Opracowanie: Dariusz Przybylski
Wersja dokumentu: 7.VII.2010

DOKUMENTACJA UŻYTKOWA UTM

(Unified Threat Management)

kompleksowe zabezpieczenie sieci firmowych

1 OGÓLNY OPIS SYSTEMU

Zintegrowane rozwiązanie do ochrony sieci firmowej na styku z internetem oparte jest na rozwiązaniu open source - Linux dystrybucja DEBIAN GNU/Linux ver 5.0.1 Lenny kernel 2.6

Modelowy systemu klasy UTM składa się z następujących elementów:

- **FIREWALL** oparty o skrypt IPTABLES w którym polityka wszystkich łańcuchów INPUT, OUTPUT i FORWARD domyślnie ustawiona jest na DROP, przepuszczany jest tylko jawnie zadeklarowany ruch (tylko jawnie zaakceptowane przez kierownictwo usługi), reszta pakietów TCP/IP zapisywana jest do LOGów systemowych i dalej poddawana szczegółowej analizie. Tak zbudowana polityka na firewallu zabezpiecza zarazem od strony WAN jak i LAN (należy zaznaczyć, że to rozwiązanie pozbawione jest wady w której większość typowych firewalli pozwala na zestawienie dowolnego połączenia zainicjowanego od wewnątrz sieci – czyli strefy zaufanej co w przypadku sprytnych trojanów/robaków internetowych sprawia że firewall staje się otwarty na świat zewnętrzny).

- **IDS/IPS** (*Intrusion Detection System, Intrusion Prevention System* – systemy wykrywania i zapobiegania włamaniom) oparty również o sygnatury SNORTa i analizę logów systemowych (ważnym elementem rozwiązania jest natychmiastowe powiadamianie o wszelkich anomaliach na wskazane konto e-maila administratora - widać szybko co się dzieje i można podjąć odpowiednie kroki zapobiegawcze). Dodatkowo tak skonstruowany system IPS wykonuje auto-blokadę na okres kwarantanny 3600sek dla podejrzanego o atak adresu IP. Potencjalny atakujący numer IP zarówno od strony WAN jak i LAN jest odcinany od routera i ten fakt jest natychmiastowo przesyłany drogą mailową do administratora.

- **PROXY** (typowe usługi jak WWW, POCZTA przepuszczane są przez kontrolę sprawdzania zawartości treści oraz kontrola przez system antywirusowy CLAMAV. Program antywirusowy z projektu opensource jest aktualizowany kilka razy dziennie. W przypadku stron blokowane są treści uznane za szkodliwe na podstawie również metod słownikowych (administrator ustala które kategorie są szkodliwe np. pornografia itp, a ponadto może sam tworzyć tzw czarne i białe listy). Oprócz treści mogą być także blokowane pliki do pobrania ze stron np. filtr na krytyczne rozszerzenia EXE, MP3 itp W przypadku poczty wskazane krytyczne pliki w załącznikach mogą być dezaktywowane poprzez zmianę rozszerzenia co zapobiega automatycznemu uruchomieniu - jak ma miejsce w przypadku wielu wirusów skryptowych). Można też ustawić, że poczta zawirusowana jest automatycznie usuwana przed dotarciem do odbiorcy (a np. treść maila może być odkładana na serwerze do dalszej analizy). To rozwiązanie ma bardzo dużo możliwości i może być dowolnie skalowane zależnie od obowiązującej polityki bezpieczeństwa w danej firmie. Dodatkowo dołączony jest moduł,

który pokazuje statystyki odwiedzanych i blokowanych stron w różnych kategoriach tematycznych. W ramach usług proxy należy również dodać że rozwiązanie posiada cachowanie zapytań DNS co przy dużym obciążeniu sieci przekłada się na szybkość działania całego systemu.

- **BEZPIECZEŃSTWO** samego rozwiązania - kontrola SPÓJNOŚCI i STABILNOŚCI odbywa się na wielu płaszczyznach - na wypadek skutecznego ataku na system cyklicznie sprawdzany jest stan systemu operacyjnego pod kontem **INTEGRALNOŚCI** – tzn. czy wszystkie programy/pakiety i ustawienia konfiguracyjne nie uległy jakiejkolwiek nieautoryzowanej zmianie, czy na dysku nie pojawiły się jakiekolwiek nowe wpisy, trojany, backdoory, rootkity, wirusy itp Ponadto sprawdzane są fizyczne elementy komputera np. temperatura, stan coolera - które wpływają na stabilna pracę całości rozwiązania (oczywiście tak jak poprzednio raport przychodzi na maila lub w formie skróconej na sms). Dodatkowo w prezentowanym rozwiązaniu przyjęto model oparty na statycznej tablicy ARP (funkcja ta zapobiega między innymi atakom typu „man in the middle")

- **DHCP** kontrolowane przydzielanie adresów IP w sieci LAN. Usługa obejmuje sprawdzanie adresów IP w oparciu o MAC adres kart sieciowych użytkowników końcowych co jest szczególnie ważne z uwagi na logowanie zdarzeń i jednoznaczną identyfikację komputerów w sieci. Administrator UTM samodzielnie przydziela adresy według listy.

-**QoS** dynamiczny podział pasma (upload/download) - specjalny skrypt HTB reguluje zakres przydzielonego pasma i zapobiega zapchaniu przez jednego użytkownika całego łącza internetowego zarówno w ruchu wychodzącym jak i przychodzącym (są programy np. typu kazaa, które skutecznie zapychają pasmo, w tym przypadku jeśli zostaną jawnie przepuszczone na firewallu przez administratora). Podobnie jak powyżej Administrator UTM samodzielnie przydziela pasmo według listy.

- **NTP** synchronizacja czasu z zewnętrznego serwera NTP co jest szczególnie ważne z uwagi na obiektywne rejestrowanie zdarzeń w dziennikach systemowych.

