Wykład 6

Temat: Fikcja literacka, czyli bezpieczne systemy operacyjne

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Po co komu nasz serwer?

- dla sportu
- kradzież danych (wszystko się przyda)
- rozsyłanie spamu (osłabia naszą reputację)
- ataki na kolejne systemy (wewnętrzne lub zewnętrzne)
- podszywanie się pod naszą usługę (np phishing)
- eliminacja konkurencji (czyli nas)
- łamanie kluczy i haseł (po co marnować swój prąd?)
- bitcoin (jw.)

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Wektory ataku na system

- lokalne
    - kradzież nośników
    - uzyskanie uprawnień root (id=0) bez hasła
    - podłączenie dodatkowych urządzeń podsłuchowych
    - ...
- zdalne
    - odkrycie hasła
    - błąd w aplikacji
    - błąd w konfiguracji
    - podsłuchanie lub ingerencja w transmisję
    - ...

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt „*Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe*”
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Metody obrony

- ataki lokalne
    - dobre drzwi i zamki
    - ochrona
    - zamykane szafy rack
    - monitoring sieci lokalnej
- ataki zdalne
    - szkolenia użytkowników (ważne!)
    - inne silne hasła w każdej aplikacji (1Password, KeyPass)
    - częste aktualizowanie oprogramowania
    - szyfrowanie transmisji
    - prawidłowe stosowanie funkcji skrótu
    - rozbudowane scenariusze testów naszych aplikacji i usług
    - dwuetapowe uwierzytelnianie wszędzie gdzie się da
    - regularny i testowany backup
    - chwila namysłu zanim zrobimy zmianę konfiguracji

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Metody obrony

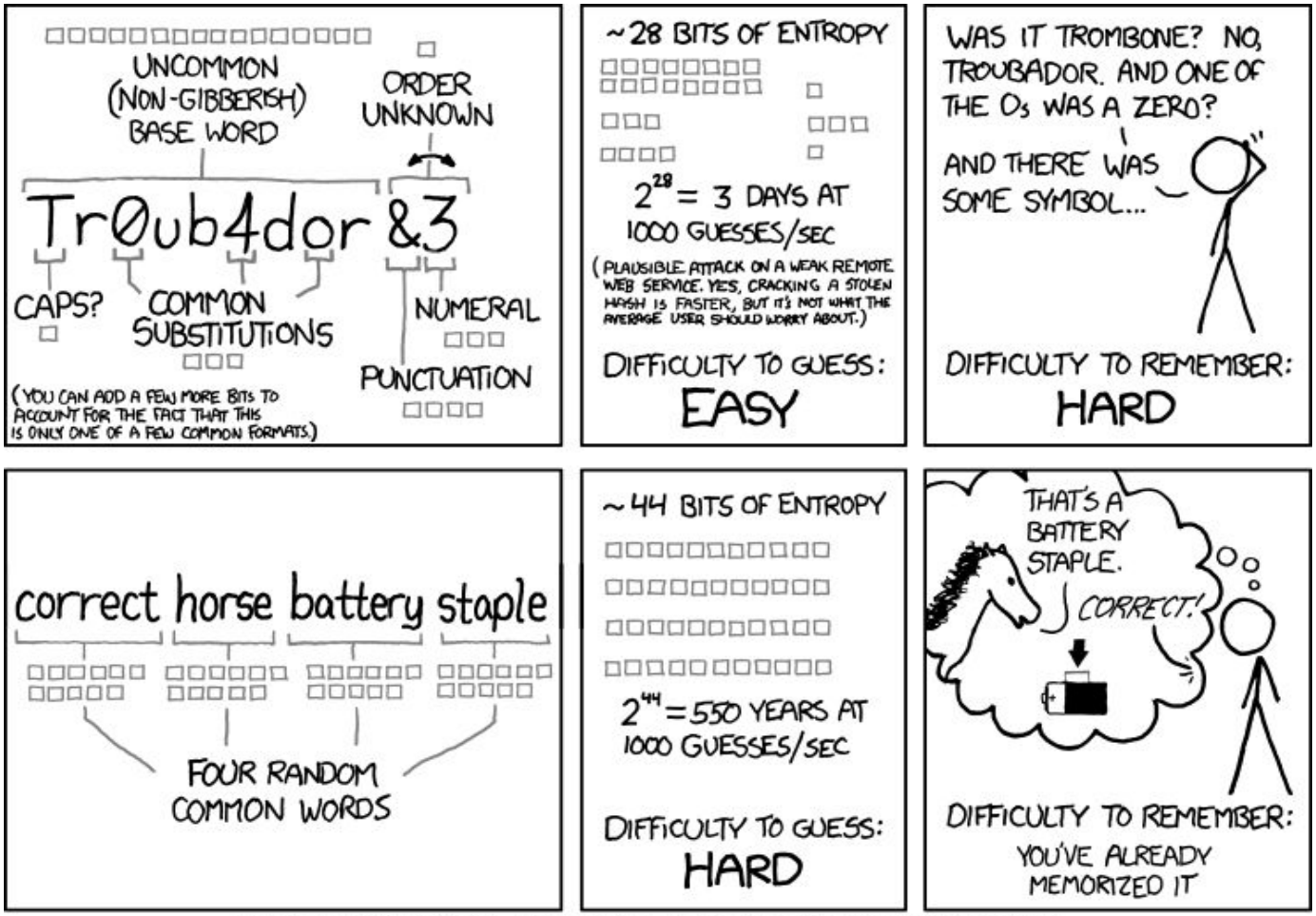
- ataki zdalne - cd
    - systemy IDS
    - monitorowanie ruchu do i z naszej sieci
    - regularny audyt bezpieczeństwa
    - przechowywanie logów na centralnym serwerze
    - w systemie uruchamiamy tylko niezbędne procesy
    - kasujemy/blokujemy niepotrzebne konta systemowe
    - powłoka /bni/false (lub inna restrykcyjna) na konta usług
    - maksymalnie restrykcyjne ustawienia zapory sieciowej

KAPITAŁ LUDZKI
CZŁOWIEK – NAJLEPSZA INWESTYCJA!

Projekt „*Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe*”
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

Kilka słów o silnych hasłach



Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08

Co robić po wykryciu włamania?

- odłączamy system od sieci lub przenosimy do sieci fizycznie wydzielonej
- uruchamiamy procedurę zmiany wszystkich haseł
- sprawdzamy logi zapory sieciowej i usług poszukując śladów ataku
- nasłuchiwanie ruchu próbującego opuścić serwer
- po odkryciu metody ataku łatamy dziurę na pozostałych maszynach i sprawdzamy czy nie zostały przejęte
- przywracamy zainfekowany serwer z pewnej kopii zapasowej lub czyścimy dokładnie dyski i instalujemy od nowa
- sporządzamy raport/notatkę z opisem incydentu i rozwiązaniem problemu

Projekt *„Przygotowanie i realizacja kierunku inżynieria biomedyczna – studia międzywydziałowe”*
współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego. Nr umowy UDA – POKL.04.01.01-00-236/08