

## Dobre Praktyki

- [Start](#)
- [Wstęp](#)
- [Uniwersalny Zestaw Zasad](#)
- [Zbędne i Niebezpieczne Aplikacje, Aktualizacja](#)
- [Autostart Aplikacji](#)
- [Wyszukanie Niezabezpieczonych Danych](#)
- [Dane Bez Właściciela](#)
- [Wyłączenie USB](#)
- [Nasłuchujące Porty](#)
- [Polityki Haseł](#)
- [Wygasanie Hasła](#)
- [Historia Haseł](#)
- [Blokowanie Kont](#)
- [Audyt Superużytkowników](#)
- [Wyszukiwanie Kont Bez Haseł](#)
- [Zabezpieczenie Kernela](#)
- [Automatyzacja Bezpieczeństwa](#)
- [Dobre Praktyki](#)
- [Praca Domowa](#)

## Sieć

- [Start](#)
- [Bezpieczeństwo Protokołów Sieciowych](#)
- [sysctl.conf](#)
- [Bezpieczeństwo SSH](#)
- [SSH – Logowanie Kluczem](#)
- [SSH – Zmiana Portu](#)
- [Dodatkowe Zabezpieczenia SSH](#)
- [SSH – Klucz z Windowsa](#)
- [Obrona Przed Najpopularniejszymi Atakami](#)
- [Dostęp Zdalny](#)
- [Wybór VPN](#)
- [Zabezpieczenia Sieci LAN, WAN](#)
- [TCP Wrappers](#)
- [Monitoring Sieci](#)
- [Aktywne Połączenia na Serwerze](#)
- [Netstat i Monitoring Połączeń](#)
- [Ochrona Przed DDoS](#)
- [Podejrzane Próby Połączeń](#)
- [Praca Domowa](#)

## Audyt

- [Start](#)
- [Audyty](#)
- [Spis Podatności](#)
- [Instalacja Lynis](#)
- [Wykonanie Audytu](#)
- [Sprawdzanie i Naprawianie Podatności](#)
- [Skanowanie Dockerfile](#)
- [Skanowanie Portów](#)
- [Nmap](#)
- [Metody Skanowania Portów](#)
- [Audyty Logów](#)
- [Narzędzia Wstępnej Analizy Logów](#)
- [Skanowanie WWW](#)
- [Łamanie Haseł Użytkowników](#)
- [Praca Domowa](#)

## Ostateczny Hardening

- [Wstęp](#)
- [Zabezpieczenia systemu operacyjnego](#)
- [IDS, HIDS i SIEM](#)
- [Systemy SIEM](#)
- [Monitorowanie Logów W Zabbix](#)
- [Instalacja SIEM](#)
- [Dodanie Zasobu Do SIEM](#)
- [Pierwszy Kontakt z SIEM](#)
- [Wykrywanie Włamań](#)
- [Raporty z SIEM](#)
- [Obrona Przed Włamaniami](#)
- [Reguły w SIEM](#)
- [W Trakcie Ataku](#)
- [Reakcja na atak](#)
- [Wektory Ataku i Wykrywanie](#)
- [Honeypot](#)
- [Usługi](#)
- [DMZ](#)
- [Praca Domowa](#)

## Firewall

- [Wstęp](#)
- [Firewall Na Linuxie](#)
- [Strefy](#)
- [Zarządzanie i Tworzenie Usług](#)
- [Odblokowanie i Blokowanie Portów](#)

- [Zarządzanie Strefami](#)
- [Źródła Ruchu](#)
- [Dostęp i Wykluczenia](#)
- [Przekierowanie Portów](#)
- [Lockdown](#)
- [Przekazywanie Wewnątrz Strefy](#)
- [NAT](#)
- [Maskarada](#)
  
- [Polityki](#)
- [Automatyzacja](#)
- [Przykład Automatyzacji – DMZ](#)
- [„Schron”](#)
- [Praca Domowa](#)
- [Podsumowanie Wiedzy](#)

## **SELinux**

- [Wstęp](#)
- [Pakiety SELinuxa](#)
- [Tryb i Polityki](#)
- [Kontekst](#)
- [Etykiety](#)
- [Przejścia Domen](#)
- [Zmiana Kontekstu](#)
- [Semanage, Reguły, Kontekst](#)
- [Zmienne Polityki](#)
- [Odblokowanie Portów](#)
- [Logi](#)
- [Audyty Logów](#)
- [Rozwiązywanie Problemów z SELinuxem](#)
- [Moduły](#)
- [ausearch, audit2allow i semodule](#)
- [Własny Skrypt](#)
- [Elementy Skryptu](#)
- [Usuwanie Modułów](#)
- [Tryb Permissive](#)
- [Seinfo i Seseach](#)
- [Praca Domowa](#)
- [Podsumowanie Wiedzy](#)

## **Kerberos i Uwierzytelnianie**

- [Wstęp](#)
- [FreeIPA](#)

- [Kerberos](#)
- [Pozostałe Elementy FreeIPA](#)
- [Przygotowanie Do Instalacji](#)
- [Kerberos – Instalacja](#)
- [Panel FreeIPA](#)
- [Konfiguracja Klienta](#)
- [Klient Kerbersosa](#)
- [Szczegóły Klienta](#)
- [Uwierzytelnianie](#)
- [Klucze i Logowanie](#)
- [2FA](#)
- [Praca Domowa](#)

## Dostęp Do Danych

- [Wstęp](#)
- [PAM](#)
- [Nadawanie Uprawnień](#)
- [Uprawnienia](#)
- [ACL i Kerberos](#)
- [Audyty Uprawnień](#)
- [Dziwne Zachowania Użytkowników](#)
- [Audyty Dostępu Do Danych](#)
- [Limitowanie Wykonywania Poleceń](#)
- [Użytkownicy w SELinux](#)
- [NAS](#)
- [Polityka Przyznawania Uprawnień](#)
- [Różne Poziomy Zabezpieczenia](#)
- [Praca Domowa](#)

## Usługi

- [Wstęp](#)
- [Zabezpieczanie Usług](#)
- [Dynamiczni Użytkownicy](#)
- [Mount Namespaces](#)
- [Hardening Usługi \(przykład\)](#)
- [Audyty i Hardening Systemd](#)
- [Audyty Dostępu Procesów](#)
- [Separacja Partycji](#)
- [setuid, setgid](#)
- [Konteneryzacja, Wirtualizacja](#)
- [Rootkity, Trojany, etc...](#)
- [Bezpieczeństwo Repozytoriów](#)
- [Bezpieczeństwo Aktualizacji](#)

- [Praca Domowa](#)

## „Shakowany” Moduł

- [Wstęp](#)
- [Jak Dobrze Zabezpieczyć Serwer?](#)
- [Powiadomienia o Zagrożeniach](#)
- [Ransomware](#)
- [Namespaces](#)
- [Rodzaje Namespaces](#)
- [PID Namespaces](#)
- [Tworzenie Namespaces](#)
- [Wylistowanie Namespaces](#)
- [fail2ban i nginx](#)
- [fail2ban – Ustawienia JAIL](#)
- [fail2ban – Dodatkowe Reguły](#)
- [Shodan](#)
- [Szyfrowanie Dysku](#)
- [Praca Domowa](#)

**Dołącz do kursu:**

<https://asdevops.pl/sec/>