Diagnostyka portów i protokołów

W sieciach opartych na protokole TCP/IP kontrola dostępu do portów jest bardzo ważnym elementem systemu zabezpieczeń. W celu znacznego zmniejszenia ryzyka włamania należy prowadzić ciągły monitoring i ograniczenia dla połączeń nawiązywanych przez aplikacje i inne komputery z naszym systemem.

Dostęp portów i protokołów do komputera

Przy użyciu protokołu TCP/IP następuje połączenie dwóch komputerów. Dwa komputery uzgadniają numer portu od 1 do 65535 oraz protokół. Przy nawiązaniu połączenia komputer inicjujący podaje adres IP komputera docelowego oraz z góry ustalony numer portu. Komputer docelowy nasłuchuje na ustalonym z góry numerze portu aż jakiś komputer – dowolny – przyśle do niego wiadomość. Komputer odbierający może sprawdzić adres komputera źródłowego oraz informacje zawarte w przesłanej wiadomości i na tej podstawie zdecydować, czy zaakceptować połączenie. Najczęściej wykorzystywanymi protokołami do komunikacji między portami są TCP i UDP.

Główne protokoły

Protokół	Opis
TCP	*Transmision Control Protocol* - dwa komputery nawiązują długotrwałe połączenie, które zapewnia niezawodne dostarczenie wiadomości.
UDP	*User Datagram Protocol*- pozwala przesłać z jednego komputera do drugiego prostą jednopakietową wiadomość.
ICMP	*Internet Control Message Protocol* – wykorzystywany jest przy diagnostyce oraz routingu. Najpopularniejszymi programami użytkowymi wykorzystującym ten protokół jest ping oraz traceoute.

Oprogramowanie sieciowe TCP/IP wykorzystują jeszcze jeden protokół o nazwie Interent Control Message Protocol (**ICMP**) do komunikacji między sobą. Wiadomości ICMP nie zawierają numerów portów, ponieważ są przetwarzane przez sam stos TCP/IP. Przykładem wiadomości ICMP jest pakiet ECHO wysyłany przez polecenia trybu wierszowego Ping i Tracert.
W rzeczywistości TCP/IP to zbiór wielu protokołów, które umożliwiają m.in. wysyłanie/odbieranie poczty elektronicznej (SMTP – POP3 – IMAP), ściąganie plików (FTP), przeglądanie stron WWW (HTTP), lokalizację hostów (IP) czy automatyczne otrzymywanie adresów IP (DHCP).

Popularne porty i protokoły

Port	Protokół	Opis
21	FTP	File Transem Protocol
22, 65301	PC Anywhere	PC Anywhere wersje do 7.51
23	Telnet	Połączenie terminala znakowego
25	SMTP	Simple Mail Transfer Protocol
80	HTTP	Hypertext Transfer Protocol
110	POP3	Post Office Protocol wersja 3
119	NNTP	Network News Transfer Protocol
123	NTP	Network Time Protocol
135	epmap	Endpoint Mapper
137, 138, 139	NETBIOS	NetBIOS przez TCP/IP
143	IMAP	Internet Message Access Protocol
161	SNMP	Simple Network Management Protocol
443	HTTPS	Secure HTTP
445	SMB	Server Message Block przez TCP/IP
1723	PPTP	Point-to-Point Tunneling Protocol
1900, 5000	UPnP	Universal Plug and Play
3389	RDP	Remote Desktop Protocol (usługi terminalowe)
5190	AOL	America Online, AOL Instant Messenger
5631, 5632	PC Anywhere	PC Anywhere wersja 7.52 I nowsze
5900, 59xx	VNC	Virtual Network Computing

Kompletny i oficjalny wykaz portów i ich przeznaczenia znajduje się na stronie: *http://www.iana.org/assignments/port-numbers* oraz na polskiej lokalizacji: *http://portal.aplus.pl/staticpages/znane.txt.*

