
# Akademia Handlowa Nauk Stosowanych w Radomiu

# Bezpieczeństwo systemów komputerowych Laboratorium 1

**Radom 2021/2022**

# 1. Cel zadania

Systemy Unix-Like słyną przede wszystkim ze standardowych procedur zabezpieczenia systemu przed ewentualnym atakiem zdalnym lub lokalnym. Celem niniejszego laboratorium będzie poznanie zasad i możliwości zabezpieczenia systemu od strony lokalnej.

# 2. Potrzebne narzędzia.

- kompletny zestaw komputerowy z systemem operacyjnym Linux, dowolna dystrybucja
- nośnik USB lub narzędzie do tworzenia obrazów USB (+montowanie)

LUB

- kompletny zestaw komputerowy z dowolnym system operacyjnym
- oprogramowanie do wirtualizacji (VMWare, Hyper-B, VirtualBox, kvm)
- dowolna dystrybucja systemu Linux

LUB

- kompletny zestaw komputerowy z systemem operacyjnym Windows w wersji co najmniej 10
- uruchomiony składnik Podystem systemu Linux w systemie Windows
- dostęp do Windows Store celem pobrania dowolnej dystrybucji systemu Linux dla Windows

# 3. Informacje wstępne

Systemy Unix-like, szczególnie najnowsze i najpopularniejsze dystrybucje, uchodzą za jedne z lepiej zabezpieczonych systemów operacyjnych. Chociaż informacje o ich możliwościach ochronnych nie są w pełni odzwierciedlone w rzeczywistości - często zdarza się, że oprogramowanie stosowane w tych systemach ma określone luki i braki w zabezpieczeniach – to rozwiązania stosowane tuż na poziomie pierwszej konfiguracji są jednymi z lepszych:

- Brak dostępu domyślnego użytkownika do folderów spoza /home/<nazwa_uzytkownika>
- Narzędzia do aktualizacji i konfiguracji systemu zarezerwowane są dla super użytkownika
- Skrypt sudo pozwalajacy/zabraniający wykonywania określonych czynności w systemie
- Domyślnie uruchomiony i skonfigurowany filtr sieciowy (firewall), rezydujący bezpośrenio w jądrze systemu
- Możliwość instalacji na szyfrowanej partycji, możliwość szyfrowania rozruchu systemu
- Blokowanie dostępu do zarządzania zdalnego (wymaga najczęściej wstępnej konfiguracji, ręcznego uruchomienia)

Systemy te podlegają stałej modyfikacji, dodawane są nowe narzędzia, które niwelują problemy poprzednich wersji. Niejednokrotnie wykorzystywane skrypty są przebudowywane, zmieniane ich wstępne opcje. Wszystko to powoduje, że rozwiązania te faktycznie mogą sprawiać wrażenie nie do pokonania.
Jakkolwiek rozwiązania te mogą być dość bezpieczne trzeba mieć na uwadze, że należy stale podnosić bezpieczeństwo naszego systemu wykonując dodatkową, indywidualną konfigurację elementów zabezpieczających system. Indywidualna konfiguracja ma taką zaletę, że nie w razie ewentualnego ataku domyślne kierunki ataku będą dla atakującego niewystarczające - będzie musiał próbować indywidualnego podejścia, co z kolei nam, administratorom, da więcej czasu na obronę naszych zasobów.
Laboratorium nie skupia się jedynie na elementach lokalnych lecz obejmuje także niektóre aspekty bezpieczeństwa sieciowego, które w przypadku systemu Unix-like jest tożsame z sieciowym (systemy Unix-like naturalnie konfigurowane są jako systemy pracujące w sieci).

# 4. Przebieg.

Laboratorium ma charakter doświadczalno-praktyczny i ma na celu ukazanie podstawowych możliwości narzędzi i konfiguracji dowolnego systemu Unix-like na różnych etapach konfiguracji:

- Zainstalować systemu na szyfrowanym dysku twardym wykorzystującym jedną z dostępnych technologii (np. LUKS); należy wskazać zalety i wady takiej konfiguracji do użytku codziennego jak i biznesowego (np. utworzenie takiego rozwiązania na serwerze HTTP).
- Przetestować i wskazać aspekty bezpieczeństwa instalacji systemu na logicznym wolumenie (LVM).
- Sprawdzić możliwości edycji grub w taki sposób, by niemożliwe było wyświetlenie menu wyboru systemu. Czy takie rozwiązanie ma wady ewentualnie czy jest możliwość ominięcia tego rozwiązania? Czy bezpośredni dostęp do edycji menu grub może nieść konsekwencje dla lokalnego systemu Unix-like?
- Sprawdzić możliwości zablokowania szybkiej edycji startowa systemu (np. by była możliwa jedynie po podaniu hasła). Omówić sensowność takiego rozwiązania.
- Częstą słabością systemu informatycznego jest podawanie przez pracowników haseł do usług (przykładowo przy logowaniu systemu). Określone rozwiązania technologiczne w systemach Linux pozwalają na utworzenie nośnika autoryzacyjnego. Proszę sprawdzić możliwość logowania się do systemu przy pomocy tak przygotowanego nośnika. Proszę wskazać mocne i słabe strony tego rozwiązania
- Niekiedy może być pożądane uruchamianie systemu z zewnętrznego nośnika (np. USB lub poprze sieć). Systemy Unix-like umożliwiają takie działanie. Proszę spróbować spreparować system do takiego uruchamiania.
- Sudo to świetne narzędzie pozwalające na nadawanie lub odbieranie uprawnień określonym użytkownikom oraz grupom. Należy przepatrzeć kilka scenariuszy użycia sudo, w tym nadawania konkretnemu użytkownikowi praw superużytkownika, zezwolenie na uruchamianie określonych skryptów, nadanie uprawnienia do wykonywania określonych czynności.
- Systemy Unix-like posiadają zestawy dodatkowych zabezpieczeń, pozwalających na lepszą kontrolę przepływu danych, dostępu do danych, czy sposobu weryfikacji osoby zalogowanej. Należy sprawdzić i ocenić przydatność jednego z zestawów (może to być np. grsecurity, SELinux lub AppArmor).

# 5. Zakończenie

Rozwiązanie należy przesłać w postaci PDF zawierającym opis wykonywanych czynności oraz zrzuty ekranowe dokumentujące działanie określonej funkcjonalności na adres piotr_dobosz@int.pl, w temacie wiadomości zawierając frazę [AHNS_BSK].

# 6. Dodatki

https://www.linuxuprising.com/2021/02/how-to-login-with-usb-flash-drive.html
https://linuxconfig.org/linux-authentication-login-with-usb-device
https://askubuntu.com/questions/136165/how-to-create-an-iso-image-from-a-bunch-of-files-on-the-file-system
https://alternativeto.net/software/apparmor/