4. Instalacje oprogramowania (notatki)

Plik ten zawiera przydatne komendy wykorzystywane w kursie

Zarządzanie oprogramowaniem - przykłady

```
# Redhat / CentOS
[root@fedora ~]#
yum list nmap
yum list bind*
yum search ettercap
yum provides python
yum install nmap
yum groupinstall php
yum update nmap
yum groupupdate php
yum remove nmap
yum groupremove php
yum localinstall plik.rpm
```

Więcej informacji o wybranych menadżerach oprogramowania

```
# Redhat / CentOS
yum --help

# Debian / Ubuntu
apt-get --help

# Arch Linux / Manjaro
packman --help
```

Instalacja programów za pomocą instalatorów

Instalacja programów za pomocą instalatorów przebiega podobnie jak w systemie Windows i polega na uruchomieniu programu:

1. Aby uruchomić program, należy najpierw nadać plikowi prawo do uruchamiania, używając komendy: `chmod u+x nazwa_pliku`
2. Teraz można go uruchomić, stosując komendę: `./nazwa_pliku`

W przypadku instalacji w trybie graficznym wystarczy dwukrotnie kliknąć plik.

Kompilacja z plików źródłowych

```
tar -xvf plik.tar # dla plików tar
tar -xvzf plik.tar.gz # dla plików tar.gz
tar -xvjf plik.tar.bz2 # dla plików tar.bz2
./configure
make install
make uninstall
make clean
```

Suma kontrolna – jak sprawdzić?

- Do sprawdzenia sumy **MD5** użyj `md5sum`

```
man md5sum
```

- Do sprawdzenia sumy **SHA-1** użyj `sha1sum`

```
man sha1sum
```

- Do sprawdzenia sumy **SHA-256** użyj `sha256sum`

```
man sha256sum
```

Monitorowanie działania oprogramowania po uruchomieniu

Dodatkowo podczas pierwszego uruchomienia zainstalowanego programu możesz sprawdzić, czy w trakcie jego działania nie dochodzi do dodatkowego ruchu sieciowego, którego wcześniej nie było.

W tym celu możesz posłużyć się takimi programami jak:

- **tcpdump**

```
# Redhat / CentOS
yum install tcpdump
man tcpdump
```

- **wireshark**

```
# Redhat / CentOS
yum install wireshark
man wireshark
```

Lab - video Tips&tricks

Tips&tricks

1. Szyfruj komunikację danych dla serwera Linux, wykorzystując:
    - Klucze I certyfikaty
    - SCP / SSH / RSYNC / SFTP
    - SSHFS FUSE
    - GnuPG
    - OpenVPN
    - Lighttpd SSL
    - SSL dla APACHE
    - SSL dla NGINX
2. Unikaj korzystania z usług FTP, Telnet i Rlogin / Rsh w systemie Linux

```
 yum erase xinetd ypserv tftp-server telnet-server rsh-server
 sudo apt-get --purge remove xinetd nis yp-tools tftpd atftpd tftpd-hpa telnetd
rsh-server rsh-redone-server
```

3. Zminimalizuj oprogramowanie, aby zminimalizować lukę w systemie Linux

```
yum list installed
yum list packageName
yum remove packageName
```

```
dpkg --list
dpkg --info packageName
apt-get remove packageName
```

4. Jedna usługa sieciowa na system lub maszynę wirtualną.
    - XEN
    - OpenVZ
5. Aktualizuj jądro Linuksa i oprogramowanie

```
yum update
apt-get update && apt-get upgrade
```

    - Powiadomienia pocztą dla CentOS
    - Aktualizacja z pomocą CRON
    - Powiadomienia bezpieczeństwa Debian

```
sudo apt-get install unattended-upgrades apt-listchanges bsd-mailx
```

6. Użyj rozszerzeń zabezpieczeń systemu Linux
    - Linux Kernel Security (SELinux vs AppArmor vs Grsecurity
7. SELinux
    - Oficjalna dokumentacja REDHat’a
8. Konta użytkowników systemu Linux i polityka silnych haseł
    - John The Ripper
    - Konfigurowanie pam_cracklib.so
9. Wyłącz niechciane usługi systemu Linux

```
chkconfig --list I grep '3:on'
```

```
service serviceName stop
chkconfig serviceName off
```

```
systemctl list-unit-files --type=service
systemctl list-dependencies graphical.target
```

```
systemctl disable service
systemctl disable httpd.service
```

```
systemctl status service
systemctl status httpd.service
```

```
journalctl
journalctl -u network.service
journalctl -u ssh.service
journalctl -f
journalctl -k
```

10. Usuń X Window Systems (X11)
    - Jak wyłączyć I usunąć X WINDOW SYSTEM

    ```
    /etc/inittab # id:3:initdefault:
    yum groupremove "X Window System"
    yum group remove "GNOME Desktop"
    yum group remove "KDE Plasma Workspaces"
    yum group remove "Server with GUI"
    yum group remove "MATE Desktop"
    ```

11. Użyj usługi scentralizowanego uwierzytelniania
    - Znajdowanie I usuwanie niechcianych kont
    - Usługa OpenLDAP
12. Kerberos
    - Kerberos
    - Kerberos na RedHat
13. Logowanie i audyt
    - Lokalizacje plików dziennika systemu Linux
    - Jak wysłać logi do zdalnego hosta logów
    - Jak rotować pliki dziennika?
14. Bezpieczny serwer OpenSSH
    - Najlepsze praktyki serwera SSH
    - Duwskładnikowe uwierzytelnianie google – synchronizacja z OpenSSH
15. Zainstaluj i używaj systemu wykrywania włamań
    - 5 Najlepszych rozwiązań NIDS
    - AIDE - HIDS
16. Zainstaluj orpogramowanie do wykrywania rootkitów.
    - Tutorial oprogramowania rkhunter
17. Wyłącz urządzenia USB / Firewire / Thunderbolt

    ```
    echo 'install usb-storage /bin/true' >> /etc/modprobe.d/disable-usb-
    storage.conf

    echo "blacklist firewire-core" >> /etc/modprobe.d/firewire.conf
    echo "blacklist thunderbolt" >> /etc/modprobe.d/thunderbolt.conf
    ```

18. Użyj fail2ban / denyhost jako IDS

```
sudo apt-get install fail2ban
sudo yum install fail2ban
sudo vi /etc/fail2ban/jail.conf
sudo systemctl restart fail2ban.service
```

19. Zabezpiecz serwer Apache / PHP / NGINX

```
ServerTokens Prod
ServerSignature Off
TraceEnable Off
Opcje wszystkie -Indeksy
Nagłówek jest zawsze nieustawiony X-Powered—By

sudo systemctl restart apache2.service
sudo systemctl restart https.service
```

    - Jak wykryć błędną konfigurację NGINX

20. Kopie zapasowe*

    - Debian / Ubuntu Linux Instalowanie i konfigurowanie zdalnej migawki systemu plików za pomocą narzędzia rsnapshot Incremental Backup Utility
    - Jak ustawić remote snapshot na CentOS RedHat
    - Jak wykonać kopię zapasową serwera internetowego
    - Jak utworzyć kopię zapasową w systemie Linux korzystając z rsync

PS: Ostatecznie w nagraniu wyszło 20 Tips & tricks ;)