T: Serwer plików.

Zadanie1:

Wykorzystując serwis internetowy Wikipedii odszukaj informacje na temat serwera plików.

Zadanie2:

Odszukaj serwery plików w szkolnej sieci komputerowej. Jak tego dokonać?

Zadanie3:

Skonfiguruj system Windows XP tak, by spełniał rolę serwera plików.

Zadanie4:

Zapoznaj się z informacjami publikowanymi na następującej witrynie internetowej
http://technet.microsoft.com/pl-pl/library/cc728059%28WS.10%29.aspx

Przypomnienie:

Źródło poniższych informacji http://sieci-komputerowe.w.interia.pl/referaty/referat4-3.html

Do zarządzania serwerami plików możemy posłużyć się czterema podstawowymi narzędziami:
- Eksploratorem Windows – ponieważ daje dostęp zarówno do dysków, jak i udostępnionych folderów.
- Konsolą Zarządzanie serwerem plików – ponieważ jest konsolą o konkretnym przeznaczeniu, koncentrującą się na dyskach i udziałach.
- Poleceniem net share – ponieważ to narzędzie wiersza poleceń może posłużyć do tworzenia skryptów związanych z udostępnieniem plików.
- Poleceniem diskpart – ponieważ zostało stworzone do zarządzania dyskami, woluminami i partycjami.

Microsoft Windows wykorzystuje kilka portów do realizacji swoich funkcji sieciowych. W starszych wersjach, do Windows Me/NT, były to porty 137, 138 oraz 139. Od Windows 2000 Server message lock wysyłane są przez port 445. Oczywiście, wersje Windows od 2000 są zgodne w dół, a więc obie procedury mogą funkcjonować równolegle.

Port 137

Obsługuje tzw. NetBIOS Name Service. Za jego pomocą Windows przyporządkowuje wzajemnie - podobnie jak w DNS - nazwy komputerów i adresy IP. W określonych wypadkach może to powodować następującą sytuację - jeżeli użytkownik surfuje na windowsowym serwerze WWW, ten ostatni wysyła zapytanie do portu 137 komputera użytkownika. Dzieje się tak, ponieważ serwer windowsowy wykorzystuje funkcję winsock gethostbyaddr() do odczytania nazwy odległego komputera. Funkcja ta jest jednak tak zaimplementowana w Windows, że najpierw następuje próba odczytu przez NetBIOS, a dopiero w razie niepowodzenia wykorzystywany jest odczyt przez DNS. Tego rodzaju ruch powinien być generalnie zabroniony, zarówno wchodzący, jak i wychodzący. Jeżeli dwie sieci windowsowe mają wymieniać dane przez Internet, generalnie należy zastosować VPN.

Port 138

Kryje się za nim usługa NetBIOS datagram service. Za jej pomocą Windows rozsyła głównie informacje o sieci Windows, najczęściej w formie rozgłaszania. Na przykład usługa Windows computerbrowser wykorzystuje informacje NetBIOS do sporządzenia aktualnej listy komputerów w sieci Windows, wyświetlanej w oknie Otoczenie sieciowe. Największe niebezpieczeństwo związane z usługą datagram service polega na tym, że haker może przekonać Windows za pomocą sfałszowanych pakietów, iż jego komputer należy do lokalnej sieci, a więc może w ten sposób obejść różnice zabezpieczeń odnoszących się do komputerów lokalnych i internetowych. Również i tu obowiązuje zasada, że port ten należy zamknąć w obu kierunkach.

Port 139

Przez tę usługę NetBIOS Session Service odbywa się właściwa wymiana danych w sieciach Windows. Jeżeli port ten jest otwarty, haker może się połączyć z komputerem i próbować zhakować udostępnianie plików i drukarek. Najczęściej wykorzystywana metoda to atak siłowy, polegający na wypróbowaniu jak największej liczby prawdopodobnych haseł. Otwarty port 139 może powodować jeszcze inne problemy. Usługa Windows Messenger nasłuchuje tu w oczekiwaniu na wiadomości, przesyłane za pomocą net send, co często jest wykorzystywane do spamowania. W takim wypadku użytkownik nie

otrzymuje e-mailu; od razu otwiera się okno z wiadomością nadesłaną przez spamera. Dlatego port ten powinien być zamknięty w obu kierunkach.

Sieć Microsoft - port 135

Nawet jeśli port 139 jest zamknięty, nie chroni nas to do końca przed spamem nadsyłanym z wykorzystaniem Messengera. Polecenie net send wykorzystuje nieudokumentowaną funkcje usługi Microsoft RPC, która w porcie 135 (epmap, endpoint mapper) nasłuchuje w oczekiwaniu na nadchodzące zapytania RPC. Usługa ta oferuje m.in. połączenie z Messengerem, a więc net send może wykorzystać tę drogę jako alternatywę, gdy normalny dostęp przez port 139 nie jest możliwy. Są już narzędzia do rozsyłania spamu, które wykorzystują tę metodę.

Port 445

W Windows 2000 Microsoft rozszerzył protokół SMB o możliwość wykonywania przez TCP/IP, z pominięciem okrężnej drogi "NetBIOS over TCP/IP". Windows używa w tym celu wyłącznie portu 445 (microsoft-ds). W otoczeniu składającym się wyłącznie z Windows 2000, XP i .NET Server 2003 można go wyłączyć, odznaczając NetBIOS over TCP/IP w opcjach karty sieciowej. Na skutek tego odczytywanie nazw w sieci LAN będzie się odbywało tylko przez DNS, ale już nie poprzez WINS lub rozgłaszanie NetBIOS. Potrzebny jest zatem albo serwer DNS w sieci LAN, który będzie zarządzał również lokalnymi komputerami (choćby Windows 2000 jako serwer DHCP i DNS), lub na każdym komputerze trzeba założyć listę hostów. Dla portu 445 obowiązuje zasada, że ruch SMB dozwolony jest tylko wewnątrz sieci LAN. Poprzez port 445 rozpowszechniany jest Rozproszony Serwer Plików DFS.