

Forum:[Hack Forums](#)

Thread: [Beginner's Tutorial: Using Nuclei for Vulnerability Scanning](#)

captn_nemo - January 28, 2025, 12:27 pm

Beginner's Tutorial: Using Nuclei for Vulnerability Scanning

Nuclei is a fast, template-based vulnerability scanner designed for security professionals and bug bounty hunters.

It uses YAML templates to detect vulnerabilities across web applications, networks, and services with minimal false positives.

Below is a step-by-step guide to get started with Nuclei, including installation, basic usage, and exploitation techniques.

1. Installation

Option 1: Pre-built Binaries

Download the latest binary for your OS from the Nuclei GitHub releases and add it to your PATH:

Code wget

```
https://github.com/projectdiscovery/nuclei/releases/download/v3.3.8/nuclei_3.3.8_linux_amd64.zip
```

```
unzip nuclei_3.3.8_linux_amd64.zip
```

```
mv nuclei /usr/local/bin/
```

Verify installation:

Code nuclei -version # Should display the installed version

Option 2: Docker

Pull the official image:

Code docker pull projectdiscovery/nuclei:latest

Run a scan via Docker:

Code docker run -it projectdiscovery/nuclei -u https://example.com

Option 3: Go Install

If Go is installed, use:

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

2. Updating Templates

Nuclei relies on templates to detect vulnerabilities. Update them regularly:

Code nuclei -ut

3. Basic Scanning

Scan a Single Target

Code `nuclei -u https://example.com # Scans with all default templates`

Scan Multiple Targets

Create a `targets.txt` file with one URL per line and run:

Code `nuclei -l targets.txt -o results.txt # Outputs findings to results.txt`

Use Specific Templates

Code `nuclei -u https://example.com -t cves/ -t exposures/ # Scans using templates in the "cves" and "exposures" folders`

4. Filtering Templates

By Tags (e.g., `cve`, `jira`):

Code `nuclei -u https://example.com -tags cve -severity critical,high`

By Author (e.g., `geeknik`):

Code `nuclei -l targets.txt -author geeknik`

Exclude Templates:

Code `nuclei -u https://example.com -etags info -exclude-templates technologies/`

5. Advanced Scanning

Rate Limiting

Avoid overwhelming targets:

Code `nuclei -l targets.txt -rl 20 -c 5 # 20 requests/sec, 5 concurrent templates`

Custom Headers

Add headers (e.g., `User-Agent`, `Auth tokens`):

Code `nuclei -u https://example.com -H "User-Agent: Mozilla/5.0" -H "Authorization: Bearer token"`

Debugging

View requests/responses for troubleshooting:

Code `nuclei -u https://example.com -debug`

6. Integration with Other Tools

Combine Nuclei with tools like `subfinder` for automated workflows:

Code `subfinder -d example.com -silent | nuclei -t cves/ -o results.txt`

7. Writing Custom Templates

Create a YAML file (e.g., `custom-template.yaml`) to detect new vulnerabilities:

Code id: exposed-htpasswd

info:

name: Exposed .htpasswd File

author: yourname

severity: high

tags: exposure,config

http:

- method: GET

path:

- "{{BaseURL}}/.htpasswd"

matchers:

- type: word

words:

- ":{SHA}"

- ":{SHA}"

condition: or

- type: status

status:

- 200

Validate and run the template:

Code `nuclei -validate -t custom-template.yaml # Checks for errors`

`nuclei -u https://example.com -t custom-template.yaml`

8. Best Practices & Troubleshooting

Avoid Over-Scanning: Use rate limits (-rl) and template filters to minimize network impact.

Resume Scans: Use -resume if a scan is interrupted.

Common Errors: Template Errors: Run `nuclei -validate` to check template syntax

Installation Issues: Ensure Go is properly installed and PATH is configured

Resources

Official Templates: [nuclei-templates GitHub](#)

Documentation: [Nuclei Documentation](#)

By following this guide, you can efficiently use Nuclei to identify and exploit vulnerabilities.

This was just an introduction, Nuclei has so much more to offer.

Especially the possibility to easily write templates makes this tool very valuable.

If a mistake has crept in somewhere, please let me know.

If you have any suggestions, please let me know.

RootRXXT - January 28, 2025, 12:28 pm

very in depth, HQ KB article, spinning up another Kali instance and testing shortly. Thanks for the post!

captn_nemo - January 28, 2025, 11:36 pm

(Jan 28, 2025 01:28 PM)RootRXXT Wrote: [\[CITE\]](#) very in depth, HQ KB article, spinning up another Kali instance and testing shortly. Thanks for the post!

Thanks, you can start nuclei with Docker as described above or for windows just download the

binary from their Github.

Stanley - *January 31, 2025, 5:43 am*

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley