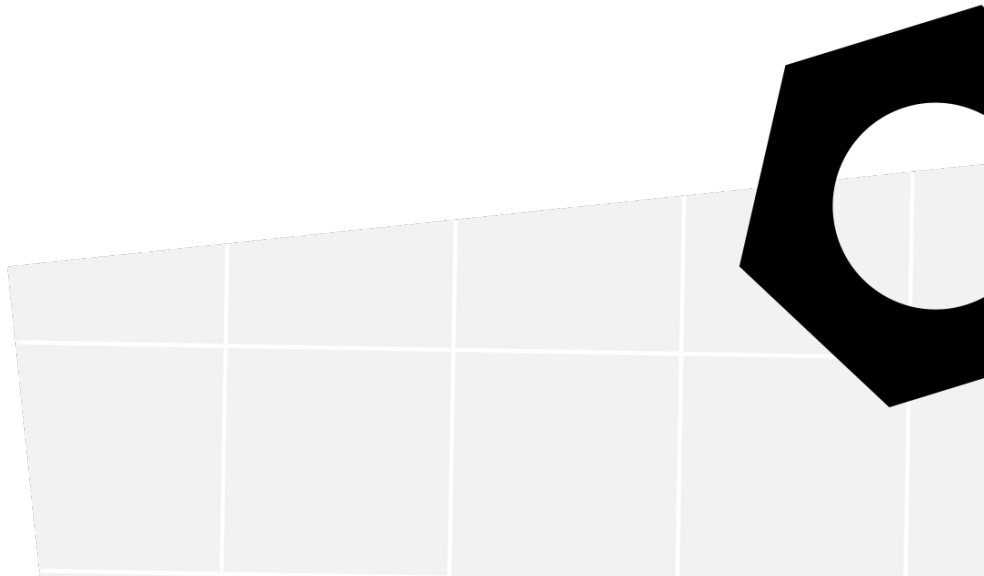
Projekt 2: Omijanie zabezpieczeń



software
development
academy

Projekt praktyczny jest podsumowaniem dotychczasowych zajęć oraz okazją do zastosowania zdobytej wiedzy w celu rozwiązania postawionych zadań.

Projekt wymaga zastosowania w praktyce wiedzy nt. sieci komputerowych, systemów Linux i Windows, metod omijania zabezpieczeń oraz umiejętności programowania w Pythonie*.

* opcjonalnie

software
development
academy

Plan projektu

- Podział na grupy projektowe (max. 3 osoby)*
- Zapoznanie się z zadaniami i wymaganiami (warunkami zaliczenia)
- Przygotowanie środowiska projektowego (z pomocą trenera)
- Realizacja zadań projektowych

* istnieje możliwość wykonywania projektu w grupie jednoosobowej ;)

Wymagania

- Wykonanie przez grupę podstawowych zadań projektowych
- Dostarczenie raportu z projektu w formie publicznego repozytorium na GitHubie
- Raport powinien zawierać:
  - chronologiczny opis realizacji zadań projektowych
  - uruchomione programy, wykonane komendy oraz ich efekt
  - screenshoty
  - inne elementy wzbogacające raport (jeżeli grupa uważa je za istotne)

Środowisko projektowe / narzędzia

Na środowisko projektowe składają się:

- maszyna wirtualna Kali Linux
- maszyna wirtualna Windows 7
- maszyna wirtualna SDA z przekazanego pliku .ova. Link do OVA :)
- telefon
- dodatkowe urządzenie “z Wi-Fi” (np. drugi telefon lub laptop)

Dodatkowo na potrzeby projektu wykorzystywane są zasoby zewnętrzne zdefiniowane w poszczególnych zadaniach.

Maszyny wirtualne oraz telefon powinny znajdować się w **tej samej sieci**. W ustawieniach sieciowych maszyny wirtualnej w VirtualBox najlepiej wybrać adapter sieciowy zmostkowany (bridged), tak aby maszyny mogły zarówno komunikować się ze sobą jak i miały dostęp do Internetu.

Zadania do wykonania

Na projekt składa się 9 odrębnych zadań:

- 6 zadań podstawowych
- 3 zadań dla chętnych

Warunkiem zaliczenia projektu jest wykonanie przez grupę zadań podstawowych.

Pomimo określonego celu, zadania mają **formę otwartą** i nie ma narzuconej konkretnej metody rozwiązania.

Wskazówki do zadań

Zadania projektowe należy rozwiązać na podstawie wiedzy zdobytej **od początku trwania kursu** i **w oparciu o materiały dostępne w bazie wiedzy**.

