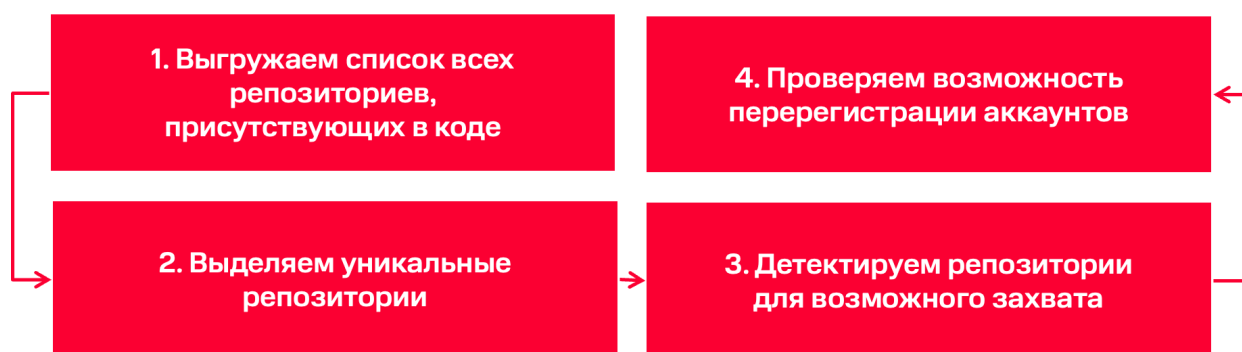


RED

Методика проверки кода на уязвимости РероJacking

Описание инструментов и методов исследования кода



Данная инструкция позволит найти в коде все ссылки на репозитории, контроль над которыми может быть получен злоумышленниками. Методика поиска уязвимых зависимостей создана на основе исследования команды MTC RED ART, в ходе которого были проверены и успешно применены все нижеперечисленные компоненты.

1. Извлечение ссылок, ведущих на GitHub

Для получения списка ссылок, ведущих на <https://github.com> из вашего репозитория, потребуется:

- 1.1 Скачать скрипт `pars_url.py` из нашего набора https://github.com/RED-Advanced-Research-Team/Supply_chain_research.
- 1.2 Создать текстовый файл `MY_rep.txt` в том же каталоге, где расположен `pars_url.py`.
- 1.3 Записать в `MY_rep.txt` полный путь до вашего репозитория (например, https://github.com/RED-Advanced-Research-Team/Supply_chain_research).
- 1.4 Результатом выполнения скрипта будет создание файла `return_github.txt`, который будет содержать все ссылки из вашего кода ведущие на <https://github.com/>.

2. Получение битых ссылок (corrupted links)

Для поиска битых ссылок вам потребуется применить утилиту, входящую в стандартный набор Kali Linux — `nuclei` (инструмент для отправки запросов на основе шаблонов с ожиданием заданного ответа).

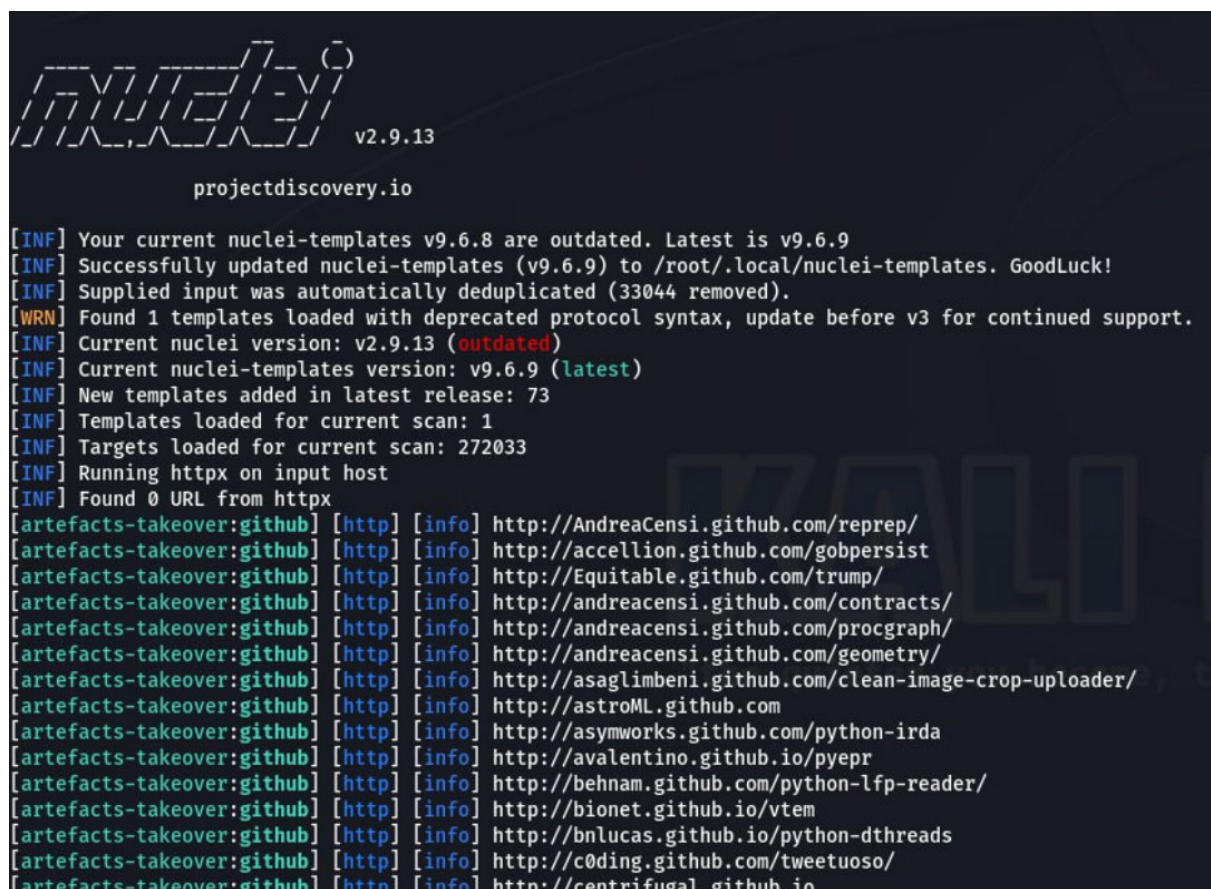
2.1 Для получения необходимого результата вам потребуется шаблон для `nuclei`, который даст команду реагировать на следующие фразы: "Sign in to GitHub" и "a GitHub Pages site here For root URLs". Готовый шаблон с этими функциями лежит в нашем репозитории под названием `artefacts_github.yaml`.

