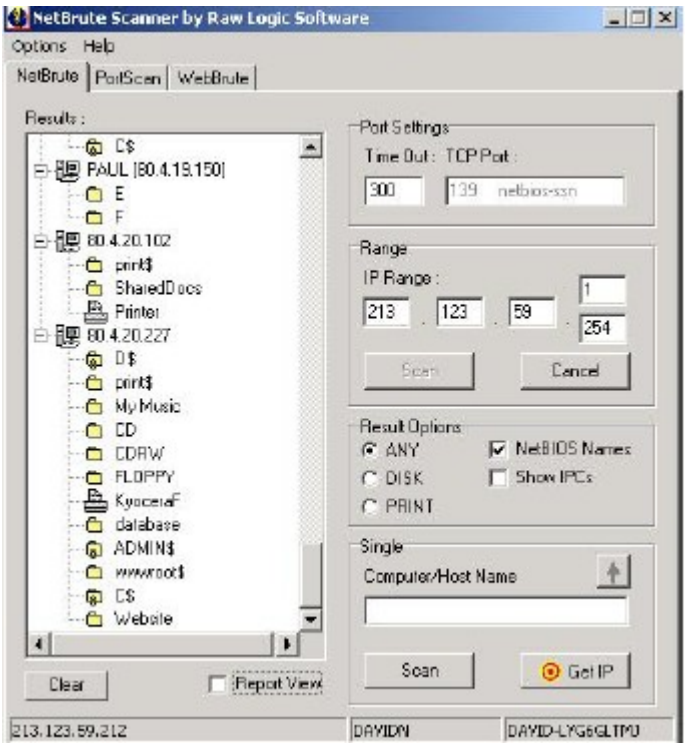
HACKING

Jak uzyskać dostęp do systemów innych ludzi

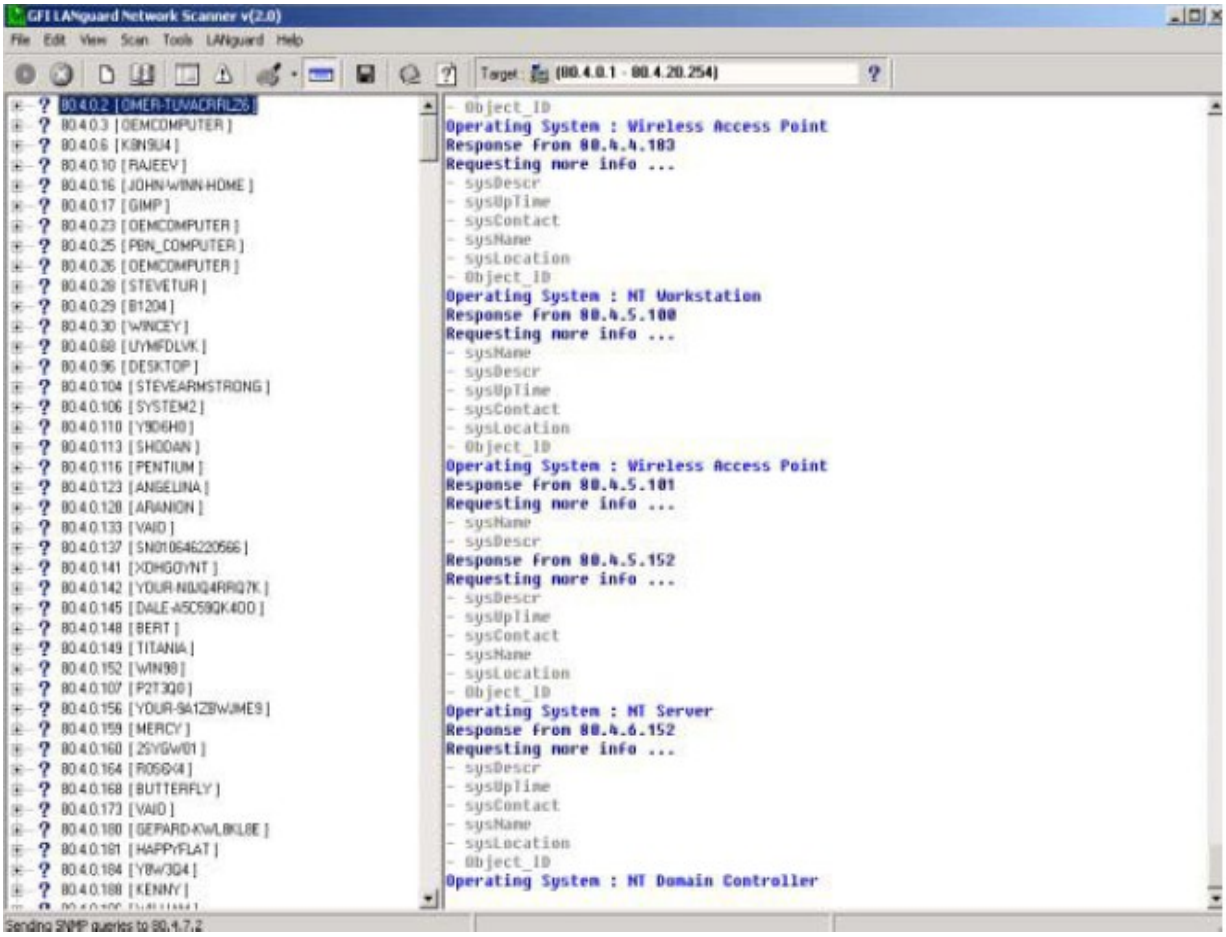
WPRROWADZENIE

Autor nie ponosi żadnej odpowiedzialności za nadużycie tych informacji. Jest przeznaczony tylko dla celów edukacyjnych. Możesz być zaskoczony w jaki sposób jesteś narażony. Jako refleksję dodałem sekcję o dostępie do bazy danych ze względu na liczbę żądań. Wiekszość skutecznych ataków na systemy komputerowe przez Internet można przypisać wykorzystaniu luk w zabezpieczeniach oprogramowania i systemów operacyjnych. Te kilka luk w zabezpieczeniach oprogramowania stanowi większość skutecznych ataków, po prostu napastnicy są oportunistami – wybierają najłatwieszą i najwygodniejszą trasę. Wykorzystują najlepiej znane wady z najbardziej skutecznymi i powszechnie dostępnymi narzędziami ataku. Większość oprogramowania, w tym systemy operacyjne i aplikacje, zawiera skrypty lub programy instalacyjne. Celem tych programów instalacyjnych jest możliwość instalacji systemów tak szybko jak to możliwe, z włączonymi najczęściej używanymi funkcjami, z najmniejszą ilością pracy wykonywanej przez administratora. Aby osiągnąć ten cel, skrypty te instalują więcej komponentów niż potrzebne jest użytkownikowi. Filozofia sprzedawcy jest taka , aby włączyć funkcje, które nie są potrzebne, niż wykonywać instalację użytkownikowi funkcji , które mu są potrzebne. Takie podejście , chociaż wygodne dla użytkownika, tworzy wiele niebezpiecznych luk z bezpieczeństwie ponieważ użytkownicy nie zarządzają aktywnie i nie poprawiają komponentów oprogramowania, których nie używają. Ponadto, wielu użytkowników nie zdaje sobie sprawy co faktycznie jest zainstalowane, pozostawiając niebezpieczne próbki w systemie, ponieważ użytkownicy nie wiedzą że one istnieją. Te niepoprawione usługi dostarczają ścieżki atakującemu na przejęcie twojego komputera. Dla systemów operacyjnych, domyślne instalacje niemal zawsze obejmują usługi zewnętrzne i odpowiednie dla otwartych portów. Atakujący włamują siędo systemu