

Bezpieczeństwo danych na dysku w świecie internetu SCR - Systemy Operacyjne

Michał Wieczorek

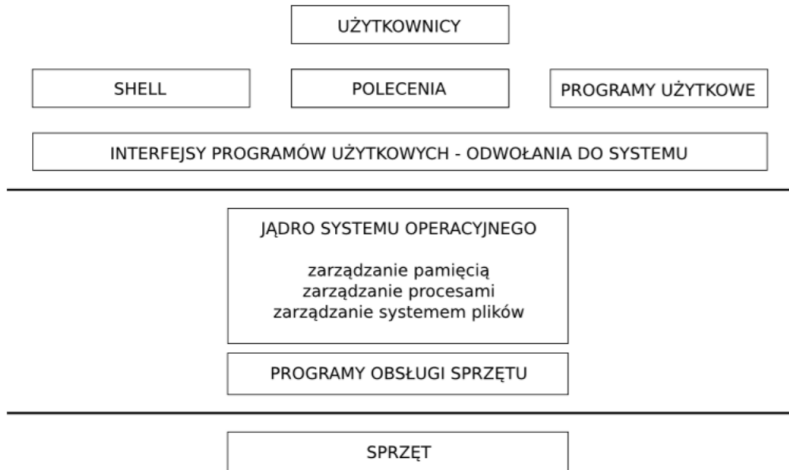
Automatyka i Robotyka, Wydział Elektroniki
Politechnika Wrocławska

26 listopada 2017

Plan prezentacji

- 1 Spis treści
- 2 Struktura systemu
- 3 Rodzaje zagrożeń
 - Buffer Overflow
 - Exploit
 - Kernel drivers
 - Statystyka
- 4 Metody zabezpieczania
 - Filtrowanie ruchu sieciowego
 - Wykrywanie włamań i kontrola plików
 - Ograniczenie szkód wywołanych włamaniem

Struktura systemu



Rodzaje zagrożeń



Rodzaje zagrożeń

CVE-2016-8655

Linux Kernel Flaw

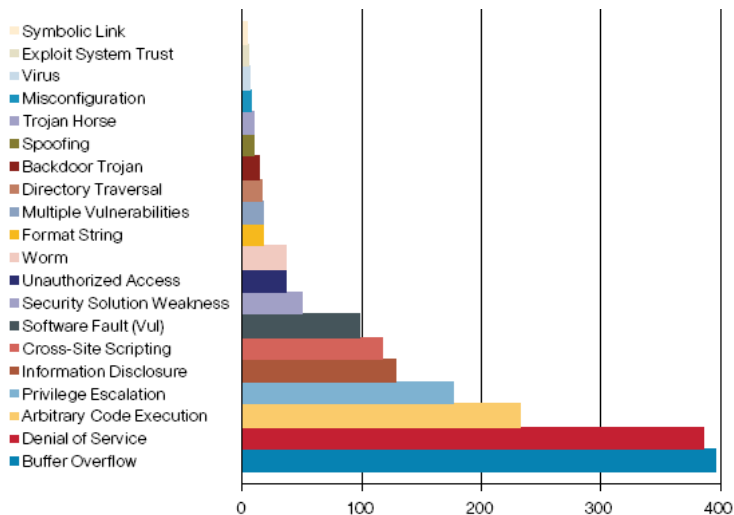
Exploit to Gain a Root Shell



Rodzaje zagrożeń



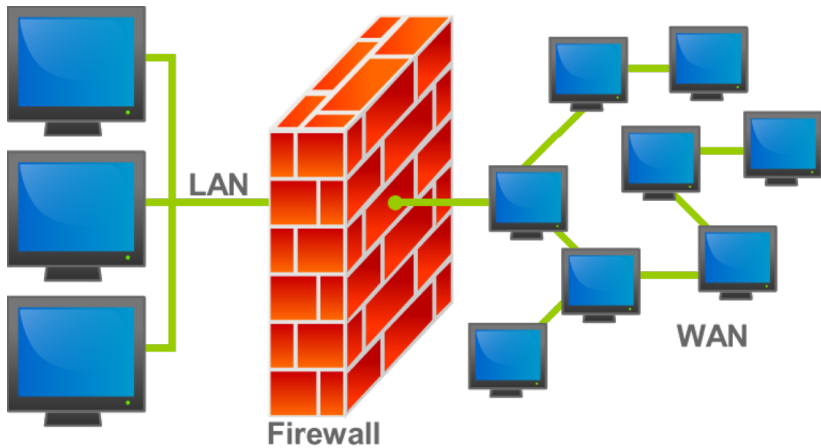
Rodzaje zagrożeń



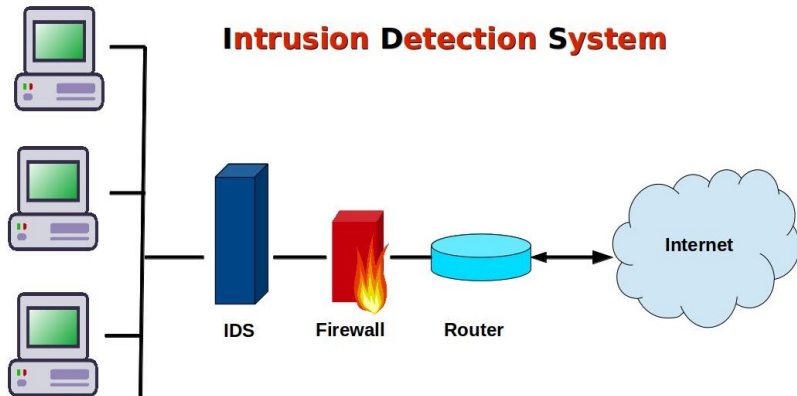
Podział zabezpieczeń na 3 główne grupy

- Mechanizmy filtrowania ruchu sieciowego
- Wykrywanie włamań i kontrola plików
- Ograniczenie szkód wywołanych włamaniem

Filtrowanie ruchu sieciowego



Wykrywanie włamań i kontrola plików



Ograniczenie szkód wywołanych włamaniami



Zakończenie

Dziękuję za uwagę :)