Awillix

Обзор Open Source продуктов

Для построения инфраструктуры, защиты и аудита

РИФ / 2023

РОССИЙСКИЙ
ИНТЕРНЕТ ФОРУМ

AWILLIX

Александр Герасимов

- Этичный хакер
- Эксперт в области тестирования на проникновение
- Сооснователь Awillix
- Автор телеграм-канала Just Security.

о компании

Awillix

Одна из лучших offensive-компаний на рынке кибербезопасности. Мы защищаем клиентов от киберугроз, выявляя сложные уязвимости и связанные с ними риски. Снимаем страхи бизнеса в отношении кибербезопасности и помогаем эффективнее расходовать бюджет, рекомендуя самые оптимальные решения.

Awillix

Какие у вас первые мысли при слове Open Source?

Первые мысли об Open Source?

Первые мысли об Open Source?

- Нерабочие решения

Первые мысли об Open Source?

- Нерабочие решения
- Небезопасно

Первые мысли об Open Source?

- Нерабочие решения
- Небезопасно
- Неудобно

Первые мысли об Open Source?

- Нерабочие решения
- Небезопасно
- Неудобно
- Нет поддержки

Как по факту?

- Множество решений практически под любую задачу;
- Постоянно аудируются независимыми исследователями;
- Можно изменять под свои нужды;
- Хорошая поддержка от разработчиков и коммьюнити;
- Не попадут под санкции.

Примеры Open Source

- **Hashicorp Vault** (Построение инфраструктуры)

  ☆ 27.1к звёзд 🕓 16.8к коммитов

- **Wazuh** (Защита инфраструктуры и устройств)

  ☆ 5.6к звёзд 🕓 28к коммитов

- **Nuclei** (Анализ защищенности и аудит)

  ☆ 11.7к звёзд 🕓 3.9к коммитов

Давайте построим ИТ на Open Source

Приведем примеры и разберем характеристики решений для:

- Построения базовых процессов ИТ;
- Защиты инфраструктуры и устройств;
- Анализа защищенности.

Инфраструктура

- **PKI**
  - OpenSSL
  - EJBCA
  - Vault
  - CFSSL
- **Виртуализация**
  - Proxmox
  - OpenStack
- **VPN**
  - OpenVPN
  - WireGuard
- **Tickets / Support**
  - OSTicket
  - FreeScout
- **IAM/IDM**
  - Keycloak
  - OpenIAM

Пример внедрения PKI

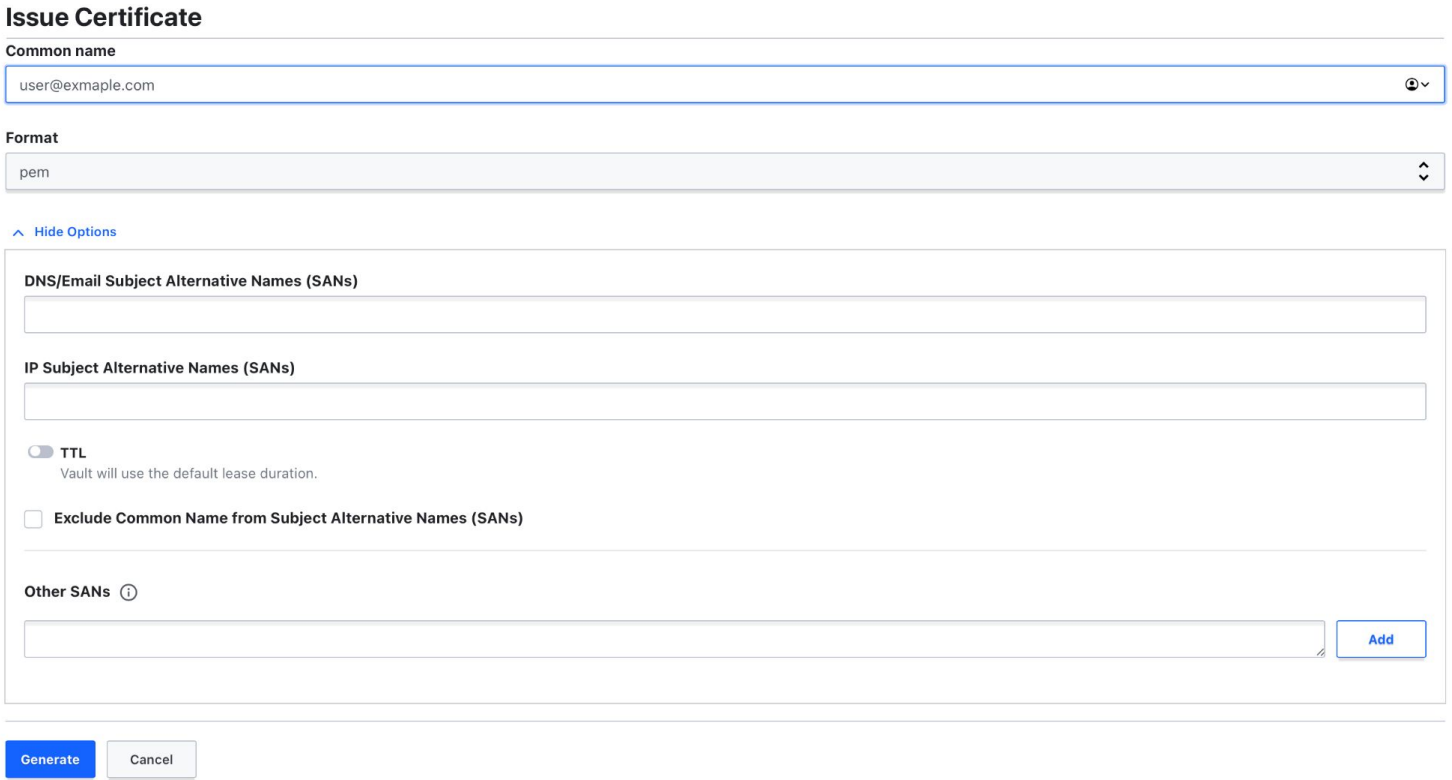
Что ждем от PKI:

- Подпись и шифрование сообщений во внутренней почте;
- Аутентификация по сертификатам;
- SSL сертификаты для сервисов;
- CRL списки;
- Шаблоны сертификатов;
- Удобный интерфейс или API.

Пример внедрения PKI

Решение	CRL	Веб интерфейс	Шаблоны	Быстрый деплой	Удобство	Итог
Vault	●	●	●	●	●	1
EJBCA	●	●	●	○	●	2
CFSSL	○	○	●	●	○	3
OpenSSL	●		●	●		4

Выпуск сертификата в Vault



Аудит инфраструктуры и приложений

- **Анализ защищенности**
  - Nuclei
  - Nmap + Vulners
  - OpenVAS
- **Мониторинг инфраструктуры**
  - Naabu
  - Nmap
- **Анализ кода**
  - Semgrep
  - SonarQube
- **Анализ зависимостей**
  - dependency check
  - Trivy

Пример внедрения анализа защищенности

Что хотим от анализа защищенности инфраструктуры

- Поиск известных уязвимостей;
- Поиск недостатков конфигурации;
- Пароли по умолчанию;
- Использование своих правил.

Пример внедрения анализа защищенности

Решение	Веб-интерфейс	Кастомизация	Быстрота деплоя	Удобство	Итог
Nuclei		●	●	●	1
OpenVas	●			●	2
Nmap + Vulners		●	●	◐	3
Tsunami		◐	●	●	3

Сектор приз!

Пример построения автоматизированного поиска уязвимостей и мониторинга

Что будем делать?