przez te porty. W większości przypadków im mniej portów masz otwartych, tym mniej możliwości ma atakujący aby wykorzystać lukę bezpieczeństwa sieci. W przypadku aplikacji, instalacja domyślna zawiera zwykle niepotrzebne próbki programów lub skrypty. Jedną z najpoważniejszych luk w serwerach WWW są próbki skryptów; atakujący używa tych skrytpów do złamania systemu lub uzyskania informacji na jego temat. W większości przypadków, administrator systemu którego system jest naruszony nie zdaje sobie sprawy z zainstalowanych przykładowych skryptów. Takie skrypty są problemem, poneważ zazwyczaj nie przechodzą przez ten sam proces kontroli jakości jak pozostałe oprogramowanie. W rzeczywistości są one szokująco źle napisane w wielu przypadkach. Sprawdzanie błędów jest często zapominane a takie skrypty oferują podatny grunt dla ataków przepełnienia bufora. Najprostszy sposób aby uzyskać dostęp do systemu to po porstu udostępnianie plików i drukarek. Jest to stosowane aby zezwolić innym osobom w sieci LAN na współdzielenie plików, drukarek i połączeń internetowych. Jeśli komputer ma włączone udostępnianie plików i drukarki, to w rzeczywistości daje współdzielenie tych zasobów, często, w całym Internecie! Wynika to głównie z faktu, że Netbios był pierwotnie

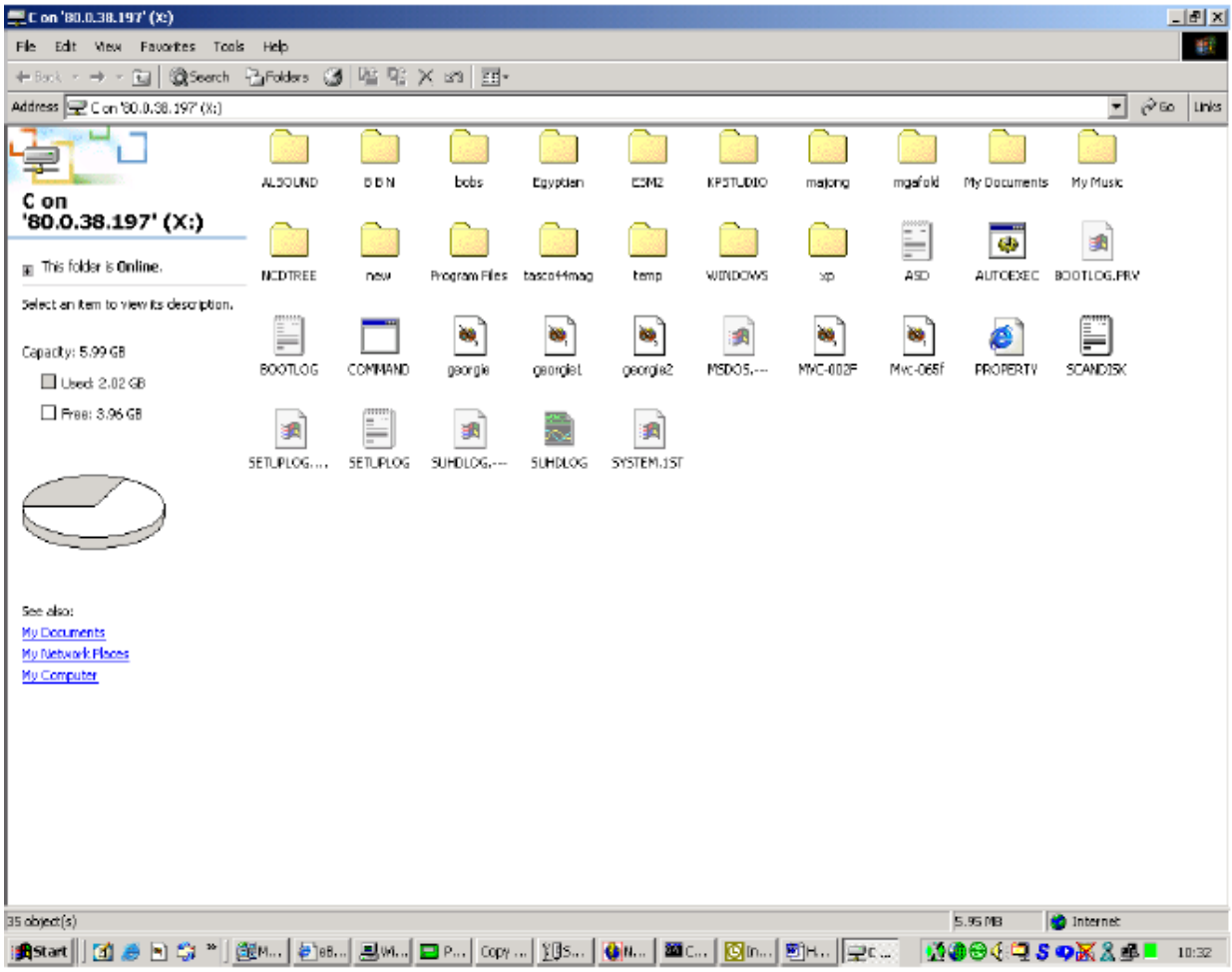
przeznaczony dla sieci lokalnych (LAN), gdzie zaufane współdzielenie zasobów miało sens z wielu powodów. Nigdy nie miało to "wyjść na świat".
Po pierwsze, wyszukujemy przy użyciu skanera Netbios, dla systemu z włączonym współdzieleniem. Program taki jak Netbrute formy raw Logic Software jest idealny. Programy te mogą pomóc hackerom jak i administratorom sieci. Uruchom skanowanie podsiec, na przykład w zakresie adresów IP od 80.1.1.1 do 80.1.1.254. Wybierz system, który ma cały dysk współdzielony (Byłbyś zdziwiony ile ludzi jest tak głupich!!!), pojawią się wyniki takie jak \\80.5.7.2\C lub podobne. Po prostu skopiuj i wklej ten link do paska adresowego Windows Explorera i wciśnij Enter! To jest zrzut działania Netbrute:



Aby uzyskać informacje bardziej wszechstronne, użyj narzędzia takiego jak Languard Network Scanner. Zwraca ono informacje takie jak nazwy domen, nazwy logowania i wiele innych. Oto jego zrzut:



Czy muszę coś dodawać? Jeśli znajdziesz system w którym katalog główny C: jest współdzielony, wtedy na systemie Windows 9.x będziesz miał dostęp o całego dysku twardego. W systemach Windows NT/2000, będziesz miał dostęp tylko zgodne z uprawnieniami dostępu do pliku NTFS. Oto zrzut ekranu Windows Explorera wskazującego katalog główny:



Możesz nawet odwzorować go na dysku sieciowym (użyj narzędzia > map network drive), takie to proste! Aby uzyskać lepsze wyniki, polecam wybór systemów z "lepszym niż modemowe" połączeniem. Jeśli nie wiesz od czego zacząć, wypróbuj swój adres IP. Aby to zrobić wykonaj następujące czynności:

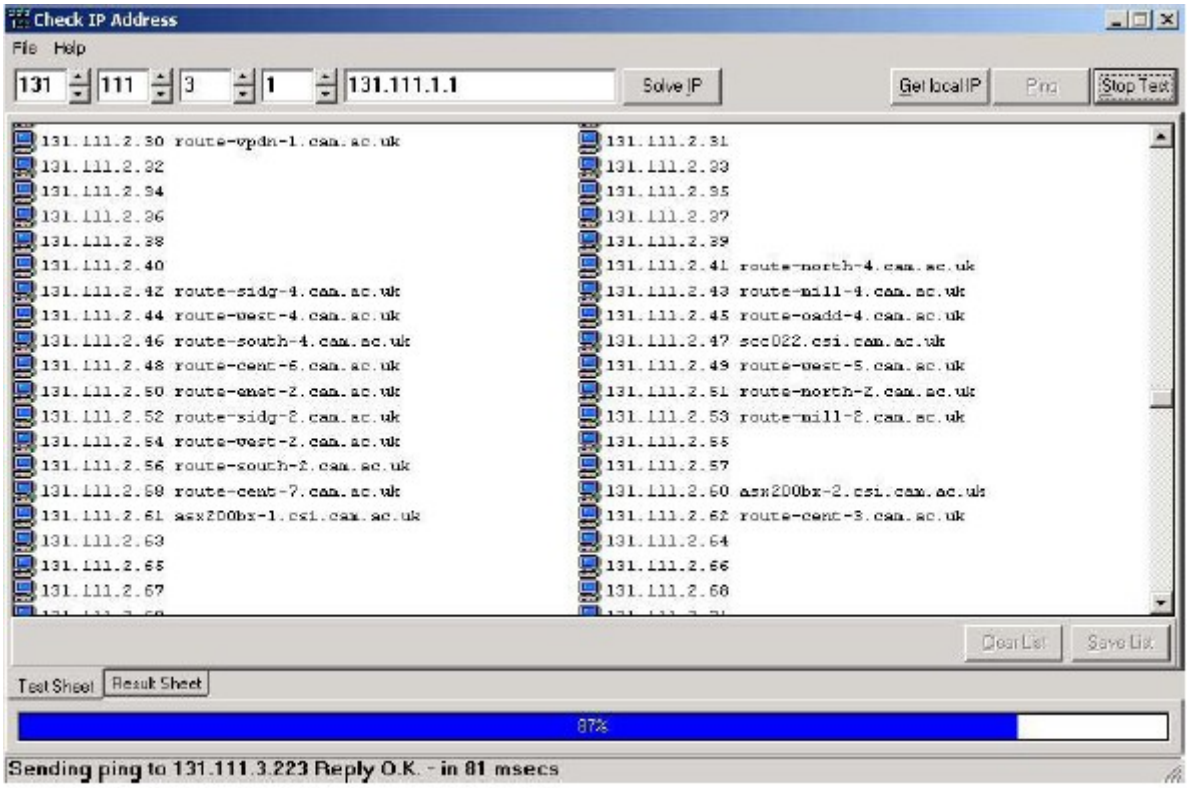
- Dla Windows 9.x, przejdź do Start > Programy > Akcesoria > Wiersz poleceń i wpisz "Winiconfig aby uzyskać sój adres IP
- Dla Windows NT/2000 przejdź do Start > Programy > Akcesoria > Wiersz poleceń i wpisz "ipconfig"

Zwróci to twój adres IP. Jeśli używasz połączenia modemowego, będziesz musiał połączyć się pierwszy. Dla "zawsze na kablu" pomiń ten krok. Następnie należy uruchomić skanowanie podsieci, np. jeśli adres IP 164.99.32.212 wtedy spróbuj skanowa od 164.99.34.1 do 164.99.34.254. To powinno wystarczyć na początek. Miłej zabawy...

Skanowanie IP

To proste skanowanie po prostu pinguje zakres adresów IP aby znaleźć aktywne komputery. Zwróć uwagę ,że bardziej wyrafinowane skanery będą używały różnych protokołów (takich jak SNMP sweep) o wykonanie tej samej rzeczy. Jest to bardzo prosta technika która

wymaga trochę wyjaśnień. Jest jednak użyteczna dla nazwy domeny również zwracanej



Skanowanie Portów

Ta sekcja wprowadza wiele technik używanych do określania jaki port (lub podobne abstrakcyjne protokoły) hosty nasłuchują połączenia. Porty te stanowią potencjalne kanały komunikacyjne. Odwzorowanie ich istnienia ułatwia wymianę informacji z hostem, a więc jest bardzo przydatne dla osób pragnących poznać ich środowisko sieciowe, szczególnie hackerów. Mimo tego o czym słyszeliście z mediów, nie jest to wyłącznie port TCP 80, wyorzystywany przez protokół przeysłu hipertektu (HTTP) Każdy kto opiera się wyłącznie WWW dla uzyskiwania informacji może też uzyskać średni poziom biegłości. Ta sekcja ma służyć jako wprowadzenai do sztuki skanowania portów, w której system hosta można przekonać do zdradzenia swoich tajemnic. Aby to zrobić trzeba mieć dostęp do skanera portów. Istnieje wiele zarówno darmowych jak i za niewielką opłata. Powinien on mieć wszystkie te cechy:

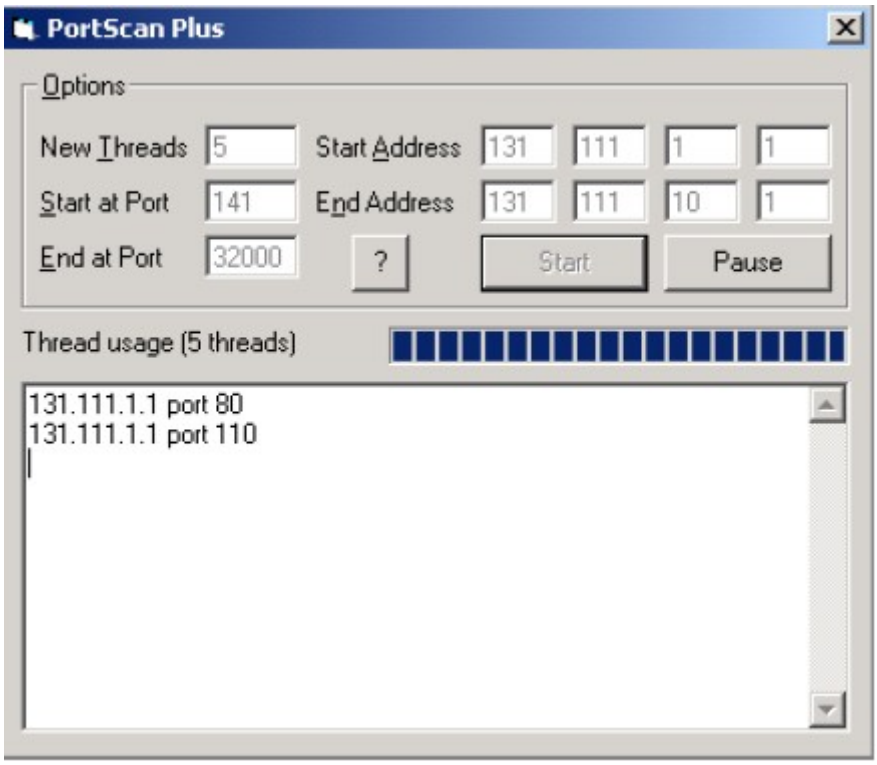
- dynamiczne obliczanie czasu opóźnienia: Niektóre skanery wymagają dostarczenia opóźnienia między wysyłaniem pakietów. Ale jak mam wiedzieć czego używać? Zawsze można je spingować, ale to jest bolesne,a także czas reakcj hostów zmienia się dramatycznie gdy są floodowane zapytaniami. Podstawową techniką znajdowania początkowego opóźnienia jest czas wewnętrznej funkcji "pinh", Można też próbować connect() do zamkniętego portu na komputerze docelowym. Można też wybrać odpowiednią wartość domyślną.

- Retransmisja: Niektóre skanery tylko wysyłają wszystkie pakiety zapytania i zbierają odpowiedzi. Ale to prowadzi do fałszywych dodatnio lub ujemnie w przypadku kiedy pakiety są odrzucane. Jest to szczególnie ważne dla "ujemnego" stylu skanowania UDP i FIN, gdzie tym czego szukasz jest port który NIE odpowiada.
- Skanowanie portu równoległego: Niektóre skanery po prostu skanują porty liniowo, jeden po drugim, aż do 65535. To rzeczywiście działa dla TCP w bardzo szybkiej sieci lokalnej, ale szybkość taka nie jest akceptowalna w szerszych sieciach takich jak Internet. Najlepiej używać non-blocking I/O i skanowania równoległego we wszystkich trybach TCP i UDP.
- Elastyczna specyfikacja portu: Nie zawsze chesz skanować wszystkie 65535 portów! Ponadto, skanery które pozwalają tylko na skanowanie portów 1 – N nie spełniają potrzeb. Skaner powinien zezwalać na określenie dowolnej liczby portów i zakresu skanowania. Na przykład, '21-25,80-113' jest często przydatne jeśli tylko sondujesz najczęściej używane usługi.
- Elastyczna specyfikacja celu: Możesz często chcieć skanować więcej niż jeden host i z pewnością nie chcesz nasłuchiwać każdego pojedynczego hosta w dużej sieci! Użyteczne jest skanowanie, powiedzmy podsieci przy np 131.111.11.0 – 131.111.11.254
- Wykrywani hostów w dół: Niektóre skanery umozliwiają skanowanie dużych sieci, ale marnują mnóstwo czasu na skanowanie 65535 portów martwego hosta! Irytujące! Zalecam stosowanie skanera, który pozwala na przerwy czasowe.
- Wykrywanie adresu IP: Z jakiegoś powodu, wiele skanerów prosi o podanie twojego adresu IP jako jednego z parametrów. Nie chcesz wykonywać 'ipconfig' i wyszukiwać bieżącego adresu IP przy każdym połączeniu. Oczywiście, widziałem skanery wymagajace rekompilacji przy każdej zmianie adresu!.

W rzeczywistości jest 65535 portów;jednak usługi jakie znamy najlepiej są na portach o niskich numerach. Oto kilka z nich:

FTP	21
Telnet	23
SMTP	25
HTTP	80
POP3	110

Mimo ,że usługi mogą być skonfigurowane do używania innych portów, jest to bardzo nietypowe. Porty powyżej 1024 wydają się być używane przez system operacyjny. Zasadniczo skaner portów wysyła pakiety danych na każdy port i nasłuchuje odpowiedzi dla określenia jakie usługi są uruchomione. Szczegółowa lista na końcu tego tekstu. Oto przykład prostego skanera portów w użyciu:



Podgląd topologii sieci

To może być użyteczne okazyjnie. Stanowi graficzne odwzorowanie zasobów sieci. Na przykład, może pokazać jakie systemy są za firewallemi które routery są on-line.

Sniffowanie pakietów

Sniffer pakietów lub analizator protokołów jest urządzeniem do podsłuchu łączy podłączanym do sieci komputerowej i podsłuchuje ruch sieciowy. Jak podłsuch telefoniczny, pozwala na podsłuchiwanie rozmów innych ludzi, program "sniffowania" umożliwia komuś nasłuchiwanie rozmów komputerów. Jednak rozmowy komputerów składają się z pozornie losowych danych binarnych. Dlatego też programy do podsłuchu sieci wyposażone są w funkcję "analizy protokołu", który pozwala im "dekodować" ruch komputerowy i rozumie go. Sniffing ma jedną przewagę nad podsłuchiwaniem telefonów: wiele sieci pozwala na "współdzielenie mediów". Oznacza t o,ze nie musisz włamywać się do węzłów dystrybyucji okablowania aby zainstalować podsłuch, możesz zrobić to z prawie każdego połączenia sieciowego, aby podsłuchiwać sąsiadów. Nazywa się to sniffowaniem w "trybie odbierania". Jednak, ta "wspólna" technologia szybko porusza się w kierunku technologii "komutowanej" gdzie nie będzie to dłużej możliwe. Nie ma jednego punktu w Internecie, gdzie można "zobaczyć" cały ruch. Łączność z Internetem wygląda podobnie do sieci rybackiej. Ruch przepływa przez sieć,a żaden pojedynczy punkt nie będzie widział wszystkiego! Internet został zbudowany aby wytrzymać atak nuklearny i przetrwać wszystkie "pojedyncze punkty awarii"

