Nuclei Template Extensive Usage

Dhiyaneshwaran | April 30, 23

Different Types of
Protocol in
Nuclei Template

HELLO!

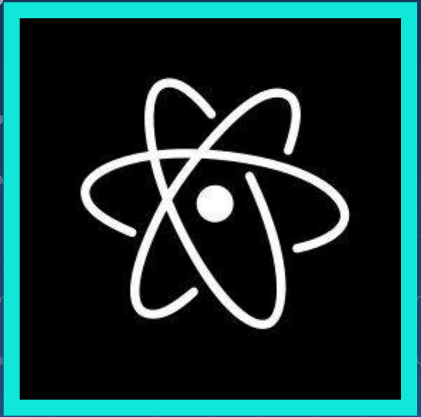
I AM DHIYANESHWARAN

AppSec Researcher at ProjectDiscovery

You can find me at @DhiyaneshDk

AGENDA

- Different Protocol Support
- Writing a Network, DNS , File Based Nuclei Template
- Live Demo



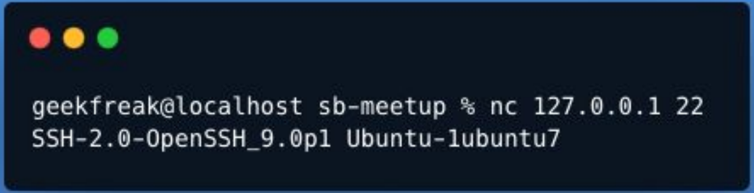
Different Protocol Support

- HTTP
- Headless
- Network
- DNS
- File
- WebSocket
- SSL

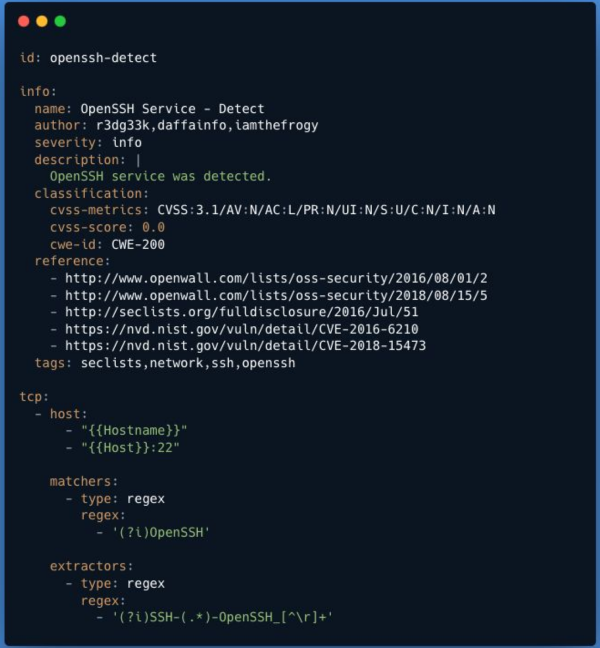
Network

- Nuclei can act as an automatable Netcat, allowing users to send bytes across the wire and receive them, while providing matching and extracting capabilities on the response.
- Network Requests start with a ***network*** block which specifies the start of the requests for the template.

Basic Network Template with word Matcher



```
geekfreak@localhost sb-meetup % nc 127.0.0.1 22
SSH-2.0-OpenSSH_9.0p1 Ubuntu-1ubuntu7
```

