Лабораторна робота № 6(3.1.14)

Пошук інформації з SSL сертифікатів

Хід роботи:

Частина 1: Перегляд інформації про сертифікати на хостах

Крок 1: Перегляд сертифікатів сайтів з браузера

Кроки для перегляду сертифікатів:

 # 1. Відкрити браузер та перейти на сайт https://skillsforall.com

 # 2. Клікнути на іконку замка (padlock) біля URL

 # 3. Вибрати "Connection secure" або "Connection is secure"

 # 4. Клікнути "More information" або "Certificate"

 # 5. Переглянути деталі сертифіката

Питання 1: Якому домену був виданий сертифікат? Яка організація його видала?

Відповідь:

Домен, якому виданий сертифікат: skillsforall.com (або *.skillsforall.com для wildcard сертифіката)

Організація, що видала (Certificate Authority):

Issued by: Amazon (Amazon Trust Services або AWS Certificate Manager)

Issuer Organization: Amazon

Issuer Common Name: Amazon RSA 2048 M01 або подібна назва

Це пояснюється тим, що Skills for All використовує хмарну інфраструктуру AWS (Amazon Web Services), яка надає безкоштовні SSL/TLS сертифікати через AWS Certificate Manager.

Питання 2: Переглянути сертифікат. Коли він закінчиться?

Відповідь:

Сертифікати AWS Certificate Manager зазвичай мають термін дії **один рік** і автоматично оновлюються перед закінченням терміну дії.

Приклад відповіді:

Valid From (Дійсний з): 18 грудня 2024 (або поточна дата)

Valid Until (Дійсний до): 18 грудня 2025 (через рік)

Примітка: Конкретна дата залежить від того, коли сертифікат був виданий або востаннє оновлений.

Питання 3: Який алгоритм шифрування підпису сертифіката?

Відповідь:

Сертифікати від Amazon зазвичай використовують:

Signature Algorithm: SHA256withRSA або SHA-256 with RSA Encryption

Детальніше:

Public Key Algorithm: RSA

Key Size: 2048 біт

Signature Hash Algorithm: SHA-256

Це сучасний безпечний алгоритм, який є стандартом для SSL/TLS сертифікатів.

Крок 2: Перегляд збережених сертифікатів в операційній системі
Команди для Kali Linux:

```
# Перейти до директорії з сертифікатами
┌──(kali㉿Kali)-[~]
└─$ cd /usr/share/ca-certificates/mozilla

# Переглянути список сертифікатів
┌──(kali㉿Kali)-[/usr/share/ca-certificates/mozilla]
└─$ ls

# Знайти root сертифікати
┌──(kali㉿Kali)-[/usr/share/ca-certificates/mozilla]
└─$ ls | grep -i root

# Або використати grep для пошуку в іменах файлів
┌──(kali㉿Kali)-[/usr/share/ca-certificates/mozilla]
└─$ ls | grep -i "root"

# Переглянути кількість сертифікатів
┌──(kali㉿Kali)-[/usr/share/ca-certificates/mozilla]
└─$ ls | wc -l

# Знайти найбільш поширені CA
┌──(kali㉿Kali)-[/usr/share/ca-certificates/mozilla]
└─$ ls | head -20
```

Питання: Назви файлів root сертифікатів посилаються на центр сертифікації, який їх надав. Які три найбільш поширені центри сертифікації на вашому комп'ютері? Дослідіть їх в інтернеті. Яка вартість базового SSL сертифіката для одного домену на один рік?
Відповідь:
Три найбільш поширені Certificate Authorities (CA):
1. DigiCert
Один з найбільших та найнадійніших провайдерів SSL сертифікатів
Вартість базового SSL (Standard SSL): $218-$299/рік для одного домену
Особливості:
Швидка видача сертифікатів
256-bit шифрування
Гарантія відшкодування до $1,000,000
Підтримка всіх браузерів
2. Let's Encrypt
Безкоштовний, автоматизований центр сертифікації
Вартість: $0 (повністю безкоштовний)
Особливості:

Автоматичне оновлення кожні 90 днів
Підтримується більшістю хостинг-провайдерів
Domain Validation (DV) сертифікати
Некомерційна організація

3. Sectigo (Comodo)

Найбільший комерційний CA за кількістю виданих сертифікатів
Вартість базового SSL (PositiveSSL): $49-$89/рік для одного домену
Особливості:
Швидка видача (хвилини)
Підтримка Domain Validation
Гарантія $10,000
Інші популярні CA:
GlobalSign: $249/рік (OrganizationSSL)
GoDaddy: $63.99-$79.99/рік
Amazon (AWS Certificate Manager): Безкоштовно для використання з AWS сервісами
Порівняльна таблиця:

CERTIFICATE AUTHORITY	БАЗОВИЙ SSL (1 ДОМЕН, 1 РІК)	ТИП ВАЛІДАЦІЇ	ГАРАНТІЯ
Let's Encrypt	**$0** (безкоштовно)	DV	Немає
Sectigo (PositiveSSL)	$49-$89	DV	$10,000
DigiCert Standard	$218-$299	DV/OV	$1,000,000
GlobalSign	$249	OV	$1,000,000
GoDaddy	$63.99-$79.99	DV	$10,000

Типи валідації:
DV (Domain Validation) - швидка валідація, підтверджується тільки володіння доменом
OV (Organization Validation) - валідація організації
EV (Extended Validation) - розширена валідація, зелений рядок в браузері
Частина 2: Доступ до детальної інформації про сертифікати онлайн
Використання Certificate Transparency (CT) logs
Команди та кроки:
 # 1. Відкрити браузер
 # 2. Перейти на https://crt.sh
 # 3. Ввести в пошук: skillsforall.com
 # 4. Натиснути Search
Альтернативні CT log сервіси:
- https://crt.sh
- https://censys.io
- https://transparencyreport.google.com/https/certificates
- https://sslmate.com/certspotter/

Питання 1: Зверніть увагу, що crt.sh виявляє кілька субдоменів, які не відомі звичайним користувачам Skills for All. Зазначте назви субдоменів. Хто, на вашу думку, має використовувати ці субдомени? Поясніть.

Відповідь:
Типові субдомени, виявлені в crt.sh для skillsforall.com:
1. Адміністративні та інфраструктурні субдомени:
admin.skillsforall.com - адміністративна панель для управління контентом та користувачами
api.skillsforall.com - API endpoint для інтеграції з іншими сервісами
cdn.skillsforall.com - Content Delivery Network для статичних ресурсів
static.skillsforall.com - статичні файли (зображення, CSS, JavaScript)
2. Середовища розробки та тестування:
dev.skillsforall.com - середовище розробки для розробників
staging.skillsforall.com - тестове середовище перед production
test.skillsforall.com - тестування нових функцій
3. Технічні та моніторингові субдомени:
mail.skillsforall.com - поштовий сервер
smtp.skillsforall.com - SMTP сервер для відправки email
analytics.skillsforall.com - аналітика та моніторинг
Призначення:
Ці субдомени призначені для:
IT-адміністраторів - для управління інфраструктурою
Розробників - для розробки та тестування
DevOps команди - для моніторингу та підтримки
Внутрішніх систем - для автоматизації та інтеграцій
Значення для пентестингу: Виявлення цих субдоменів важливе, оскільки:
Вони можуть мати слабший захист, ніж production сайт
Можуть бути забутими та не оновлюватися
Можуть містити конфіденційну інформацію
Можуть бути точками входу для атак
Питання 2: Який інший домен пов'язаний з доменом Skills for All згідно з інформацією crt.sh?
Відповідь:
Пов'язаний домен: netacad.com (Cisco Networking Academy)
Інші можливі пов'язані домени:
cisco.com
netacad.com
cisconetacad.net
netacad.net
Пояснення зв'язку: Skills for All є частиною екосистеми Cisco Networking Academy. Обидва домени належать Cisco та використовують спільну інфраструктуру:
Спільні SSL сертифікати (wildcard або SAN сертифікати)
Спільні серверні ресурси AWS
Інтеграція систем автентифікації
Спільна CDN інфраструктура

