Możliwości Zeroshell-a [About Zeroshell]

Zeroshell jest dystrybucją Linuksa dla serwerów i urządzeń wbudowanych mającą na celu zapewnienie podstawowych usług sieciowych.

Jest ona dostępna w postaci obrazu na CD lub Compact Flash i może być konfigurowana i administrowana przy pomocy przeglądarki internetowej

Główna charakterystyka tej dystrybucji Linuxa dotyczy zbudowania urządzenia sieciowego z możliwościami:

- Równoważenie i Failover wielu połączeń internetowych
- Połączenie modemami UMTS / HSDPA 3G
- serwer RADIUS do uwierzytelniania i automatycznego zarządzania kluczami szyfrującymi dla sieci bezprzewodowych 802.11b, 802.11g i 802.11a wspierającymi protokół 802.1x w postaci EAP-TLS, EAP-TTLS lub poprzez adres MAC klienta;
  Obsługiwane są WPA z TKIP oraz WPA2 z CCMP (802.11i kompilacje);
  Serwer RADIUS może także, w zależności od użytkownika, grupy lub adresu MAC zezwolić na dostęp na zadanym VLAN 802.1Q
- Captive Portal wspiera logowanie przez internet w sieciach przewodowych i bezprzewodowych. Jeżeli Captive Portal jest aktywny, Zeroshell działa jako bramka dla sieci, w której adresy IP (należące do wewnętrznej podsieci) są dynamicznie przydzielane poprzez DHCP. Klient chcący mieć dostęp do sieci prywatnej z zewnątrz musi dokonać autoryzacji przy użyciu metody Kerberos 5 podając nazwę użytkownika i hasło zanim firewall Zeroshell'a pozwoli mu na dostęp do internetu. Bramka Captive Portal jest często stosowana w celu zapewnienia uwierzytelnionego dostępu do Internetu w HotSpotach jako alternatywa dla protokołu 802.1X, który może być zbyt skomplikowany w konfiguracji dla użytkowników. Zeroshell implementuje funkcjonalność Captive Portal w naturalny sposób bez korzystania ze specjalnego oprogramowania takiego jak NoCat lub Chillispot.
- QoS (Quality of Service) służy do zarządzania ruchem w sieci. Pozwala na zagwarantowanie minimalnej lub ograniczenie maksymalnej przepustowości i przypisanie pierwszeństwa dla danego typu ruchu (przydatne dla wrażliwych na opóźnienia aplikacji sieciowych takich jak VoIP).

Wstępna regulacja może być stosowana dla interfejsu Ethernet VPN, BRIDGE-ów i wyrównawczych VPN. Jest to możliwe przypisanie ruchu do filtrów warstwy 7-ej, które pozwalają na dokładny przegląd pakietów (DPI). Filtry mogą być przydatne do konfiguracji VoIP i P2P

- Serwer proxy HTTP jest w stanie blokować strony internetowe zawierające wirusa. Funkcja ta jest realizowana za pomocą antywirusa ClamAV oraz serwera proxy HAVP. Serwer proxy pracuje w *trybie przezroczystym ,* w którym nie musisz skonfigurować przeglądarek internetowych użytkowników, żądania HTTP będą automatycznie przekierowywane do serwera proxy.
- Access Point z obsługą wielu SSID i VLAN przy użyciu kart sieciowych WiFi opartych na na chipsetach Atheros. Innymi słowy, Zeroshell z jedną z kart WiFi zapewnia wiarygodne uwierzytelnienie i dynamiczną wymianę kluczy

802.1x oraz protokół WPA. Oczywiście, uwierzytelnianie odbywa się za pomocą protokołu EAP-TLS oraz PEAP na zintegrowanym serwerze RADIUS