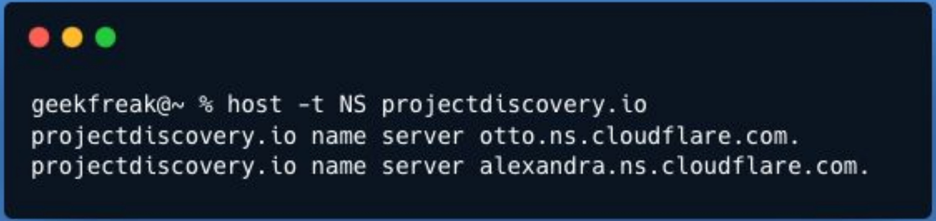


```yaml
id: openssh-detect

info:
  name: OpenSSH Service - Detect
  author: r3dg33k,daffainfo,iamthefrogy
  severity: info
  description: |
    OpenSSH service was detected.
  classification:
    cvss-metrics: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N
    cvss-score: 0.0
    cwe-id: CWE-200
  reference:
    - http://www.openwall.com/lists/oss-security/2016/08/01/2
    - http://www.openwall.com/lists/oss-security/2018/08/15/5
    - http://seclists.org/fulldisclosure/2016/Jul/51
    - https://nvd.nist.gov/vuln/detail/CVE-2016-6210
    - https://nvd.nist.gov/vuln/detail/CVE-2018-15473
  tags: seclists,network,ssh,openssh

tcp:
  - host:
      - "{{Hostname}}"
      - "{{Host}}:22"

    matchers:
      - type: regex
        regex:
          - '(?i)OpenSSH'

    extractors:
      - type: regex
        regex:
          - '(?i)SSH-(.*)-OpenSSH_[^\r]+'
```

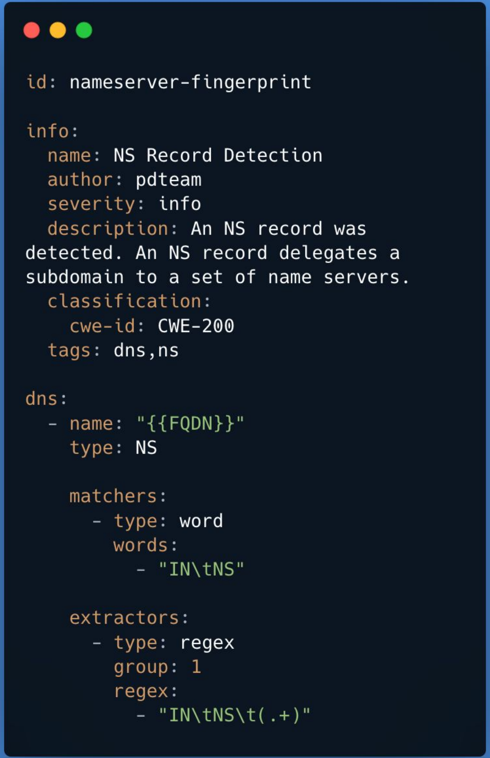
DNS

- DNS protocol can be modelled in nuclei with ease. Fully Customizable DNS requests can be sent by nuclei to nameservers and matching/extracting can be performed on their response.
- DNS Requests start with a ***dns*** block which specifies the start of the requests for the template.

Writing DNS Template with extractors matcher



```
geekfreak@~ % host -t NS projectdiscovery.io
projectdiscovery.io name server otto.ns.cloudflare.com.
projectdiscovery.io name server alexandra.ns.cloudflare.com.
```

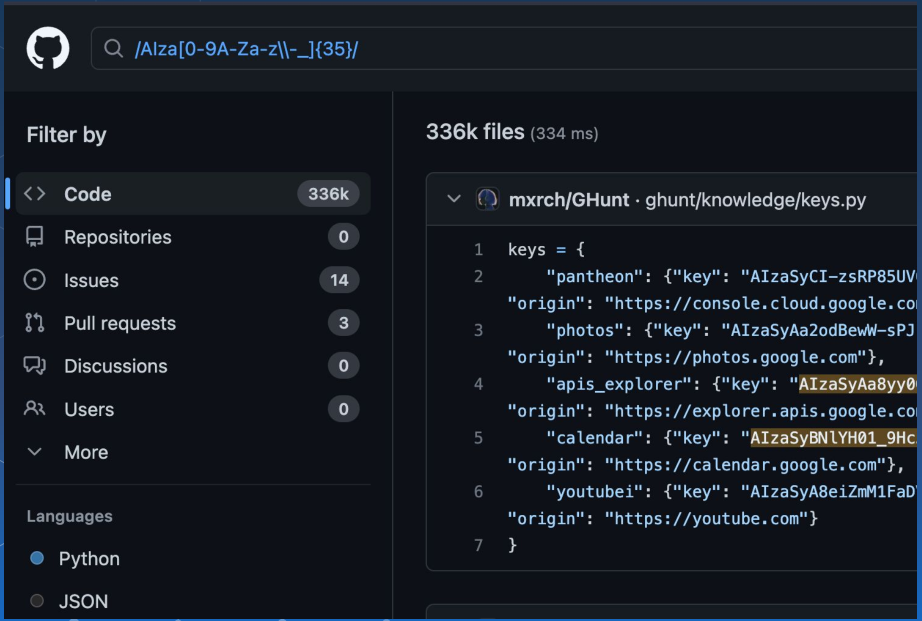


```yaml
id: nameserver-fingerprint

info:
  name: NS Record Detection
  author: pdteam
  severity: info
  description: An NS record was
detected. An NS record delegates a
subdomain to a set of name servers.
  classification:
    cwe-id: CWE-200
  tags: dns,ns

dns:
  - name: "{{FQDN}}"
    type: NS

    matchers:
      - type: word
        words:
          - "IN\tNS"

    extractors:
      - type: regex
        group: 1
        regex:
          - "IN\tNS\t(.+)"
```

