1. **Co to jest czarna lista w poczcie elektronicznej?**

Jest to lista serwerów niebezpiecznych przez możliwość wysyłania za ich pomocą SPAM-ów. Lista komputerów od których poczta nie jest przyjmowana.

1. **Jakie wersje serwerów Windows są preferowane do roli serwerów?**

# Windows 2000 serwer

Windows 2003 serwer

Windows NT

1. **W jakich zastosowaniach niezbędne jest użycie systemu Windows jako serwera?**

Jeżeli potrzebna jest usługa, która wymaga systemu Windows i nie można jej zastąpić. Przykładem może być ASP (ASP (Active Server Page) jest technologią Microsoft-u służącą do tworzenia dynamicznych stron WWW po stronie serwera).

1. **Jakie są podstawowe zadania administratora?**
   * Zarządzanie użytkownikami i zasobami,
   * Zarządzanie usługami sieciowymi (poczta elektroniczna)
   * Wybór sprzętu i najlepsza konfiguracja
   * Archiwizacja danych
   * Aktualizacja danych
   * Ochrona antywirusowa
2. **Na czym polega błąd w procedurze powiadamiania, czy aby nie zawiera wirusa na serwerze pocztowym?**

Antywirus wykrywa wirusa w liście i pisze do nadawcy, że od niego wysłano wirusa ale nadawca nie istnieje, ponieważ wirus go zmienił a tylko kontakt ściągnął ze skrzynki.

1. **Co daje użycie macierzy RAID 0 w porównaniu z pojedynczym dyskiem?**

Raid 0 polega na podziale danych na mniejsze fragmenty danych i zapisywanie ich na dwóch oddzielnych dyskach, które powinny być o jednakowych parametrach tzn. jednakowa pojemność, prędkość obrotowa itd. Zapis danych w ten sposób znacznie przyśpiesza ich zapis.

1. **Co daje użycie macierzy RAID 1 w porównaniu z pojedynczym dyskiem?**

Raid 1 polega na jednoczesnym zapisie tych samych danych na dwa dyski jest to tak zwany mirroring. Zapis danych w ten sposób zabezpiecza nas przed utratą danych w wyniku uszkodzenia jednego z dysków, ponieważ te same dane znajdują się na dwóch różnych dyskach.

1. **Co to jest RAID 0 + 1?**

Jest to połączenie raidu 0 i raidu 1. Do tej macierzy potrzebujemy min. czterech dysków. Dane zapisywane są za pomocą raid 0 i jednocześnie jest wykonywany raid 1 dla dysków pracujących w raid 0. Cały czas jest tworzona kopia dysków pracujących w raid 0.

1. **Co to jest RAID 5?**

Jest to połączenie trzech dysków w macierz. Dane zapisywane są na dwóch dyskach a na trzecim jest zapisywana kod parzystości obliczany przez kontroler. W wyniku uszkodzenia jednego z dysków dane można odzyskać dzięki kodom parzystości.

1. **Wady pełnej archiwizacji?**

Za każdym razem archiwizowane są wszystkie dane co wydłuża czas archiwizacji, zwiększa koszt oraz liczbę nośników.

1. **Jak często należy wykonywać archiwizację i dlaczego?**

Archiwizację należy wykonywać, gdy utrata przechowywanych danych niesie za sobą straty. Archiwizację należy przeprowadzać tak często aby w momencie awarii straty były jak najmniejsze.

1. **Co to jest Archiwizacja przyrostowa?**

Jest to archiwizacja, która zapisuje wszystkie zmienione lub nowoutworzone pliki od ostatniej archiwizacji pełnej lub przyrostowej. Oznacza ona plików jako zarchiwizowanych. Do późniejszego odzyskania danych potrzebna jest ostatnia archiwizacja pełna i wszystkie przyrostowe wykonane od momentu wykonania archiwizacji pełnej. Wtedy gdy obciążenie jest małe lepiej wykonać archiwizację pełną.

1. **Co to jest Archiwizacja różnicowa?**

Jest to archiwizacja, która zapisuje wszystkie zmienione lub nowoutworzone pliki od ostatniej archiwizacji pełnej lub różnicowej. Nie oznacza ona plików jako zarchiwizowanych. Do odzyskania danych potrzebna jest ostatnia archiwizacja pełna i ostatnia archiwizacja różnicowa. Wtedy gdy obciążenie jest małe lepiej wykonać archiwizację pełną.

