Wstęp

Test penetracyjny to praktyczna weryfikacja bezpieczeństwa systemu komputerowego, polegająca na symulowaniu realnych ataków w kontrolowanym środowisku. Proces ten odbywa się w ścisłych ramach formalnych, na podstawie autoryzacji udzielonej przez właściciela systemu. Pozwala on na zidentyfikowanie zarówno znanych podatności, jak i krytycznych luk – w tym nawet najnowsze, nieznane dotąd luki (tzw. 0-day).

Decyzja o przeprowadzeniu testów penetracyjnych powinna wynikać z określonej motywacji organizacji, która może mieć charakter zewnętrzny lub wewnętrzny.

Motywacje zewnętrzne wynikają najczęściej z wymogów prawnych i regulacyjnych. Przykładowo instytucje finansowe, takie jak banki, mają obowiązek weryfikowania bezpieczeństwa swoich systemów, m.in. poprzez testy penetracyjne. Podobne wymagania nakładają także przepisy dotyczące krajowego systemu cyberbezpieczeństwa czy standard PCI DSS dla firm przetwarzających dane kart płatniczych.

Motywacje wewnętrzne pojawiają się wtedy, gdy organizacja sama chce ocenić poziom bezpieczeństwa swoich systemów i infrastruktury. Test penetracyjny jest jednak tylko jednym z elementów szerszego procesu zarządzania bezpieczeństwem, który obejmuje również m.in. inwentaryzację zasobów oraz wdrażanie polityk bezpieczeństwa.

Istotnym powodem przeprowadzania testów jest także rosnące ryzyko cyberataków, w tym ataków ransomware. Organizacje, które nie weryfikują poziomu bezpieczeństwa, narażają się na poważne konsekwencje, takie jak wycieki danych, przestoje w działalności czy kary związane z naruszeniem przepisów o ochronie danych osobowych (np. RODO).

Dodatkową motywacją może być możliwość uzyskania lub obniżenia kosztów ubezpieczenia od cyberryzyk oraz chęć niezależnej oceny działań wewnętrznego zespołu bezpieczeństwa. Zewnętrzne testy pozwalają spojrzeć na systemy z innej perspektywy i mogą pomóc wykryć problemy, które wcześniej zostały pominięte.

