

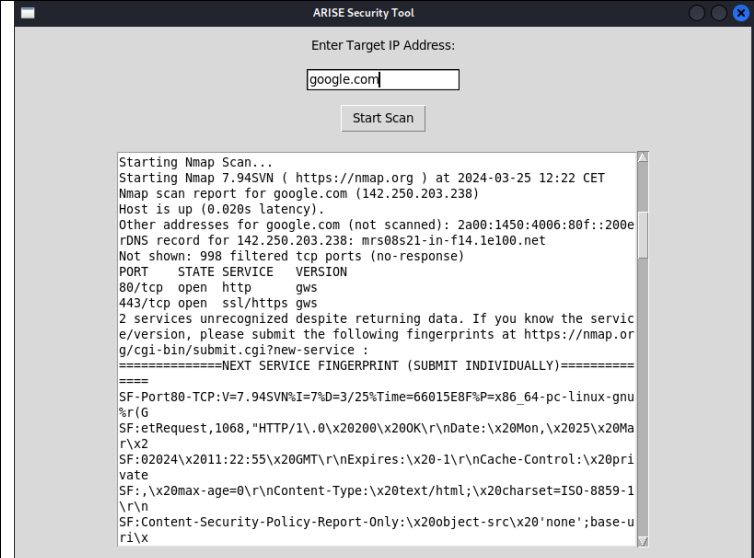


**A.R.I.S.E**

Security Tool

## 1. A.R.I.S.E SECURITY TOOL

A.R.I.S.E Security tool est un outil de sécurité numérique conçu pour protéger les entreprises des cybermenaces. Pensez à ARISE comme à un gardien qui vérifie les serrures et les alarmes de votre entreprise dans l'espace numérique. Il utilise un outil appelé Nmap pour scanner votre réseau, identifiant les services que vous utilisez et vérifiant s'ils sont à jour et sécurisés. Ensuite, il utilise Dirb pour découvrir des zones cachées ou sensibles de votre site web qui pourraient être vulnérables. Si Nmap trouve des services connus, ARISE consulte Searchsploit pour vérifier s'il existe des failles de sécurité connues liées à ces services, vous donnant ainsi une idée claire de ce qui doit être renforcé. ARISE est facile à utiliser : vous lui donnez une adresse IP, et il fait le reste, fournissant un rapport sur la sécurité de votre réseau. C'est comme avoir un expert en sécurité qui surveille en permanence votre entreprise contre les intrusions, sans nécessiter de connaissances techniques approfondies.

	<p>Son interface est simple à utiliser : elle permet de réaliser un scan et d'identifier les failles de sécurité, offrant la possibilité d'exporter les résultats très facilement. Il suffit d'entrer un nom de domaine ou une adresse IP. Le logiciel permet à chacun de nos collaborateurs d'effectuer des analyses qui peuvent être examinées par l'entreprise ou transmises à nos collaborateurs pour une analyse approfondie et la correction des éventuels problèmes de sécurité.</p>
--	---

ARISE offre une interface intuitive permettant à tous les collaborateurs, quel que soit leur niveau technique, de scanner des adresses IP ou des noms de domaine pour identifier les failles de sécurité. Les résultats, facilement exportables, peuvent servir à des analyses internes ou être partagés pour des examens plus approfondis, facilitant ainsi la correction des vulnérabilités détectées.

## 2. PYTHON

ARISE est entièrement développé en Python et utilise des programmes open-source, ce qui garantit une facilité d'évolution. Il intègre des outils de cybersécurité avancés et régulièrement mis à jour, rendant son utilisation très efficace. Les fonctions sont traitées de manière efficace.

```
def add_output(self, text):
    self.output_text.insert(tk.END, text + "\n")
    self.output_text.see(tk.END)

def start_scan_thread(self):
    ip_address = self.ip_entry.get()
    if not ip_address:
        messagebox.showwarning("Warning", "Please enter an IP address.")
        return
    threading.Thread(target=self.perform_scans, args=(ip_address,), daemon=True).start()

def perform_scans(self, ip_address):
    # Step 1: Nmap Scan
    self.add_output("Starting Nmap Scan...")
    try:
        nmap_result = subprocess.check_output(["nmap", "-sV", ip_address], text=True)
        self.add_output(nmap_result)
        # Extracting services for Searchsploit
        services = re.findall(r'(\d+/\tcp\s+open\s+\S+)\s+(\.+)', nmap_result)
        for service in services:
            port, service_name = service
            self.add_output(f"Searching exploits for: {service_name}...")
            try:
                exploits = subprocess.check_output(["searchsploit", service_name], text=True)
```

## 3. PREREQUIS

Pour faire fonctionner ARISE sous Windows, voici les prérequis essentiels :

- Windows Subsystem for Linux (WSL) : Installez WSL pour créer un environnement Linux sous Windows. Kali Linux via WSL est recommandé pour bénéficier d'un ensemble complet d'outils de cybersécurité déjà intégrés.
- Python : Assurez-vous que Python est installé dans votre environnement Kali Linux sur WSL. Python est nécessaire pour exécuter ARISE et interagir avec les outils de cybersécurité.

Aucune librairie Python supplémentaire n'est nécessaire pour le fonctionnement de base d'ARISE, car il utilise principalement des outils de cybersécurité disponibles via l'environnement Kali Linux.