Dodatkowo zalecane jest wspomaganie się ogólnodostępną wiedzą z serwisów takich jak Stack Overflow, YouTube czy blogów.

Zadanie 1 - Łamanie haseł (met. brute-force) 1/3

Środowisko: Kali Linux

Dla podanych niżej hashy określ **typ wykorzystanego algorytmu hashującego**, a następnie **złam hasło metodą brute-force**.

Każde hasło składa się z maksymalnie 5 znaków (**tylko cyfry**).

1. 81dc9bdb52d04dc20036dbd8313ed055
2. b021d0862bc76b0995927902ec697d97b5080341a53cd90b780f50fd5886f4160bbb9d4a573b76c23004c9b3a44ac95cfde45399e3357d1f651b556dfbd0d58f
3. 7aaa0f57
4. 31bca02094eb78126a517b206a88c73cfa9ec6f704c7030d18212cace820f025f00bf0ea68dbf3f3a5436ca63b53bf7bf80ad8d5de7d8359d0b7fed9dbc3ab99

Zadanie 1 - Łamanie haseł (met. brute-force) 2/3

Środowisko: Kali Linux

Dla podanych niżej hashy określ **typ wykorzystanego algorytmu hashującego**, a następnie **złam hasło metodą brute-force**.

Każde hasło składa się z maksymalnie 5 znaków (**małe i wielkie litery**).

1. 9e66d646cfb6c84d06a42ee1975ffaae90352bd016da18f51721e2042d9067dcb120accc574105b43139b6c9c887dda8202eff20cc4b98bad7b3be1e471b3aa5
2. 8a04bd2d079ee38f1af784317c4e2442625518780ccff3213feb2e207d2be42ca0760fd8476184a004b71bcb5841db5cd0a546b9b8870f1cafee57991077c4a9

Zadanie 1 - Łamanie haseł (met. brute-force) 3/3

Środowisko: Kali Linux

Dla podanego niżej hasha określ **typ wykorzystanego algorytmu hashującego**, a następnie **złam hasło metodą brute-force**.

Hasło składa się z **dokładnie z 6 znaków alfanumerycznych**.
W miarę możliwości skorzystaj z GPU lub wykonaj zadanie po zajęciach.

1. 44d9886c0a57ddbfdb31aa936bd498bf2ab70f741ee47047851e768db953fc4e43f92be953e205a3d1b3ab752ed90379444b651b582b0bc209a739a624e109da

Zadanie 2 – Łamanie haseł (met. słownikowa) 1/2

Środowisko: Kali Linux

Dla podanych niżej hashy określ **typ wykorzystanego algorytmu hashującego**, a następnie **złam hasło metodą słownikową**.

Hasła pochodzą ze słownika **rockyou-50**.

1. 9fd8301ac24fb88e65d9d7cd1dd1b1ec
2. 7f9a6871b86f40c330132c4fc42cda59
3. 6104df369888589d6dbea304b59a32d4
4. 276f8db0b86edaa7fc805516c852c889
5. 04dac8afe0ca501587bad66f6b5ce5ad

Zadanie 2 – Łamanie haseł (met. słownikowa) 2/2

Środowisko: Kali Linux

Dla podanych niżej hashy określ **typ wykorzystanego algorytmu hashującego**, a następnie **złam hasło metodą słownikową**.

Hasła pochodzą ze słownika **rockyou-50**.

1. 7ab6888935567386376037e042524d27fc8a24ef87b1944449f6a0179991dbdbc481e98db4e70f6df0e04d1a69d8e7101d881379cf1966c992100389da7f3e9a
2. 470c62e301c771f12d91a242efbd41c5e467cba7419c664f784dbc8a20820abaf6ed43e09b0cda994824f14425db3e6d525a7aafa5d093a6a5f6bf7e3ec25dfa

Zadanie 3 - Atak na sieć Wi-Fi

Środowisko: Kali Linux, telefon, urządzenie dodatkowe

1. Na telefonie utwórz hotspot (punkt dostępowy) z siecią zabezpieczoną w standardzie **WPA2-PSK**. Sam wybierz hasło do sieci.
2. Dodatkowym urządzeniem (np. drugi telefon lub laptop) podłącz się do utworzonej sieci.
3. Z użyciem zestawu narzędzi **aircrack-ng** przeprowadź atak na sieć Wi-Fi:
    a. wykonaj deautentykację podłączonych urządzeń
    b. przechwyć **4-way handshake**
4. **Złam hasło**, które sam ustawiłeś (dowolnie wybraną metodą).

