Instrukcja nr. X

Skaner sieciowy NESSUS

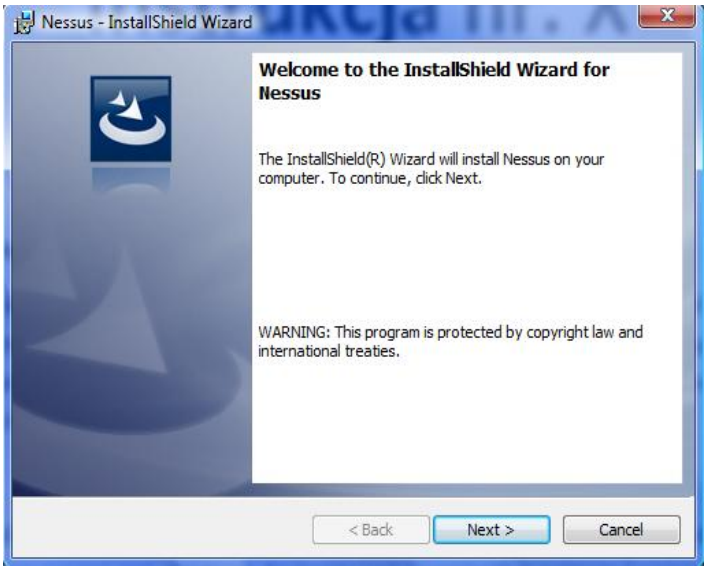
1. Informacje ogólne:

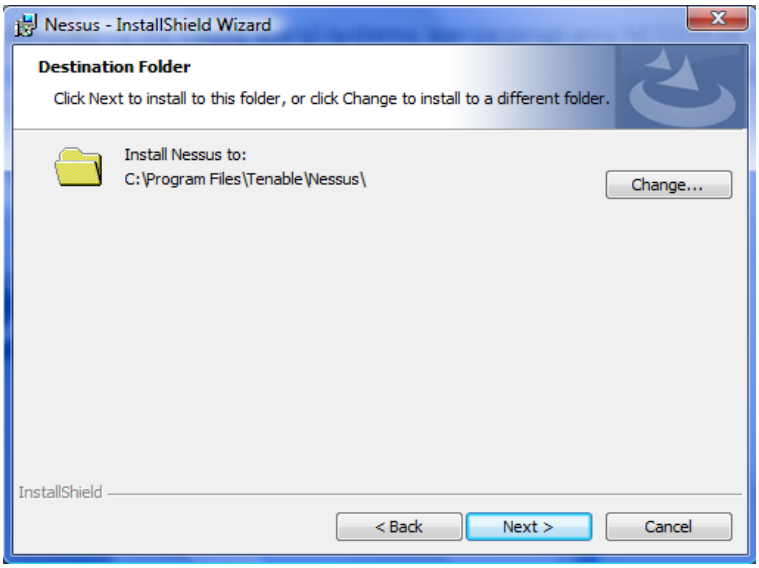
Nessus jest to skaner sieciowy, który prócz zwykłego sprawdzania które porty nasłuchują na danym komputerze, sprawdza je również pod kątem podatności na różnego rodzaju ataki. Po wykonaniu skanowania NESSUS wskazuje odpowiednie łatki które pozwolą na zabezpieczenie się przed wykorzystywaniem znalezionych luk.