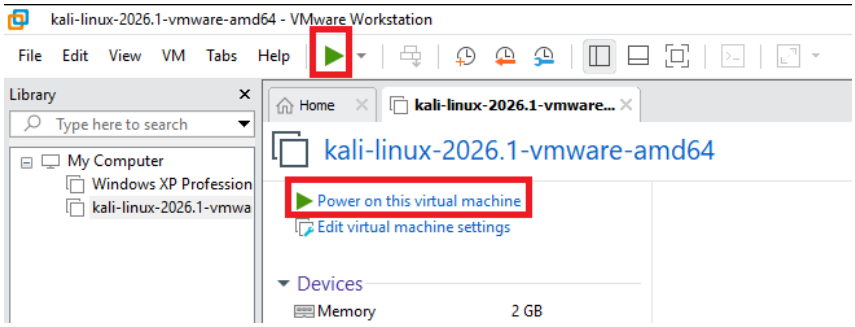
I. Przygotowanie środowiska pracy

1. Uruchom program **VMware Workstation Pro**.

2. Zaimportuj pobraną maszynę. Przejdź do `File -> Open`, a następnie wybierz plik `.ovf` wskazany przez prowadzącego.

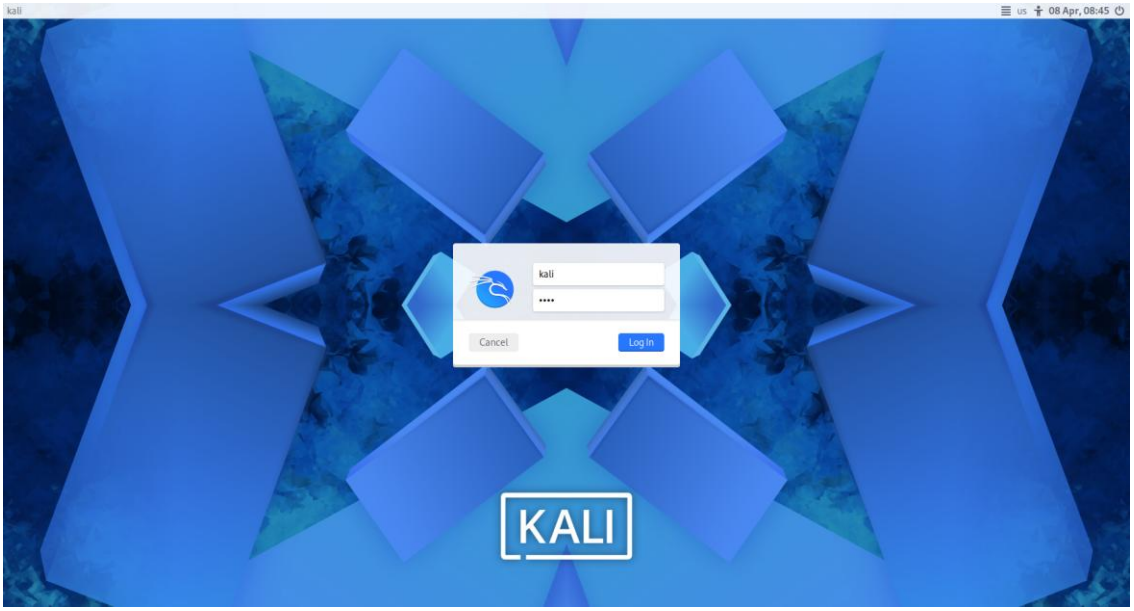
3. Nadaj maszynie wirtualnej nazwę oraz wskaż lokalizację, do której ma zostać zaimportowana. Następnie naciśnij przycisk `Import`.

4. Po zakończeniu procesu importowania uruchom maszynę wirtualną, klikając zieloną ikonę Start (trójkąt).

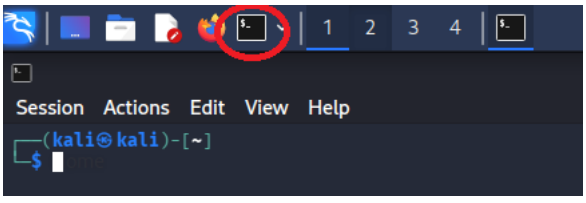


5. Zaloguj się do maszyny Kali Linux, używając następujących danych:

użytkownik: `kali` hasło: `kali`



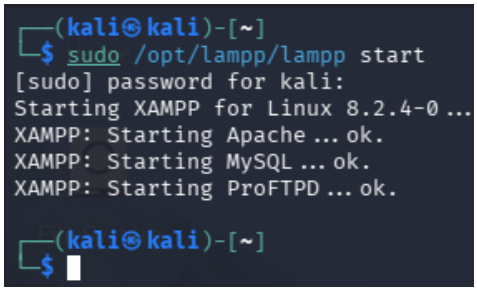
6. Po zalogowaniu uruchom terminal Kali Linux.



7. W terminalu wykonaj poniższe polecenie, które uruchamia serwer wymagany w kolejnej części instrukcji:

```
sudo /opt/lampp/lampp start
```

