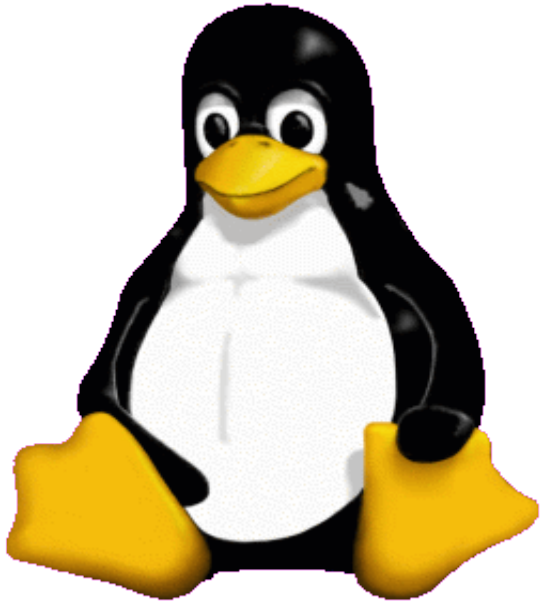
Bezpieczny serwer sieciowy Linux



Jacek Lach
jlach@star.iinf.polsl.gliwice.pl

Plan wykładu

- Start systemu
- Zabezpieczenie systemu po instalacji

Start systemu

- BIOS
- Boot loader (MBR, PBR)
- Jądro systemu
- proces init - tworzenie procesów zawartych w pliku inittab, uzyskanie odpowiedniego poziomu pracy
- poziom pracy (runlevel) - stan systemu, w którym uruchomiony jest pewien ustalony zbiór procesów

Poziomy pracy

- 0 - używany przy zatrzymywaniu systemu (halt)
- 1 - poziom jednoużytkownikowy
- 6 - poziom używany przy restarcie systemu
- 2 ... 5 - poziomy pracy wieloużytkownikowej
- 7 ... 9 - nieudokumentowane
- S, s - uruchomienie powłoki administratora
- inittab -> skrypt startu systemu
- /etc/rc.d/rcX.d -> skrypty startowe usług

Skrypty /etc/rc.d

- /etc/rc.d/rc3.d/S85httpd -> /etc/init.d/httpd

```
$ /etc/init.d/httpd
Usage: httpd {start | stop | restart | reload...}

$ ls /etc/rc.d/rc3.d
[...]
K74apmd   S10network    S56xinetd     S91smb
[...]
```

Bezpieczna instalacja

- Wybór dystrybucji
- Podział dysku na partycje
- Instalacja offline
- Podłączanie do sieci

Przed startem

- Usunięcie nadmiarowych pakietów.
- Weryfikacja domyślnej konfiguracji systemu.
- Zainstalowanie dostępnych poprawek.
- Utworzenie kopii zapasowej systemu.
- Utworzenie kopii plików systemu zarządzania pakietami.

Zarządzanie kontami

- Ograniczanie praw użytkowników do minimum.
- Kontrola powtarzających się, nieudanych prób logowania do systemu.
- Kontrola haseł użytkowników:
  - wszystkie konta powinny mieć hasło
  - hasła nie powinny dać się łatwo odgadnąć
- Konta nieaktywne powinny być zablokowane: hasło: *, shell: /bin/false
- Konta nieużywane powinny być usunięte.

Zarządzanie grupami

- User-private groups (UPG)
- Hasło grupy:
  - dostęp do zasobów grupy na podstawie zawartości pliku grup
  - dostęp do zasobów grupy na podstawie hasła

Konto użytkownika root

- Wykorzystywać tylko w przypadkach naprawdę uzasadnionych.
- Nigdy nie używaj narzędzi przesyłających hasło bez szyfrowania.
- /etc/securetty zawiera bezpieczne konsole.
- Nigdy nie loguj się zdalnie na konto root.
- Zmienna PATH nie powinna zawierać “.” i katalogów, w których użytkownicy mogą pisać.

Hasła w systemie Linux

- Tradycyjnie zapisywane w /etc/passwd
- Ochrona haseł: shadow passwords
- Systemy haseł jednorazowych.
- Postarzanie haseł.
- Wybór dobrego hasła.

Plik /etc/shadow

```
bin:*:10790:0:99999:7:::
daemon:*:10790:0:99999:7:::
adm:*:10790:0:99999:7:::
zenek:$1$uFu[...]UFm0:11550:0:99999:7:::134537332
```

Dobór haseł

- Cechy dobrego hasła:
  - nie jest zwiazane z użytkownikiem (nazwą, danymi personalnymi)
  - nie bazuje na słowach ze słownika
  - można je łatwo zapamiętać
- Sposoby generacji dobrego hasła:
  - układ graficzny
  - zdania (całe i skróty)
  - hasła losowe