2. Instalacja:

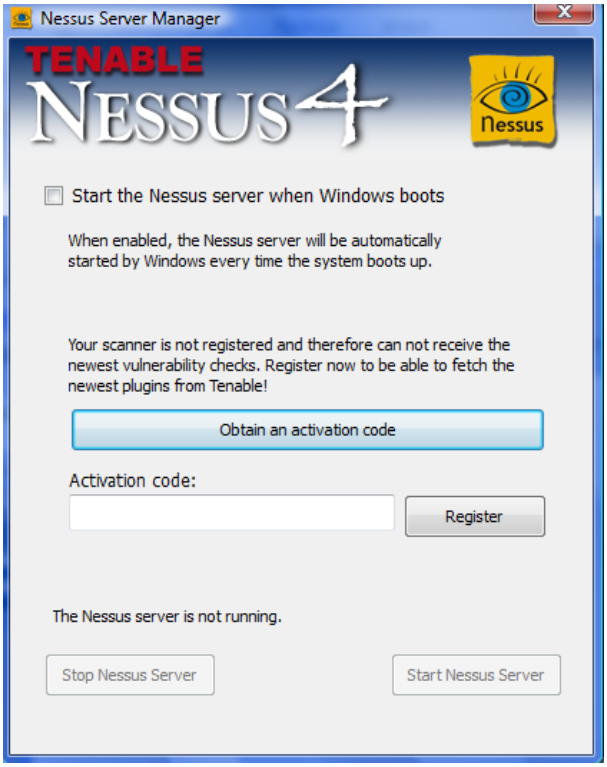
a.) Ściągamy odpowiednią dla naszej wersji systemu wersję programu NESSUS ze strony producenta www.nessus.org, program dostępny jest na wszystkie najpopularniejsze systemy operacyjne. W naszej instrukcji posłużymy się wersją na system Windows.

b.)Instalujemy program w domyślnej lokalizacji.





3. Pierwsze uruchomienie:



a.) Uruchamiamy plik Nessus Server Manager który został utworzony na pulpicie.

b.) Klikamy na przycisk „Obtain an activation code" który przekierowuje nas na strone producenta gdzie po wybraniu opcji „HomeFeed" podajemy E-mail aby otrzymać klucz aktywacji.

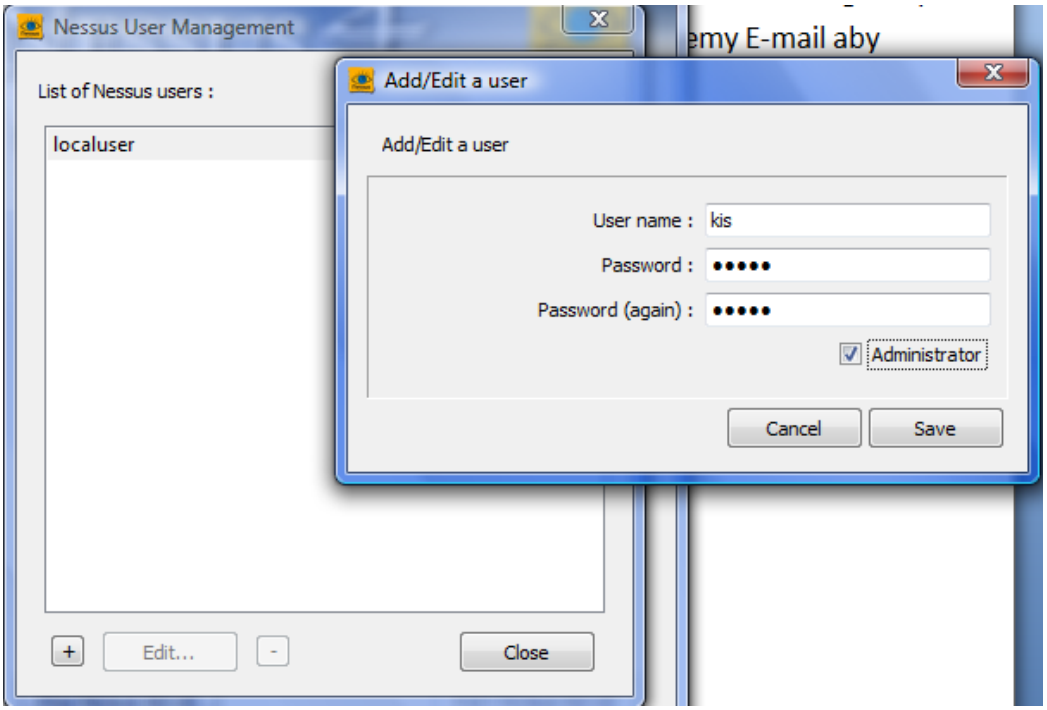
c.) Po otrzymaniu na skrzynkę klucza wpisujemy go w pole Activation code i klikamy na „Register". Po zarejestrowaniu program ściągnie najnowsze pluginy.