- **ZARZĄDZANIE** poprzez przeglądarkę internetową (nie potrzebna znajomość poleceń linuxa) -przede wszystkim dotyczy zwłaszcza zarządzania usługami proxy (ustalanie kto i co może lub nie oraz sprawdzanie logów odwiedzanych stron internetowych) oprócz tego jest specjalna edytowalna lista na której nanosi się nazwę użytkownika adres IP, adres MAC, i przydzielone pasmo na download i upload. Wszystko w miarę przyjazny, przystępny i wygodny sposób dla osób nie będących informatykami.

- **MONITORING** środowisko zostało dodatkowo wyposażone w narzędzia do monitorowania stanu systemu poprzez przeglądarkę internetową . W dosyć przyjazny sposób można oglądać stan logów na wykresach czasowych w różnych kategoriach tematycznych. Dodatkowo wybrane raporty są przesyłane na pocztę e-mail do administratora a także przesyłane SMS przez bramkę operatora komórkowego.

- **VPN** (Virtual Private Network) w przedstawionym rozwiązaniu tunel VPN client-to-site ma zapewnić bezpieczne połączenie z samym serwerem UTM (dostęp do konsoli, ze względów bezpieczeństwa usługa SSH działa tylko na poziomie interfejsu lokalnego) oraz z siecią od strony interfejsu LAN (zdalna dostęp do zasobów serwerów lokalnych). Instalator klienta Windows do pobrania ze strony www.openvpn.net w sekcji Community Software - Downloads

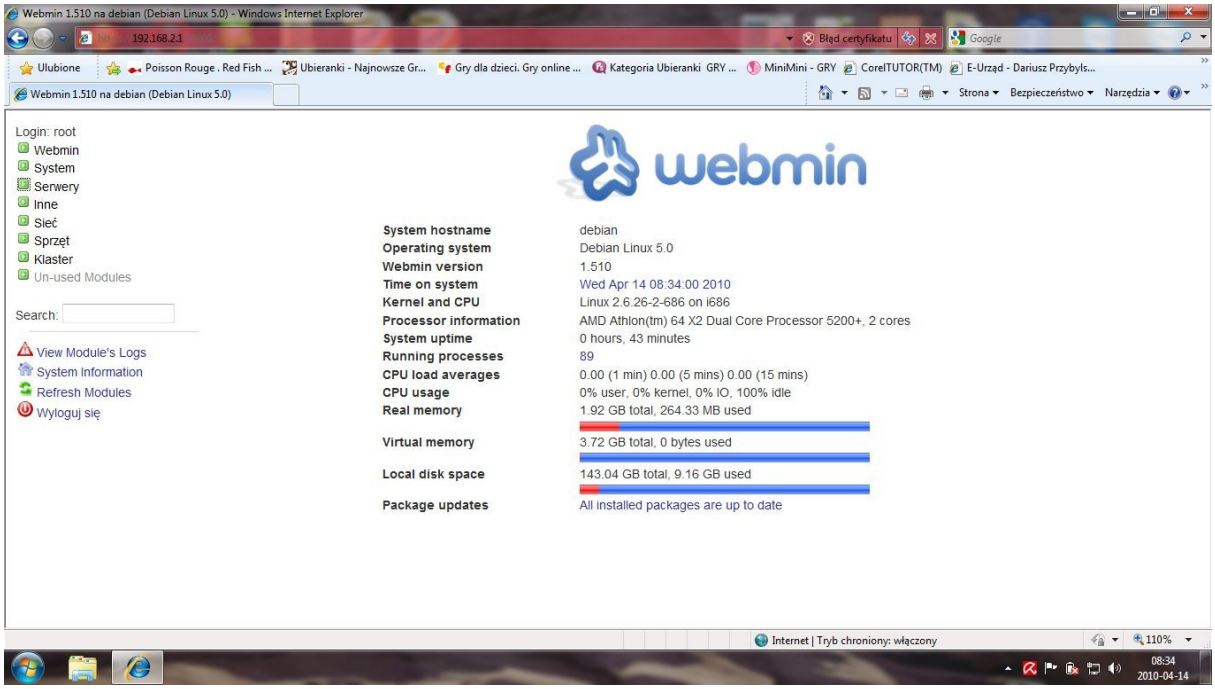
2. INSTRUKCJA ADMINISTRATORA

monitorowanie i zarządzanie przedstawionym systemem klasy UTM odbywa się z poziomu dowolnej przeglądarki internetowej zainstalowanej w sieci LAN (w obecnie zdefiniowanej polityce ustawiony brak dostępu z sieci WAN do konsoli SSH)

wykaz dostępnych usług http:
ZARZADZANIE i RAPORTOWANIE ZDARZEŃ (WEBMIN): **https://192.168.1.1:10000/**
MONITOROWANIE SYSTEMU (LINUXSTAT): **http://192.168.1.1:85/lstat/lstat.cgi**
ZBIORCZY RAPORT PROXY SQUID (CALAMARIS): **http://192.168.1.1:85/calamaris/**
RAPORT PROXY SQUID (SARG): **http://192.168.1.1:85/squid-reports/** (dostępny również z poziomu WEBMIN)

WEBMIN:

Po pomyślnym zalogowaniu widać stronę internetową jak poniżej:

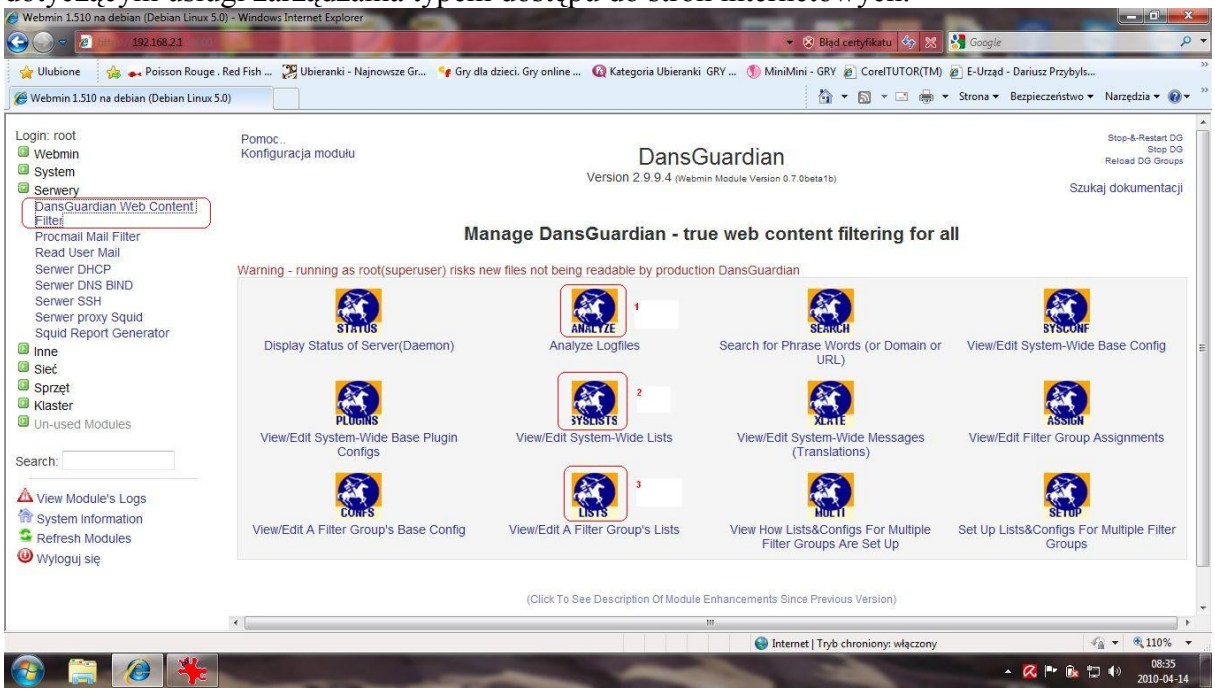


na pierwszym ekranie można odczytać najważniejsze parametry pracy routera UTM

- Time on system (aktualny czas na serwerze)
- System uptime (czas pracy serwera od ostatniego startu)
- CPU load averages (średnie obciążenie procesora)
- Real memory (rzeczywiste użycie pamięci operacyjnej RAM)
- Local disk space (realna zajetość dysków)
- Operating system, Processor information (wersja systemu operacyjnego i typ procesora maszyny)
- Running processes (liczba uruchomionych zadań na serwerze)
- Kernel and cpu (wersja kompilacji jądra systemu linux)
- Virtual memory (rzeczywiste wykorzystanie pamięci buforowej Swap)

Zarządzanie usługą WWW DansGuardian

W grupie menu SERWERY znajduje się moduł zarządzania filtrem kontekstowym dotyczącym usługi zarządzania typem dostępu do stron internetowych.



Jak przedstawiono na ekranie powyżej główne istotne grupy zarządzania i monitoringu filtra URL znajdują się w trzech grupach (opisanych numerami 1,2,3):

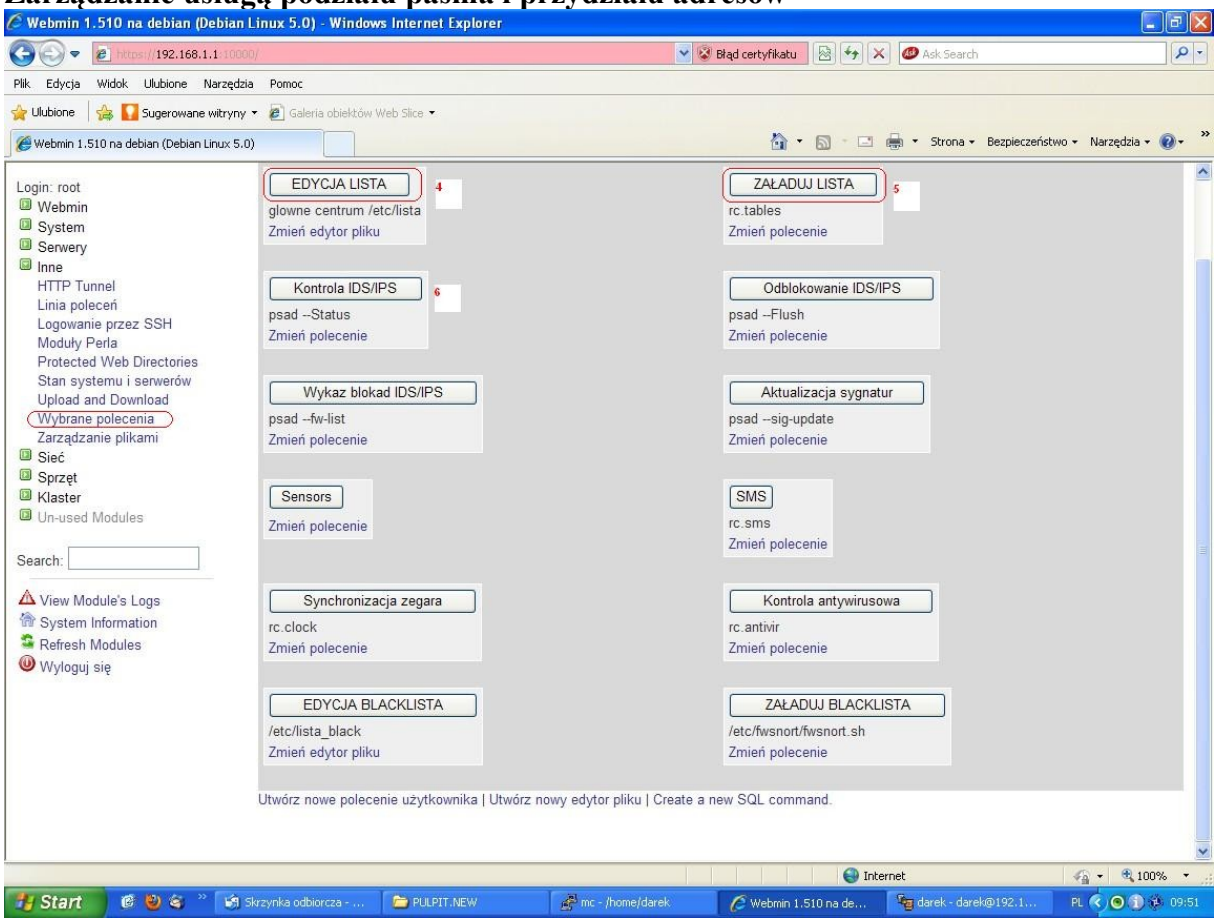
1) **Analyze Logfiles** (przegląd zdarzeń zarejestrowanych w ruchu WWW w dowolnym podziale tematycznym).
- można oglądać LOGI według zadanego zakresu dat zdarzenia (Enter Date Range)
- adresu IP danego użytkownika (Enter Client IP Adrdess)
- adresu domenowego URL (Enter a Site Name)
- różnych zarejestrowanych zdarzeń blokad i kryteriów (Choose a Reason Action)