Po wykonaniu polecenia system poprosi o podanie hasła administratora: `kali`



II. Testowanie narzędzia OWASP ZAP

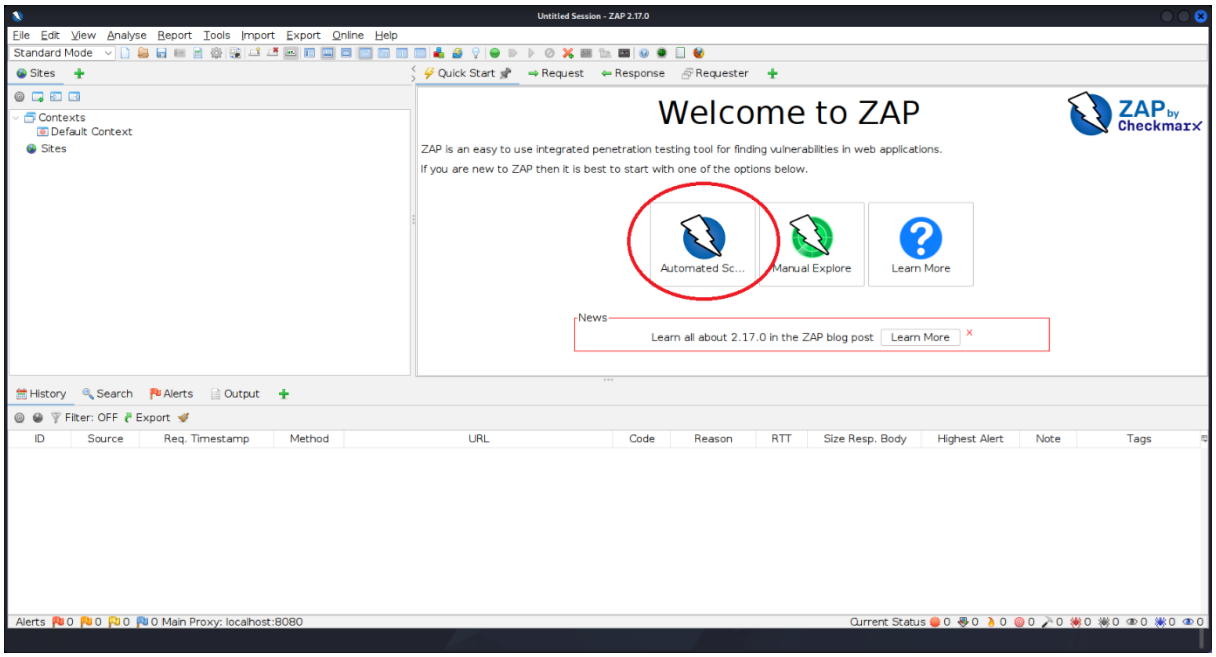
Testami penetracyjnymi zajmują się zazwyczaj specjaliści wyposażeni w dedykowane, profesjonalne oprogramowanie. Na rynku dostępnych jest wiele narzędzi, takich jak Burp Suite Professional czy Nessus, jednak są to rozwiązania komercyjne.

W związku z tym podczas zajęć zostanie wykorzystane narzędzie OWASP ZAP (Zed Attack Proxy). Jest to jedno z najpopularniejszych narzędzi typu open source służących do testowania bezpieczeństwa aplikacji webowych. Program posiada licencję umożliwiającą jego wykorzystanie również w zastosowaniach komercyjnych bez konieczności ponoszenia opłat.

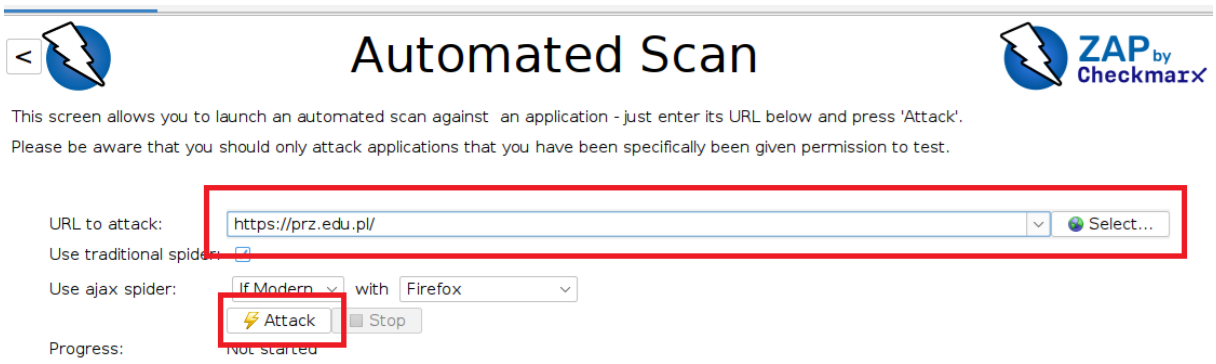
1. Uruchom program z poziomu pulpitu lub wpisz w terminalu następującą komendę:

```
zaproxy
```