Zapobiega to również pojedynczemu punktowi sniffowania. Rozważmy taką sytuację: masz dwa komputery w biurze komunikujące się ze sobą i oba są w Internecie. Wybierają bezpośrednią drogę komunikacji, a ruch nigdy nie przechodzi przez zewnętrzną część publiczną Internetu. Wszelka komunikacja gdziekolwiek w sieci jest oparta na zasadzie "jak najmniejsze koszty". Ethernet został zbudowany wokół "wspólnej" zasady: wszystkie komputeryu w sieci lokalnej współdzielą ten sam kabel. Implikue to ot ,że wszystkie komputry moga "widzieć" cały ruch na tym kablu. Dlatego sprzęt Ethernet jest budowany w "filtrem" który ignoruje cały ruch, który nie należy do niego. Czyni to przez ignorowanie wszystkich ramek których adres MAC nie pasuje do ich własnych. Program podsłuchujący skutecznie wyłącza ten filtr, ustawiając sprzęt Ethernet na "tryb odbierania". Zatem, Marek może zobaczyć cały ruch między Alicją i Robertem, tak długo jak są na tym samym kablu Ethernetu. Ponieważ wiele komputerów może spółdzielić jedne kabel Ethernetu, każdy musi mieć indywidualny identyfikator. Nie dzieje się tak przy modemach dial-up, ponieważ zakłada się ,że wszelkie dane przesyłane do modemu do drugiej strony linii telefonicznej.Ale kiedy wysyłsza dane do przez Ethernet musi być jasne do jakiego komputera masz zamiar wysłać te dane. Oczywiście, w wielu przypadkach dzisiaj tylko dwa komputery rozmawiają ze sobą, ale trzeba pamiętać ,że Ethernet został zaprojektowany dla tysięcy komputerów podłączonych do jednego kabla. Osiąga się to przez umieszczenie unikalnej 12 cyfrowej liczby szesnastkowej w każdym elemencie sprzętu Ethernet. Ethernet został stworzony do przenoszenia innego ruchu niż TCP/IP, a TCP/IP został stowrzonydo uruchamiania w stsosunku do innych kabli (np. linia dial-up, które nie używają Ethernetu). Na przykład wielu użytowników domowych instalacji 'NetBEUI' dla udostępniania plików i drukarek, ponieważ jest nie powiązany z TCP/IP,a więc hackerzy z całego Internetu nie mogą dostać się na ich dyski twarde. Surowa transmisja i odbieranie w Ethernecie jest regulowana przez urządzenia Ethernet. Nie możesz po prostu wysłać surowych danych przez kabel, najpierw musisz zrobić coś abyu zrozumiał to Ethernet. W taki sam sposób nie możesz trzymać list w skrzynce pocztowej, musisz najpierw włożyć go do koperty ,zaadresować i nakleić znaczek. Poniżej jest krótkie wyjaśnienie jak to działa:

Alicja ma adres IP: 10.0.0.23
Bernard ma adres IP: 192.168.100.54
Żeby pogadać z Bernardem, Alicja musi stworzyć pakiet IP w formie 10.0.0,23 --> 192.168.100.54. Gdy taki pakiet przechodzi przez Internet, będzie przekazywany z routera na router. W związku z tym alicja musi ręcznie dołączyć do pierwszego routera. Każdy router po drodze będzie badał adres docelowy IP (192.168.100.54) i decydował jaki prawidłowy tor powinien być wybrany. Wszystko co Alicja wie to połączenie lokalne do pierwszego routera i ewentualnie adres IP Bernarda. Alicja nie wie nic o strukturze Internetu i drodze jaka przebywa pakiet. Alicja przekazuje do routera żeby wysłał pakiet. Używa do tego Ethernetu. Ramka Ethernetu wygląda następująco:
Oznacza to ,że stos TCP/IP w komputerze Alicji może stworzyć

pakiet o długości 100 bajtów(powiedzmy 20 bajtów dla info IP, 20 bajtów dla info TCP i 60 bajtów danych). Stos TCP/IP wysyła go do modułu Ethernet, co wstawia 14 bajtów z przodu adresu przeznaczenia MAC, adresu źródłowego MAC i ethertype 0x0800 aby wskazać ,że na drugim końcu stos TCP/IP powinien przetwarzać ramki. Dołącza również 4 bajty na końcu sumy kontrolnej / CRC(sprawdzenie czy ramka zostanie uszkodzona w przewodzie). Karta następnie wysyła bity do kabla. Wszystkie karty sprzętowe na kablu widzą ramkę,wliczając w to kartę routera, sniffera pakietów oraz innych komputerów. Właściwe karty jednak mają chip sprzętowy, który porównuje ramki "przeznaczenia MAC" z własnym adresem MAC. Jeśli nie pasują, wtedy odrzuca ramki. Odbywa się to na poziomie sprzętowym,więc komputer do któego podłączono kartę jest zupełnie nieświadomy tego procesu. Kiedy karta routera Ethernet widzi te ramki, odczytuje je i usuwa czołowe 14 bajtów i końcowe 4 bajty. Wygląda na 0x0800 ethertype i decyduje o wysłaniu ich do stosu TCP/IP (który prawdopodobnie przekazuje je do kolejnego routera w łańcuchu do miejsca przeznaczenia).W powyższym scenariuszu, tylko ROUTER komputera przypuszczalnie widzi ramkę Ethernet, a wszystkie inne komputery je ignorują Podłuch jednak łamie te zasady i kopiuje również ramki dołączone do sieci. Abyś mógł zobaczyć swój adres Ethernet zrób co następuje
Uruchom program "ipconfig /all" z wiersza poleceń. Pokaże się adres MAC twojej karty. Oto przykład:

Windows NT IP Configuration
Host Name . . . . . : sample.robertgraham.com
DNS Servers . . . . . : 192.0.2.254
Node Type . . . . . : Hybrid
NetBIOS Scope ID. . . . . :

IP Routing Enabled. . . . : Yes
WINS Proxy Enabled. . . . : No
NetBIOS Resolution Uses DNS : No
Ethernet adapter SC12001:

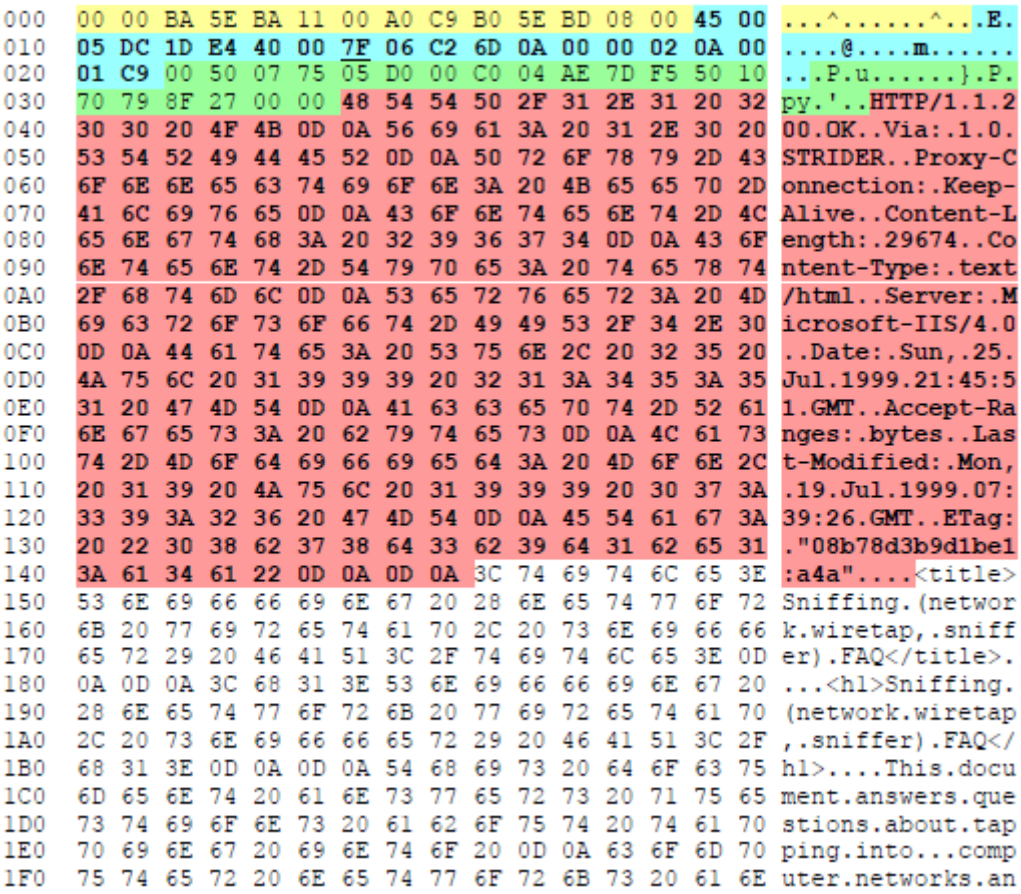
Description . . . . . : DEC DC21140 PCI Fast Ethernet Adapter

Physical Address. . . . . : 00-40-05-A5-4F-9D
DHCP Enabled. . . . . : No
IP Address. . . . . : 192.0.2.160
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.0.2.1
Primary WINS Server . . . . : 192.0.2.253
Linux
Run the program “ifconfig”. Here is a sample result:

eth0 Link encap:Ethernet HWaddr 08:00:17:0A:36:3E
inet addr:192.0.2.161 Bcast:192.0.2.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1137249 errors:0 dropped:0 overruns:0
TX packets:994976 errors:0 dropped:0 overruns:0

Interrupt:5 Base address:0x300

Solaris: Użyj polecenia "arp" lub "netstat -p", które wylistują lokalny interfejs między wejściamio ARP
Oto przykładowy pakiet przed dekodowaniem:



Jest to standardowa reprezentacja "szesnastkowego zrzutu" pakietu sieciowego, przed zdekodowaniem. Zrzut szesanstkowy ma trzy kolumny: offset każej linii, dane szesnastkowe i odpowiednik ASCII. Pakiet zawiera 14 bajtowy nagłówek Ethernetowy, 20 bajtowy nagłówek IP, 20 bajtowy nagłówek TCP, nagłówek HTTP kończący się dwoma wysuwami linii (0D 0A 0D 0A) a potem dane. Powodem pokazania zarówno szesnastkowo jak i w ASCII jest to ,że czasami jedne są łatwiejsze do odczytania od drugich. Na przykład, w górnej części pakietu, ASCII wygląda bezużytecznie, ale szesnastkowo jest czytelny, i można powiedzieć,że mój adres MAC to 00-00-BA-5E-BA-11. Każdy pakiet zawiera 14 bajtowy nagłówek Ethernet, 20 bajtowy nagłówek IP, 20 bajtowy nagłówek TCP nagłówek HTTP kończący się dwoma wysuwami linii (0D 0A 0D 0A) a potem dane. Muszę wyjaśnić słowo szesnastkowo. Słowo "dziesiętny" ma źródło "dec" czyli 10. Ozancza to ,że istnieje 10 cyfr w systemie numeracji:

0,1,2,3,4,5,6,7,8,9

Słowo "szesnastkowy" ma źródło "hex" oznaczające 6 i "dec"; dodając je razem otrzymujemy 16. Oznacza to ,że jest szesnaście cyfr w systemie numeracji: 0,1,2,3,4,5,6,7,8,9, A,B,C,D,E,F

Jest to przydatne, ponieważ wszystkie dane przechowywane są przez

komputer jako "bity" (binary – digits, oznaczające dwie cyfry 0 i 1), ale wszystkie bity są pogrupowane w 8 bitowe jednostki wane "bajtami" lub "oktetami", które w teorii mają 256 cyfr. Bity są dwoma małymi źródłami danych, ponieważ wszystko co widzimy w strumieniu wygląda 00101010101000010101010110101101101011111011, co jest nieczytelne. Podobnie przy użycou 256 cyfr byłoby to niemożliwe: kto jest w stanie zapamiętać ,że jest wiele różnych cyfr? Szesnastka łamie "bajt" na 4 bity "nibble", które mają 16 kombinacji (256 = 16 x 16). To pozwala nam przedstawić każdybajt jako dwie cyfry szesnastkowe. System szesnastkowy pozwala ludziom technicznie zwizualizować podstawowe dane binarne. To jest wyjaśnienie szesnastkowego systemu numeracji

0000 = 0 0001 = 1 0010 = 2 0011 = 3
0100 = 4 0101 = 5 0110 = 6 0111 = 7
1000 = 8 1001 = 9 1010 = A 1011 = B
1100 = C 1101 = D 1110 = E 1111 = F

Innymi słowy, kiedy spotkasz heksadecymalną cyfrę "B" powienieneś natychmiast uwidocznić jej wzorzec bitowy jako "1011" w swojej głowie. Jest to jak zapamiętywanie tabliczki mnożenia jako dziecko. W systemie szesnastkowym często cyfra jest poprzedzona specjalnym znakiem(-ami) Na przykład, kiedy pojawia się cyfra "12", jest to "dwanaście" (dziesiętnie) czy "osiemnaścnie" (szesnastkowo)? Jeśli jest coś heksadecymalne, często jest zapisywane jako "0x12","x12" lub "$12". Były to preferowne wersje, ponieważ musi reprezentować wiele języków programowania. Oczywiście nie jest to konieczne dla zrzutów szesnstkowych, ponieważ fakt ,że chcemy to tak przedstawić założyliśmy wcześniej. Komputery przedstawiają wszystko jako liczby. Oznacza to ,że tekst jaki czytasz jest reprezentowany w komputerze jako liczby.ASCII jest jedną z takich reprezentacji. W ASCII litera "A" jest przedstawiana liczbą 65, lub szesnastkowo 0x41. Litera "B" to 66/0x42. A proces kontynuujemy dla wszystkich znaków, liczb, znaków interpunkcyjnych i tak dalej. Jeśli spojrzeć na klawiaturę angielską, będzie liczyć 32 znaki przestankowe, 10 cyfr dziesiętnych, 26 liter i 26 liter więcej jeśli wziąść pod uwagę duże / małe litery. Daje to do 94 różnych znaków. Binarnie potrzebujesz 7 bitów do reprezentacji takiej liczby kombinacji . W zrzucie szesnastkowym, zauważ ,że kolumny ASCII zawierają wiele kropek. Bajt posiada 256 kombinacji, ale możemy zobaczyćtylko 94 z nich. Każdy znak który nie jest jednym z nich jest pokazywany jako kropka. Tak czy inaczej, jeśli chcesz spróbować sniffowania pakietu, masz dość informacji aby zacząć. Możesz ściągnąć pakiet sniffujący z sieci. Spróbuj swoich sił!

