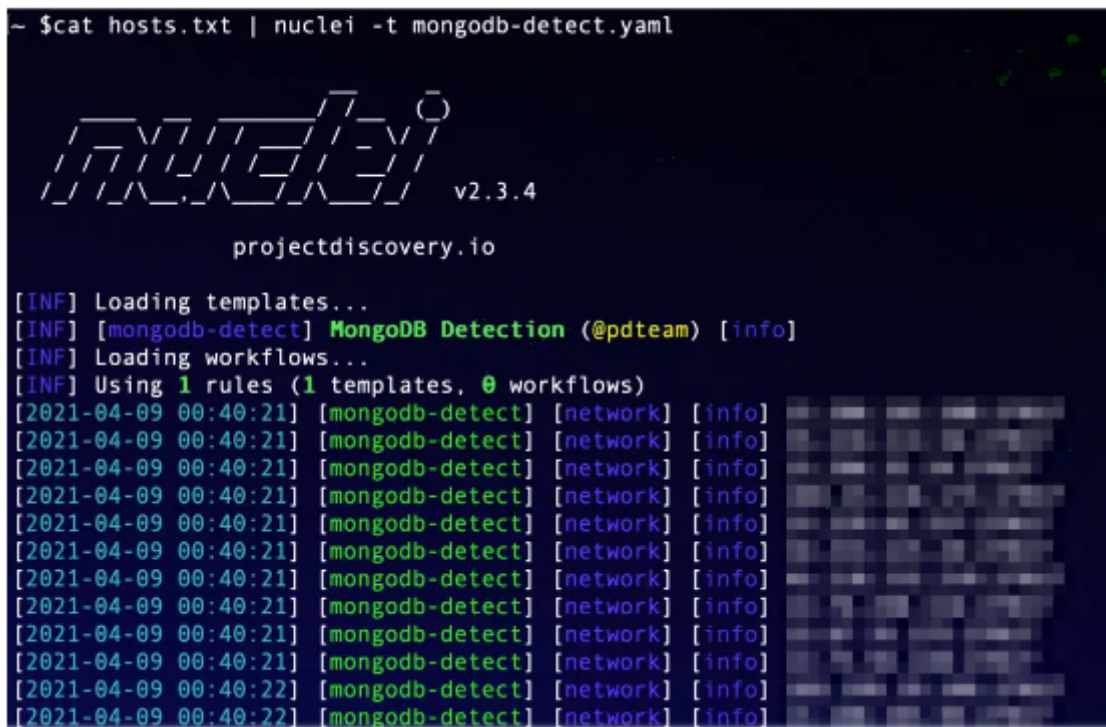


[CTI] Nuclei

Introduction

Le logiciel Nuclei permet de tester l'exploitabilité d'une vulnérabilité sur des systèmes grâce à des templates au format YML.

```
~ $cat hosts.txt | nuclei -t mongodb-detect.yaml
```



```
nuclei v2.3.4
projectdiscovery.io

[INF] Loading templates...
[INF] [mongodb-detect] MongoDB Detection (@pdteam) [info]
[INF] Loading workflows...
[INF] Using 1 rules (1 templates, 0 workflows)
[2021-04-09 00:40:21] [mongodb-detect] [network] [info] 10.10.10.10:27017
[2021-04-09 00:40:21] [mongodb-detect] [network] [info] 10.10.10.11:27017
[2021-04-09 00:40:21] [mongodb-detect] [network] [info] 10.10.10.12:27017
[2021-04-09 00:40:21] [mongodb-detect] [network] [info] 10.10.10.13:27017
[2021-04-09 00:40:21] [mongodb-detect] [network] [info] 10.10.10.14:27017
[2021-04-09 00:40:21] [mongodb-detect] [network] [info] 10.10.10.15:27017
[2021-04-09 00:40:21] [mongodb-detect] [network] [info] 10.10.10.16:27017
[2021-04-09 00:40:21] [mongodb-detect] [network] [info] 10.10.10.17:27017
[2021-04-09 00:40:21] [mongodb-detect] [network] [info] 10.10.10.18:27017
[2021-04-09 00:40:21] [mongodb-detect] [network] [info] 10.10.10.19:27017
[2021-04-09 00:40:22] [mongodb-detect] [network] [info] 10.10.10.20:27017
[2021-04-09 00:40:22] [mongodb-detect] [network] [info] 10.10.10.21:27017
```

Installation & MAJ

Projet

- <https://github.com/projectdiscovery/nuclei>

Installation

Pour installer Nuclei (go doit être installé au préalable) :

```
go install -v github.com/projectdiscovery/nuclei/v3/cmd/nuclei@latest
```

MAJ

Pour mettre à jour **Nuclei** :

```
nuclei -update
```

Pour mettre à jour les **templates** :

```
nuclei update
```

Manuel

Exemple template

Voici un exemple de template pour une CVE SSH (**cve-2024-6387.yaml**) :

```
id: CVE-2024-6387
```

```
info:
```

```
  name: RegreSSHion detect (based on software version)
```

```
  author: UnaPibaGeek
```

```
  severity: High
```

```
  description: Regression (CVE-2024-6387) software version checker.
```

```
  classification:
```

```
    cve-id: CVE-2024-6387
```

```
  metadata:
```

```
    max-request: 2
```

```
    vendor: OpenSSH
```

```
    product: OpenSSH
```

```
    tags: cve,cve2024,regression,openssh,ssh
```

```
tcp:
```

```
  - host:
```

```
    - '{{Hostname}}'
```

```
    - '{{Host}}:22'
```

```
inputs:
```

```
- data: "SSH-2.0-OpenSSH_9.0\r\n"

matchers:
  - type: regex
    part: body
    regex:
      - 'OpenSSH_(8\.[5-9]p[1-2]?|9\.[0-7]p[1-2]?|[0-3]\.[0-9]p[1-2]?|4\.[0-3]p[1-2]?)'
```

- 'OpenSSH_(8\.[5-9]p[1-2]?|9\.[0-7]p[1-2]?|[0-3]\.[0-9]p[1-2]?|4\.[0-3]p[1-2]?|?)'

Ici nous ciblerons des adresses IPs que nous indiquerons dans le fichier **ips.txt** :

192.168.5.40

En cas d'attaque web, il peut s'agir d'URL et non d'adresse IP.

```
nuclei -t cve-20224-6387.yaml -l ips.txt
```

Updated 2 July 2024 09:45:33 by Elieroc