Śledzenie aktywnych portów

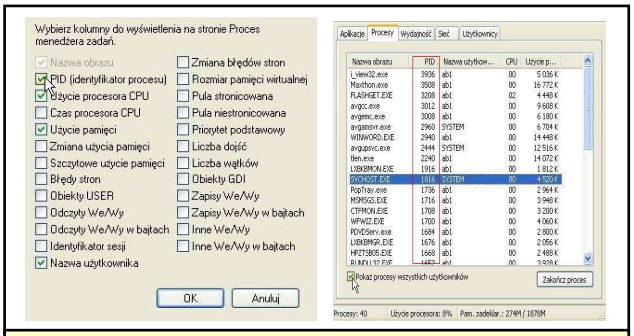
Dla ograniczenia liczby aktywnych portów niezbędna jest ich analiza. Aby dowiedzieć się, które porty są aktywne w systemie i które programy z nich korzystają, można posłużyć się trzema narzędziami wbudowanymi w system Windows (XP i 2000):

- menedżer zadań,
- polecenie Netstat,
- polecenie Tasklist lub Tlist (Windows 2000).

Menedżer zadań – podaje aktualnie uruchomione procesy. Uruchamiając menedżera zadań wybieramy zakładkę procesy, ponadto zaznaczamy pole wyboru „*pokaż procesy wszystkich użytkowników*”. Menedżer zadań domyślnie nie

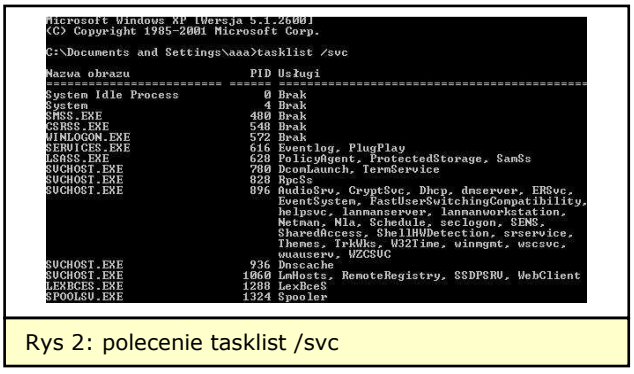
pokazuje identyfikatora PID. Dobrze jest jednak uruchomić widok pokazywania PID, identyfikatory PID okażą się pomocne przy poleceniu Netstat. W tym celu wykonujemy:

1. Menu opcje > widok > wybierz kolumny,
2. W nowym oknie zaznaczamy *„PID (identyfikator procesu)”*



Rys 1: ustanawianie widoku PID, widok kolumny PID.

Tasklist- standardowo instaluje się wraz z instalacją systemu Windows XP. Najbardziej przydatną jego opcją do wiązania usług z portami jest opcja **/svc**, wyświetla nazwy usług wraz z ich numerami PID i nazwami obrazów wykonywalnych (plików.exe). Po użyciu polecenia: **tasklist /svc** będziemy posiadali dostęp do poniższych informacji.



Rys 2: polecenie tasklist /svc

Korzystając z polecenia tasklist z kluczem /Fi otrzymamy tylko informacje o konkretnym zadaniu. Jeśli chcemy zweryfikować, która usługa wykonywana jest np. z PID 1584 wpisujemy w wierszu polecenia: **tasklist /svc /fi "pid eq 1584"**

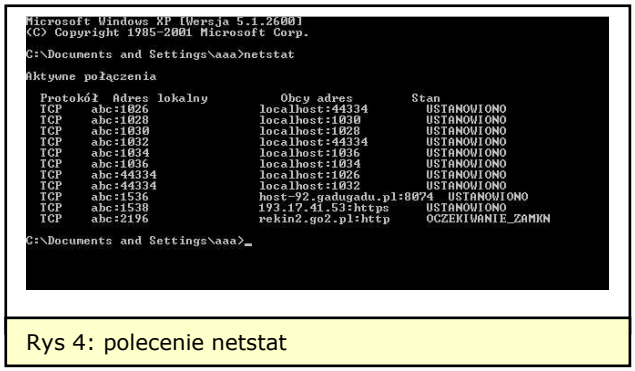
Rys 3: polecenie tasklist /svc /fi „pid eq 1584”

w powyższym przykładzie PID 1584 jest identyfikatorem usługi Kerio Personal Firewall 4.