Hasła - przykłady

- Użytkownik: herakles
- Złe hasła:
  selkareh, herakles10, dejanira, h3r4k135, qwerty
- Dobre hasła:
- alwosk1928eidj
- dwkkluh1i2m3z4c
- **`$ head -c 9 /dev/random | mmencode`**
  o5Wv1l1CBgKY

Bezpieczny start

- Lokalizacja serwera.
- Wyłączenie możliwości startu z płyty CD lub dyskietki.
- Zabezpieczenie hasłem dostępu do konfiguracji BIOS.
- Zabezpieczenie hasłem programu startującego (LILO)

Zabezpieczanie LILO

- Uruchamianie jądra
  - wybór obrazu jądra
  - przekazywanie parametrów podczas uruchamiania
- Uzyskiwanie dostępu do konta administracyjnego:
  - Tryb single
    `LILO: linux single`
  - Wskazanie programu init
    `LILO: linux init=/bin/bash`

Zabezpieczanie LILO

- lilo.conf
  hasło zapisane jawnym tekstem -> ustawienie restrykcyjnych praw dostępu (600)
  - password = haslo
    wymuszenie wprowadzenia hasła w celu uruchomienia wybranego obrazu/wszystkich obrazów
  - restricted
    ograniczenie wymagania hasła do uruchamiania systemu z parametrami (brak opcji uniemożliwia zdalny restart serwera)

Określenie działających usług

- netstat / nmap
  określenie działających usług
- Skąd się wzięły usługi, które udostępniam?
  - Skrypty /etc/rc.d
  - "Super serwer" inetd / xinetd

Super serwer

- Oczekuje na wskazanych portach na połączenia
- Dokonuje sprawdzenia połączenia pod kątem:
  - źródła połączenia
  - czasu połączenia
  - ilości połączeń
- Przekazuje połączenia do odpowiednich usług
- Współpraca z tcp_wrappers

TCP_wrappers

- Uzyskanie kontroli dostępu poprzez dodatkowe mechanizmy weryfikacji połączenia.
- Przechwycenie wywołania usługi przez super serwer, wykonanie dodatkowych testów.
- /etc/hosts.allow
  /etc/hosts.deny

inetd - konfiguracja

- Plik konfiguracyjny: /etc/inetd.conf

```
#ftp    stream  tcp     nowait  root    /
   usr/sbin/tcpd  in.ftpd -l -a

telnet stream  tcp     nowait  root    /
   usr/sbin/tcpd  in.telnetd
```

xinetd - konfiguracja

- Plik konfiguracyjny: /etc/xinetd.conf

```
service telnet
{
        disable = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
}
```

xinetd - zalety

- Możliwość ograniczania dostępu na podstawie czasu
- Ochrona przed atakami typu DoS
  - Ograniczenie liczby demonów określonej usługi
  - Ograniczenie całkowitej liczby procesów uruchomionych przez xinetd
  - Ograniczenie rozmiarów logów
- Usługi mogą być związane z wybranym interfejsem

Prawa dostępu do plików

- **`ls -l /bin/vi`**
  `-rwxr-xr-x 1 root  root 386120 mar 28  2002 /bin/vi`
- Prawa:
  - r - odczyt
  - w - zapis
  - x - wykonywanie
  - s - set UID (SUID) lub set GID (SGID)

umask

- Wbudowana funkcja powłoki ustawiająca końcowe wartości praw dostępu.
- Wyznaczanie praw:
  żądane prawa AND negacja maski
- Prawa: 666, maska: 027

```
110 110 110 - prawa
111 101 000 - maska
110 100 000  (640) - wynik
```