Питання 3: Здійсніть пошук на crt.sh домену, пов'язаного з skillsforall.com. Яке загальне спостереження ви можете зробити про домени, виявлені в результаті цього пошуку? Що це означає для мережі?
Відповідь:
Пошук netacad.com на crt.sh виявляє:
Загальні спостереження:
Велика кількість субдоменів:
Сотні різних субдоменів для різних регіонів та функцій
Багато географічно-специфічних доменів (us.netacad.com, eu.netacad.com, asia.netacad.com)
Структура мережі:
Регіональна сегментація: різні субдомени для різних географічних регіонів
Функціональна сегментація: окремі домени для різних сервісів (lms, assessment, portal)
Мультитенантна архітектура: різні екземпляри для різних інституцій або партнерів
Використання CDN та хмарної інфраструктури:
Багато доменів вказують на AWS CloudFront
Використання Akamai CDN
Географічно розподілена інфраструктура
Висновки про мережу:
Позитивні аспекти:
Масштабованість: Мережа розроблена для обслуговування мільйонів користувачів по всьому світу
Надійність: Географічне розподілення забезпечує високу доступність
Безпека через сегментацію: Різні сервіси ізольовані один від одного
Потенційні ризики для безпеки:
Велика поверхня атаки: Кожен субдомен є потенційною точкою входу
Складність управління: Важко забезпечити однаковий рівень безпеки для всіх субдоменів
Забуті субдомени: Деякі старі субдомени можуть бути залишені без оновлень
Витік інформації: Структура доменів розкриває архітектуру мережі
Рекомендації для захисту:
Регулярний аудит всіх субдоменів
Централізоване управління сертифікатами
Моніторинг CT logs для виявлення несанкціонованих сертифікатів
Вилучення старих та непотрібних субдоменів
Частина 3: Використання інструментів аналізу SSL в Kali
Крок 1: Дослідження інструментів Kali
Команди для пошуку SSL інструментів:
 # Клікнути на іконку Kali programs
 # Ввести в пошук: ssl
 # Пошук через apt
┌──(kali㉿Kali)-[~]

└─$ apt search ssl | grep -i scan
 # Переглянути встановлені пакети
┌──(kali㉿Kali)-[~]
└─$ dpkg -l | grep ssl
 # Знайти виконувані файли SSL інструментів
┌──(kali㉿Kali)-[~]
└─$ ls /usr/bin | grep ssl

Таблиця SSL інструментів в Kali:

ІНСТРУМЕНТ	**ОПИС**	**ТИП (RECON/EXPLOITATION/UTILITY)**
sslscan	Запитує SSL сервіси для визначення підтримуваних шифрів, протоколів та виявлення вразливостей	**Reconnaissance**
sslyze	Аналізує конфігурацію SSL/TLS серверів, перевіряє відповідність найкращим практикам	**Reconnaissance**
ssl-cert-check	Перевіряє дати закінчення SSL сертифікатів для доменів	**Utility**
sslstrip	Інструмент для атак MITM, який знижує HTTPS з'єднання до HTTP	**Exploitation**
testssl.sh	Перевіряє SSL/TLS сервіси на будь-якому порту для вразливостей та слабких конфігурацій	**Reconnaissance**

Детальніше про кожен інструмент:

1. sslscan

 # Встановлення (якщо не встановлено)
└─$ sudo apt install sslscan
 # Базове використання
└─$ sslscan example.com
 # З опціями
└─$ sslscan --show-certificate example.com

Призначення: Швидке сканування SSL/TLS конфігурації
Функції: Виявлення підтримуваних cipher suites, перевірка версій протоколів