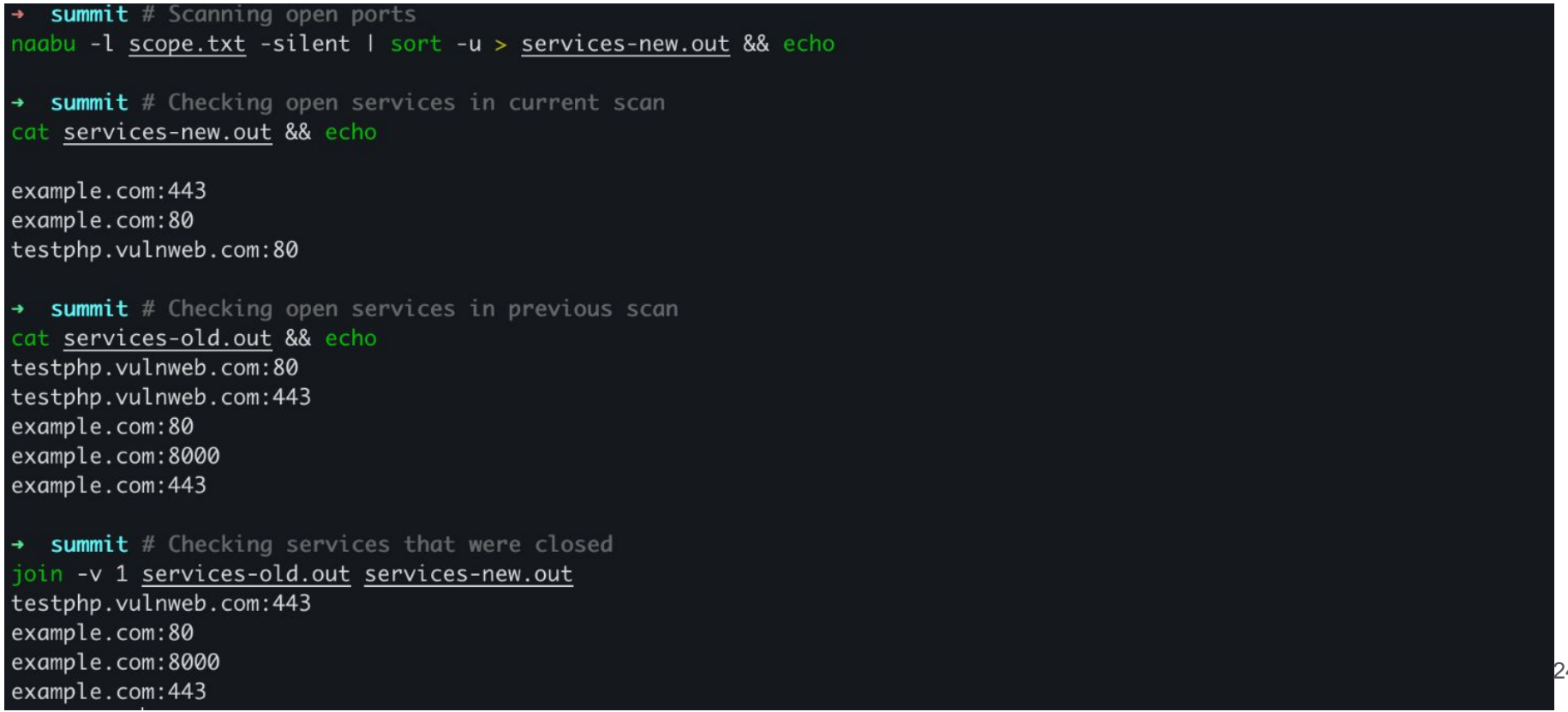
- Построим непрерывный мониторинг внешний инфраструктуры;
- Сделаем простой анализ защищенности;
- Выявим типичные уязвимости.

Что будем использовать: Naabu / httpx / Nuclei / Owasp ZAP

Мониторинг

```
# Monitoring (should run periodically)

naabu -l scope.txt -silent | sort -u > services-new.out

# Opened services
join -v 1 services-new.out services-old.out | alerting

# Closed services
join -v 1 services-old.out services-new.out | alerting

cp services-new.out services-old.out
```

Пример работы мониторинга



Анализ защищенности инфраструктуры

```
# Network Assessment

nuclei -l services-new.out -silent -nc -o nuclei.out | sort -u | alerting
```

Пример работы сканера

```
➜  summit nuclei -l services-new.out -silent -nc -o  nuclei.out | sort -u
[azure-domain-tenant] [http] [info] https://login.microsoftonline.com:443/example.com/v2.0/.well-known/openid-configuration [c7c08208-4f4d-45f1-83cd-5e2f491ab786]
[clientaccesspolicy] [http] [info] http://testphp.vulnweb.com:80/clientaccesspolicy.xml
[deprecated-tls] [ssl] [info] example.com [tls10]
[deprecated-tls] [ssl] [info] example.com [tls11]
[deprecated-tls] [ssl] [info] example.com [tls12]
[dnssec-detection] [dns] [info] example.com
[http-missing-security-headers:access-control-allow-credentials] [http] [info] http://example.com:80
[http-missing-security-headers:access-control-allow-credentials] [http] [info] http://testphp.vulnweb.com:80
[http-missing-security-headers:access-control-allow-credentials] [http] [info] https://example.com:443
[http-missing-security-headers:access-control-allow-headers] [http] [info] http://example.com:80
[http-missing-security-headers:access-control-allow-headers] [http] [info] http://testphp.vulnweb.com:80
[http-missing-security-headers:access-control-allow-headers] [http] [info] https://example.com:443
[http-missing-security-headers:access-control-allow-methods] [http] [info] http://example.com:80
[http-missing-security-headers:access-control-allow-methods] [http] [info] http://testphp.vulnweb.com:80
[http-missing-security-headers:access-control-allow-methods] [http] [info] https://example.com:443
[http-missing-security-headers:access-control-allow-origin] [http] [info] http://example.com:80
[http-missing-security-headers:access-control-allow-origin] [http] [info] http://testphp.vulnweb.com:80
[http-missing-security-headers:access-control-allow-origin] [http] [info] https://example.com:443
[http-missing-security-headers:access-control-expose-headers] [http] [info] http://example.com:80
[http-missing-security-headers:access-control-expose-headers] [http] [info] http://testphp.vulnweb.com:80
[http-missing-security-headers:access-control-expose-headers] [http] [info] https://example.com:443
```