(Operacja ta może potrwać nawet kilkadziesiąt minut)

d.) Domyślnie serwer uruchamia się po procesie uaktualniania pluginów.

4. Pierwsze skanowanie (localhost)

a.) W otworzonym managerze klikamy na „Manage Account" i tworzymy konto z uprawnieniami Administrator.

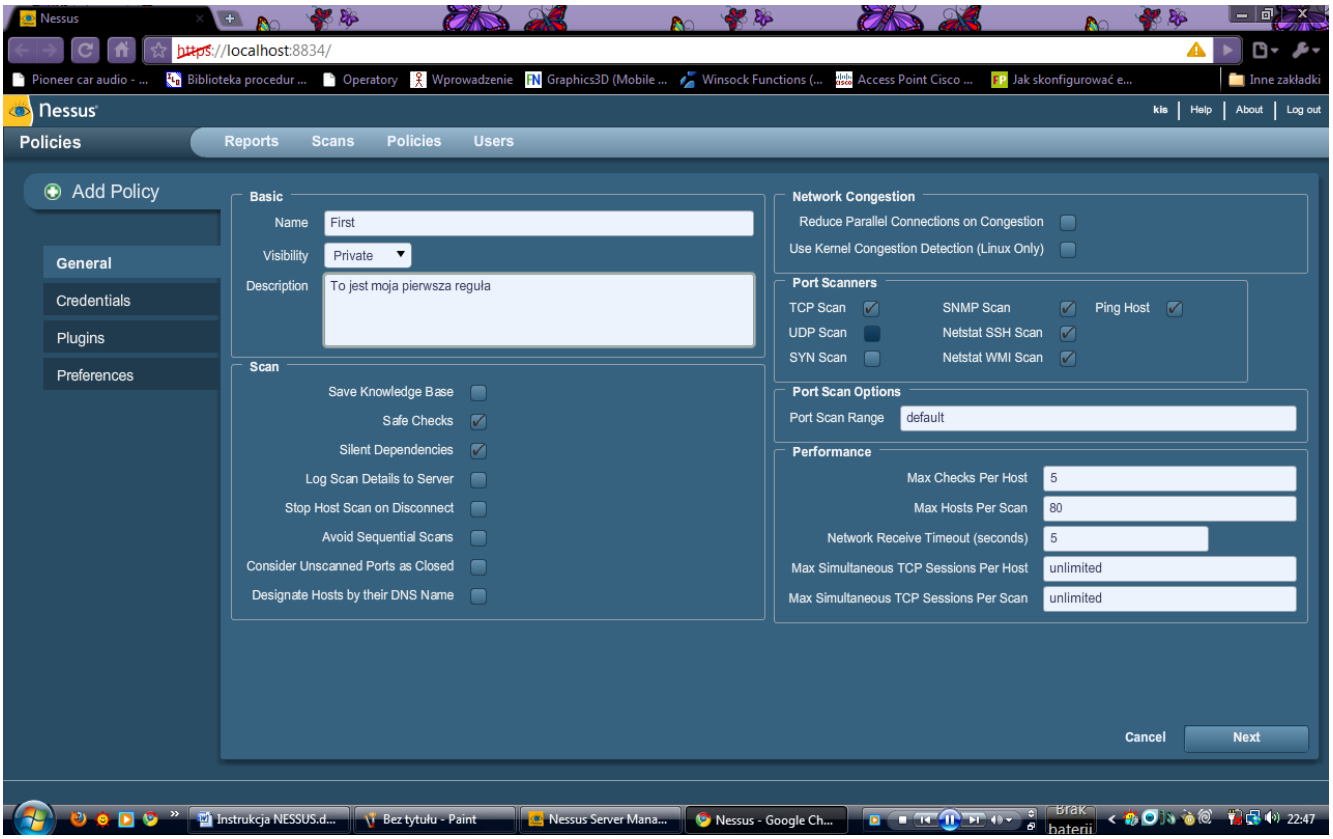


b.) Odpalamy plik Nessus Client który został utworzony na pulpicie i potwierdzamy certyfikat bezpieczeństwa.

