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

Ćwiczenie - Zapory sieciowe w Windows

Zapora Windows Defender Wyszukujemy -> Windows Defender -> otwieramy program

Zamykanie otwartych portów i blokowanie protokołów Aby ręcznie zamknąć porty i protokoły, należy:

1. kliknąć prawym przyciskiem myszy Moje miejsca sieciowe i wybrać Właściwości w celu otwarcia folderu Połączenia sieciowe.
2. Klikamy teraz prawym przyciskiem myszy połączenie, dla którego chcemy zamknąć porty, i wybieramy Właściwości.
3. Wybieramy pozycję Protokół internetowy (TCP/IP) i klikamy przycisk Właściwości.
4. Na karcie Ogólne klikamy przycisk Zaawansowane. Wybieramy kartę Opcje, podświetlamy pozycję Filtrowanie TCP/IP i klikamy przycisk Właściwości.
5. Pojawi się okno dialogowe Filtrowanie TCP/IP. Aby zablokować porty TCP, porty UDP i protokoły IP, należy dla każdego z tych elementów wybrać opcję Pozwalaj tylko. Spowoduje to skuteczne zablokowanie wszystkich portów TCP, UDP oraz protokołów IP.

Ochrona komputera za pomocą Zapory systemu Windows Wyłączenie firewall z poziomu terminala

```
netsh advfirewall set allprofiles state off
```

Usunięcie wszystkich reguł

```
netsh advfirewall firewall delete rule name=all
```

Dostęp do komputera za pomoca RDP dla wybranych adresów ipv4

```
netsh advfirewall firewall add rule name="0zdalny" dir=in interface=any profile=domain
action=allow localport=3389 protocol=TCP remoteip=192.168.12,192.168.1.100
```

Ograniczenie odpowiedzi na ping do wybranych adresów ipv4 na wszystkich profilach

```
# Reguły przychodzące
netsh advfirewall firewall add rule name="0inICMPv4" dir=in interface=any profile=any
action=allow protocol=ICMPv4 remoteip=192.168.12,192.168.1.100
# Reguły wychodzące
netsh advfirewall firewall add rule name="0outICMPv4" dir=out interface=any
profile=any action=allow protocol=ICMPv4 remoteip=192.168.12,192.168.1.100
```

Przekierowanie listy reguł do pliku

```
netsh advfirewall firewall show rule name=all
```

Przywracanie ustawień fabrycznych zapory sieciowej

```
netsh advfirewall reset
```

Eksportowanie i importowanie ustawień zapory sieciowej

```
netsh advfirewall export “C:\zapora_siecowa.wfw”
netsh advfirewall import “C:\zapora_siecowa.wfw”
```

Analogicznie możemy filtrować połączenia konfigurując zaporę ogniową w systemach Linux/Unix przy użyciu narzędzi, np. `netfilter`, `iptables`, `nftables`.

Ćwiczenie - Bezpieczeństwo sieci

Jednym z programów służących monitorowania ruchu ARP w sieci jest `Arpwatch`. Jego działanie polega na monitorowaniu interfejsu w trybie nasłuchiwania (ang. promiscuous mode) i na rejestrowaniu obserwowanych w czasie par MAC-IP.

Pobranie i instalacja programu:

```
wget ftp://ftp.ee.lbl.gov/arpwatch.tar.gz
tar -xzvf arpwatch.tar.gz
cd arpwatch-2.1a15
# Po pobraniu programu `Arpwatch` należy go skompilować i zainstalować w tradycyjny sposób za pomocą polecenia:
./configure && make && make install
```

Alternatywnie instalacja w Ubuntu/Debian

```
sudo apt install arpwatch
```

Gdy program `Arpwatch` ma działać w komputerze wyposażonym w kilka interfejsów, należy w wierszu poleceń wskazać interfejs, na którym program będzie nasłuchiwał. Służy do tego opcja -i.

```
arpwatch -i iface
```

Wszystkie dostrzeżone pary MAC-IP program Arpwatch odnotowuje są w dzienniku zdarzeń w postaci zapisów: *Nov 1 00:39:08 zul arpwatch: new station 192.168.0.65 0:50:ba:85:85:ca*

Tworzenie statycznych tablic ARP

```
# Dodanie statycznego wpisu do tablicy ARP
sudo arp -s 192.168.1.34 08:00:27:13:4c:9b
# Wyświetlenie tablicy ARP
arp -a -n
# Eksport tablicy do pliku
arp -e > lista_adresow.txt
```

Inwentaryzacja sieci

```
# Skanowanie hosta z pomocą programu nmap
nmap 192.168.1.18
# Skanowanie zakresu adresów
nmap 192.168.1.0/24
# Wykrywanie systemu operacyjnego wykorzystując półotwarcie TCP
sudo nmap -sS -O 192.168.1.18
```

Śledzenie luk w zabezpieczeniach, przydatne linki:

- BugTraq - Na liście BugTraq producenci publicznie ogłaszają luki w bezpieczeństwie zgłoszone im przez osoby zajmujące się analizą zabezpieczeń lub odkryte przez nich samych. Dla ogłaszanych tu luk bezpieczeństwa zwykle w tym samym czasie udostępniane są łatki lub sposoby obejścia problemu, ponieważ sami producenci są często tymi, którzy je ujawniają.
- Full-Disclosure - Full-Disclosure często informuje o lukach w zabezpieczeniach zgłaszanych przez niezależnych analityków bezpieczeństwa, z którymi producenci nie chcieli współpracować i naprawić znalezionych przez nich błędów.
- SecurityFocus - witryna prowadząca listę dyskusyjną BugTraq, ma również źródło RSS - SecurityFocus RSS
- NVD - National Vulnerability Database - oferuje kanał RSS zawierający informacje o najnowszych lukach w zabezpieczeniach dodanych do bazy NIST RSS
- Cassandra - monitoruje bazy danych Secunia oraz National Vulnerability Database. Wyszukuje codziennie dodawane nowe luki w zabezpieczeniach. Po zarejestrowaniu się w serwisie możemy podać producentów i produkty, którymi jesteśmy zainteresowani, a Cassandra przyśle do nas e-mail z informacją, jeśli pojawią się jakieś związane z nimi zgłoszenia. Jest dziełem projektu CERIAS z Purdue University

Ćwiczenie - Rejestracja zdarzeń

Rejestruj zamykanie i działania logowania do Podglądu zdarzeń w Windows

1. Klikamy równocześnie znak Windowsa na klawiaturze i literę R tak aby otwrzyć interfejs `Uruchom`
2. Wpisujemy `gpedit.msc`
3. Wybieramy *Konfiguracja komputera -> Ustawienia systemu Windows -> Ustawienia zabezpieczeń -> Zasady lokalne -> Zasady inspekcji -> Przeprowadź inspekcję zdarzeń logowania*
4. W otwartym oknie *Przeprowadź inspekcję zdarzeń logowania zaznaczamy* `Sukces` oraz `Niepowodzenie`
5. Restartujemy system *Windows*
6. Następnie, przeglądamy logi dziennika: *Panel sterowania -> Wydajność i konserwacja -> Narzędzia administracyjne -> Podgląd zdarzeń -> Zabezpieczenia*

Analogicznie możemy rejestrować zdarzenia i przeglądać je w systemie Linux/Unix przy użyciu narzędzi `systemd`, `journalctl` oraz `syslog`