Kontrola wydarzeń w sieci.

Podsłuchiwanie to monitorowanie ruchu w sieci, czyli intruz odczytuje nieswoje pakiety, które przechodzą przez jego interfejs sieciowy. Używa się do tego programów zwanych snifferami.

Sniffery to programy specjalizujące się w przechwytywaniu pakietów sieciowych i odfiltrowywaniu z nich interesujących informacji (login, hasło, adresy IP, itp.). Sniffery wykorzystywane są przez hackerów, agencje wywiadowcze, instytucje zajmujące się pomiarem ruchu w sieci, administratorów sieci, programistów testujących aplikacje sieciowe. Sniffery potrafią interpretować praktycznie wszystkie protokoły, czyli w przypadku nieszyfrowanych (Telnet, FTP, HTTP, SMTP, POP3, protokołów wykorzystywanych przez większość komunikatorów internetowych), mogą w zasadzie mieć pełną wiedzę na temat przesyłanych danych.

netstat – jeden z najbardziej wszechstronnych i rozbudowanych programów narzędziowych odnoszących się do połączeń sieciowych. Polecenie netstat dostępne jest z linii poleceń w systemie Unix i zbliżonych oraz w systemach opartych na Windows. Służy do wyświetlania aktywnych połączeń sieciowych TCP a także: portów, na których komputer nasłuchuje, tabeli trasowania protokołu IP, statystyki sieci Ethernet, statystyki protokołu IPv4 (dla protokołów IP, ICMP, TCP i UDP), statystyki protokołu IPv6 (dla protokołów IPv6, ICMPv6, TCP przez IPv6 i UDP przez IPv6) oraz połączeń NAT i komunikatów netlinkowych.
Polecenie netstat użyte bez parametrów powoduje wyświetlenie aktywnych połączeń protokołu TCP.

Network Mapper - Nmap jest narzędziem do eksploracji sieci i audytów bezpieczeństwa.
Wykorzystując niskopoziomowe pakiety przesyłane do konkretnych adresów sieciowych, może być źródłem informacji o dostępności hosta, typu systemu operacyjnego na jakim pracuje użytkownik, rodzaju firewalla, a także wielu innych informacji, Nmap wyróżnia sześć stanów portu:

otwarty – to pakiety UDP lub połączenia TCP są akceptowane na tym porcie. Porty otwarte mogą być nieocenionym źródłem wiedzy o usługach dostępnych w sieci;

zamknięty – to połączenia inicjowane przez Nmapa są odbierane, jednakże w żaden sposób obsługiwane. Porty zamknięte są pomocne przy sprawdzaniu aktywności hosta;

filtrowany – to Nmap nie jest w stanie ustalić, czy port jest otwarty ze względu na działające firewalle. Taki port dostarcza znikomą ilość informacji. Powoduje również, że Nmap jest zmuszony wysyłać

wielokrotnie pakiety (w celu uniknięcia ich zaginięcia w wypadku gwałtownego przeciążenia sieci), co znacznie spowalnia proces;

niefiltrowany – to port jest dostępny, jednakże nie można ustalić jego dokładniejszego stanu. Nie wiadomo, czy ów port jest w rzeczywistości otwarty czy zamknięty;

otwarty | filtrowany – to port jest albo otwarty, albo filtrowany;

zamknięty | filtrowany – to port jest albo zamknięty, albo filtrowany;

Żeby skanowanie można było nazwać w jakikolwiek sposób sensownym, musi składać się z dwóch głównych członów: skanowania oraz obiektu skanowanego. np. nmap -O 73.14.180.255.

```
# skanuje wszystkie porty i wyswietla poszerzone informacje
nmap -v target.example.com

# skanuje metoda Stealth SYN caly segment sieci (255 adresow ip)
# z proba odgadniecia systemu operacyjnego
sudo nmap -sS -O target.example.com/24

# skanuje metoda Xmas tree pierwsza polowke segmentu sieci
# tylko wybrane porty: sshd, DNS, pop3d, imapd, i 4564???
nmap -sX -p 22,53,110,143,4564 198.116.*.1-127

# skanuje w standardowy sposob cala domene
host -l company.com | cut  -d  -f 4 | ./nmap -v -iL -

# rozszerzone, zaawansowane testy (-A), z agresywnym ustawieniem
# opoznien (skrocone timeouty oczekiwania na odpowiedzi)
nmap -A -T4 scanme.nmap.org
```

Iftop nasłuchuje na wskazanym interfejsie i wyświetla w czasie rzeczywistym zużywane pasmo w czasie połączenia danych par hostów.