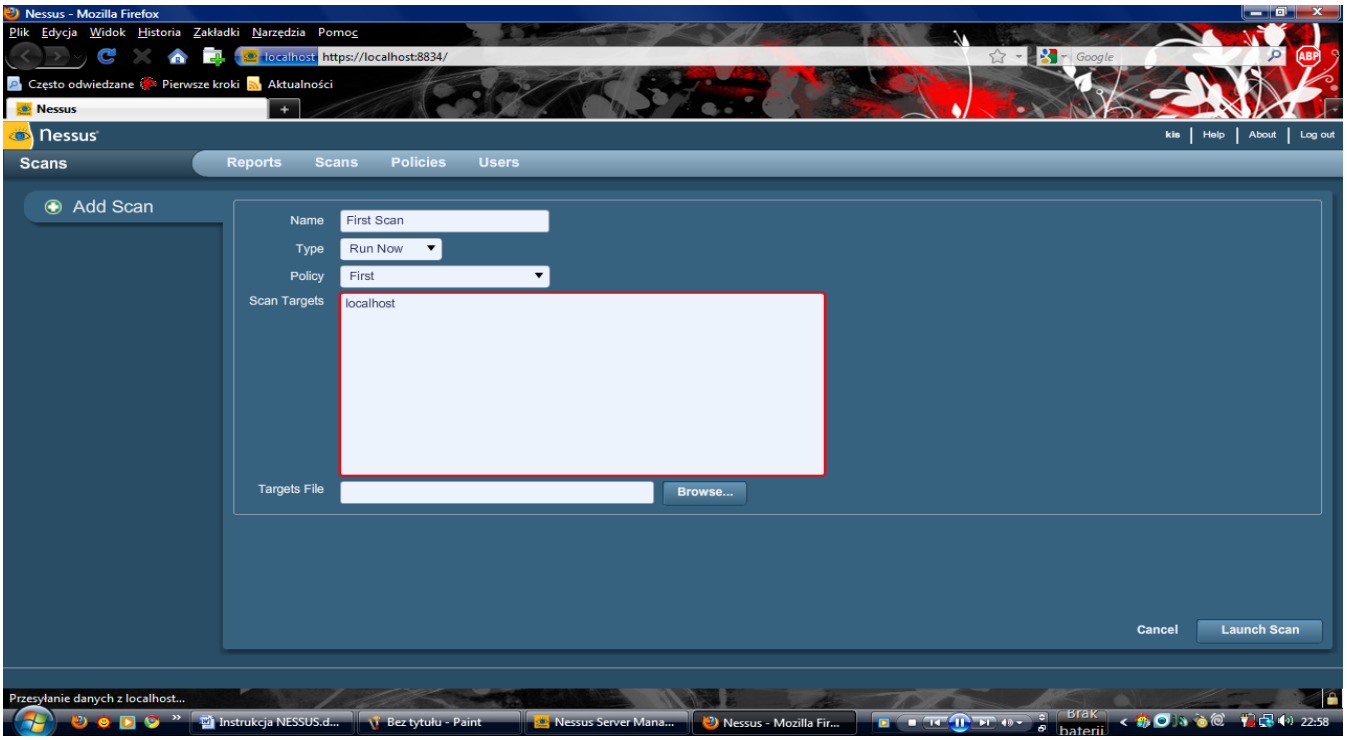
c.) Wpisujemy dane z utworzonego wcześniej konta, zostaje uruchomiony główny interfejs skanera.

d.) W zakładce „Policies” klikamy „add” i wypełniamy pole „name”. W tej zakładce możemy ustawić bardzo wiele opcji skanowania między innymi rodzaj pakietów używanych do testów(dokładny opis wszystkich opcji znajduje się w rozdziale 6).

