

Pentest Vulnerability Report : Alpha

Table des matières

<i>Cible</i>	3
<i>Attaquant</i>	3
<i>Titre de la vulnérabilité</i>	3
<i>Description de la vulnérabilité</i>	3
<i>Éléments affectés</i>	3
<i>Préalables</i>	3
<i>Mise en place</i>	4
<i>Proof of concept</i>	4
<i>Impact</i>	9
<i>Mitigation</i>	9

Cible

Le domaine local « rs.io »

Attaquant

Les Rogue Sentinels

Titre de la vulnérabilité

OSINT : reconnaissance passive

Description de la vulnérabilité

Nous allons utiliser des informations présentes sur le site pour trouver d'autres informations à l'aide de recherches sur internet.

Éléments affectés

Nous affectons le réseau local créé par le toolkit sur notre machine virtuelle Kali Linux 64 bits.

Préalables

- Un toolkit qui nous est donné.
- Réseau de machines. (rs.io)

Mise en place

Ce proof of concept est conçu sur une machine virtuelle Kali Linux 64 bits.

Notre cible est donnée il s'agit du domaine local « rs.io »

Nous installons le toolkit fourni sur un Kali Linux 64 bits avec cette ligne de commande :

```
➔ wget https://raw.githubusercontent.com/RogueSentinels/hacker-toolkit/main/attack.sh &&  
  chmod +x attack.sh
```

Nous préparons notre station de travail avec :

```
➔ sudo ./attack.sh workstation-setup
```

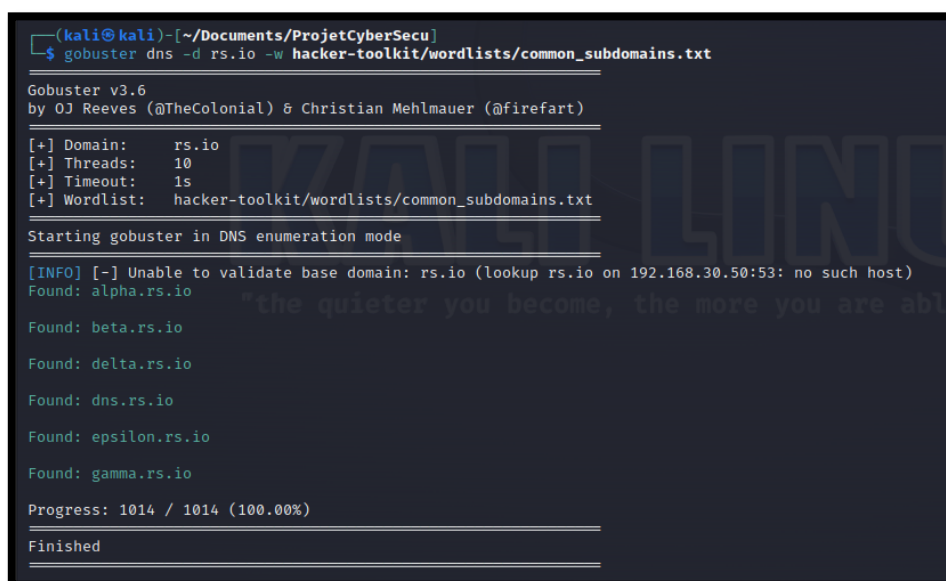
Et nous lançons l'attaque avec :

```
➔ sudo ./attack.sh up
```

Proof of concept

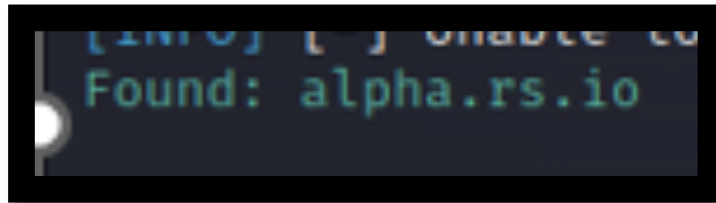
1) Chercher les sous-domaines avec gobuster.

```
➔ gobuster dns -d rs.io -w hacker-toolkit/wordlists/common_subdomains.txt
```