(brak wypełnionego pola formularza zapytania oznacza wybór ALL – wszystko)

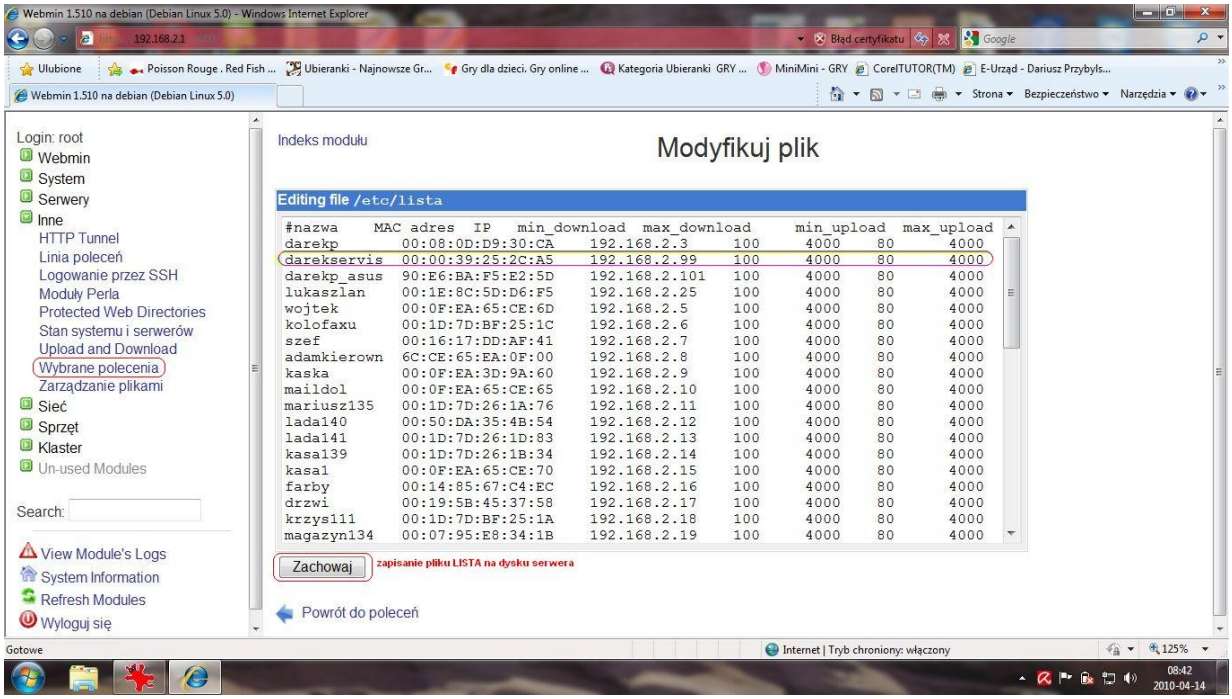
2) **View/Edit Systems-Wide Lists** (możliwośc wprowadzenia czarnej i białej listy na IP konkretnych użytkowników sieci)
- podział na Banned IP list (lista adresów zablokowanych dla usługi WWW)
- Exeption IP list (lista adresów IP wyłączonych spod sprawdzania filtrów słownikowych)

3) **View/Edit A Filter Group's Lists** (lista 25 filtrów kontekstowych WWW)
- tu między innymi odgórnie ustawiamy strony zablokowane BANNED lub odblokowane EXCEPTION
- Banned site list (lista stron www uznanych przez kierownictwo za zablokowane)
- Exception site list (strony odblokowane ze sprawdzania filtra słownikowego)
- Banned extension list (lista zablokowanych rozszerzeń np.: .exe, .com .pif, .vbs)
- Exception extension list (lista rozszerzeń plików dopuszczonych do pobrania np.: .xls, .doc, .zip itp. według polityki firmy)