Анализ защищенности веб-приложений

```
# Web Assessment

httpx -l services-new.out -silent -nc -o web.out
for url in $(cat web.out); zap-baseline.py -t $url | alerting
```

Пример автоматизированного поиска уязвимостей и мониторинга

```
→  summit # Web Assessment

/usr/local/bin/httpx -l services-new.out -silent -nc -o web.out
for url in $(cat web.out); docker run --rm owasp/zap2docker-weekly zap-baseline.py -t $url -l WARN
http://testphp.vulnweb.com
Total of 63 URLs
WARN-NEW: In Page Banner Information Leak [10009] x 3
        http://testphp.vulnweb.com/sitemap.xml (404 Not Found)
        http://testphp.vulnweb.com/robots.txt (404 Not Found)
        http://testphp.vulnweb.com/high (404 Not Found)
WARN-NEW: Missing Anti-clickjacking Header [10020] x 12
        http://testphp.vulnweb.com/ (200 OK)
        http://testphp.vulnweb.com/index.php (200 OK)
        http://testphp.vulnweb.com/guestbook.php (200 OK)
        http://testphp.vulnweb.com/cart.php (200 OK)
        http://testphp.vulnweb.com (200 OK)
WARN-NEW: X-Content-Type-Options Header Missing [10021] x 11
        http://testphp.vulnweb.com/ (200 OK)
        http://testphp.vulnweb.com/cart.php (200 OK)
        http://testphp.vulnweb.com/index.php (200 OK)
        http://testphp.vulnweb.com/artists.php (200 OK)
        http://testphp.vulnweb.com/guestbook.php (200 OK)
WARN-NEW: Server Leaks Version Information via "Server" HTTP Response Header Field [10036] x 11
        http://testphp.vulnweb.com/ (200 OK)
        http://testphp.vulnweb.com/robots.txt (404 Not Found)
        http://testphp.vulnweb.com/sitemap.xml (404 Not Found)
        http://testphp.vulnweb.com/cart.php (200 OK)
        http://testphp.vulnweb.com/index.php (200 OK)
WARN-NEW: Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) [10037] x 12
        http://testphp.vulnweb.com/ (200 OK)
        http://testphp.vulnweb.com/index.php (200 OK)
        http://testphp.vulnweb.com/cart.php (200 OK)
        http://testphp.vulnweb.com/userinfo.php (302 Found)
        http://testphp.vulnweb.com/guestbook.php (200 OK)
```

Защита инфраструктуры и мониторинг событий

Мониторинг сети и реагирование:

- Suricata
- Zeek
- AlienVault OSSIM
- ELK Siem

Защита инфраструктуры и мониторинг событий

Мониторинг конечных точек и расследование:

- Wazuuh
- OSSEC
- TheHive

Защита инфраструктуры и мониторинг событий

Сетевая защита:

- pfSense
- OPNsens

Защита инфраструктуры и мониторинг событий

Балансировка и защита на L7

- Nginx + ModSecurity
- NAXSI

Полезные ссылки для поиска Open Source решений

github.com/Penetrum-Security/Security-List

github.com/nimari/OpenSourceCyberSecurity/blob/main/Tools.md

github.com/fabacab/awesome-cybersecurity-blueteam

Спасибо за внимание!

Пишите на почту **info@awillix.ru** с темой **«РИФ»**
и мы проконсультируем вас **бесплатно.**

Just Security

1 481 подписчик

Подписывайтесь на наш
← телеграм-канал @JustSecurity