



PROIDEA

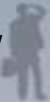

Fundacja Wspierania Edukacji Informatycznej

“Linux w realiach (nie)bezpiecznego e-Świata”

Marcin Kopeć & Przemysław Skowron
Spotkanie Open Source – 23.02.05 – Kraków

Linux w realiach (nie) bezpiecznego e-Świata

Plan:

- Dlaczego tu jesteśmy?
- Obalmy kilka stereotypów 
- Zagrożenia w przyrodzie, a system Linux
- Zalecenia 
- Podsumowanie



PROIDEA
Fundacja Wspierania Edukacji Informatycznej

Dlaczego tu jesteśmy?

- Edukacja drogą do bezpieczniejszego e-Świata:
 - Najlepszy hardware, software, polityki nie zapewnią bezpieczeństwa dla infrastruktury teleinformatycznej,
 - Najśłabszym ogniwem był, jest i będzie człowiek.
 - Brak świadomości o zagrożeniach nie daje szansy na wystawienie odpowiedniej obrony.

Linux w realiach (nie) bezpiecznego e-Świata

Dlaczego tu jesteśmy?

- W różnych środowiskach krążą niesłychane herezje:

Herezja #0x00

“Jako użytkownik LINUXa składam szczerze kondolencje wszystkim posiadaczom WINDOWSa

spróbuj napisać wirusa pod Linuxa :-))))”



PROIDEA

Fundacja Wspierania Edukacji Informatycznej

Dlaczego tu jesteśmy?

- W różnych środowiskach krążą niesłychane herezje:

Herezja #0x01

“Tak. Całkowicie popieram kolegę!!! Sam mam Mandrakelinux 10.1 i żadne wirusy czy trojany mi nie straszne. Pozdrawiam wszystkich linuxowców.”



PROIDEA
Fundacja Wspierania Edukacji Informatycznej

Linux w realiach (nie) bezpiecznego e-Świata

Dlaczego tu jesteśmy?

- W różnych środowiskach krążą niesłychane herezje:

Herezja #0x02

“Only one remote hole in the default install, in more than 8 years!”

Dlaczego tu jesteśmy?

- Mamy dość FANATYZMU w dowolnej formie:
 - Fanatycy utrudniają egzystencję innym użytkownikom, a brak świadomości pozwala im wierzyć w niestworzone rzeczy,
 - Nie “*nawracamy*”, edukujemy.



Dlaczego tu jesteśmy?

- Przyda się luzniejszy dzień ;-)

... bo tak naprawdę ... to praca
nauczyciela/trenera/instruktora/wychowawcy
nie jest prosta w żadnej formie.



PROIDEA

Fundacja Wspierania Edukacji Informatycznej

Obalmy kilka stereotypów

- “*Używam systemu Linux, jestem zwolniony z myślenia*”
 - Linux, *BSD, Solaris (już wkrótce!), etc. wciąż są tylko systemami operacyjnymi dającymi Wam szansę na wykorzystanie zasobów sprzętowych.



PROIDEA

Fundacja Wspierania Edukacji Informatycznej

Obalmy kilka stereotypów

- *“Moja dystrybucja jest najlepsza!”*
 - Twój system (dystrybucja) jest tak dobry jak Ty jesteś dobrym użytkownikiem, administratorem, aż w końcu inżynierem i architektem.
- Święte wojny dla (n/c)



Linux w realiach (nie) bezpiecznego e-Świata

Obalmy kilka stereotypów

• *“Nie obawiam się Twojego ataku robaczku :-)”*

- Slapper.Worm.b
- Ramen.worm
- Adore.Worm
- Slapper.Worm
- Brutessh

• Who next?



PROIDEA

Fundacja Wspierania Edukacji Informatycznej

Linux w realiach (nie) bezpiecznego e-Świata

Obalmy kilka stereotypów

- chakierzyna Rzeczypospolitej Polski:
 - system Linux (obecnie) nie jest trudniejszy w instalacji/obsłudze niż rozwiązania z Redmond,
- Użytkownicy Debiana nie są lepsi od użytkowników Red Hat'a
- więcej oprogramowania do celów “złośliwych”



PROIDEA

Fundacja Wspierania Edukacji Informatycznej

Zagrożenia w przyrodzie:

- Robaki:
 - Rozprzestrzeniają się przez sieć,
 - Wykorzystują błędy w oprogramowaniu, konfiguracji i nieuwadze,
 - Są bezlitosne, coraz bardziej samodzielne i bezczelne

Zagrożenia w przyrodzie:

- Robaki:

- Jak z nimi walczyć?

- Firewall,
 - Rozważna **aktualizacja** oprogramowania
 - Sumy MD5



Zagrożenia w przyrodzie:

- Trojany:
 - “*Dziękuję, możesz odejść*” - system z działającym trojanem nie jest już Twoim systemem.
- Wykorzystują naiwność i brak uwagi użytkownika,
- Walka podobnie jak z robakami



PROIDEA

Fundacja Wspierania Edukacji Informatycznej

Zagrożenia w przyrodzie:

- Inżynieria Socjalna:

- “zobacz jak przyśpieszy Ci system”
- “hehe, mam root'a!”

<pisklak> jak zainstalować ten pakiet?

<g0d> rpm -e --nodeps kernel

<g0d> później rpm -i pakiet

<pisklak> dzięki!



PROIDEA

Fundacja Wspierania Edukacji Informatycznej

Linux w realiach (nie) bezpiecznego e-Świata

Zalecenia:

- Instalujemy system
- Weryfikujemy samodzielnie startujące aplikacje
- Ustawiamy Firewall
- Uruchamiamy dostęp do sieci
- Cyklicznie uaktualniamy pakiety weryfikując sumy MD5
- Nie instalujemy oprogramowania z wątpliwego źródła
- Nie wykonujemy nieznananych poleceń



PROIDEA

Fundacja Wspierania Edukacji Informatycznej

NIE PRACUJEMY JAKO ROOT!!!

Linux w realiach (nie) bezpiecznego e-Świata

Wujek Dobra Rada radzi:

- Strona producenta (Vendor)
- Listy dyskusyjne (bugtraq, vuln-dev, etc.)
- CERT Polska (<http://www.cert.pl>)
- Secunia (<http://secunia.com>)
- OSVDB (<http://www.osvdb.org>)



PROIDEA
Fundacja Wspierania Edukacji Informatycznej

Security Announce:

Wyniki badań pracownika firmy Symantec porażająco obnażyły sposób podejścia developerów kernela do zgłaszania i rozpowszechniania informacji o błędach bezpieczeństwa.

NetBSD, OpenBSD, FreeBSD, Solaris, mają się całkiem dobrze.



PROIDEA

Fundacja Wspierania Edukacji Informatycznej

Podsumowanie:

- Zdecydowanie mniejsza ilość wirusów dla Linuksa wiąże się ściśle z jego popularnością,
- Open Sources daje możliwości dokonania wglądu w implementowane mechanizmy bezpieczeństwa, ale go **nie zapewnia**
- Wolność wyboru i dostęp do specyfikacji/kodu szansą na wypełnienie nadmiaru wolnego(?!) czasu ;-)



PROIDEA

Fundacja Wspierania Edukacji Informatycznej

Dziękujemy za uwagę.

marcin.kopec@proidea.org.pl

przemyslaw.skowron@proidea.org.pl