Moteurs de recherche

Vous cherchez un truc en cybersécurité ?

Si vous travaillez dans la cybersécurité, vous savez à quel point il est difficile d'avoir les bons outils pour explorer et analyser les données. Voici 10 moteurs de recherche un peut spéciaux que tout professionnel devrait connaître, avec une explication de ce que chacun permet de faire:

1. Shodan
Le moteur de recherche des objets connectés. Shodan vous permet d'explorer les serveurs, caméras, dispositifs IoT et autres appareils connectés à Internet. Parfait pour identifier les équipements vulnérables.
2. Censys
Analyse des services sur Internet. Censys cartographie les services exposés et fournit des informations détaillées sur les systèmes en ligne, facilitant la détection des failles de sécurité.
3. Hunter
Recherche d'adresses email. Hunter est idéal pour trouver les adresses email associées à un domaine. Utilisé souvent dans les campagnes de phishing ou d'investigation en cybersécurité.
4. urlscan.io
Analyse des URL suspectes. Ce service analyse les sites web pour identifier les comportements malveillants, les redirections, ou les contenus cachés. Très utile pour évaluer les menaces liées aux URL.
5. grep.app

Recherche dans le code source public. Grep.app vous aide à trouver des fragments de code partagés en public, ce qui peut révéler des informations sensibles ou des erreurs de configuration.
6. intelx.io
Outils d'OSINT. IntelX vous permet d'accéder à des bases de données, archives web et documents divulgués publiquement pour mener des enquêtes approfondies.
7. wigle.net
Cartographie des réseaux WiFi. Wigle vous aide à identifier les réseaux WiFi dans le monde entier. Utile pour les recherches sur les vulnérabilités réseaux.
8. FullHunt (Attack Surface)
Analyse de la surface d'attaque. FullHunt permet d'identifier et de surveiller les failles de sécurité dans les systèmes exposés sur Internet.
9. Vulners (Vulnerabilities)
Recherche de vulnérabilités. Vulners est un moteur de recherche de vulnérabilités connu qui compile les CVE (Common Vulnerabilities and Exposures).
10. viz.greynoise (Threat Intel)
GreyNoise aide à distinguer les activités malveillantes réelles des bruits de fond (scans automatisés, bots), permettant d'allouer vos ressources plus efficacement.

Ces outils couvrent tout, des serveurs vulnérables aux réseaux WiFi non sécurisés, en passant par

la collecte d’informations OSINT. Ils sont incontournables pour tout professionnel de la cybersécurité !

Revision #1
Created 2024-10-31 08:02:05 UTC by Admin
Updated 2024-10-31 08:03:05 UTC by Admin