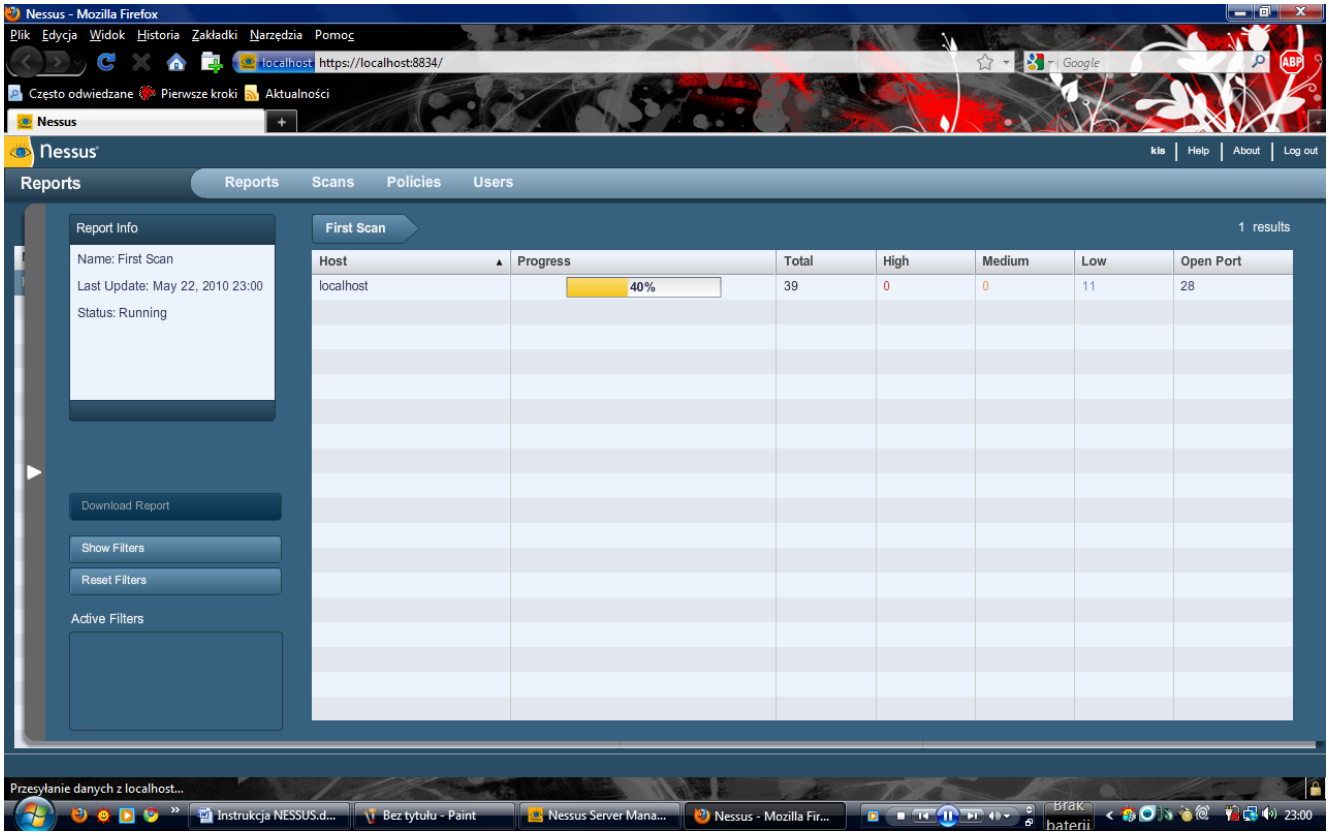
Zostawiamy na razie domyślne ustawienia, klikamy next, a na końcu submit.



