**Wrocław 01.10.2024**

**CYBERBEZPIECZEŃSTWO**

**Lab 1**

**1. Wstęp**

Zapewnienie wysokiego poziomu bezpieczeństwa systemów teleinformatycznych wiąże się z koniecznością konfiguracji wielu elementów sprzętowych i programowych takich jak m.in. sieci VPN, systemy kontroli dostępu, zapory ogniowe (ang. firewall), systemy wykrywania włamań (IDS), systemów antywirusowych, systemów SIEM, itp. Poprawna konfiguracja wszystkich elementów oraz ostateczna weryfikacja osiągniętego rzeczywistego poziomu bezpieczeństwa w takim środowisku wymaga o wiele więcej wiedzy i wysiłku niż tylko uruchomienie zautomatyzowanych narzędzi. Fałszywe poczucie bezpieczeństwa może łatwo spowodować utratę krytycznych danych i zasobów.

Zaawansowane testy bezpieczeństwa dla środowisk o wysokim poziomie złożoności wykracza poza podstawowe domyślne konfiguracje czy też automatyczne skanowanie. Na zajęciach laboratoryjnych realizowanych w ramach kursu Cyberbezpieczeństwo, dokonamy krótkiego przeglądu wybranych zagadnień, problemów, technik i narzędzi, które są istotne dla właściwego rozumienia i kształtowania poziomu bezpieczeństwa systemów teleinformatycznych.

Pierwsza część semestru poświęcona jest wybranym problemom bezpieczeństwa związanych z historyczną i współczesną kryptografią. W tej części zilustrujemy podstawowe założenia i możliwości algorytmów kryptograficznych z użyciem wybranych narzędzi takich jak CrypTool. Ćwiczenia pozwolą na poznanie podstawowych typów algorytmów jak i też zwrócą uwagę na potencjalne problemy i słabości wykorzystywanych w ochronie systemów algorytmów kryptograficznych. Poznamy najważniejsze kierunki we współczesnej kryptografii oraz podstawowe zasady, jak dobrać najodpowiedniejsze algorytmy i jak z nich korzystać. Mając wiedzę z tej części będziemy w stanie zapewnić poufność i zweryfikować integralność danych.

Druga część semestru poświęcona jest przeglądowi wybranych zagadnień z procesu oceny poziomu bezpieczeństwa, a który to proces nazywany jest testami penetracyjnymi. W tym kontekście poznamy rolę i znaczenie tzw. białego wywiadu sieciowego (ang. Open Source Inteligence), pasywnego i aktywnego rekonesansu czy też narzędzia wspomagające proces oceny bezpieczeństwa usług sieciowych, a w tym aplikacji webowych. Oprócz wybranych elementów testów penetracyjnych, poznamy również podstawowe metody zarządzania bezpieczeństwem komunikacji z wykorzystaniem aplikacji wspomagających definiowanie sieci VPN.

W trakcie jednego semestru nie jest możliwe poznanie, a tym bardziej zgłębienie wszystkich istotnych zagadnień dotyczących cyberbezpieczeństwa, ale mamy nadzieję, że ten semestr pozwoli zdobyć podstawową wiedzę i umiejętności w zakresie zarówno ochrony, jak i też oceny bezpieczeństwa systemów teleinformatycznych oraz pozwoli zainteresowanym tematyką bezpieczeństwa na dalsze samodzielne zgłębianie tego niezwykle istotnego nie tylko dla informatyki działu wiedzy.

**2. Agenda**

## Lab1 - Wstęp

## Lab2 – Podstawowe techniki kryptograficzne

## Lab3 – Algorytmy strumieniowe i blokowe

## Lab4 – Algorytmy asymetryczne

## Lab5 – Ataki na algorytmy kryptograficzne

## Lab6 – Kryptograficzne funkcje skrótu

## Lab7 – Zastosowania algorytmów kryptograficznych

## Lab8 – Zagrożenia w sieciach informatycznych

## Lab9 – Bezpieczna komunikacja sieciowa

## Lab10 – OSINT

## Lab11 – Rekonesans sieciowy

## Lab12 – Wykorzystanie podatności

## Lab13 – Bezpieczeństwo WEB cz.1

## Lab14 – Bezpieczeństwo WEB cz.2

## Lab15 – Powtórzenie wiadomości

**3.Podstwowe informacje i zasady pracy.**

Student powinien być przygotowany do każdego laboratorium. Oznacza to, że powinien najpierw przeczytać instrukcję i zapoznać się z elementami wymienionymi we wstępie.