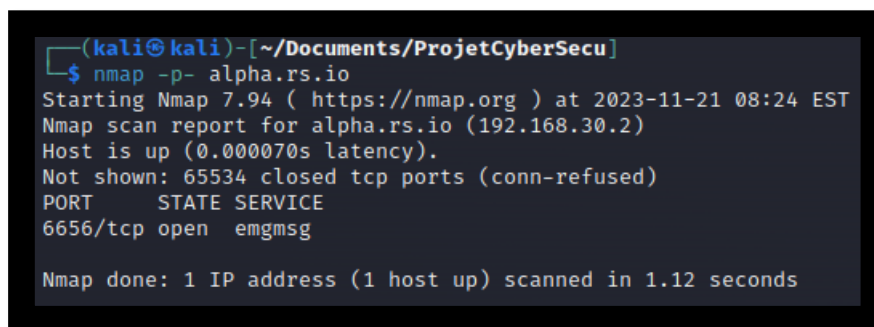
```
(kali@kali)~[~/Documents/ProjetCyberSecu]  
$ gobuster dns -d rs.io -w hacker-toolkit/wordlists/common_subdomains.txt  
  
Gobuster v3.6  
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)  
  
[+] Domain:      rs.io  
[+] Threads:     10  
[+] Timeout:     1s  
[+] Wordlist:     hacker-toolkit/wordlists/common_subdomains.txt  
  
Starting gobuster in DNS enumeration mode  
  
[INFO] [-] Unable to validate base domain: rs.io (lookup rs.io on 192.168.30.50:53: no such host)  
Found: alpha.rs.io  
Found: beta.rs.io  
Found: delta.rs.io  
Found: dns.rs.io  
Found: epsilon.rs.io  
Found: gamma.rs.io  
  
Progress: 1014 / 1014 (100.00%)  
Finished
```

2) Trouver le sous-domaine `alpha.rs.io`

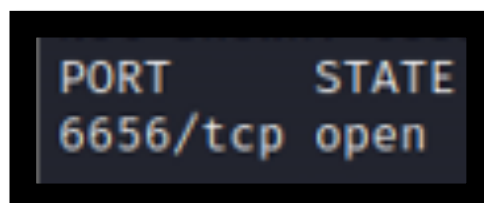


3) Scan de port avec nmap sur le sous-domaine.

➔ `nmap -p- alpha.rs.io`



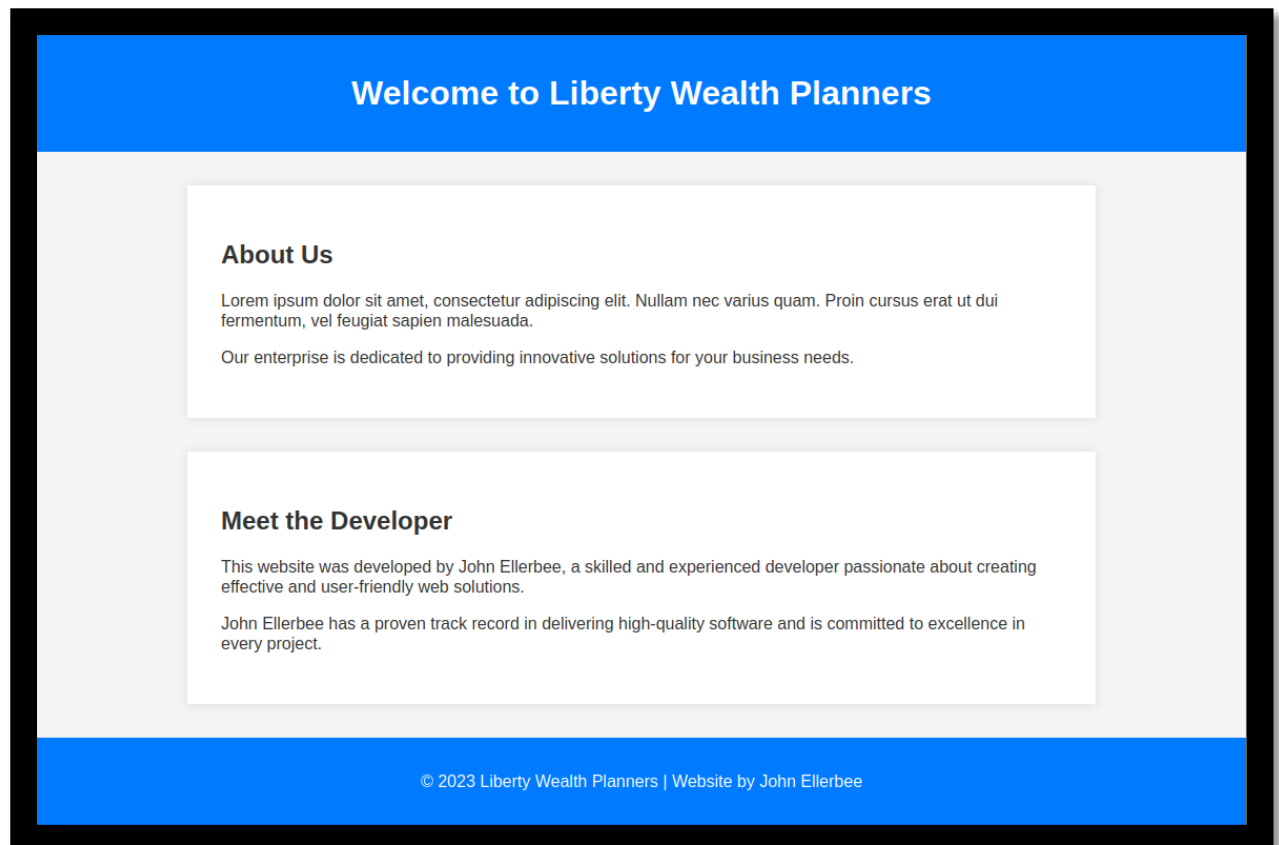
4) Trouver le port 6656 avec un serveur nginx qui tourne.



