Kurs DevOps

Lista 4

5 i 6 listopada 2025

Jako że zazwyczaj w dużych grupach znajduje się co najmniej jeden użytkownik Windowsa, to informuje się, iż zadania należy wykonywać z linii poleceń, o ile nie powiedziano inaczej w treści.

Zadanie 1.
Zapoznaj się z `docker swarm`, przygotuj jego krótkie omówienie i zademonstruj przykładowe użycie.

Zadanie 2.
Zapoznaj się z `docker network`. Utwórz sieć dockera typu `bridge` i podłącz do niej 2 kontenery. Pokaż, że kontenery te są w stanie się komunikować. Czy są w stanie połączyć się z Internetem? Jak to zablokować?

Zadanie 3.
Przedstaw i zademonstruj użycie polecenia `unshare` i `nsenter`. Uruchom kontener dockera i pokaż, że separacja przestrzeni PID-ów rzeczywiście zachodzi. Użyj `nsenter`, by wejść do kontenera i uruchomić shella.

Uruchom dowolny proces z użyciem `firejail`, który ograniczy dostęp do systemu plików. Pokaż, że przy pomocy `nsenter` można uruchomić shella w tym ograniczonym widoku.

Zadanie 4.
Zaimplementuj własny kontener w stylu Dockera przy pomocy `unshare` i `nsenter`. Stwórz przestrzenie nazw zmapowane do plików, następnie:

- Zmapuj (ang. bind) katalog z hosta, który będzie pełnił funkcję współdzielonego wolumenu.
- Skonfiguruj gid i uid użytkownika.
- Zapewnij zamontowanie wymaganych plików systemowych (np. procfs).
- Skonfiguruj interfejs sieciowy do komunikacji z hostem (`veth(4)`, `ip-netns(8)`).
- Pokaż, że Twój kontener działa i jesteś w stanie go używać, w sposób odizolowany od reszty systemu.

Zadanie 5.
Wytłumacz czym są capabilities powiązane z plikami. Przy pomocy `getcap` znajdź wszystkie pliki binarne w Twoim systemie, które używają tej funkcjonalności. Czy dodatkowe uprawnienia są uzasadnione?

Uruchom kontener dockera i sprawdź z użyciem `ps` jakie uprawnienia otrzymują procesy wewnątrz kontenera. Czy widzisz jakieś ryzyko?

Pokaż, w jaki sposób uruchomić kontener ograniczając mu uprawnienia przyznawane domyślnie.

Zadanie 6.
Wyjaśnij czym jest SELinux i jak można go zastosować w celu zabezpieczenia kontenera dockera. Zademonstruj taką konfigurację na jakimś przykładzie.