W trakcie zajęć studenci wykonują czynności opisane w instrukcji i zapisują wyniki w raporcie z zajęć. Raport powinien również zawierać odpowiedzi na pytania i/lub rozwiązania problemów. Po zakończeniu zajęć studenci muszą zamieścić swoje raporty w miejscu wskazanym przez prowadzącego. Podczas kolejnych zajęci studenci powinni być przygotowani do odpowiedzi na pytania związane z wykonywaną pracą i raportem.

Każdy student powinien:

1. Śledzić bieżące informacje na stronach kursu na <http://eportal.pwr.wroc.pl/>, MS Teams, oraz przesyłanych na e-mail
2. Ogólna procedura
   1. Pobierz instrukcję laboratoryjną
   2. Dowiedz się, co jest potrzebne do pomyślnego wykonania laboratorium (co powinieneś wiedzieć, jakich narzędzi użyć itp.)
   3. Wykonaj polecenia zawarte w instrukcji
   4. Po (w trakcie) wykonywania poleceń sporządź raport zawierający w szczególności:
      * krótkie podsumowanie wykonanych kroków i otrzymanych wyników (zrzuty ekranowe, wywołania instrukcji z parametrami, itp.) – Uwaga! Istotny jest również styl prezentacji, nie chodzi o to, aby w raporcie znalazło się „100 zrzutów ekranowych”.
      * podsumowanie przebiegu i otrzymanych wyników ćwiczenia, odpowiedź na pytania (jeżeli są w instrukcji laboratoryjnej)
   5. Przekaż raport na <http://eportal.pwr.wroc.pl/>
   6. Każdy raport podlega ocenie.
   7. Ocena (liczba punktów) za raport odpowiada jego zawartości oraz uzależniona jest również od punktualności przekazywanych wyników.
   8. Do wcześniej wykonanych raportów, czy też podczas laboratorium prowadzący może zadać dodatkowe pytania związane z treścią laboratorium czy też tematem ćwiczenia.
3. **Narzędzia**
   1. **CrypTool 1**

Aplikacja CrypTool jest darmową aplikacją e-learningową dla systemu Windows. Można go używać do analizowania algorytmów kryptograficznych jak i ich praktycznego stosowania. Aktualna wersja aplikacji CrypTool ([Download](https://www.cryptool.org/en/ct1-downloads))) jest używana na całym świecie. Wspiera ona zarówno współczesne metody nauczania w szkołach i na uczelniach, jak i szkolenia dla pracowników i urzędników.

Aktualna wersja oferuje następujące możliwości:

* Liczne klasyczne i nowoczesne algorytmy kryptograficzne (szyfrowanie i odszyfrowywanie, generowanie kluczy, bezpieczne hasła, uwierzytelnianie, bezpieczne protokoły, ...)
* Wizualizacja kilku metod (np. Cezar, Enigma, RSA, Diffie-Hellman, podpisy cyfrowe, AES)
* Kryptoanaliza niektórych algorytmów (np. Vigenère, RSA, AES)
* Metody kryptoanalityczne (np. entropia, n-gramy, autokorelacja)
* Metody pomocnicze (np. testy pierwszości, faktoryzacja, kodowanie Base64)
* Przewodnik po teorii liczb
* Kompleksowa pomoc online
* Skrypt pomocniczy z dodatkowymi informacjami na temat kryptologii
  1. **VirtualBox**

Pobierz i zainstaluj najnowszą wersję [Oracle VirtualBox](https://www.virtualbox.org/) lub inne oprogramowanie witualizacyjne, które pozwoli Ci uruchomić narzędzia wymagane w laboratoriach (Cryptool, Kali Linux, itp.). Wspierana obecnie wersja to 6.1.38.