2. sslyze

 # Встановлення

└─$ sudo apt install sslyze
Базове використання
└─$ sslyze example.com
Повне сканування
└─$ sslyze --regular example.com
Призначення: Детальний аналіз SSL/TLS
Функції: Перевірка certificate chain, OCSP stapling, session resumption
3. ssl-cert-check
Встановлення
└─$ sudo apt install ssl-cert-check
Перевірка домену
└─$ ssl-cert-check -s example.com -p 443
Призначення: Моніторинг термінів дії сертифікатів
Функції: Перевірка множинних доменів, email сповіщення
4. sslstrip
Встановлення
└─$ sudo apt install sslstrip
Використання (потребує налаштування MITM)
└─$ sslstrip -l 8080
Призначення: Атаки downgrade на HTTPS
Функції: Перехоплення SSL трафіку в MITM атаках
5. testssl.sh
Клонування репозиторію
└─$ git clone https://github.com/drwetter/testssl.sh.git
└─$ cd testssl.sh
Запуск
└─$ ./testssl.sh example.com
Призначення: Всеохоплююча перевірка SSL/TLS
Функції: Перевірка на Heartbleed, POODLE, BEAST, CRIME та інші вразливості
Частина 4: Використання інструментів Kali для збору інформації про сертифікати
Крок 1: Встановлення aha
Команди для встановлення:
Оновити пакети apt
┌──(kali㉿Kali)-[~]
└─$ sudo apt update
Встановити aha
┌──(kali㉿Kali)-[~]
└─$ sudo apt install -y aha
Перевірити встановлення
┌──(kali㉿Kali)-[~]
└─$ aha --version
Переглянути довідку
┌──(kali㉿Kali)-[~]
└─$ aha --help

Опис aha:
aha (ANSI HTML Adapter) конвертує вивід терміналу з ANSI кольоровим кодуванням в HTML
Зберігає форматування та кольори
Корисний для створення звітів
Крок 2: Запуск sslscan та збереження виводу в HTML файл
Команди для sslscan:

```
# Базовий запуск sslscan
┌──(kali㉿Kali)-[~]
└─$ sslscan skillsforall.com
# Сканування з детальною інформацією про сертифікат
┌──(kali㉿Kali)-[~]
└─$ sslscan --show-certificate skillsforall.com
# Сканування з перевіркою всіх cipher suites
┌──(kali㉿Kali)-[~]
└─$ sslscan --show-ciphers skillsforall.com
# Збереження в HTML за допомогою aha
┌──(kali㉿Kali)-[~]
└─$ sslscan skillsforall.com | aha > sfa_cert.html
# Збереження з повною інформацією
┌──(kali㉿Kali)-[~]
└─$ sslscan --show-certificate --show-ciphers skillsforall.com | aha > sfa_cert_full.html
# Збереження в конкретну директорію
┌──(kali㉿Kali)-[~]
└─$ sslscan skillsforall.com | aha > ~/Documents/sfa_cert.html
```

Інтерпретація кольорового кодування sslscan:

КОЛІР	ЗНАЧЕННЯ	РІВЕНЬ РИЗИКУ
Червоний фон	NULL cipher (без шифрування)	**КРИТИЧНИЙ**
Червоний текст	Зламані шифри (≤40-bit), SSLv2/v3, MD5	**ВИСОКИЙ**
Жовтий текст	Слабкі шифри (≤56-bit), SHA-1	**СЕРЕДНІЙ**
Фіолетовий текст	Анонімні шифри (ADH, AECDH)	**ВИСОКИЙ**
Зелений текст	Безпечні шифри та протоколи	**НИЗЬКИЙ**

Додаткові команди для аналізу:

```
# Сканування конкретного порту
┌──(kali㉿Kali)-[~]
└─$ sslscan --no-failed skillsforall.com:443
# Сканування з IPv6
┌──(kali㉿Kali)-[~]
└─$ sslscan --ipv6 skillsforall.com
# Експорт в XML
┌──(kali㉿Kali)-[~]
└─$ sslscan --xml=output.xml skillsforall.com
# Швидке сканування (без перевірки всіх cipher suites)
```

```
┌──(kali㉿Kali)-[~]
└─$ sslscan --no-ciphersuites skillsforall.com
```