Tlist – oferuje podobne informacje. W Windows 2000 instalacja tego składnika znajduje się na płycie CD-ROM w folderze \Support\Tools.

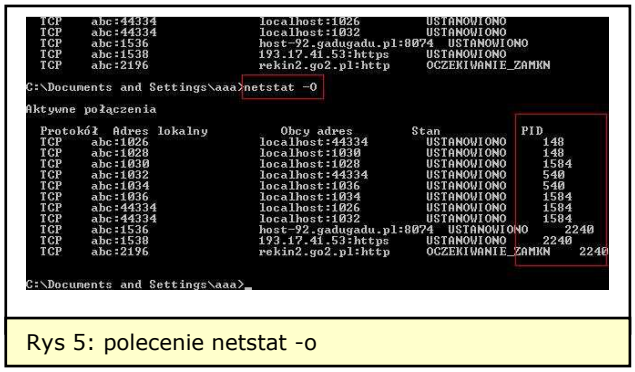
Netstat - pozwala na uzyskanie wielu szczegółowych informacji na temat portów. Polecenia Netstat używamy w wierszu polecenia. Oto jego kilka wariancji:

- polecenie **netstat** – wyświetla wszystkie aktualnie używane porty.



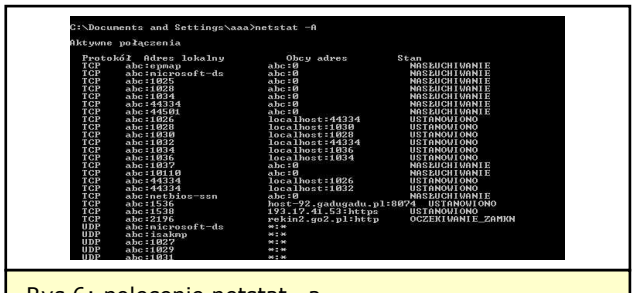
Rys 4: polecenie netstat

- polecenie **netstat -o** - przekazuje informacje, który program używa każdego połączenia. Powoduje wyświetlenie identyfikatorem, który otworzył połączenie. Przy użyciu identyfikatora PID, który podaje Netstat można odszukać nazwę programu w Menedżerze zadań. Jesli w systemie nie ma aktywnych połączeń sieciowych, polecenie to nie wyświetla niczego.



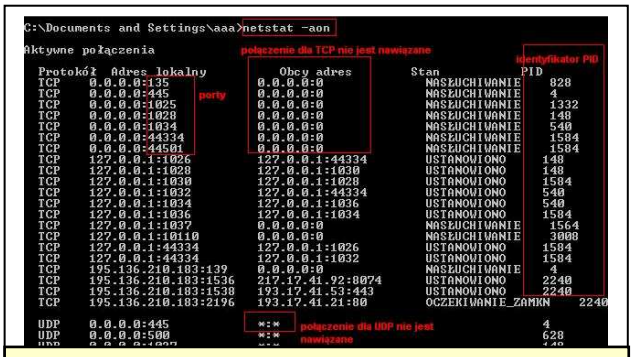
Rys 5: polecenie netstat -o

- polecenie **netstat -a**- pokazuje wszystkie porty z jakąkolwiek aktywnością, łącznie z nasłuchującymi na nich programami.



Rys 6: polecenie netstat –a

- najciekawszym poleceniem jest użycie **netstat -aon**- połączenie opcji -A i -O z opcją -N powoduje wyświetlenie adresów IP i numerów portów zamiast nazw



Rys 7: polecenie netstat -aon

Pole obcy adres zawiera same zera w przypadku połączeń TCP, a *:* w przypadku połączeń UDP. Obie wartości wskazują, że porty czekają na odebranie wiadomości od dowolnego adresu IP i dowolnego portu.
Teraz można ustalić, które programy nasłuchują na tych portach, zaczynając od góry:
port 135 - zgodnie z listą IANA (tabela) należy do usługi Microsoft Locator Service (Endpoint Mapper). Port ten jest otwarty przez proces PID równym 828.
PID 828 - zgodnie z listą menedżera zadań jest to Svchost.exe.
Według **Taskslist** jest to identyfikator podsystemu RPC (RPCSS)
W powyższy sposób analizujemy wszystkie porty znajdujące się po wpisaniu polecenia netstat –aon