* 1. **Kali Linux**

Podczas badań laboratoryjnych będziemy korzystać głównie z narzędzi bezpieczeństwa zawartych w [Kali Linux. Kali Linux (Kali)](https://www.kali.org/downloads/) to dystrybucja Linuksa, która została opracowana z naciskiem na zadanie testowania bezpieczeństwa. Poprzednio Kali Linux był znany jako BackTrack. Kali Linux zawiera szereg narzędzi, które mogą być używane podczas procesu testów penetracyjnych. Narzędzia do testów penetracyjnych zawarte w systemie Kali Linux można podzielić na następujące kategorie:

* + **Information gathering**: Kategoria ta zawiera kilka narzędzi, które mogą być wykorzystane do zbierania informacji o DNS, IDS/IPS, skanowaniu sieci, systemach operacyjnych, routing, SSL, SMB, VPN, voice over IP, SNMP, adresach e-mail i VPN.
  + **Vulnerability assessment**: W tej kategorii można znaleźć narzędzia do skanowania luk bezpieczeństwa. Zawiera ona również narzędzia do oceny sieci Cisco oraz narzędzia do oceny luk w kilku serwerach baz danych. Kategoria ta zawiera również kilka narzędzi do usuwania luk.
  + **Web applications**: Kategoria ta zawiera narzędzia związane z aplikacjami internetowymi, takie jak skaner systemu zarządzania treścią, eksploitacja baz danych, fuzzery aplikacji internetowych, proxy aplikacji internetowych, web crawlery i skanery luk internetowych.
  + **Password attacks**: W tej kategorii znajduje się kilka narzędzi, które mogą być wykorzystane do przeprowadzania ataków na hasła, zarówno w trybie online, jak i offline.
  + **Exploitation tools**: Kategoria ta zawiera narzędzia, które mogą być wykorzystane do wykorzystania luk występujących w środowisku docelowym. Można tu znaleźć narzędzia do eksploitowania sieci, Internetu i bazy danych. Zawiera również narzędzia do przeprowadzania społecznych ataków i zdobywania informacji.
  + **Sniffing and spoofing**: Narzędzia z tej kategorii mogą być używane do podsłuchiwania sieci i przechwytywania ruchu sieciowego. Kategoria ta obejmuje również narzędzia do spoofingu sieciowego, takie jak Ettercap i Yersinia.
  + **Maintaining access**: Narzędzia w tej kategorii będą mogły pomóc w utrzymaniu dostępu do maszyny docelowej. Być może będziesz musiał uzyskać najwyższy poziom uprawnień w maszynie, zanim będziesz mógł wykorzystać narzędzia z tej kategorii. Tutaj możesz znaleźć narzędzia do backdooringu systemu operacyjnego i aplikacji internetowej oraz tunelowania.
  + **Reporting tools**: W tej kategorii znajdziesz narzędzia, które pomogą Ci udokumentować proces i wyniki testów penetracyjnych.
  + **System services**: Kategoria ta zawiera kilka usług, które mogą być użyteczne podczas wykonywania zadań testowych, takich jak: usługa Apache, usługa MySQL, usługa SSH oraz usługa Metasploit.

Aby ułatwić życie testera penetracyjnego, Kali Linux dostarczył nam kategorię o nazwie **Top 10 Security Tools**. Jak sugeruje nazwa, jest to 10 najlepszych narzędzi bezpieczeństwa powszechnie używanych przez pentesterów. Narzędzia wchodzące w skład tej kategorii to aircrack-ng, burp-suite, hydra, john, maltego, metasploit, nmap, sqlmap, wireshark i propxy.

Poza tym, że Kali Linux zawiera narzędzia, które mogą być użyte do zadania testowania penetracyjnego, jest również wyposażony w kilka narzędzi, które można wykorzystać do następujących celów:

* + **Wireless attacks**: Kategoria ta obejmuje narzędzia do atakowania urządzeń Bluetooth, RFID/ NFC i bezprzewodowych.
  + **Reverse engineering**: Ta kategoria zawiera narzędzia, które mogą być używane do debugowania programu lub dezasemblacji pliku wykonywalnego.
  + **Stress testing**: Ta kategoria zawiera narzędzia, które mogą być wykorzystane do pomocy w testach warunków skrajnych w sieci, środowisku bezprzewodowym, sieci Web i środowisku VOIP.
  + **Hardware hacking**: Narzędzia z tej kategorii mogą być używane w pracy z urządzeniami Android czy Anduino.
  + **Forensics**: W tej kategorii znajduje się kilka narzędzi, które mogą być wykorzystane w cyfrowych badaniach śledczych, takich jak pozyskiwanie obrazu dysku twardego, odzyskiwanie plików i analizowanie obrazu dysku twardego. Aby prawidłowo korzystać z możliwości kryminalistycznych w Kali Linux, musisz przejść do Kali Linux Forensics | No Drives or Swap Mount w menu startowym. Dzięki tej opcji, Kali Linux nie będzie montował dysków automatycznie, co pozwoli zachować ich integralność.
  1. **Metasploitable**

[Metasploitable 2](https://sourceforge.net/projects/metasploitable/) ma wiele luk w systemie operacyjnym, sieci i aplikacjach internetowych. Informacje o podatnościach zawartych w Metasploitable 2 można znaleźć na stronie [Rapid7 site](https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/).

