Search Skills – Habilidades de Pesquisa na Cibersegurança

Objetivo da Sala

Vivemos em uma era de excesso de informação. Esta sala ensina a desenvolver **habilidades de pesquisa eficazes**, essenciais para profissionais de segurança cibernética, focando em:

- Avaliação de fontes de informação
- Uso eficiente de motores de busca
- Utilização de buscadores especializados
- Leitura de documentação técnica
- Uso de redes sociais e notícias para investigação

---

1. Avaliação de Fontes de Informação

Com qualquer um podendo publicar conteúdo online, é essencial **avaliar a credibilidade** do que lemos. Para isso, considere:

- **Fonte**: A autoria é confiável? A pessoa ou organização tem autoridade sobre o tema?
- **Evidência e lógica**: Há dados confiáveis e raciocínio lógico para sustentar as alegações?
- **Objetividade**: O conteúdo é imparcial? Ou tenta promover um produto/ideologia?
- **Corroboração**: Outras fontes confiáveis confirmam a mesma informação?

---

2. Motores de Busca e Operadores Avançados

Motores comuns:

- Google
- Bing
- DuckDuckGo

Operadores úteis (Google):

- `"frase exata"` → Ex: `"passive reconnaissance"`
- `site:` → Ex: `site:tryhackme.com success stories`
- `-` → Ex: `pyramids -tourism`
- `filetype:` → Ex: `filetype:ppt cyber security`

Estes comandos permitem **refinar pesquisas** e localizar **informações mais específicas**.

---

3. Buscadores Especializados

Shodan

Busca dispositivos conectados à internet (servidores, IoT, etc.). Exemplo: `apache 2.4.1` mostra servidores com essa versão.

Censys

Similar ao Shodan, mas foca em **hosts, domínios e certificados**. Ideal para auditorias de rede.

VirusTotal

Verifica arquivos e URLs com diversos antivírus. Também permite verificar hashes de arquivos.

Have I Been Pwned (HIBP)

Informa se um e-mail foi exposto em **vazamentos de dados**.

---

4. Fontes Técnicas Importantes

CVE – Common Vulnerabilities and Exposures

Catálogo padronizado de vulnerabilidades com identificadores únicos (ex: `CVE-2024-29988`). Útil para pesquisar falhas conhecidas.

Exploit Database

Banco de dados com códigos de exploração (exploits) verificados, úteis para testes em ambientes controlados (com permissão legal).

GitHub

Repositório onde se encontram **ferramentas, PoCs** e **exploits** relacionados a vulnerabilidades (ex: Heartbleed).

---

5. Leitura de Documentação Técnica

Linux (man pages)

Comando `man` exibe a documentação dos comandos. Ex: `man ip`.

Microsoft Docs

Documentação oficial da Microsoft, útil para comandos como `ipconfig` e muito mais.

Documentações Oficiais de Produtos

Exemplos:

- Snort
- Apache HTTP Server
- PHP
- Node.js

Documentações oficiais são as **fontes mais completas e atualizadas** sobre um software.

Conclusão

A habilidade de **pesquisar e validar informações corretamente** é fundamental na área de cibersegurança. Ao dominar os mecanismos de busca, validar fontes e acessar ferramentas especializadas, você se torna mais eficiente, analítico e crítico — características essenciais para analistas defensivos e ofensivos.