Przyjmowanie właściwej postawy obronnej w zadanych kanałach komunikacji (1/2)

Bezpieczeństwo systemu Linux

Wynajdywanie udostępnionych katalogów o rozluźnionych uprawnieniach

```
sudo find / -type d \( -perm -g+w -o -perm -o+w \) -exec ls -lad {} \;
# odszukujemy w systemie wszystkie katalogi o rozluźnionych uprawnieniach

# Ustawienie „lepkiego” bitu w uprawnieniach do katalogu, w którym zapisywać mogą wszyscy powoduje, że wszyscy mogą tworzyć w nim pliki, to jednak nikt nie może usuwać ani modyfikować plików innych użytkowników.
chmod a+t nazwa_katalogu
# ustawienie lepkiego bitu dla katalogu
```

Ustawienie atrybutu tylko do dopisywania w pliku

```
sudo echo "atrybut tylko do dopisywania nie jest ustawiony" > file
sudo chattr +a file
# zmieniamy atrybut pliku
sudo echo "atrybut tylko do dopisywania jest ustawiony" > file
# próba zakończona niepowodzeniem
sudo echo "dopisywanie do pliku" >> file
# próba zakończona powodzeniem, możemy tylko dopisywać do pliku
cat file
# wyświetlenie zawartości pliku
```

`nmap` - zwłaszcza używany na zewnątrz systemu (np. dla celów testów penetracyjnych/rekonesansu) może otrzymywać niepełny obraz otwartych portów i działających na nich usług, m. in. z powodu tego że ruch może być np. filtrowany przez zaporę sieciową. Aby w systemie Linux uzyskać listę nasłuchujących portów i ich procesów (od wewnątrz systemu) warto korzystać z polecenia `netstat`

```
sudo netstat -luntap
```

Alternatywnie do odnalezienia nasłuchujących usług możemy wykorzystać polecenie `lsof` służące do analizy listy otwartych gniazd

```
#lub
sudo lsof -i -n | egrep 'COMMAND|LISTEN'
sudo lsof -i -n | egrep 'COMMAND|LISTEN|UDP'
```

Automatyczne aktualizacje w systemie debian/ubuntu

```
# Instalacja paczki
sudo apt install unattended-upgrades

# Konfiguracja
sudo dpkg-reconfigure unattended-upgrades
# Wybieramy Tak w oknie dialogowym  dialogowym
```

```
# Instalacja paczki generuje m.in. plik /etc/apt/apt.conf.d/20auto-upgrades do którego możemy dodawać inne opcje programu apt.
# Aby wyświetlić opcje razem z domyślnymi wartościami wpisujemy
apt-config dump

# Chcąc wyświetlić zawartość pliku /etc/apt/apt.conf.d/20auto-upgrades wpisujemy
vim /etc/apt/apt.conf.d/20auto-upgrades

# Chcąc wyświetlić zawartość pliku /etc/apt/apt.conf.d/50unattended-upgrades możemy to zrobić na dwa sposoby
vim /etc/apt/apt.conf.d/50unattended-upgrades
# lub
apt-config dump | grep Unattended-Upgrade

# Poniżej zawartość wybranych plików wraz z wyjaśnieniem
# Automatyczna aktualizacja listy pakietów włączona
APT::Periodic::Update-Package-Lists "1";
# Automatyczne ściąganie dostępnych do aktualizacji paczek
APT::Periodic::Download-Upgradeable-Packages "1";
# Automatyczna aktualizacja co 7 dni
APT::Periodic::Unattended-Upgrade "7";
# Automatyczne czyszczenie cache z zainstalowanymi pakietami co 21 dni
APT::Periodic::AutocleanInterval "21";
# Test
sudo unattended-upgrade -v -d --dry-run
```

Bezpieczeństwo systemu Windows

Lista otwartych plików przez procesy, które ich używają z pomocą aplikacji `handle`. Program można pobrać ze strony https://docs.microsoft.com/en-us/sysinternals/downloads/handle

Sposób użycia

```
# Pokazanie uchwyty wszystkich otwartych w systemie plików
handle nazwa_pliku
# listę plików otwartych przez przeglądarkę Internet Explorer
handle -p iexplorer
# Chcąc odnaleźć proces Internet Explorera korzystający z zasobu, którego nazwa zawiera wyraz „handle”, należy użyć następującego polecenia:
handle -p iexplorer handle
```

Lista działających usług i otwartych portów

```
# Należy w pierwszej kolejności uruchomić konsole z uprawnieniami administratora
netstat -ab
# Pokazuje aktywne połączenia wraz z nazwą procesu
netstat -aon
# Pokazuje listy procesów razem z numerem PID
tasklist
# Wyświetlenie wszystkich procesów na komputerze
```