1. **Co to jest Archiwizacja kopiująca?**

Archiwizacja ta kopiuje wszystkie wybrane pliki ale nie oznacza ich jak zarchiwizowane. Ten rodzaj archiwizacji nie wpływa w żaden sposób na pozostałe archiwizacje.

1. **Co to jest Archiwizacja dzienna?**

Archiwizacja ta kopiuje wszystkie wybrane pliki, które zostały zmodyfikowane w dniu archiwizacji ale nie oznacza ich jak zarchiwizowane.

1. **Dlaczego stosuje się w serwerach system plików z dziennikiem?**

Pliki z dziennikiem są bezpieczniejsze a start systemu po awarii jest dużo krótszy.

1. **Jak zdalnie bezpiecznie można pracować w Linux-ie?**

Za pomocą tunelowanie w SSH programu VNC (Virtual Network Computing) lub XWindows.

1. **Jak zdalnie bezpiecznie można pracować w Windows?**

Za pomocą tunelowanie w SSH programu VNC (Virtual Network Computing) lub XWindows albo MS Terminal Server.

1. **Co to jest serwer?**

Jest to komputer udostępniający zasoby i usługi innym użytkownikom.

1. **W jakich zastosowaniach system Windows nie powinien być stosowany jako serwer?**

We wszystkich zastosowaniach, przy których nie jest to absolutnie konieczne.

1. **Dlaczego środowisko graficzne nie jest wskazane na serwerze?**

Ponieważ zajmuje zasoby i może zawierać błędy a na serwerze powinno być tylko instalowane oprogramowanie niezbędne do jego pracy.

1. **Na czym polega kontrola przekazywanie poczty (relay), podać kryteria?**

Umożliwia przekazywanie poczty do innych adresów wiadomości nadchodzących z danego adresu. Serwer poczty, który jest tak skonfigurowany, że umożliwia nieautoryzowanym użytkownikom podłączenie się do niego i wysyłanie poczty nazywany jest **open-relay.**

1. **Co to jest MBSA i jak działa?**

MBSA (Microsoft Baseline Security Analyzer) –Program umożliwia skanowanie lokalnych albo zdalnych systemów Windows w celu wykrycia typowych błędów w konfiguracji zabezpieczeń lub brakujących uaktualnień związanych z zabezpieczeniami. MSBA skanuje następujące systemy: Windows NT, Windows 2000, Windows XP, Windows 2003 Server, IIS, MS SQL Server, IE, Office

1. **Co to jest SNORT i jak działa?**

To bardzo silny sieciowy system wykrywania ataków (ang. Network Intrusion Detection System, NIDS), który daje szeroki wachlarz mechanizmów detekcji, mogących w czasie rzeczywistym dokonywać analizy ruchu i rejestrowania pakietów w sieciach opartych na protokołach IP\TCP\UDP\ICMP. Potrafi przeprowadzić analizę strumieni pakietów, wyszukiwać i dopasowywać podejrzane treści, a także wykrywać wiele ataków i anomalii, takich jak przepełnienie bufora.

1. **Co to jest IDS i jak działa?**

IDS (Intrusion Detection System) – System wykrywania ataków i blokowania ich w czasie rzeczywistym określany również jako „in-line IDS”. Atak jest blokowany przed przedostaniem się do chronionych zasobów systemu. IDS blokuje pakiety, które wykonują atak. IDS realizuje także funkcje firewall-a.

1. **Co to jest IIS?**

IIS (Internet Information Services) – Internetowe usługi informatyczne. Jest serwerem dołączonym do rodziny systemów Microsoft Windows Serwer, a także Microsoft Windows XP. Pełni rolę serwerów HTTP i FTP. Najnowszy IIS 6 korzysta z czterech głównych procesów:

* + HTTP.sys
  + WAS (Web Administration Services)
  + Procedury obsługi aplikacji \ procedury robocze
  + IIS Admin Service

1. **Co to jest Tripware?**

Jest to program napisany w C w 1992 roku. Operuje on bazą danych kluczy plików, na podstawie której stwierdza w których plikach zaszły zmiany. Porównuje on aktualne klucze plików w momencie sprawdzania z ich odpowiednikami w bazie danych, zawierającej początkowe klucze plików. Tripware operuje metodami: MD5, MD4, MD2, CRC32. Pomaga on wykryć pliki w których zostały dokonane zmiany.