Istnieje również nowasza wersja: [Metasploitable 3](https://information.rapid7.com/metasploit-framework.html).

* 1. **pfSense**

[pfSense](https://www.pfsense.org/download/) jest swobodnie dystrybuowanym i otwartym systemem operacyjnym BSD wywodzącym się z dobrze znanego projektu m0n0wall, ale o radykalnie różnych celach, takich jak wykorzystanie Packet Filter i najnowszych technologii FreeBSD.

Projekt ten może być używany zarówno jako router jak i firewall. Zawiera system pakietowy, który pozwala administratorom systemu na łatwą rozbudowę produktu bez dodawania potencjalnych luk w zabezpieczeniach do podstawowej dystrybucji.

Kluczowe funkcje obejmują najnowocześniejszą zaporę sieciową, równoważenie obciążeń przychodzących i wychodzących, tabelę stanów, NAT (Network Address Translation), wysoką dostępność, VPN (Virtual Private Network) z obsługą IPsec, PPTP i OpenVPN, serwer PPPoE, Dynam-ic DNS, portal typu captive, raportowanie i monitorowanie.

Jest to aktywnie rozwijany system operacyjny typu firewall, dystrybuowany jako Live CD, obraz ISO, w formach instalatorów w pamięci USB, a także NanoBSD/nośniki wbudowane. Obecnie obsługiwane są zarówno 64-bitowe (amd64), jak i 32-bitowe (i386) formaty sprzętowe.

* 1. **Burp suite (community edition)**

[Burp Suite](https://portswigger.net/burp) to zintegrowana platforma do przeprowadzania testów bezpieczeństwa aplikacji internetowych. Jej różnorodne narzędzia płynnie współpracują ze sobą, wspierając cały proces testowania, od wstępnego mapowania i analizy powierzchni ataku, aż po wyszukiwanie i wykorzystywanie luk w zabezpieczeniach.

Burp daje Ci pełną kontrolę, pozwalając na połączenie zaawansowanych technik manualnych z najnowocześniejszą automatyzacją, aby Twoja praca była szybsza, bardziej efektywna i przyjemniejsza.

* 1. **Snort**

System wykrywania i zapobiegania włamaniom do sieci wyróżnia się w analizie ruchu i logowaniu pakietów w sieciach IP. Poprzez analizę protokołu, wyszukiwanie treści i różne preprocesory, Snort wykrywa tysiące robaków, próby wykorzystania luk, skanowania portów i inne podejrzane zachowania. Snort wykorzystuje elastyczny, oparty na regułach język do opisu ruchu, który powinien być pobierany lub przekazywany, oraz modułowy mechanizm wykrywania. Warto również zwrócić uwagę na [Basic Analysis and Security Engine (BASE)](http://secureideas.sourceforge.net/), interfejs webowy do ostrzeżeń [Snort](https://www.snort.org/).

* 1. **OWASP ZAP**

[Zed Attack Proxy (ZAP)](https://www.zaproxy.org/) jest darmowym, open-source'owym narzędziem do testowania bezpieczeństwa, utrzymywanym w ramach projektu Open Web Application Security Project (OWASP). ZAP jest zaprojektowany specjalnie do testowania aplikacji internetowych i jest zarówno elastyczny jak i rozszerzalny.

ZAP jest narzędziem, które w istocie jest "man-in-the-middle proxy". Stoi on pomiędzy przeglądarką testera a aplikacją sieciową, dzięki czemu może przechwytywać i sprawdzać komunikaty wysyłane pomiędzy przeglądarką a aplikacją sieciową, w razie potrzeby modyfikować zawartość, a następnie przekazywać te pakiety dalej do miejsca docelowego. Może być wykorzystywany jako samodzielna aplikacja oraz jako proces wewnątrzsystemowy.