5) On ouvre le site dans le navigateur et on arrive sur une page présentant des données personnelles (nom, prénom, nom_société)

- Nom: John Ellerbee

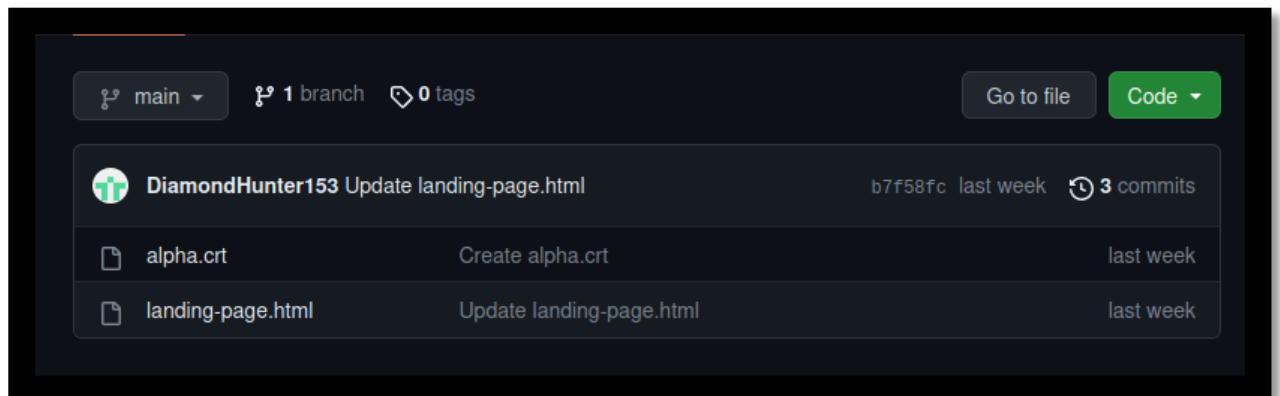
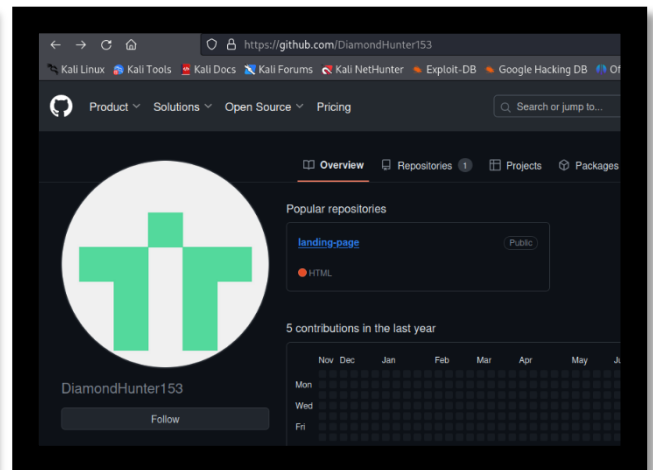
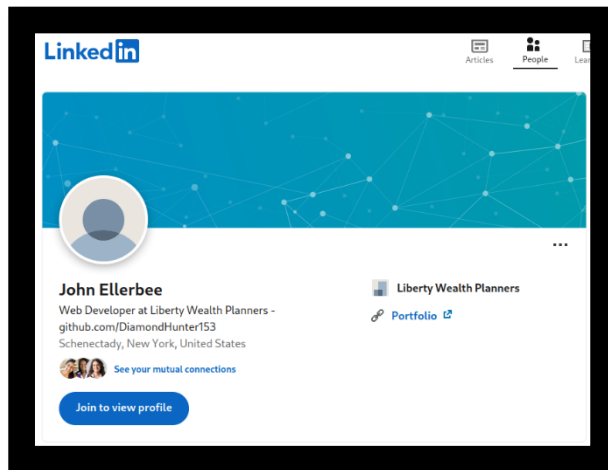
- Société: Liberty Wealth Planners



- 6) On effectue une recherche sur le nom de la personne, on trouve un compte LinkedIn d'une personne travaillant dans la société « Liberty Wealth Planners ».