e.) Przechodzimy do zakładki Scans gdzie wciskamy „add”, nadajemy znowu nazwę i w liście Policy dodajmy naszą wcześniej utworzoną politykę. Jeżeli jej nie ma to znaczy, że używana przez nas przeglądarka jest nie fajna, najlepszą będzie Mozilla Firefox ☺. W polu Scan Targets wpisujemy „localhost” i klikamy „Launch Scan”

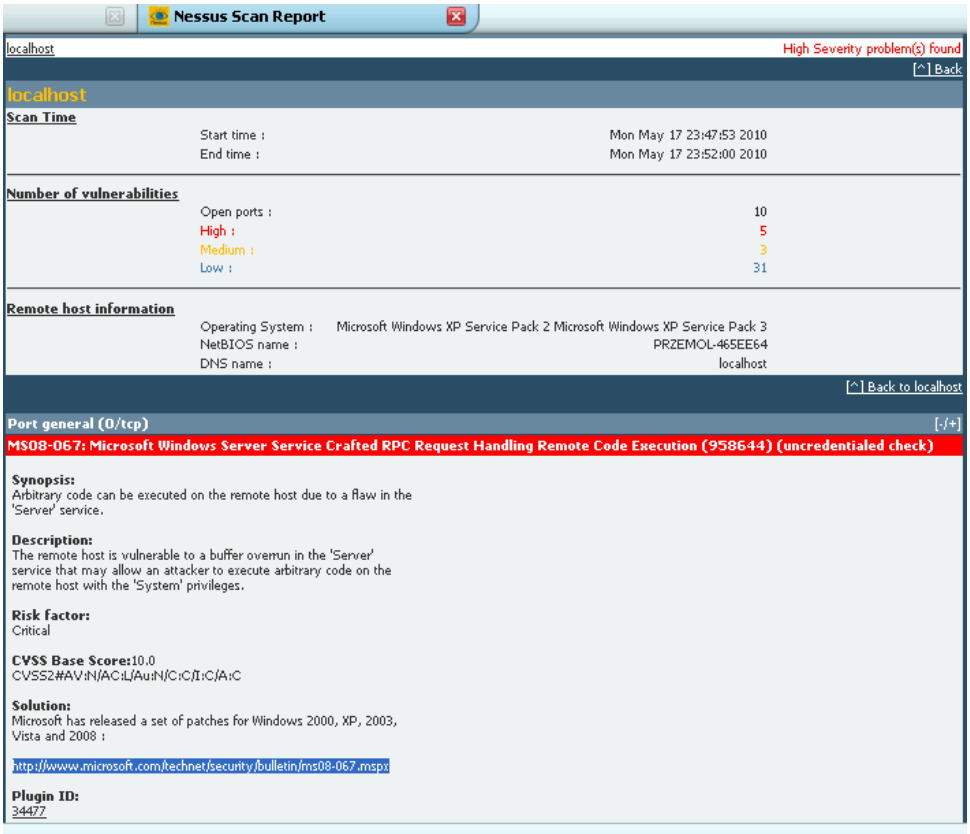


f.) Przechodzimy do zakładki Reports, zaznaczamy nasz skan i klikamy na „browse”. W tabelce będzie pokazany postęp skanowania.



