginas web indexadas.

## 💡 Para que serve?

- Reconhecimento de alvos em Red Team
- Mapeamento de possíveis credenciais vazadas
- Coleta de contatos para engenharia social
- Investigação de estrutura organizacional

Busca: “domínio: empresaexemplo.com.br”



The screenshot displays the Hunter.io web application interface. On the left is a sidebar with navigation links: Dashboard, Discover, Finder (highlighted), Verifier, Bulks, Signals, Leads, Campaigns, Integrations, and API. The main content area is titled 'Domain Search' and shows a search for 'netflix.com' with 765 results. A red arrow points to the search input field, and another red arrow points to the '765 results' count. Below the search bar, there are filters for 'Type', 'Department', and 'Show only results with'. The results list shows three entries, each with a redacted email address, a 94% confidence score, and a '3 sources' indicator. The first entry is labeled 'Publicity Manager', the second is unlabeled, and the third is labeled 'President'. Each entry has 'Save as lead' and 'Add to a campaign' buttons. On the right side, there is a 'Follow Netflix for updates' section with a 'Follow this company' button, and a 'Company' section with details about Netflix, including its email pattern, acceptance status, industry, headcount, and address. A small icon of a person with a skull and crossbones is visible in the bottom right corner.

# Obtendo E-mails de Usuários **Hunter.io**



**Busca reversa de e-mails  
e números de telefone  
com **Epieos**.**





# Criando página Web

## Fake



# Hackeando Sistema com Kali Linux



# OSINTLeak

QUER SABE SE SUAS SENHAS FORAM VAZADAS?

<https://osintleak.com/>



OsintLeak

Fortaleça seu arsenal de cibersegurança  
com **Osintleak**

Utilize o poder do Osintleak para explorar as áreas ocultas da internet em profundidade, focando em vazamentos de dados e informações da dark web para proteger seus interesses.

Procure por vazamentos



# Quer entrar na área de **Segurança da Informação?**

- 🔧 Aprenda redes, Linux e lógica de programação
- 🔧 Monte seu laboratório com VMs (Kali, Metasploitable, Windows)
- 🎯 Pratique em plataformas como TryHackMe, Hack The Box, VulnHub
- 📖 Estude OSINT, pentest e fundamentos de segurança
- 🛡️ Participe de eventos, CTFs e comunidades
- 🎓 Comece com certificações acessíveis (eJPT, Security+, OSINT-Fundamentals)
- 💼 Compartilhe aprendizados no LinkedIn e GitHub





**Obrigado pela  
participação!**

Vamos continuar conectados?