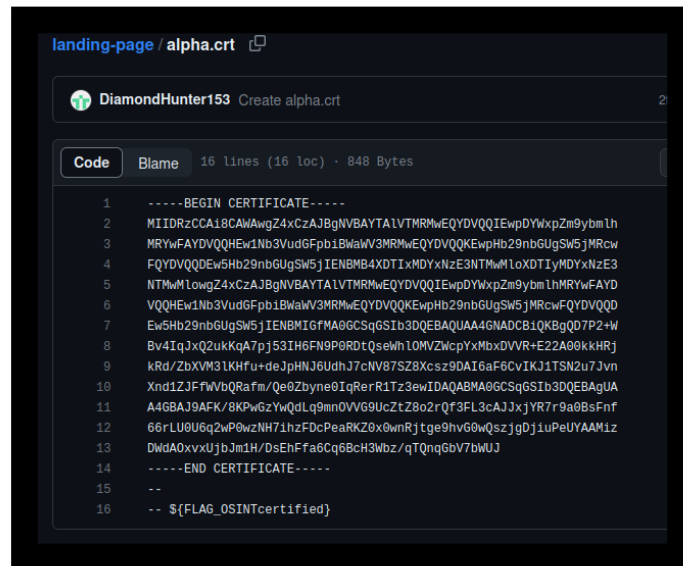


7) Ce compte LinkedIn contient un lien vers un compte github
(<https://github.com/DiamondHunter153>).



8) On y trouve un repository contenant un fichier `alpha.crt` qui contient le flag :

→ Flag = `\${FLAG_OSINTcertified}`



The screenshot shows a GitHub repository named 'landing-page' with a file named 'alpha.crt'. The file is owned by 'DiamondHunter153' and has 16 lines of code. The code is a certificate file containing a long base64-encoded string and a flag at the end.

```
1  -----BEGIN CERTIFICATE-----
2  MIIDRzCCA18CAWAgZ4xCzAJBgNVBAYTALVTMRMwEQYDVQKIExpDYWxpZm9ybmlh
3  MRYwFAYDVQQHEw1Nb3VudGFpb1BwaWV3MRMwEQYDVQKKEwpHb29nbGUGSw5jMRcw
4  FQYDVQQDEw5Hb29nbGUGSw5jIENBMBA4XDTIxMDYxNzE3NTMwMloXDTIyMDYxNzE3
5  NTMwMlowZ4xCzAJBgNVBAYTALVTMRMwEQYDVQKIExpDYWxpZm9ybmlhMRYwFAYD
6  VQKHEw1Nb3VudGFpb1BwaWV3MRMwEQYDVQKKEwpHb29nbGUGSw5jMRcwFQYDVQQD
7  Ew5Hb29nbGUGSw5jIENBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB1QKBgQD7P2+W
8  Bv4IqJxQ2ukKqA7pJ53IH6FN9P0RdtQsewhL0MVZwcpYxMbxDVVR+E22A00kkHRj
9  kRd/ZbXVM3LKHfu+deJpHNJ6UdhJ7cNV87SZ8Xcsz9DAI6aF6CvIKJ1TSN2u7Jvn
10 Xnd1ZJfFWVbQRafm/Qe0Zbyne0IqRerR1Tz3ewIDAQABMA0GCSqGSIb3DQEBAgUA
11 A4GBAJ9AFK/8KPwGzYwQdLq9mnOVV69UcZtZ8o2rQf3FL3cAJJxjYR7r9a0BsFnf
12 66rLU0U6q2wP0wzNH71hzFdcPeaRKZ0x0wnRjtge9hvG0wQszjgDjiuPeUYAAMiz
13 DwdA0xxvUjbjm1H/DsEHfFa6Cq6BcH3Wbz/qTQnqGbV7bWUJ
14 -----END CERTIFICATE-----
15 --
16 -- ${FLAG_OSINTcertified}
```

Impact

En laissant un lien vers le repository de son site, cet employé laisse la possibilité à n'importe qui d'avoir accès au site et à son certificat, ce qui pourrait faciliter de nouvelles attaques.

Mitigation

Il existe plusieurs solutions comme mettre le repository en privé, ou également ne pas commit ce genre d'informations sensibles.