2.2 Следующим шагом потребуется в произвольный каталог (например: `/opt`) перенести два файла: `return_github.txt` и `artefacts_github.yaml`.

2.3 Заключительный шаг данного этапа — выполнение команды: `nuclei -t artefacts_github.yaml -l return_github.txt -o result_github.txt -stats -elog error_github.txt`, где:

<code>-t</code>	путь до шаблона
<code>-l</code>	путь до списка со всеми ссылками GitHub, полученными из вашего кода
<code>-o</code>	файл с результатом выполнения
<code>-stats</code>	онлайн-вывод процесса обработки
<code>-elog</code>	файл с потенциально возможными ошибками

В результате выполнения команды в файле `result_github.txt` вы получите список битых ссылок из вашего кода.



```
nuclei v2.9.13
projectdiscovery.io

[INF] Your current nuclei-templates v9.6.8 are outdated. Latest is v9.6.9
[INF] Successfully updated nuclei-templates (v9.6.9) to /root/.local/nuclei-templates. GoodLuck!
[INF] Supplied input was automatically deduplicated (33044 removed).
[WRN] Found 1 templates loaded with deprecated protocol syntax, update before v3 for continued support.
[INF] Current nuclei version: v2.9.13 (outdated)
[INF] Current nuclei-templates version: v9.6.9 (latest)
[INF] New templates added in latest release: 73
[INF] Templates loaded for current scan: 1
[INF] Targets loaded for current scan: 272033
[INF] Running httpx on input host
[INF] Found 0 URL from httpx

[artefacts-takeover:github] [http] [info] http://AndreaCensi.github.com/reprep/
[artefacts-takeover:github] [http] [info] http://accellion.github.com/gobpersist
[artefacts-takeover:github] [http] [info] http://Equitable.github.com/trump/
[artefacts-takeover:github] [http] [info] http://andreaacensi.github.com/contracts/
[artefacts-takeover:github] [http] [info] http://andreaacensi.github.com/procgraph/
[artefacts-takeover:github] [http] [info] http://andreaacensi.github.com/geometry/
[artefacts-takeover:github] [http] [info] http://asaglimbeni.github.com/clean-image-crop-uploader/
[artefacts-takeover:github] [http] [info] http://astroML.github.com
[artefacts-takeover:github] [http] [info] http://asymworks.github.com/python-irda
[artefacts-takeover:github] [http] [info] http://avalentino.github.io/pyepr
[artefacts-takeover:github] [http] [info] http://behnamm.github.com/python-lfp-reader/
[artefacts-takeover:github] [http] [info] http://bionet.github.io/vtem
[artefacts-takeover:github] [http] [info] http://bnlucas.github.io/python-dthreads
[artefacts-takeover:github] [http] [info] http://c0ding.github.com/tweetuoso/
[artefacts-takeover:github] [http] [info] http://centrifugal.github.io
```

В частности, при поиске по всем публичным репозиториям Google Cloud Console и менеджерам пакетов PyPi и NPM мы обнаружили 7820 битых ссылок (corrupted links).

3. Проверка аккаунтов пользователей, доступных для перерегистрации с целью подмены репозитория по неработающим ссылкам (уязвимость для атаки типа RepoJacking)

Все битые ссылки стоит удалить из кода. Однако дополнительно мы добавим явный метод выяснить, какие из них могут быть получены злоумышленниками в любой момент через атаку типа RepoJacking.

3.1 Для подтверждения перерегистрации владельца битой ссылки вам потребуется скрипт `clicker_github.py` из нашего набора https://github.com/RED-Advanced-Research-Team/Supply_chain_research.

3.2 Также потребуется отфильтровать полученный ранее файл `result_github.txt` таким образом, чтобы в нем остались только имена пользователей (пример: из https://github.com/RED-Advanced-Research-Team/Supply_chain_research необходимо получить только `RED-Advanced-Research-Team`). Назовём новый файл `result_github_user.txt`.

3.3 Далее потребуется произвольный почтовый ящик, к которому вы имеете доступ и пароль.

3.4 Получив все необходимые компоненты, открываем файл `clicker_github.py` и заменяем два параметра – `test@mail.com` на ваш почтовый ящик и `test_password` на сгенерированный вами пароль и сохраняем.

При запуске скрипта `clicker_github.py` вы сможете в режиме реального времени наблюдать возможность перерегистрации каждого из аккаунтов в списке `result_github_user.txt`.