Zarządzanie usługą podziału pasma i przydziału adresów



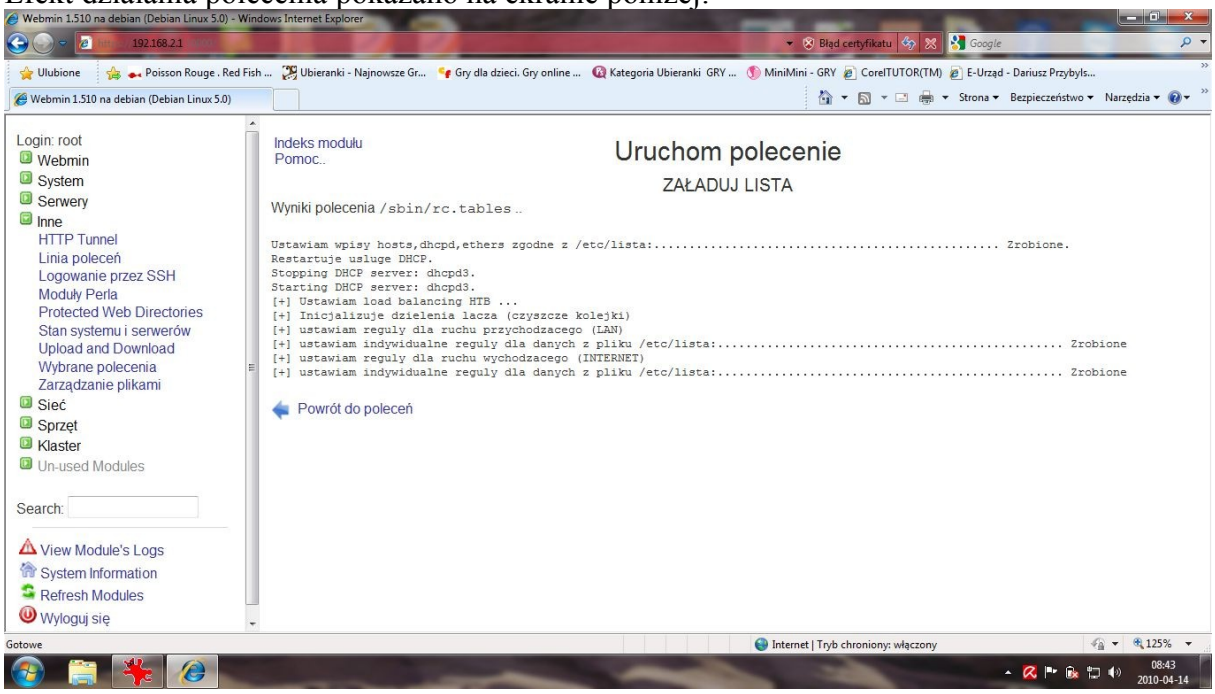
Jak pokazano na ekranie powyżej możemy edytować LISTĘ **(4)** przydzielonych adresów MAC i IP oraz podziału pasma w ruchu wychodzącym (UPLOAD) oraz ruchu przychodzącym (DOWNLOAD)



Po wybraniu przycisku „**EDYCJA LISTA**” możemy edytować główny plik konfiguracyjny usługi DHCP i HTB. Podajemy kolejno nazwę użytkownika, adres fizyczny karty sieciowej MAC, przydzielony na stałę adres IP, gwarantowany minimalny download, maksymalny możliwy do wydzierżawienia download, , gwarantowany minimalny upload, maksymalny możliwy do wydzierżawienia upload.
UWAGA: wartości minimalne download i upload muszą wynikać z otrzymanej od dostawcy wartości podzielonej przez całkowitą ilości użytkowników.
UWAGA: wartości maksymalne download i upload muszą wynikać z dowolnie przydzielonego przez nas pasma ale nie więcej niż wynika z wartości otrzymanej od dostawcy internetu
UWAGA: spacje mogą być użyte TYLKO do oddzielenia poszczególnych kolumn LISTY (spacja jest znakiem zastrzeżonym i może być w tym przypadku wykorzystana tylko jako separator kolumny). Jeden wiersz to jeden rekord (wpis) zakończony klawiszem ENTER

Po prawidłowym wypełnieniu LISTY należy zapisać plik (przycisk ZACHOWAJ), a następnie załadować listę do systemu przycikiem opisanym nr **(5) „ZAŁADUJ LISTA”**

Efekt działania polecenia pokazano na ekranie poniżej:

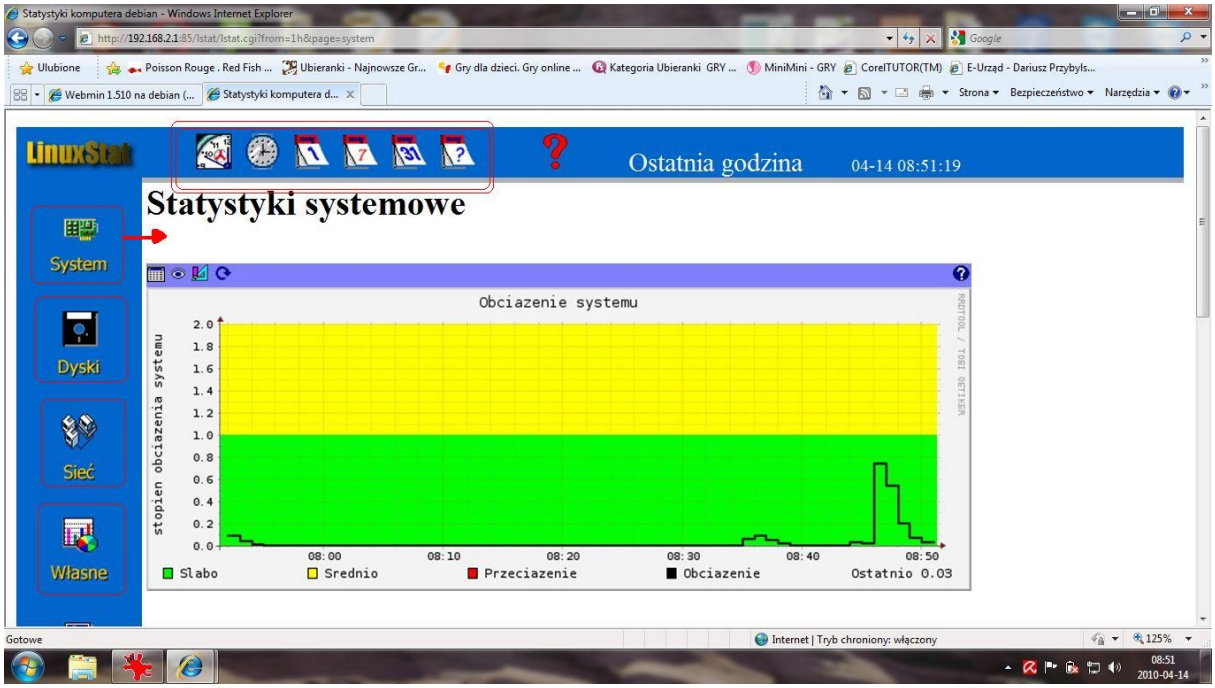


Dodatkowo pod przyciskiem oznakowanym numerem **(6)** możemy wyświetlić pełna statystykę efektów działania systemu IDS/IPS (w szczególności w zakresie zablokowanych adresów atakujących nasz system obronny oraz wiele innych cennych informacji przydatnych do analizy zagrożeń)

UWAGA: Oczywiście ilość i rodzaj przycisków w grupie menu INNE -> WYBRANE POLECENIA można dowolnie rozbudowywać według indywidualnych potrzeb administratora lub kierownictwa firmy. Na szczególną uwagę zasługuje możliwość edycji BLACKLISTY (czyli wykaz stacji-IP dla których ruch przez UTM jest całkowicie zablokowany)

LINUXSTAT

Podczas aktywnego monitoringu możemy uzyskać różne wykresy w czterech grupach tematycznych: System, Dyski, Sieć, Własne.
Dane można zbierać i przedstawiać w podziale czasowym na: ostatnia godzina, ostatnie 6 godzin, ostatni dzień, ostatni tydzień, ostatni miesiąc.