Prawa dostępu - katalogi

- ```
  ls -ld /tmp
  drwxrwxrwt  4 root root  24576 paz 26 20:17 /tmp
  ```
- Prawa:
  - r - możliwość odczytu zawartości katalogu
  - w - możliwość zapisu w katalogu (również kasowania plików w katologu)
  - x - możliwość “przejścia” przez katalog
  - s - pliki tworzone w katalogu dziedziczą grupę
  - t - pliki w katalogu z prawami do zapisu mogą być kasowane tylko przez właściciela pliku
  ```

Kontrola atrybutów plików

- Regularna kontrola plików z ustawionym bitem setuid oraz setgid.
- Kontrolowanie plików z prawem zapisu dla wszystkich.
- Wyszukiwanie plików bez właściciela.
- opcja nosuid dla partycji, na których prawo zapisu mają użytkownicy inni niż root.

Kontrola systemu plików

- Tripwire jest programem monitorującym integralność plików przy pomocy bazy sygnatur plików zgodnie z plikiem konfiguracyjnym
- Baza przechowuje sumy kontrolne plików oraz inne cechy plików. Każde kolejne uruchomienie powoduje porównanie bieżącego stanu ze stanem zapisanym w bazie.
- Najwyższy poziom bezpieczeństwa zapewnia konfiguracja tripwire po instalacji serwera.

Jądro systemu

- Dopasowanie jądra do konfiguracji serwera.
- Ustawienia dotyczące bezpieczeństwa.
- Zmiana konfiguracji systemu - proc filesystem
- Dodatkowe możliwości jądra:
  - ograniczenie dostępu do /proc
  - listy kontroli dostępu
  - losowość wybranych cech TCP/IP
  - ochrona przed atakami typu “buffer overflow”

System plików /proc

- Interfejs do struktur jądra systemu
- Informacje dotyczące procesów, urządzeń, ustawień systemu.
- Odczyt konfiguracji:
  `cat /proc/cpuinfo`
- Zmiana konfiguracji:
  `echo “1” > /proc/sys/net/ipv4/ip_forward`

Modyfikacja konfiguracji jądra

- /proc/sys zawiera bieżące ustawienia systemu.
- Modyfikacja ustawień może spowodować przyspieszenie pracy systemu, może również zachwiać stabilnością pracy sytemu.
- Próby modyfikacji konfiguracji powinny zawsze być przeprowadzane na serwerze testowym.

/proc/sys

- fs - dane dotyczące systemu plików
- kernel - parametry jądra
- vm - ustawienia dotyczące pamięci wirtualnej
- dev - parametry urządzeń
- sunrpc - konfiguracja RPC
- net - ustawienia dotyczące sieci

/proc/sys/net/ipv4

- ICMP
  - icmp_echo_ignore_all, icmp_echo_ignore_broadcasts
  - icmp_destunreach_rate, icmp_echoreply_rate, icmp_paramprob_rate, icmp_timeexeed_rate
- TCP
  - tcp_timestamps
  - tcp_syncookies

/proc/sys/net/ipv4/conf

- Konfiguracja poszczególnych interfejsów (np. eth0) lub wszystkich (all)
  - accept_source_route
  - forwarding
  - log_martians
  - rp_filter
  - secure_redirects

Zmiany w /proc

- Ciąg instrukcji echo
- sysctl
- /etc/sysctl.conf:

```
net.ipv4.ip_forward = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.ip_always_defrag = 0
kernel.sysrq = 1
```

Demon logowania

- syslogd jest usługą oczekującą na komunikaty, które umieszcza w plikach dziennika systemowego zgodnie regułami zapisanymi w pliku /etc/syslog.conf.
- Może przekazywać komunikaty do innych programów przy pomocy kolejki FIFO.
- klogd - demon współpracujący, przekazujący komunikaty od jądra.

syslog.conf

- Format pliku konfiguracyjnego:

```
# komentarz
# znak separatora: tabulator (spacja)
selektor akcja
```

- selektor:
  - usługa.poziom_ważności (facility.level)
  - symbole specjalne: *, none
- Kilka usług odziela się znakiem “,”, kilka selektorów znakiem “;”

Usługi (facilities) sysloga

- auth, authpriv
- cron
- daemon
- kern
- lpr
- mail
- mark
- news
- syslog
- user
- uucp
- local0 - local7

Poziomy (levels) sysloga

- emerg
- alert
- crit
- err
- warning
- notice
- info
- debug
- none

- poziom - określa minimalny poziom logowania
- =poziom - określa dokładnie jeden poziom
- !=poziom - wyklucza poziom

Syslog - akcje

- plik - nazwa pliku, do którego zostaną zapisane komunikaty (/var/log/messages)
- terminal - pełna nazwa urządzenia (/dev/tty12)
- @hostname - serwer z uruchomionym demonem syslog
- uzytkownik - wysyła komunikat do użytkownika przy pomocy write (user1,user2,user3)
- FIFO - wysyła komunikat do kolejki FIFO (|/

Syslog - sposoby konfiguracji

- Logowanie zbiorcze
  Komunikaty kierowane do jednego pliku i przetwarzane w większości automatycznie.
- Logowanie rozbite
  Komunikaty kierowane do wielu plików - wygodniejsze przy ręcznej kontroli plików.
- Niezależnie od sposobu zapewnić logowanie dostatecznej ilości informacji.

Rozszerzanie uprawnień użytkowników - sudo

- Brak kontroli zmian w przypadku dostępu kilku osób do konta root.
- Wszystkie prawa użytkownika root często nie są użytkownikowi potrzebne.
- Udostępnienie częściowej funkcjonalności konta administratora systemu umożliwia sudo.

sudo - zalety

- większa kontrola - rejestracja poleceń
- operator może wykonywać proste czynności bez nieograniczonych uprawnień
- hasło administratora nie musi być udostępniane
- modyfikacja przywilejów nie pociąga za sobą zmiany hasła administratora
- istnieje lista użytkowników z rozszerzonymi prawami

sudo - wady

- Niepoprawna konfiguracja udostępnia użytkownikowi konto root.
- Naruszenie bezpieczeństwa konta użytkownika otwiera drogę do rozszerzonych uprawnień - konta użytkowników muszą być chronione w tym samym stopniu co konto administracyjne.

Kolejne etapy zabezpieczania serwera

- SSH
- Systemy IDS
- Ściany ogniowe
- Zabezpieczenie usług