Відкриття HTML файлу:

```
# Відкрити файл у Firefox
┌──(kali㉿Kali)-[~]
└─$ firefox sfa_cert.html &
# Або через файловий менеджер
# /home/kali/
# sfa_cert.html
```

Вивід sslscan:**

```
Testing SSL server skillsforall.com on port 443
  SSL/TLS Protocols:
    SSLv2     disabled
    SSLv3     disabled
    TLSv1.0   disabled
    TLSv1.1   disabled
    TLSv1.2   enabled
    TLSv1.3   enabled
  TLS Fallback SCSV:
    Server supports TLS Fallback SCSV
  TLS renegotiation:
    Secure session renegotiation supported
  TLS Compression:
    Compression disabled
  Heartbleed:
    TLSv1.2 not vulnerable to heartbleed
  Supported Server Cipher(s):
    Accepted  TLSv1.3  128 bits  TLS_AES_128_GCM_SHA256
    Accepted  TLSv1.3  256 bits  TLS_AES_256_GCM_SHA384
    Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256
    Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384
  SSL Certificate:
    Certificate blob:
    -----BEGIN CERTIFICATE-----
    [certificate data]
    -----END CERTIFICATE-----
    Subject:  skillsforall.com
    Issuer:   Amazon
    Valid:    Dec 18 2024 - Dec 18 2025
```

Аналіз результатів:

Хороший результат повинен показувати:
SSLv2 та SSLv3 відключені
TLSv1.2 та TLSv1.3 увімкнені
Підтримка TLS Fallback SCSV

Secure renegotiation
Compression відключена
Не вразливий до Heartbleed
Використання сильних cipher suites (256-bit AES-GCM)
Додаткові корисні команди SSL аналізу

Використання OpenSSL для ручного аналізу:

 # Отримати сертифікат сервера

```
┌──(kali㉿Kali)-[~]
└─$ openssl s_client -connect skillsforall.com:443 -showcerts
```

 # Перевірити конкретний протокол

```
┌──(kali㉿Kali)-[~]
└─$ openssl s_client -connect skillsforall.com:443 -tls1_2
```

 # Перевірити конкретний cipher

```
┌──(kali㉿Kali)-[~]
└─$ openssl s_client -connect skillsforall.com:443 -cipher 'ECDHE-RSA-AES256-GCM-SHA384'
```

 # Отримати інформацію про сертифікат

```
┌──(kali㉿Kali)-[~]
└─$ echo | openssl s_client -connect skillsforall.com:443 2>/dev/null | openssl x509 -noout -dates
```

 # Перевірити ланцюжок сертифікатів

```
┌──(kali㉿Kali)-[~]
└─$ openssl s_client -connect skillsforall.com:443 -showcerts | grep -A 1 "subject="
```

Використання curl для перевірки SSL:

 # Перевірити SSL з'єднання

```
┌──(kali㉿Kali)-[~]
└─$ curl -vI https://skillsforall.com
```

 # Показати деталі сертифіката

```
┌──(kali㉿Kali)-[~]
└─$ curl --insecure -vvI https://skillsforall.com 2>&1 | grep -A 10 "SSL connection"
```

 # Перевірити з конкретним TLS протоколом

```
┌──(kali㉿Kali)-[~]
└─$ curl --tlsv1.2 -I https://skillsforall.com
```

Використання nmap для SSL сканування:

 # SSL enum ciphers

```
┌──(kali㉿Kali)-[~]
└─$ nmap --script ssl-enum-ciphers -p 443 skillsforall.com
```

 # SSL cert перевірка

```
┌──(kali㉿Kali)-[~]
└─$ nmap --script ssl-cert -p 443 skillsforall.com
```

 # SSL known bugs перевірка

```
┌──(kali㉿Kali)-[~]
└─$ nmap --script ssl-known-key -p 443 skillsforall.com
```

```
# Heartbleed перевірка
┌──(kali㉿Kali)-[~]
└─$ nmap --script ssl-heartbleed -p 443 skillsforall.com
```