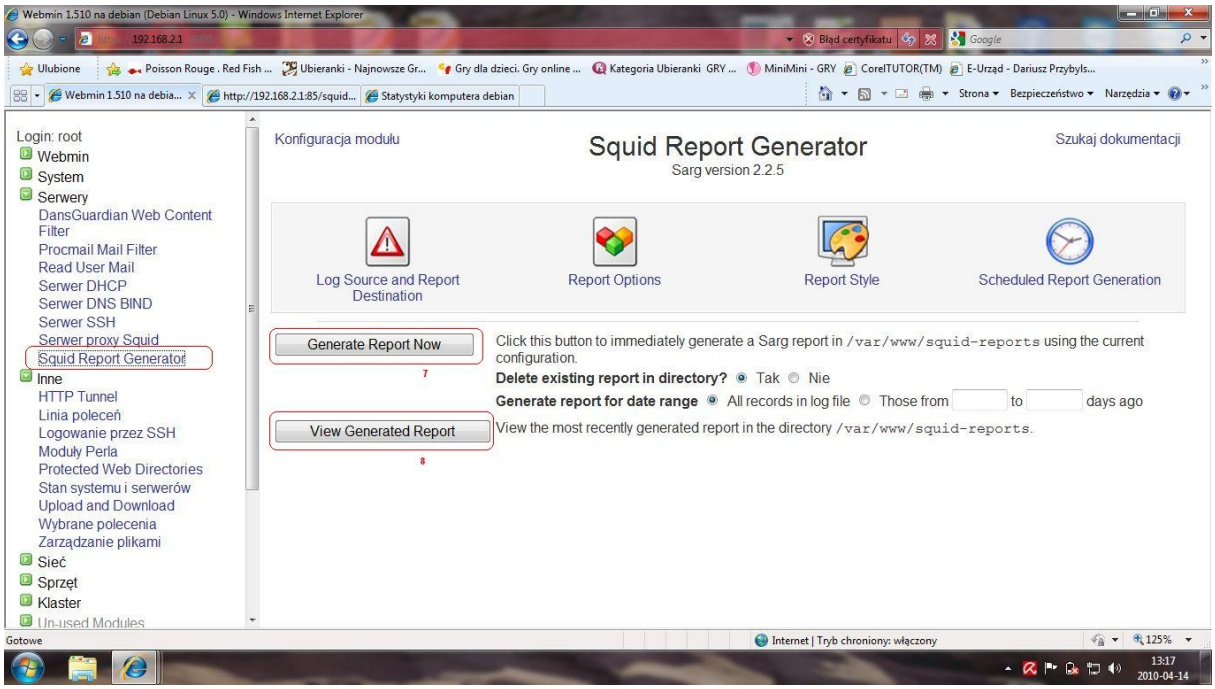


Jak pokazano na przykładowym ekranie powyżej uzyskane wykresy w szczególności dotyczą:

- Obciążenie systemu [%]
- Wykorzystanie procesora (w podziale na system i użytkowników)
- Wykorzystanie pamięci (100% na wykresie w podziale na RAM i SWAP)
- Użycie partycji dyskowych (stopień zajętości poszczególnych partycji)
- Użycie dysku (w podziale na zapis i odczyt)
- Przepustowość interfejsów sieciowych zarówno po stronie LAN i WAN (w układzie wyjście, wejście w dowolnych jednostkach: pakiet/s, bajt/s bit/s)
- Statystyki pakietów IP (np. w podziale na poszczególne usługi)
- Liczba zdarzeń wykrytych przez SNORTa (ten wykres można także wykorzystać do analizy logów pochodzących z innych systemów).
- Liczba zalogowanych użytkowników (raczej mało przydatne w serwerze typu UTM)
- Statystyki pakietów PINGa (pomiary "odległości" i "tłoku" w sieci)

SARG (Squid Analysis Report Generator)

Jest to raport opcjonalny – uzupełniający. Pozwala na zbiorczą analizę odwiedzanych serwisów WWW (zarówno w zakresie czasowym jak i ilości przesłanych Bajtów)
Na podstawie tego raportu można oceniać statystyki ogólne najczęściej odwiedzanych serwisów www bez podziału na pojedynczych użytkowników



Jak pokazano na ekranie powyżej należy w pierwszej kolejności wygenerować aktualny raport (Generate Report Now) przycisk nr **(7)**, a następnie można oglądać gotowy raport zbiorczy uruchamiając przycisk nr **(8)** (View Generated Report)
UWAGA: raport można również oglądać w postaci wykresów słupkowych