Atak na siebie

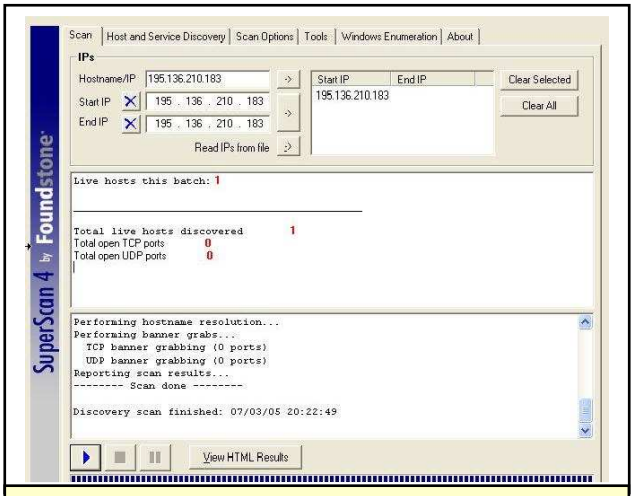
Internetowi włamywacze we wstępnej fazie ataku wykorzystują skanery portów. Umożliwia to im znalezienie potencjalnej ofiary wraz z informacjami o słabych punktach celu ataku. Uzyskują w ten sposób wiedzę na temat otwartych portów, jak również o uruchomionych usługach, pozwalają także ustalić wersję systemu operacyjnego.
Skanery portów badają kolejno porty komputera za pomocą trzyetapowego uzgadniania połączenia:

- **I** – komputer inicjujący połączenie wysyła pakiet TCP ze znacznikiem SYN;
- **II** – komputer odbierający odsyła pakiet ze znacznikiem SYN i ACK, potwierdzając żądanie utworzenia połączenia;
- **III** – komputer inicjujący odpowiada pakietem ze znacznikiem ACK, co potwierdza odebranie z serwera pakietu ze znacznikiem SYN

Usługa powyższa przeprowadzona jest w całości, gdy klient inicjuje połączenie przez otwarty port. W przypadku inicjacji połączenia przez zamknięty port, na drugim etapie następuje odesłanie pakietu ze znacznikiem RST, zrywającym połączenie. Podczas próby skanowania wyłączonego komputera nie ma żadnej odpowiedzi.

Znaczniki protokołu TCP	
Znacznik	**Funkcja**
SYN	Oznacza początek połączenia
ACK	Potwierdza odbiór poprzedniego pakietu
RST	Służy do natychmiastowego zamknięcia połączenia
FIN	Oznacza koniec połączenia TCP

Posługując się narzędziami, które wykorzystywane są przez włamywaczy możemy sprawdzić słabe punkty naszego komputera, aby je zabezpieczyć, jak również sprawdzić skuteczność naszego firewalla. Do tego celu można posłużyć się darmowym programem o nazwie SuperScan 4.0, który pozwala na badanie portów TCP i UDP oraz zdobywanie dodatkowych informacji, jak system operacyjny. Ponadto program oferuje dostęp do do wielu poleceń sieciowych, jak ping, traceoute, które pozwalają zdobywać ogólniejsze informacje o celu ataku. Wspomniay program dostępny jest na stronie:
www.foundstone.com/resources/proddesc/superscan.htm.



Rys 8: SuperScan 4.0

Sposoby ograniczeń do portów

W celu ochrony można posłużyć się takimi narzędziami, wbudowanymi w Windows, jak zapora ogniowa, filtry TCP/IP, filtry IPSec.
Zapora ogniowa systemu Windows (ICF - Windows XP) pozwala kontrolować porty otwarte dla połączeń internetowych. Zasada działania ICF polega na tym, że ignoruje każdy nieoczekiwany pakiet