1. **Co to jest MD5?**

Jest to technika zapewniająca 99,9% skuteczności w wykrywaniu zmian w plikach. Polega na przepuszczaniu plików przez system algorytmów MD (message digest). MD5 generuje dla każdego pliku 32 znakowy klucz i można go zapisywać do bazy danych takich kluczy w celu późniejszego ich porównania.

1. **Co to jest AIDE i jak działa?**

AIDE (Advanced Intrusion Detection Environment) – umożliwia sprawdzenie wielu atrybutów pliku m.in.: praw dostępu, numeru inode, rozmiaru pliku, access time, change time itd. a także kryptograficznych sum MD5, SHA i CRC32. Działa na podobnej zasadzie jak Tripware porównuje wartość klucza pliku w momencie sprawdzania z wartością klucza przechowywanego w bazie dla tego pliku.

1. **Co to jest BOTNET i jak działa?**

Termin **BOTNET** oznacza sieć zainfekowanych komputerów zwykle kontrolowanych zdalnie przez jednego użytkownika. W następujących celach:

* + Rozsyłania spam-u
  + Przeprowadzania ataków odmowy usługi DDoS
  + Zachęcania do odwiedzania pewnych witryn
  + Zdobywania wiadomości na temat właściciela zainfekowanej maszyny
  + Bezpośredniego zarabiania pieniędzy

1. **Co to jest DDoS?**

DDoS (Distributed Denial of Service) atak na systemy komputerowe lub usługi sieciowe równocześnie z wielu komputerów w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów.

1. **Co może naruszyć integralność systemu?**
   * Wirus, który powoduje zmiany
   * Człowiek
   * Robaki internetowe wnikające do systemu
2. **Co to jest Stert wirus?**

Jest to wirus komputerowy działający w tle „ukryty”. W celu jego usunięcia należy uruchomić migawkę ale z innego systemu.

1. **Co to jest HOT PLUG-IN?**

Jest to wymian komponentów na gorąco np.: wymian karty sieciowej podczas działania systemu.

1. **Co to jest SCSI?**

SCSI (Small Computet Systems Interface) – równoległa magistrala danych przeznaczona do przesyłania danych pomiędzy urządzeniami. Wszystkie podłączone do magistrali urządzenia są równorzędne. Każde urządzenie podłączone do magistrali SCSI posiada w jej obrębie unikatowy numer SCSI ID. Do kontrolera SCSI można podłączyć do 16 dysków na jednej taśmie.

1. **Co to jest system WELCOME \ LAN?**

Jest to system umożliwiający włączenie komputera z sieci. Podsystem sieciowy wymaga podtrzymania gdy komputer jest wyłączony.

1. **Co to jest CMS?**

CMS (Content Managet System) – system zarządzani treścią. Jego działanie polega na umożliwieniu użytkownikowi w prosty sposób aktualizację zawartości strony WWW za pomocą prostego interfejsu użytkownika. Interfejs ten jest zazwyczaj w postaci strony WWW wypełnionej prostymi formularzami za pomocą których można zmieniać zawartość strony.

1. **Co to jest FTP?**

FTP (File Transfer Protocol) – jest protokołem transmisji plików typu klient-serwer, który umożliwia przesyłanie plików z i na serwer za pomocą sieci TCP\IP. FTP jest protokołem 8 bitowym. FTP działa w 2 trybach **aktywnym i pasywnym.**

Jeżeli działa w trybie aktywnym wykorzystuje port 21 dla poleceń oraz 20 do przesyłanie danych. Połączenie jest nawiązywane wówczas przez serwer.

Natomiast gdy pracuje w trybie pasywnym wykorzystuje port 21 dla poleceń a port o numerze większym od 1024 do transmisji danych, gdzie obydwa połączenia zestawiane są przez klienta.

1. **Co to jest SSH?**

SSH (Secure Shell) – jest to standard protokołów komunikacyjnych używanych w sieciach komputerowych TCP\IP o architekturze klient-serwer. **SSH** to następca znanego protokołu **TELNET,** służącego do terminalowego łączenia się ze zdalnym komputerem. SSH różni się tym od TELNETU, że transfer wszystkich danych jest zaszyfrowany, oraz możliwe jest rozpoznawanie użytkowników na wiele różnych sposobów.

1. **Co to jest SFTP?**

Jest to FTP z SSH2. SFTP wywodzi się z systemów uniksowych i jego stosowanie pod windows-em nie jest wykluczone tylko należy wcześniej zainstalować emulator środowiska uniksowego pod windows-em. SFTP umożliwia szyfrowane przesyłanie plików.