Statystyczne bazy danych

Może to się wydawać odejściem od głównego naszego tematu. Czy kiedykolwiek chciałeś uzyskać od swojego pracodawcy z bazy danych informacje odnoszące się do działu kadr? W tym strasznym świeci niepewności zatrudnienia i schematów oceny pracownika, wyjaśnię

możliwe środki aby odkryć tajemnice pracodawcy. Statystyczna baza danych, w swojej prostocie, gromadzi informacje odnoszące siędo infrastruktury całych organizacji. Obejmuje dane osobowe i pracownicze. Systemy te są wdrażane przy pomocy Microsoft Access, MySQL i innych podobnych programów, ale to co mają ze sobą wspólnego to to ,że muszą być przechowywane w jednym miejscu. Jest to niezbędne do tego aby zapewnić ,że zapytania zwrócą unikalne wyniki. Należy pamiętać ,że aby wykorzystywać te informacje z powodzeniem, zakłada się praktyczną znajomość SQL (Structured Query Language) i algebry relacyjnej. Niektóre szczegóły działania są dostarczane; jednak proszę pamiętać ,że nie jest to podręcznik SQL! To jest ogromny temat. Po prostu proponuję środki, za pomocą którychm można uzyskać informacje, jakie chce ukryć przed nami administrator bazy danych. Metody próbujące ominąć ograniczenia dostępu mogą ale nie muszą działać na wszystkich systemach;

Sztuczki sprzętowe

Dla hackerów z pewną wiedzą na temat sprzętu komputerowego i elektroniki ogólnie, i którzy są przygotowani do dłubania w schematach, lutownicy czy woltomierza, sondy cyfrowej czy oscylokskopu, otwierają się nowe mozliwości. Jednym z najbardziej użytecznych zestawów to mały odbiornik radiowy (zakres MW/AM) mikrofony i magnetofonu. Radia w pobliżu komputerów, modemów i linii telefonicznych można z łatwością zebrać "świergot" komunikacji cyfrowej bez konieczności przeprowadzania fizycznych "pułapek" na telefonie. Alternatywnie petla indukcyjna z małym wzmacniaczem w pobliżu telefonu lub linii pozwala na nagrywanie i późniejszą analizę. Dzieki identyfikacji używanej pary tonów, można oddzielić rozmówców. Przez pokazanie nagranych tonów na oscyloskopie można zamrażać bity, 'zanki' i 'słowa';możesz rozebrać bity startu i zatrzymania i za pomocą tabeli ASCII, zbadać co one oznaczają. Z doświadczenia wiem ,że jest całkiem możliwe zidentyfikowanie wielu protokołów po prostu przez "spojrzenie" na oscyloskop. Technika cruder to po prostu nagrywanie i odtwarzanie sekwencji logowania;ograniczeniem jest to ,że nawet jeśli uda ci się zalogować, możesz nie wiedzieć co dalej. Nasłuchiwanie na lini telefonicznej jest również techniką stosowaną przez niektórych wysoko wyspecjalizowanych złodziei. W 1982 roku oddział Lloyd Bank Holborn został "najechany"; alarm nie zadziałał ponieważ złodzieje nagrali "wszystkie czyste" sygnały z linii telefonicznej, a następnie, podczas włamania odtworzyli naganie na linii moitorującej alarm urządzeń. Czasami hacker musi opracować ad hock bity dla oszustw sprzętowych w celu osiągnięcia własnych celów.Dostęp uzyskany do znanych finansowych usług w dużej mierze dzięki spięciu razem kilku prostych sprzętowych możliwości. Usługa jest dostępna przede wszystkim na liniach dzierżawionych. Jednak każdy terminal posiada powiązaną możliwość dial-up, w przypadku linii dzierżawionej powinny iść w dół; i dodatkowo same terminale mogą mieć dostęp do Prestel. Zatem hacker myśli ,że powinna istnieć możliwość dostępu do usługi za pomocą zwykłych urządzeń zamiast specjalnych jednostek dostarczanych wrazz z rocznym abonamentem. Uzyskanie numeru telefonu było

relatywnie proste: to po prostu kwestia wyboru ręcznego dial-up z właściwego menu i nasłuchiwanie impulsów jak przez zwykły telefon. Kolejnym krokiem było uzyskanie hasła. Właściciele terminala do którego hacker miał dostęp nei znali ich ID;nie musieli go znać ponieważ był zaprogramowany w terminalu i wysyłany automatycznie Hacker mógł umieścić micro "z przodu" całej linii i wysłać ENQ aby zobaczyć czy ID został wysłany. Zamiast tego próbował czegoś innego. Terminal był znany i programowalny, pod warunkiem ,że umiał i miał odpowiedni typ klawiatury. Inżynierowie należący do serwisu to wiedzieli. Jak hacker mógł nabyć status "inżyniera"? Stworzył następujące założenia: klawiatura używana przez klientów serwisu była prostą sprawą, brakowało wielu oczywistych klawiszy używanych w normalnych terminalach; sam terminak został stworzony przez tą firmę ,która stworzyła szereg terminali edycji podglądu danych operatorów i wydawców. Być może uzyskalio podręcznik dla obsługi terminali, wśród nich mogły pojawić się ważne wskazówki Uzyskali ksero gdzie była instrukcja zmiany ID terminali, ustawienia auto-dialera itd.