- Host-to-lan VPN z L2TP/IPsec, w którym L2TP (protokół tunelujący warstwy 2) autoryzuje się za pomocą Kerberos v5, gdzie użytkownik i hasło są zabudowane w IPsec i autoryzowane przez IKE, który wykorzystuje certyfikat X.509;
- LAN VPN z hermetyzacją pakietów Ethernet w tunelu SSL / TLS ze wsparciem dla 802.1Q VLAN i zbalansowane obciążenie sieci (zwiększenie pasma) w przypadku usterki
- Router z połączeniami statycznymi i dynamicznymi (RIPv2 z MD5 oraz logowanie czystym tekstem i algorytmami Split Horizon i Poisoned Reverse)
- Bridge 802.1d z protokołem Spanning Tree , aby uniknąć zapętlenia nawet w obecności nadmiarowych połączeń
- 802.1Q Virtual LAN (tagged VLAN)
- Firewall Stateful Packet Filter i Packet Inspection (SPI) z filtrów stosowanych w routingu i bridging-u na wszystkich typach interfejsów, w tym VPN i VLAN
- Jest możliwe odrzucenie lub kształtowanie ruchu P2P i udostępnianych plików przy pomocy IPP2P - modułu „iptables” w Firewallu i klasyfikatorze QoS
- NAT zastosowany do prywatnych adresów sieci LAN ukrytych w sieci publicznej WAN
- Przekierowanie portów TCP / UDP (PAT) do tworzenia serwerów wirtualnych. Oznacza to, że prawdziwy klaster serwerów będzie widoczny tylko jako jeden adres IP (IP z serwera wirtualnego) i każde żądanie będzie przekierowane przy pomocy algorytmu „Round Robin” do rzeczywistych serwerów
- Serwer DNS obsługujący wiele domen z automatycznym zarządzaniem „Reverse Resolution in-addr.arpa”
- Serwer DHCP wielu podsieci z możliwością stałego IP w zależności od adresu MAC klienta
- PPPoE - klient do połączenia z siecią WAN poprzez linie kablowe ADSL i DSL (wymaga odpowiedniego modemu)
- Dynamic DNS klienta używany aby z łatwością dotrzeć do hosta w sieci WAN nawet jeśli adres IP jest dynamiczny
- Serwer Syslog służy do rejestrowania i katalogowania zdarzeń wygenerowanych przez zdalne hosty w tym przez systemy uniksowe, routery, switche, WI-FI punktów dostępowych WI-FI, drukarki sieciowe i inne, urządzenia kompatybilne z protokołem syslog
- Uwierzytelnianie Kerberos 5 za pomocą zintegrowanego KDC stosowane do uwierzytelniania pomiędzy obszarami
- Autoryzacja LDAP, NIS i RADIUS
- Standard X 509 do wydawania i zarządzania certyfikatami elektronicznymi

- Interoperacyjność usługi Active Directory pod Unix i Windows używając między-platformowej autentyfikacji LDAP i Kerberos 5

Następujące funkcje będą dostępne w najbliższej przyszłości i zawarte w wydaniu 1.0.0:

- Monitor Arpwatch do monitorowania ARP zdarzeń w sieci LAN takich jak dublowanie adresów IP, przepełnienie i innych błędów
- Host to lan VPN z protokołem PPTP (Point to Point Tunneling Protocol), w MPPE (Point Microsoft do szyfrowania Punktu) i tunelowania GRE

Następujące funkcje będą dostępne w kolejnych wersjach nowszych niż 1.0.0:

- IMAP v4 serwer do zarządzania skrzynkami pocztowymi z uwierzytelnianiem oferowanym przez zintegrowany serwer Kerberos 5
- Serwer SMTP do odbierania i wysyłania poczty trasy w zależności od SMTP routingu map przechowywanych na wbudowanym serwerze LDAP. Przychodząca i wychodząca poczta jest sprawdzana przez oprogramowanie antyspamowe i antywirusowe automatycznie aktualizowane przez Internet. Ponadto wspierany jest dynamiczy klient DNS, który automatycznie uaktualnia DNS MX rekord. Można mieć serwer poczty dla domeny również jeśli adres WAN IP nie jest przypisane statycznie.
- Uwierzytelnianie kart Smart Card za pomocą protokołu PKINIT który łączy w sobie Kerberos5 i standard X.509. Niestety, w przeciwieństwie do innych funkcji, nie jest możliwe wsparcie uwierzytelniania kart inteligentnych w krótkim czasie, ponieważ MIT Kerberos v5 nie implementuje jeszcze protokołu PKINIT

Zeroshell jest dystrybucją na CD, co oznacza, że nie ma potrzeby, instalowania go na dysku twardym, może działać bezpośrednio z płyty CD na której jest rozpowszechniany. Oczywiście baza danych, zawierająca wszystkie dane i ustawienia mogą być zapisywane na twardych dyskach i pamięciach USB. Wszelkie poprawki błędów bezpieczeństwa można pobrać z systemu automatycznej aktualizacji przez Internet i zainstalować w bazie danych. Te poprawki zostaną automatycznie usunięte z bazy danych przez kolejne wydania Zeroshell na CD już zawierającej aktualizacje.

Zeroshell jest również dostępny na karcie Compact Flash
Jest to przydatne jeśli musisz uruchomić program z karty zamiast z CDROM, na przykład w urządzeniach wbudowanych w urządzenia sieciowe.
Compact Flash powinien mieć 400MB wolnej pamięci do przechowywania konfiguracji i danych.

Nazwa Zeroshell podkreśla fakt, że chociaż jest to oprogramowanie przewidziane dla systemu Linux to wszystkie operacje administracyjne mogą być wykonywane poprzez interfejs WWW. Po wpisaniu adresu IP do przeglądarki można dokonać konfiguracji. Zeroshell został pomyślnie przetestowany z Firefoksem 1.0.6 +, Internet Explorer 6 +, Netscape 7.2 + e Mozilla 1.7.3 +.

Kompilacja Zeroshell

Zeroshell nie opiera się na konkretnej dystrybucji Linuxa. Autor dostarczył całe oprogramowanie w postaci kodu źródłowego w tar.gz lub tar.bz2
Aby uzyskać listę wykorzystanego oprogramowania zajrzyj tutaj