Zadanie 4 - Analiza ruchu HTTP

Środowisko: Kali Linux

1. Rozpocznij monitorowanie ruchu sieciowego (narzędziem Wireshark).
2. W przeglądarce nawiąż połączenie z http://testphp.vulnweb.com/login.php
3. Wykonaj próbę logowania (dowolne dane).
4. Odszukaj w zapisanym ruchu swoje dane logowania.

Dla porównania powtórz ćwiczenie z logowaniem np. do Facebooka (również dowolne, nieprawdziwe dane logowania).

Zadanie 5 - Analiza ruchu SSH

Środowisko: Kali Linux, maszyna SDA z projektu 1

1. Rozpocznij monitorowanie ruchu sieciowego (narzędziem Wireshark).
2. Nawiąż połączenie pomiędzy Kalim a SDA po SSH.
3. Stwórz pliki sekret1.txt i sekret2.txt z tajnymi hasłami.
4. Edytuj konfigurację vsFTPd, żeby umożliwić wgrywanie plików po FTP.
5. Zakończ połączenie po SSH.
6. Spróbuj poszukać w zapisanym ruchu sieciowym zawartość plików sekret1.txt i sekret2.txt

Dane logowania do SDA: uranus/butterfly, root/666

Zadanie 6 – Analiza ruchu FTP

Środowisko: Kali Linux, maszyna SDA z projektu 1

1. Rozpocznij monitorowanie ruchu sieciowego (narzędziem Wireshark).
2. Nawiąż połączenie pomiędzy Kalim a SDA po FTP.
3. Prześlij z Kaliego do SDA zwykły plik tekstowy (z własną zawartością).
4. Ściągnij z SDA do Kaliego pliki sekret1.txt i sekret2.txt
5. Zakończ połączenie.
6. Odszukaj w zapisanym ruchu sieciowym zawartość przesłanego i ściągniętych plików.

Dane logowania do SDA: uranus/butterfly, root/666

Zadania dodatkowe

Zadania dla chętnych

software
development
academy

Zadanie 7 - Eternal Blue

Atakujący: Kali Linux | **Ofiara:** Windows 7

1. Przygotuj maszynę wirtualną z podatnością MS17-010 (np. Windows 7) i umieść ją w tej samej sieci co Kali Linux.

Atakujący:

2. Wykryj i potwierdź podatność (np. nmapem).
3. Wykorzystaj podatność korzystając z frameworka Metasploit (nie jest wymagana eskalacja uprawnień).

Dla chętnych:

1. Wykorzystaj podatność MS17-010 bez użycia Metasploita.

Kali Linux Live USB

Zadania dla chętnych

software
development
academy

Przygotowanie Live USB

1. Korzystając z instrukcji przygotuj bootowalnego pendriva z systemem Kali Linux
2. W opcjach BIOSu zmień kolejność bootowania (pendrive z Kalim powinien znaleźć się na pierwszym miejscu).
3. Uruchom ponownie komputer.
4. Komputer powinien uruchomić się z pendriva z Kalim zamiast z dysku z głównym systemem operacyjnym.

Kolejne zadania (dla chętnych) wymagają korzystania z Kaliego Live USB, a nie z maszyny wirtualnej.

Zadanie 8 – MITM przez ARP poisoning

Atakujący: Kali Linux | **Ofiara:** telefon

Atakujący:

1. Wykonaj atak MITM techniką ARP poisoning (ARP spoofing)[1]

Ofiara:

1. W przeglądarce nawiąż połączenie z http://testphp.vulnweb.com/login.php.
2. Wykonaj próbę logowania (dowolne dane).

Atakujący:

1. Odszukaj w zapisanym ruchu dane logowania ofiary.

1 - np. narzędziem arpspoof

Zadanie 9 – SSL Stripping

Atakujący: Kali Linux | **Ofiara:** telefon

Atakujący:

1. Wykonaj atak MITM techniką ARP poisoning (ARP spoofing)[1]
2. Wykonaj atak SSL stripping[2]

Ofiara:

1. W przeglądarce nawiąż połączenie z NUTZINDIA.com
2. Wykonaj próbę logowania (dowolne dane).

Atakujący:

1. Odszukaj w zapisanym ruchu dane logowania ofiary.

1 - narzędziem arpspoof
2 - narzędziem sslstrip