Linux i Unix dla początkujących

Unix stał się systemem prostawowym Internetu.W rzeczywistości Unix jest najczęściej używanym systemem operacyjnym w świecie komputerów z większą mocą niż PC. Ale Unix dla elity hackerów nadal pozostaje podstawowym systemem operacyjnym. Do tej pory przyjmowaliśmy ,że uzywamy konta shell dostarczanego przez dostawcę Internetu. Konto powłoki pozwala wydawać polecenia na jednym z komputerów dostawcy Internetu. Ale nie musisz zależeć od komputera swojego dostawcy Internetu, która pozwala ci pogrywać z Unix. Możesz uruchomić Unix na swoim komputerze z połączeniem SLIP lub PPP przez bezpośrednie połączenie z Internetem.Notka: Połączenia Serial Line Internet Protocol (SLIP) i Point-to-Point Protocol (PPP) dają ci tymczasowy adres Internet Protocol (IP), który pozwala ci być podłączonym bezpośrednio do Internetu. Możesz użyć połączeń SLIP i PPP aby połączyć się z przeglądarką, która ci daje tylko zdjęcia zamiast tekstu. Zaletą korzystania z jednego z tych bezpośrednich połączeń dla działalności hackingu jest to,że nie pozostawiają za sobą śladu w postaci pliku dziennika powłoki dla administratora systemu ISP dla przestudiowania. Nawet jeśli nie łamiesz prawa, plik dziennika powłoki pozwala ci pozwala ci wyknać wiele hackowania, co może być wystarczające aby administrator zamknął konto. Jaki jest najlepszy rodzaj komputera do uruchomienia Unix? Jeśli nie jesteś bogatym hackerem który nie myśli o zakupie stacji roboczej Sun SPARC, prawdopodobnie będzie to jakiś PC. Istnieją prawie niezliczone warianty Unix, które działają na komputerach PC, a kilka dla komputerów Mac. Większość z nich jest za darmo do pobrania, lub tanio dostępne na CD-ROM. Trzy najpopularniejsze odmiany systemu Unix, które działają na komputerach PC to Sun Solaris, FreeBSD i Linux. Linux ma jednak tę zaletę ,że jest dostępny w różnych wariantach (dzięki czemu można mieszać i dopasowywać programy z różnych ofert Linux). Co ważniejsze, Linux ma bogatą dokumentację zarówno podręcznikową , na grupach dyuskusyjnych i stronach WWW.Notka historyczna: Linux

został stworzony w 1991 roku przez grupę prowadzoną przez Linusa Torvaldsa na Uniwersytecie w Helsinkach. Linux jest chroniony prawem autorskim na zasadach licencji GNU General Public Licesne. Zgodnie z tą licencją, Linux może być redystrybuowany do każdego z kodem źródłowym. Każdy może sprzedawać warianty Linuksa, modyfikować go. Ale jeśli ktoś zmodyfikuje kod źródłowy nie może się domagać praw autorskich do tego co zrobił z Linux. Każy kto sprzedaje zmodyfikowaną wersję Linux musi dostarczyć kod źródłowy do kupujących i umożliwić im używanie go w swoich produktach handlowych bez naliczania opłat licencyjnych. Takie rozwiązanie jest znane jako 'copyleft'. Linux składa się z samego systemu operacyjnego (tzw. 'kernel') oraz zbioru programów. Kernel, jak wszystkie typy Unix, jest wielozadaniowym systemem operacyjnym dla wielu użytkowników systemu operacyjnego. Mimo,że używa innej struktury plików, zatem nie jest nie jest bezpośrednio kompatybilny z DOS i Windows , jest na tyle elastyczny,że wiele programów DOS i Windows może być uruchamianych w systemie Linux. Programy powiązane, które pochodzą z większości dystrybucji Linuksa mogą obejmować:

- program shella (Bourne Again Shell - BASH - jest najpopularniejszy)
- kompilatory dla języków programowania takich jak Fortran-77,C,C++, Pascal, LISP, Modula-2, Ada, Basic i Smaltalk
- X (czasami nazywany X-Windows), graficzny interfejns użytkownika
- programy użytkowe takie jak czytnik e-mail Pine i Elm

Jaki Linux wybrać? To zależy od tego co naprawdę chcesz robić. RedHat Linux słynie z najłatwiejszej instalacji Moim podejściem jest zebranie kilku dystrybucji i wybranie z każdej to co najlepsze. Jednak instalacja Linuksa nie jest dla ludzi o słabych nerwach. Oto kilka porad jak ją przetrwać:

1. Mimo,że można uruchomić Linuksa na Pc 286 z 4 MB RAM i dwóch dyskietkach, znacznie lepiej jest mieć 486 z więcej jak 8 MB RAM, CD-ROM i przynajmniej 200 MB wolnego miejsca na dysku twardym
2. Dowiedz się jak najwięcej o typie płyty głównej ,modemie, dysku twardym, CD-ROMie i karcie graficznej. Jeśli masz jakąś dokumentację na ich temat to dobrze.
3. Lepiej jest używać sprzętu, który jest markowy i nowoczesny w komputerze. Ponieważ Linuks jest darmowy, nie oferuje sterowników dla najnowszego sprzętu.
4. Przed rozpoczęciem instalacji należy wykonać kopię zapasową dysku twardego!
5. Weź więcej niż jeden dysk z dystrybucją Linuksa. W wielu przypadkach ,każda dystrybucja Linuksa ma różne programy użytkowe, emulatory systemów operacyjnych, kompilatory i inne. Dodaj je wszystkie do systemu.
6. Kup książkę lub dwie o systemie Linuks.

Teraz masz zagwarantowane ,że nawet po tych wszystkich 6 radach nadal będziesz miał problemy z instalacją Linuksa. Dobrze jest wykorzystać internetowe zasoby odnoszące się do instalacji Linuksa. A co z bezpieczeństwem Linuksa? Tak , Linuks jako system oiperacyjny jest niedoskonały. Wybitnie hackowalny, jeśli chcesz wiedzieć.

Numery portów i usługi

Dane te pochodzą z Internet Assigned Numbers Authority (IANA) . IANA utrzymuje Assigned Numbers RFC. Wpisy w tym pliku są w takim samym formacie co w standardowym pliku /etc/services Berkeley UNIX. Istnieją również połączenia między protokołem i nazwami usług i ich odpowiednikami w RFC (ich standardowa dokumentacja). Plik ma dwie sekcje: Dobrzez znane numery portów : numery portów jakie przydziela IANA do Registered Port Numbers i numery portów których IANA nie przydziela. Dostarcza to listy, które porty są używane przez usługi.
PORTY PRZYPISANE NA STAŁE
Porty przypisane na stałe są kontrolowane i przypisywane przez IANA i w większości systemów mogą być tylko używane przez procesy systemowe (lub roota) lub przez programy wykonywane przez uprzywilejowanych użytkowników. Porty są używane w TCP [RFC793] do nazw kończących logiczne połączenia które prowadzą rozmowy długodystansowe. W celu świadczenia usług dla nieznanych osób dzwoniących, usługa kontaktuje sie ze zdefiniowanym portem. Ta lista określa port używany przez proces serwera jako port kontaktu. Port kontaktu jest czasami nazywany "portami przypisanymi na stałe". O ile to możliwe, te same porty są przypisyweane do Udp[RFC768]. Przypisane porty używają małej części możliwej numery portów. Przez wiele lat przypisywane porty były w zakresie 0 – 255. Ostatnio zakres ten zarządzany przez IANA rozszerzył sie do zakresu 0-1023