* 1. **Kilka innych narzędzi, które mogą okazać się przydatne**
* [Network Security Toolkit (NST 32)](http://www.networksecuritytoolkit.org/nst/index.html)
* [Fedora Security Spin](https://fedoraproject.org/wiki/Security_Lab)
* [BackBox](https://www.backbox.org/)
* [Parrot Security](https://www.parrotsec.org/)
* [Talis OS](https://tails.boum.org/index.en.html)
* [Qubes OS](https://www.qubes-os.org/)

1. **Konfiguracja środowiska**
2. Skonfiguruj maszynę wirtualną za pomocą VirtualBox
   1. Zdefiniuj nową sieć NAT (VirtualBox – Narzędzia – Ikona listy - Sieć)

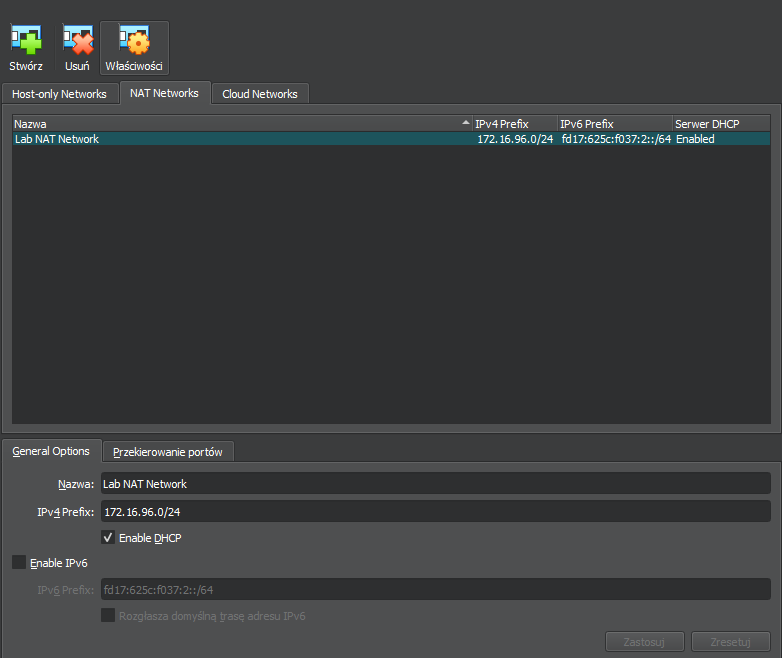
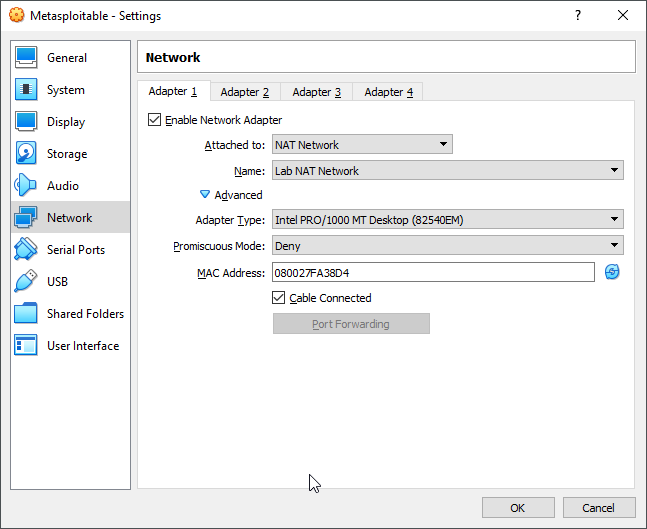


Fig.1 Konfiguracja sieci –

* 1. Stwórz maszyny wirtualne: Kali, Metasploitable oraz inne rekomendowane przez prowadzącego
  2. Skonfiguruj interfejsy sieciowe maszyn (połącz je z wcześniej stworzoną siecią NAT)



* 1. Uruchom wszystkie maszyny korzystając z poniższych danych:
     1. Kali (stud,stud),
     2. Ubuntu Server (stud, stud)
     3. Metasploitable (msfadmin,msfadmin)
  2. (Opcjonalnie) W celu uzyskania połączenia SSH do maszyny wirtualnej z maszyny hosta należy:
     1. Otworzyć terminal
     2. Przejść do folderu z zainstalowanym VirtualBoxem
     3. Wykonać następujące polecenie:

**VBoxManage.exe guestproperty enumerate "Kali Lab 2022/2023"**

* + 1. Adres IP można sprawdzić tutaj:

Obraz zawierający tekst, zrzut ekranu, chmura

Opis wygenerowany automatycznie

* 1. Zaktualizuj pakiety Kali
     1. apt-get update
     2. apt-get upgrade
  2. Sprawdź adresy IP maszyn wirtualnych (ifconfig) i zweryfikuj możliwość komunikacji pomiędzy maszynami (ping)
  3. Skonfiguruj udostępniane foldery
     1. Podczas wykonywania testów penetracyjnych, może pojawić się potrzeba dzielenia folderów pomiędzy maszyną fizyczną a maszynami wirtualnymi np. by zapisać wyniki testów na dysku maszyny hostującej.
  4. HTTP
     1. Wpisz następującą komendę w konsoli, aby uruchomić serwer HTTP Apache: **service apache2 start**
     2. W przypadku bezbłędnej konfiguracji, system wyświetli następującą wiadomością: [....] Starting web server: apache2 ok
     3. Następujące komendy wyłączą serwer HTTP: **service apache2 stop**
     4. W przypadku bezbłędnej konfiguracji, system wyświetli następującą wiadomością: [....] Stopping web server: apache2 ok waiting
     5. Należy pamiętać, że restart lub wyłączenie maszyny wirtualnej skutkuje wyłączeniem serwera Apache. Oprogramowanie Apache daje możliwość automatycznego uruchamiania serwera HTTP przy starcie systemu, wystarczy w konsoli wpisać komendę:

**update-rc.d apache2 defaults**

* 1. **MySQL**
     1. Wpisz następującą komendę w konsoli:

**service mysql start**

* + 1. Następnie, wyświetli się wiadomość:

**[ ok ] Starting MySQL database server: mysqld . . ..**

**[info] Checking for tables which need an upgrade, are corrupt or were not closed cleanly..**

* + 1. Użyj klienta MySQL, aby sprawdzić czy serwer z bazą jest już uruchomiony oraz, aby się z nim połączyć. Utwórz użytkownika (root), korzystając z poniższej komendy:

**mysql -u root –p**

* + 1. System wyświetli następujące komunikaty:

**Enter password:**

**Welcome to the MySQL monitor. Commands end with ; or \g.**

**Your MySQL connection id is 42**

**Server version: 5.5.30-1 (Debian)**

Od teraz możesz wykonywać komendy SQL w konsoli. Aby rozłączyć się z serwerem wystarczy w konsoli wpisać quit

* + 1. Wykonaj następujące kroki, aby zatrzymać serwis MySQL:
       1. GUI  
          **Kali Linux** | **System Services** | **MySQL** | **mysql stop**;
       2. Konsola  
          **service mysql stop**
    2. Po tym, system wyświetli następującą wiadomość:

**[ ok ] Stopping MySQL database server: mysqld.**

* + 1. Tak jak w przypadku serwera Apache, można użyć następującej komendy, aby serwer MySQL uruchamiał się automatycznie po starcie maszyny wirtualnej:

**update-rc.d mysql defaults**

* 1. SSH
     1. Wpisz następującą komendę w konsoli:

**service ssh start**

* + 1. Następnie, wyświetli się wiadomość:

**[ ok ] Starting OpenBSD Secure Shell server: sshd.**

* + 1. Wpisz w konsoli następującą komendę, aby zatrzymać serwis SSH:

**service ssh stop**

* + 1. Po tym, system wyświetli następującą wiadomość:

**[ ok ] Stopping OpenBSD Secure Shell server: sshd.**

* + 1. Serwer SSH może być uruchamiany automatycznie po starcie Kali Linux:

**update-rc.d ssh defaults**

1. **Pytania**
2. Jaki jest cel i zakres testów penetracyjnych?
3. Jaka jest różnica między testami penetracyjnymi a wykrywaniem podatności?
4. Co to jest „etyczny hacking”?
5. Jakie są podstawowe rodzaje testów penetracyjnych?
6. Opisz krótko (cel, zakres) niektóre metodologie testów penetracyjnych (OSSTMM, ISSAF, OWASP, WASC-TC, PTES)