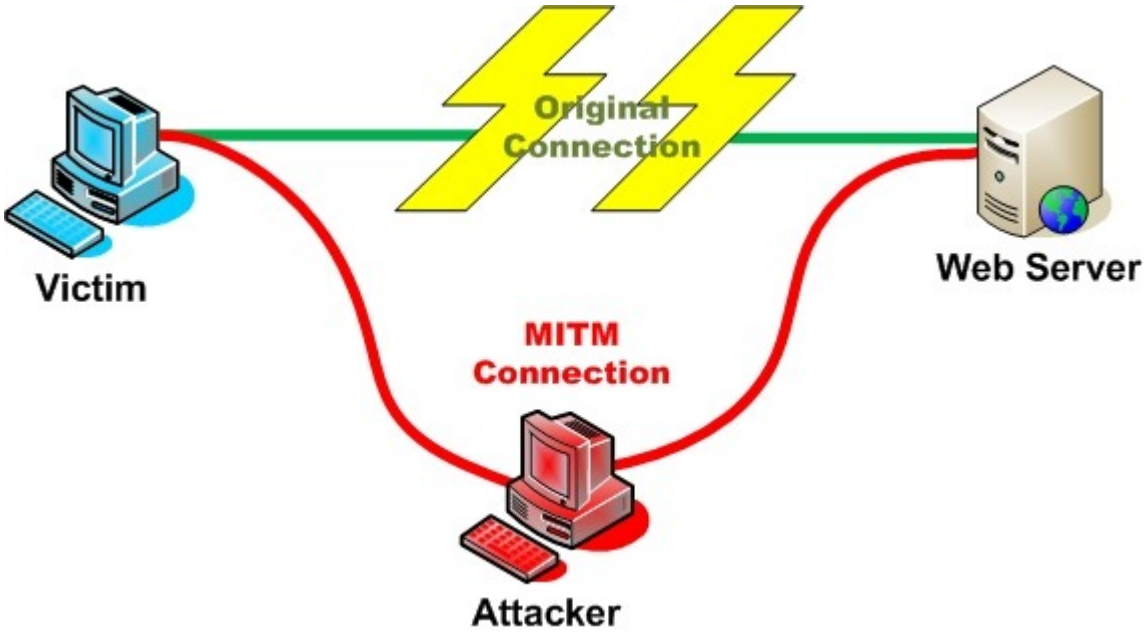
3. DLACZEGO LISTA JEST WAŻNA

Podstawowe pytanie: dlaczego warto mieć spis MAC adresów wszystkich stacji, które się będą łączyły z serwerem UTM i dalej z internetem?

Małe dodatkowe wyjaśnienie odnośnie LISTY - otóż w tym moim rozwiązaniu założyłem że TYLKO te stacje które są na liście (czyli mają wpisany poprawnie MAC i IP) są autoryzowane w sieci LAN i mogą mieć wyjście do internetu, każdy inny komputer (np. prywatny przyniesiony z domu) nie dostanie się na zewnątrz i nie dostanie automatycznie adresu IP (jest to pewne utrudnienie, ale sprytny użytkownik może wpisać sobie poprawny adres ręcznie) i komunikować się w sieci LAN (aczkolwiek nie wyjdzie do WAN)
Można z tego mechanizmu zrezygnować bez uszczerbku dla pozostałych usług, ale takie rozwiązanie zapobiega jednemu z najgroźniejszych dzisiaj form ataku nazywanym powszechnie: Atak man in the middle. **Polega to na modyfikacji tablicy Address Resolution Protocol (ARP),** opisywany w literaturze jako **zatrucie ARP** , **ARP spoofing** lub **ARP Poison Routing**,
(poniżej zamieściłem ilustrację oraz linki które to dokładniej opisują)

Reasumując LISTA załatwia kilka problemów:

- możliwość sterowania przepustowością poszczególnych stacji (regulacja pasma upload i download)
- stałe powiązanie MAC i IP w DHCP (daje praktycznie 100% identyfikacji użytkownika - co, kto i kiedy)
- zapobiega podłączaniu "obcych" komputerów (np. przyniesiony przez pracownika notebook z domu nie połączy się z internetem i nic nie wyśle i nie odbierze)
- no i najważniejsze zapobiega atakowi "man in the middle" (opisany w tym punkcie)



Ciekawe artykuły:
http://pl.wikipedia.org/wiki/ARP_Spoofing
http://pl.wikipedia.org/wiki/Atak_man_in_the_middle

4. SKÓCONY OPIS KONFIGURACJI KLIENTA VPN

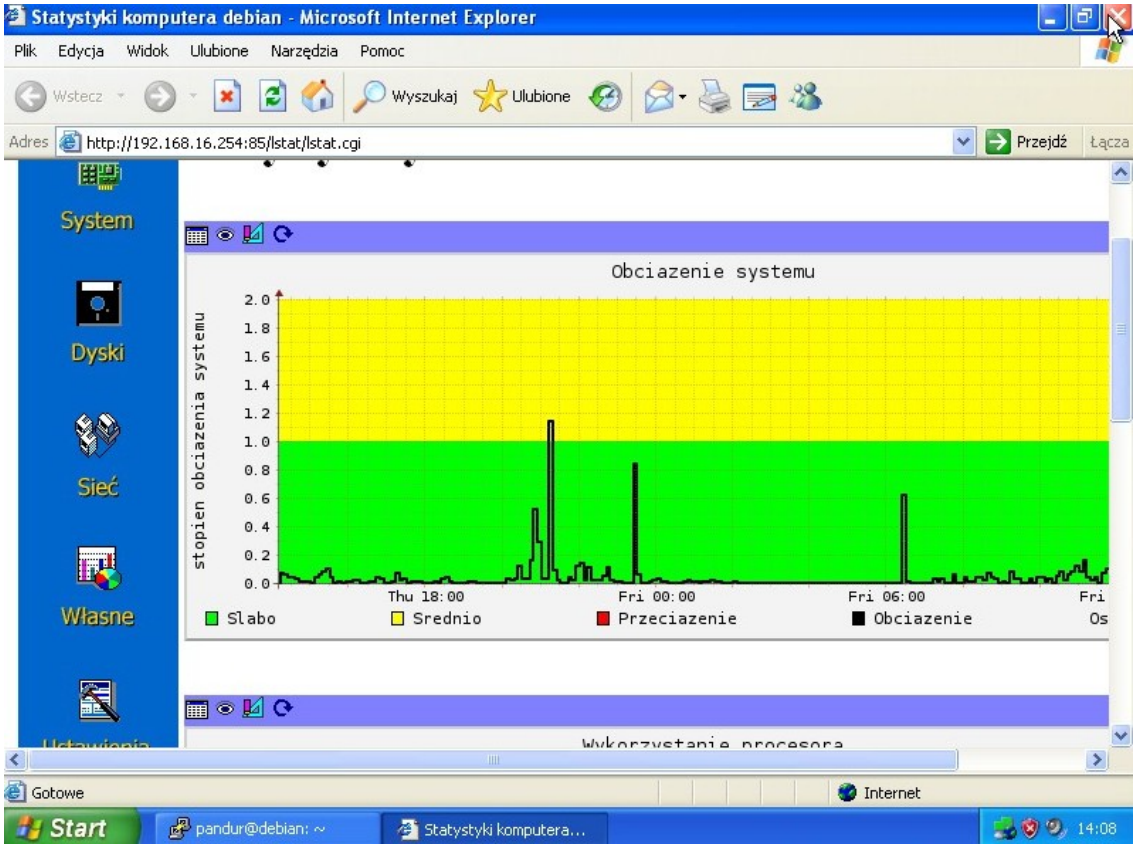
Jak zechcesz zarządzać serwerem lub mieć dostęp do firmowej sieci lokalnej z domu to musisz wykonać następujące czynności:

1 krok:
zainstaluj na domowym komputerze program **openvpn-2.1.1-install.exe** (można go pobrać za darmo ze strony: ***www.openvpn.net***)
w czasie instalacji na wszystkie pytania odpowiadamy twierdząco
(po instalacji pojawi się skrót do klienta openvpn na pulpicie swojego domowego komputera)

2 krok:
następnie wgraj otrzymane certyfikaty i plik konfiguracyjny do katalogu
C:\Program Files\OpenVPN\config
tzn.: należy wgrać nie zmieniając ich nazw wszystkie otrzymane certyfikaty czyli pliki z rozszerzeniem PEM oraz jeden plik konfiguracyjny: client.ovpn

3 krok:
uruchom program co objawi się widoczną na dole ekranu w polu systemowym ikoną z dwoma komputerkami na tle globusa. (jak widać poniżej na zdjęciu)
następnie po kliknięciu prawym klawiszem myszki wybierz opcję CONNECT
potem już możesz pracować analogicznie jak w pracy
(np. https://192.168.2.1:10000/ - to dostęp do webmina itp)

4 krok:
po zakończeniu pracy rozłączamy kanał VPN klikamy prawym klawiszem myszki i wywołujemy DISCONNECT.



5. SYNTETYCZNY OPIS TECHNICZNY SYSTEMU UTM

Wykaz pakietów które zostały wykorzystane przy budowaniu prezentowanego rozwiązania UTM w oparciu o system Linux dystrybucja Debin 5.0.1 Lenny kernel 2.6.26:

- integralność systemu: TRIPWIRE
- synchronizacja czasu: RDATE
- kontrola antywirusowa: CLAMAV
- anty malware (rootkity itp): RKHUNTER, CHKROOTKIT, UNHIDE
- bezpieczeństwo serwera SSH: DENYHOSTS
- proxy EMAIL: P3SCAN + RENATTACH
- proxy WWW: SQUID + DANSGUARDIAN + DGLOG + SARG+CALAMARIS
- proxy DNS (cache only): BIND9
- firewall IPTABLES: własny skrypt IPTABLES (polityka wszystkich łańcuchów INPUT, OUTPUT i FORWARD domyslnie ustawiona na DROP, przepuszczam tylko jawnie zadeklarowany ruch, reszta do LOGów)
- zarządzanie pasmem QoS: własny skrypt HTB oparty na TC
- system IDS/IPS: PSAD (super polecam! – monitorowanie wszelkich anomalii sieciowych również z poziomu LANu)
- dodatkowa ochrona w oparciu o sygnatury - konwersja reguł SNORT na iptables: FWSNORT
- serwer DHCP: DHCP3-SERVER (stałe powiązanie MAC z IP)
- powiadamianie mail: EXIM4
- kontrola sprzętu (temperatura, prędkość obrotowa coolera, napięcia CPU itp): LM-SENSOR, MONDO
- zarządzanie: WEBMIN (zwłaszcza w zakresie dansguardian i dglog ułatwienie zarządzania i monitorowania przez przeglądarkę IE)
- wizualizacja logów: LSTAT, RRDTOOL, APACHE2
- powiadamianie SMS: skrypt python wykorzystujący konto mBox operatora orange.pl
- szyfrowanie połączeń VPN oparte o: OpenSSL, OpenVPN (Instalator klienta Windows do pobrania ze strony www.openvpn.net w zakładce Community Software – sekcja Downloads)

6. SKRÓCONY OPIS METODOLOGII ATAKU HAKERSKIEGO

1) Rozpoznanie, wywiad (wsparcie: socjotechniki)
Sniffer - program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i ewentualne analizowanie danych przepływających w sieci
Fingerprinting - rozpoznawanie systemu operacyjnego i usług,
Exploit - program mający na celu wykorzystanie błędów w oprogramowaniu (typowa technika: buffer overflow)
ARP spoofing to atak sieciowy, który pozwala atakującemu przechwytywać dane przesyłane w obrębie segmentu sieci lokalnej (Man in the middle)

2) Modyfikacja, infekcja, ukrywanie
Backdoor (Trojan) -luka w zabezpieczeniach systemu utworzona umyślnie w celu późniejszego wykorzystania
Rootkit - narzędzie pomocne we włamaniach do systemów informatycznych. Ukrywa on niebezpieczne pliki i procesy, które umożliwiają utrzymanie
kontroli nad systemem
Robak komputerowy – samoreplikujący się program komputerowy, podobny do wirusa komputerowego.

3) Przejęcie kontroli:
Botnet - grupa komputerów zainfekowanych złośliwym oprogramowaniem (np. robakiem) pozostającym w ukryciu przed użytkownikiem i
pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami w ramach botnetu.
Pojedynczy komputer w takiej sieci nazywany jest komputerem **zombie**

4) Właściwy atak - wykorzystanie (głównie):
DDoS (Distributed Denial of Service) - odmowa usługi, wymuszenia
SPAM - wysyłania niechcianej korespondencji
Wyłudzanie pieniędzy od reklamodawców
Kradzież informacji