Na głównym ekranie aktywne połączenia, a więc pary adresów komputerów pomiędzy którymi jest połączenie.

Dalsze 3 kolumny liczb to średnie obciążenie łącza liczone odpowiednio przez ostatnie 2, 10 i 40 sekund. Ruch możemy obserwować zarówno w obu kierunkach (przychodzący i wychodzący jak przedstawiono na powyższym screen'ie), jak i tylko przychodzący bądź wychodzący – przełączamy klawiszem "t".

W podsumowaniu widzimy linie “TX” i “RX“, czyli wysyłane i odbierane dane, gdzie “cum” to ich całkowita “waga” od początku uruchomienia iftop, a “peak” to wartości szczytowe w tym czasie. Natomiast kolumna “rates” to ilości danych w okresach 2, 10 i 40 sekund.

Mimo że iftop przedstawia informacje na jednym ekranie, to mamy spory wpływ na sposób ich przedstawiania. Wszystkie funkcje dostępne są przy pomocy klawisza “?“. I tak na przykład możemy włączyć możliwość wyświetlania wykresów zajętości pasma na skali logarytmicznej bądź liniowej: klawisz “L” – rodzaj skali, “B” – pasmo z ostatnich 2, 10, bądź 40 sekund, “b” – wyłączenie/załączenie skali.

Tcpdump - jest to rozbudowane narzędzie do podsłuchiwania ruchu na interfejsie sieciowym. Działa na poziomie TCP-IP i ma wiele opcji filtrowania.

Można nim np. też podglądać cały ruch bajt po bajcie (w sensie danych protokołu TCP-IP) uruchamiając go z opcją -XXX

Nie jest zbyt przyjazny użytkownikowi, o czym można sie przekonac ogladając strony manuala (man tcpdump).

Zastosowania

- śledzenie błędów aplikacji używających komunikacji sieciowej
- analizowanie konfiguracji samej sieci np. trasowania
- przechwytywanie komunikacji sieciowej innych użytkowników. Niektóre protokoły jak telnet lub HTTP przesyłają informacje w postaci niezaszyfrowanej. Użytkownik kontrolujący router lub bramę po drodze transmisji może użyć tcpdumpa aby przechwycić informacje jak np. login lub hasło.

Monitorowanie całego ruchu z wyjątkiem bieżącego połączenia ssh:

```
tcpdump -i eth0 -nN -vvv -xX -s 1500 port not 22
```

Odfiltrowanie również portu 123, badanie całych pakietów:

```
tcpdump -i eth0 -nN -vvv -xX -s 0 port not 22  and port not 123
```

Filtrowanie konkretnego hosta:

```
tcpdump -i eth0 -nN -vvv -xX  port not 22 and host 81.169.158.205
```

Wyświetlanie tylko adresu IP i małej porcji danych, przerwij po 20-tu pakietach:

```
tcpdump -i eth0 -nN  -s 1500 port not 22 -c 20
```

Wykrywanie ataków DOS przez wyświetlanie pakietów SYN na wszystkich interfejsach:

```
tcpdump 'tcp[13] & 2 == 2'
```

dsniff - jest to program z pakietu dsniff. W najbardziej podstawej (bezparametryzowej) wersji można go użyć do wychwytywania najciekawszych (najbardziej pikantnych) informacji, np. haseł z większości nieszyfrowanych protokołów.

wireshark - jest to duży program posiadający dosyć wygodne GUI. Można nim podglądać całe przebiegi konkretnych połączeń, w praktyce chyba najwygodniejszy do ogólnego monitorowania ruchu w sieci.

http://testywydajnosci.pl/przeglad-narzedzi-do-monitorowania-ruchu-sieciowego/