przychodzący i kończy połączenie, o ile nie zachodzą dwa warunki:
a) pakiet jest zaadresowany do portu, który ma zgodę na połączenie przychodzące,
b) pakiet ma włączoną tylko flagę SYN.
Zapora działa w trybie niewykrywalnym (jest niewidoczna dla skanerów). Systemowy firewall jest narzędziem, które nie daje wielu możliwości konfiguracji. Dlatego też zazwyczaj stosuje się alternatywne oprogramowanie, narzędzia, które są dostępne w sieci i pełnią funkcje zapory ogniowej. Do naczelnych produktów z tego zakresu należą: Outpost Firewall w wersji Free oraz PRO, Personal Firewall, VisNetic Firewall, BlackICE PC Protection, Kerio Personal Firewall, Personal Firewall, Personal Firewall Plus (McAfee), Sygate Personal Firewall, Sygate Personal Firewall PRO, Norton Internet Security, Norton Personal Firewall, Tiny Personal Firewall, ZoneAlarm, ZoneAlarm PRO. Wymienione produkty należą do czołowych zapór ogniowych i cieszą się uznaniem wśród ekspertów od zabezpieczeń.
Windows XP oraz Windows 2000 pozwalają na stosowanie filtrów TCP/IP. Możliwości tej opcji są niewielkie, gdyż filtrowanie ogranicza się jedynie do pakietów przychodzących i nie ma możliwości filtrowania na podstawie adresów IP.
Konfigurowanie filtrów TCP/IP wygląda następująco:
- w panelu sterowania otwieramy *„połączenia sieciowe”* **>** klikamy prawym przyciskiem myszki *„połączenia lokalne”* > *„właściwości”*,
- na zakładce *„ogólne”* zaznaczamy pozycję *„protokół internetowy (TCP/IP)* > *„właściwości”*, w nowym oknie, w zakładce *„ogólne”* klikamy na *„zaawansowane”*,
- w następnym oknie otwieramy zakładkę *„opcje”*, w polu *„ustawienia opcjonalne”* zaznaczamy pozycję *„filtrowanie TCP/IP”* i klikamy przycisk *„właściwości”*,
- w oknie dialogowym filtrowanie TCP/IP zaznaczamy pole *„włącz filtrowanie TCP/IP (wszystkie karty)”***.**

Rys 9: ustawienie filtrów TCP/IP

IPSec jest solidnym mechanizmem zabezpieczającym, starającym się ukryć wszelkie mankamenty IP. Identyfikuje konkretny ruch IP za pomocą modelu filtrowania, zidentyfikowany ruch może zostać zablokowany, przepuszczony dalej lub zabezpieczony z pomocą uwierzytelnienia lub zaszyfrowania, bądź obu tych metod jednocześnie. Negocjuje bezpieczne połączenie między dwoma komputerami. Działania zabezpieczające mają miejsce w obu komputerach. IPSec obejmuje także inne protokoły zabezpieczeń, poza TCP/IP, łącznie z filtrowaniem pakietów. Filtry IPSec są zazwyczaj wykorzystywane przez bardzo zaawansowanych administratorów.
W trosce o właściwe zabezpieczenie dostępu sieciowego należy pamiętać również o kontroli usług systemowych, pod kątem, które usługi i aplikacje używają otwartych portów. Ponadto należy wyłączyć wszelkie niepotrzebne usługi w systemie operacyjnym. Reasumując, podstawowymi zabiegami, które pomogą nam wzmocnić nasze bezpieczeństwo jest stosowanie:
- zapory ogniowej, którą należy uprzednio przetestować pod kątem jakości jej pracy,
- kontroli usług systemowych i aplikacji, które wykorzystują otwarte porty,
- korzystanie z filtrowania TCP/IP poprzez blokowanie dostępu do portów, które nie muszą być otwarte,
- wyłączenie w systemie niepotrzebnych usług,
- korzystanie z narzędzi Tasklist, Netstat oraz menedżer zadań.

Magdalena Psykowska

Źródła:

1. Bott E, Siechert C, *Bezpieczeństwo Windows XP i Windows 2000,* Warszawa 2003,
2. *http://pl.wikipedia.org*,
3. Janus R, *Zdradliwe porty*, PC Word Komputer Nr 01/2005,
4. *Encyklopedia wiedzy komputerowej*, Komputer Świat Nr 3/03.