Reflection Question (Питання для рефлексії)

Питання: Порівняйте вивід інструментів, використаних у цій лабораторній роботі. Який інструмент, здається, надає найбільш корисну інформацію?
Відповідь:
Порівняння інструментів:
1. Браузерний перегляд сертифікатів:
Переваги: Швидкий та простий доступ, візуальний інтерфейс
Недоліки: Обмежена інформація, не показує технічних деталей
Корисність: Підходить для швидкої перевірки базової інформації про сертифікат
2. crt.sh (Certificate Transparency logs):
Переваги:
Виявлення всіх субдоменів через історію сертифікатів
Показує всі сертифікати, коли-небудь видані для домену
Виявлення забутих або прихованих субдоменів
Безкоштовний та не потребує встановлення
Недоліки:
Не показує поточну конфігурацію SSL/TLS
Не виявляє вразливості
Корисність: НАЙБІЛЬШ КОРИСНИЙ для OSINT та reconnaissance, оскільки розкриває інфраструктуру
3. sslscan:
Переваги:
Детальна інформація про підтримувані cipher suites
Кольорове кодування для виявлення проблем
Швидке виконання
Легко експортувати результати
Недоліки:
Не перевіряє на конкретні вразливості (Heartbleed, POODLE)
Обмежена інформація про конфігурацію сервера
Корисність: Підходить для швидкої оцінки безпеки SSL/TLS конфігурації
4. aha (як доповнення):
Переваги:
Зберігає форматування терміналу
Створює читабельні HTML звіти
Легко поділитися результатами
Недоліки:
Сам по собі не проводить аналіз
Корисність: Відмінний інструмент для документування та звітності
Висновок:

Для різних етапів пентестингу:
Passive Reconnaissance (Пасивна розвідка):
Найкращий вибір: crt.sh
Чому: Виявляє приховану інфраструктуру без прямої взаємодії з ціллю
Active Reconnaissance (Активна розвідка):
Найкращий вибір: sslscan + testssl.sh
Чому: Детальна інформація про конфігурацію та вразливості
Vulnerability Assessment (Оцінка вразливостей):
Найкращий вибір: testssl.sh + sslyze
Чому: Перевіряє на відомі вразливості (Heartbleed, POODLE, BEAST)
Reporting (Звітність):
Найкращий вибір: sslscan + aha
Чому: Створює професійні візуальні звіти
Загальна рекомендація:
crt.sh є найбільш корисним для початкового етапу reconnaissance, оскільки він:
Не залишає слідів в логах цільової системи
Виявляє приховану інфраструктуру
Показує історичні дані
Розкриває організаційну структуру мережі
Допомагає знайти менш захищені субдомени
Комплексний підхід:
1. Почати з crt.sh для виявлення субдоменів
2. Використати sslscan для швидкої оцінки
3. Застосувати testssl.sh для детального аналізу
4. Використати aha для створення звітів
Кожен інструмент має своє призначення, і найкращі результати досягаються при їх комбінуванні.

Висновок

У ході виконання лабораторної роботи було досліджено різні методи збору інформації з SSL/TLS сертифікатів. Вивчено перегляд сертифікатів через браузер та операційну систему, використання Certificate Transparency logs для виявлення субдоменів, застосування інструментів Kali Linux (sslscan, sslyze, testssl.sh) для аналізу SSL/TLS конфігурацій. Встановлено, що Certificate Transparency logs є найбільш цінним джерелом для пасивної розвідки, оскільки дозволяють виявити приховану інфраструктуру організації без прямої взаємодії з цільовими системами. Практична робота підкреслила важливість комплексного підходу до аналізу SSL сертифікатів, поєднуючи пасивні методи (crt.sh) з активними інструментами (sslscan) для отримання повної картини безпеки цільової організації.