

Projekt, tematy, Bezpieczeństwo i ochrona danych

dr inż. Grzegorz J. Nalepa

wiosna 2007

1 Sposób opracowania

1.1 Organizacja zajęć

- grupy 2 lub 3 osobowe, konieczna *praktyczna* umiejętność pracy z Linuxem
- ponad 20 tematów opisowych i praktycznych, do doprecyzowania
- ok. 4 spotkania dla grupy
- realizacja konkretnów celów zgodnie z harmonogramem

1.2 Cel projektu

Rozwinięcie wiedzy nt. bezpieczeństwa i ochrony danych poprzez opracowanie konkretnego problemu w postaci:

1. *opisu*, przeglądu dokumentacji i opracowań,
2. *praktycznych* testów konkretnych technologii,
3. ew. *prezentacji* wyników, ok. 15min.

1.3 Organizacja pracy

milestones:

1. wstępny przegląd dokumentacji do wybranej podgrupy tematów, **9/26.2**,
2. wybór tematu, **26.2/5.3**,
3. plan pracy, *na piśmie*, przegląd tematyki, **12/19.3**,
4. konsultacje zakresu tematu, **2.4**,
5. szkic opisu + wyniki prac praktycznych, **16/23.4**,
6. wersja robocza całości + wszystkie wyniki praktyczne, **14.5**
7. wersja do recenzji, **21/28.5**
8. wersja finalna + ew. plan prezentacji, **4.6**
9. prezentacja wyników, ocena **11.6**

1.4 Rezultaty projektu

1. pismne opracowanie, opis problemu,
2. ew. pisemne opracowanie praktycznych eksperymentów, ew. pliki
3. ew. prezentacja

Format źródłowy opisów: L^AT_EX, word95, format wynikowy: PS/PDF, HTML. Format wynikowy prezentacji: slajdy w PDF.

2 Dziedziny

Systemy firewall Opis koncepcji systemu firewall. Opis konkretnej implementacji - jakie aspekty koncepcji realizuje. Przegląd dostępnych narzędzi do konfigurowania i zarządzania. Opis i ew. rozwinięcie przykładowego zastosowania. Praktyczne zastosowanie implementacji do wybranego przykładu. Podsumowanie.

TEMATY:

- próba budowy prostego firewall (Linux, BSD)
- próba budowy prostego VPN
- narzędzia wspomagające projektowanie systemów Firewall

Systemy MAC/ACL Opis koncepcji. Opis implementacji - jakie aspekty koncepcji realizuje. Przegląd dostępnych narzędzi do konfigurowania i zarządzania.

TEMATY:

- FreeBSD MAC http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/mac.html
- Linux GrSecurity ACL grsecurity.net
- SeLinux www.nsa.gov/selinux
- RSBAC Linux www.rsbac.org
- LIDS Linux lids.org

Systemy przechowywania danych Opis tematyki, zagadnień. Opis implementacji - jakie aspekty koncepcji realizuje. Przegląd dostępnych narzędzi do konfigurowania i zarządzania.

TEMATY:

- Linux LVM2 i software RAID
- Linux EVMS
- FreeBSD Vinum
- System plików Coda i inne rozproszone systemy plików
- AFS i klastrowe systemy plików
- porównanie kryptograficznych systemów plików Linux (aes-loop, dmccrypt),
- porównanie kryptograficznych systemów plików Free/NET/OpenBSD,
- rozwiązania dla kopii zapasowych: Bacula.

Bezpieczeństwo sieciowe Opis wybranego zagadnienia. Wybór praktycznego problemu. Przegląd narzędzi, testy.

TEMATY:

- narzędzia do bieżącego monitorowania ruchu w sieci, przegląd,
- monitorowanie usług sieciowych Nagios
- syntetyczny przegląd zabezpieczeń GrSecurity

Audyt i wykrywanie wtargnięć Opis problematyki. Wybór narzędzi i opracowanie przykładu. Analiza. Narzędzia wspomagające.

TEMATY:

- Systemy badania spójności systemu plików: Tripwire, AIDE, Samhain, itp.
- SNORT a zintegrowane systemy IDS, narzędzia
- próba zbudowania honeypot,
- sieciowe IDS: Prelude

Bezpieczne programowanie problematyka naruszenia ochrony pamięci

TEMATY:

- techniki bezpiecznego programowania, narzędzia diagnostyczne (electricfence/valgrind),
- zabezpieczenia systemowe, PaX, stack protection, stack randomization grsecurity, i inne

Systemy wysokodostępne Wirtualizacja usług a bezpieczeństwo

TEMATY:

- wirtualizacja usług w Linuxie, VirtualServer
- wirtualizacja i emulacja: UML, Xen, VWware a Bochs, WINE, DosEMU

Bezpieczeństwo SBD *TEMATY:*

- zabezpieczanie dostępu do PostgreSQL, uwierzytelnianie, mechanizmy bezpieczeństwa w SQL i PL/PostgreSQL
- spójność i dostępność danych w PostgreSQL, backupy, replikacja, itp.

Bezpieczeństwo WWW *TEMATY:*

- podstawowe strategie zabezpieczanie Apache, przegląd
- Apache i modSecurity.org
- bezpieczeństwo PHP, zabezpieczanie środowiska PHP przez administratora Apache
- bezpieczeństwo PHP, strategie bezpiecznego programowania
- konfiguracja Apache w środowisku chroot/jail