File

- Nuclei allows modelling templates that can match/extract on filesystem too.
- File Based Template start with a ***file*** block which specifies the start of the template.

File Template with word Matcher

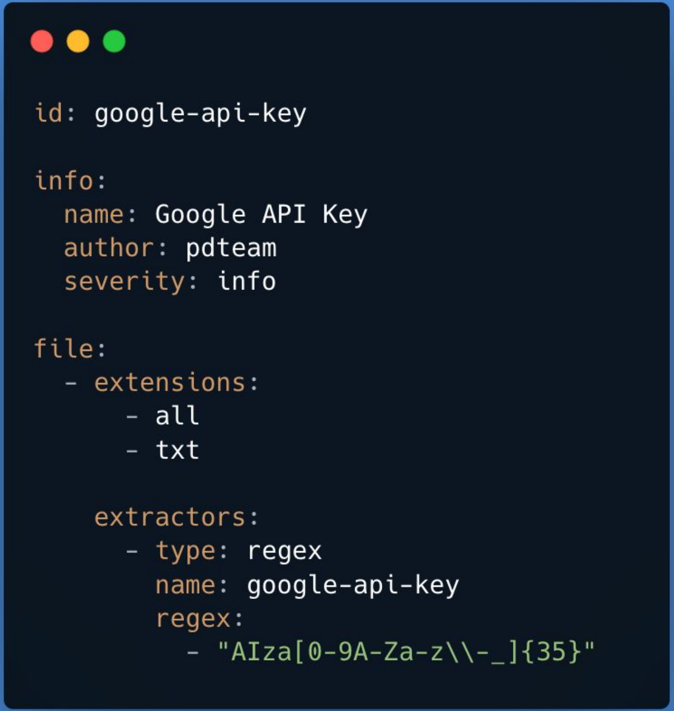


/AIza[0-9A-Za-z\\-_]{35}/

336k files (334 ms)

mxrch/GHunt · ghunt/knowledge/keys.py

```
keys = {
    "pantheon": {"key": "AIzaSyCI-zsRP85UV
"origin": "https://console.cloud.google.co
    "photos": {"key": "AIzaSyAa2odBewW-sPJ
"origin": "https://photos.google.com"},
    "apis_explorer": {"key": "AIzaSyAa8yy0
"origin": "https://explorer.apis.google.co
    "calendar": {"key": "AIzaSyBNlYH01_9Hc
"origin": "https://calendar.google.com"},
    "youtubei": {"key": "AIzaSyA8eiZmM1FaD
"origin": "https://youtube.com"}
}
```



```
id: google-api-key

info:
  name: Google API Key
  author: pdteam
  severity: info

file:
  - extensions:
      - all
      - txt

    extractors:
      - type: regex
        name: google-api-key
        regex:
          - "AIza[0-9A-Za-z\\-_]{35}"
```

Reference

- Writing Network Templates with Nuclei
- Nuclei Unleashed - Quickly write complex exploits
- Secrets Scanning with Nuclei
- Nuclei - Fuzz all the things
- Hack with Automation !!! – Geek Freak

First Template

THANKS!

ANY QUESTIONS?

Feel Free to

Join our Discord Server