2. Po uruchomieniu programu wybierz opcję `Automated Scan`.



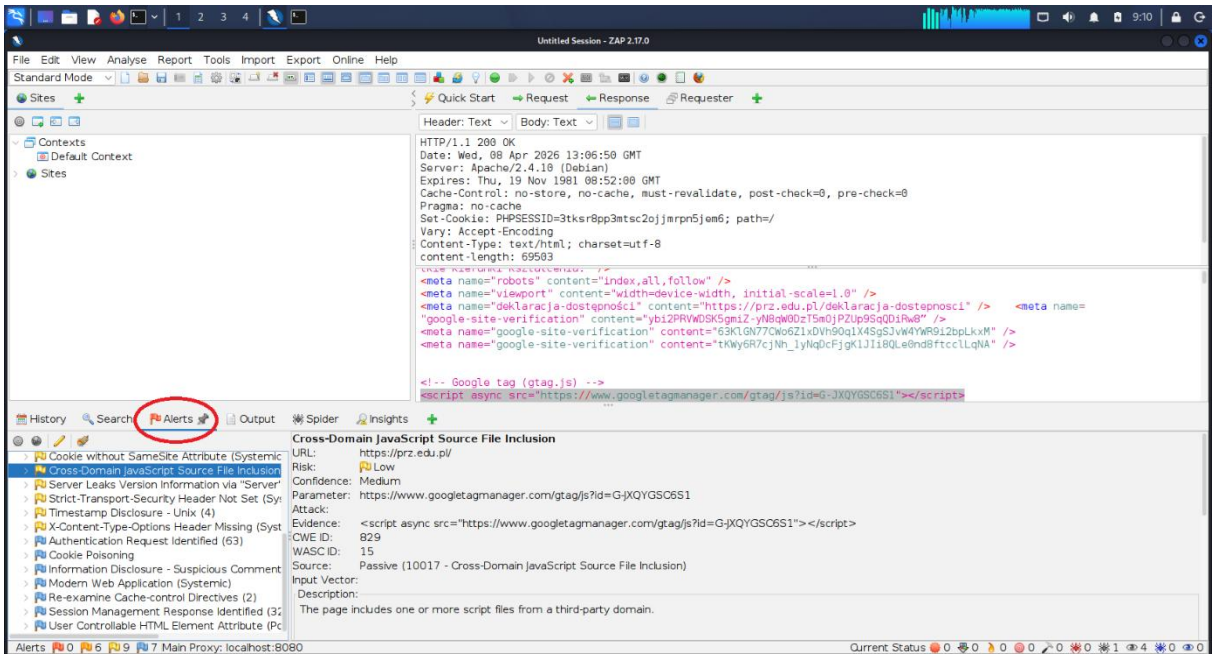
3. W polu URL wprowadź adres aplikacji, która ma zostać przeskanowana: https://prz.edu.pl/ Następnie wybierz przycisk `Attack`, aby rozpocząć skanowanie.



4. Po zakończeniu skanowania przejdź do zakładki `Alerts`. Możesz tutaj przejrzeć wszystkie wykryne podatności i zagrożenia po rozwinięciu drzewa zagrożeń możemy znaleźć szczegółowe informacje o błędach, w tym ich klasyfikacje CWE51, czy nawet proponowane rozwiązanie problemu.

   W tej sekcji można przejrzeć wszystkie wykryte podatności oraz zagrożenia. Po rozwinięciu drzewa zagrożeń dostępne są szczegółowe informacje dotyczące znalezionych błędów, w tym:

   - opis podatności,
   - klasyfikacja według CWE (Common Weakness Enumeration),
   - poziom zagrożenia,
   - proponowane rozwiązania problemu.



5. Po zakończeniu analizy wyników zamknij program, klikając ikonę X w prawym górnym rogu okna.

III. Testowanie narzędzia h8mail

Program h8mail to narzędzie z zakresu OSINT (Open Source Intelligence) służące do sprawdzania, czy dany adres e-mail pojawił się w wyciekach danych z różnych serwisów internetowych.

Narzędzie przeszukuje publiczne bazy wycieków (data breaches) oraz różne źródła w Internecie, aby znaleźć informacje powiązane z podanym adresem e-mail.

1. W systemie Kali Linux uruchom terminal i wpisz polecenie:

```
h8mail -h
```

Polecenie wyświetli pomoc oraz listę dostępnych opcji programu.

2. Następnie sprawdź, czy Twój adres e-mail pojawił się w znanych wyciekach danych, wpisując polecenie:

```
h8mail -t twój_adres_meil
```

`-t` – określa adres e-mail, który ma zostać sprawdzony w bazach wycieków danych.

Po wykonaniu polecenia narzędzie sprawdzi, czy podany adres e-mail występuje w znanych wyciekach danych.
Jeśli adres został znaleziony w wycieku, program może wyświetlić informacje takie jak:

- nazwa serwisu, z którego nastąpił wyciek,
- data wycieku,
- typ ujawnionych danych (np. e-mail, hasło).