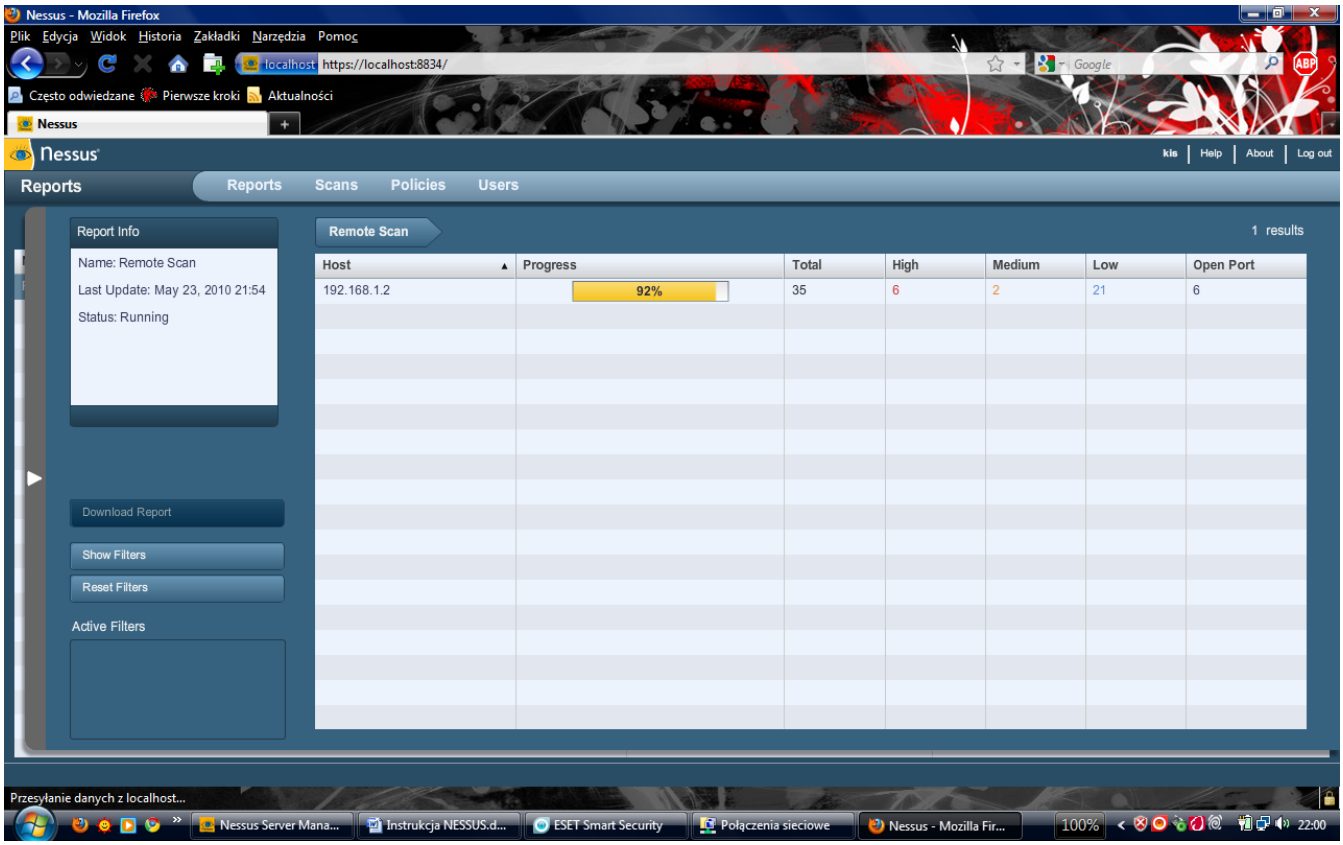
g.) Po zakończenie skanowania w tabelce pokaże się informacja odnośnie ilości zagrożeń sklasyfikowanych w 3 poziomach(High,Medium,Low) oraz liczba otwartych portów.

h.) Wciskamy przycisk „Download Raport” i wybieramy opcję „HTML export”. Dostajemy szczegółowy raport odnośnie luk w bezpieczeństwie naszego systemu, często dostępne są również zalecenia odnośnie łatania.

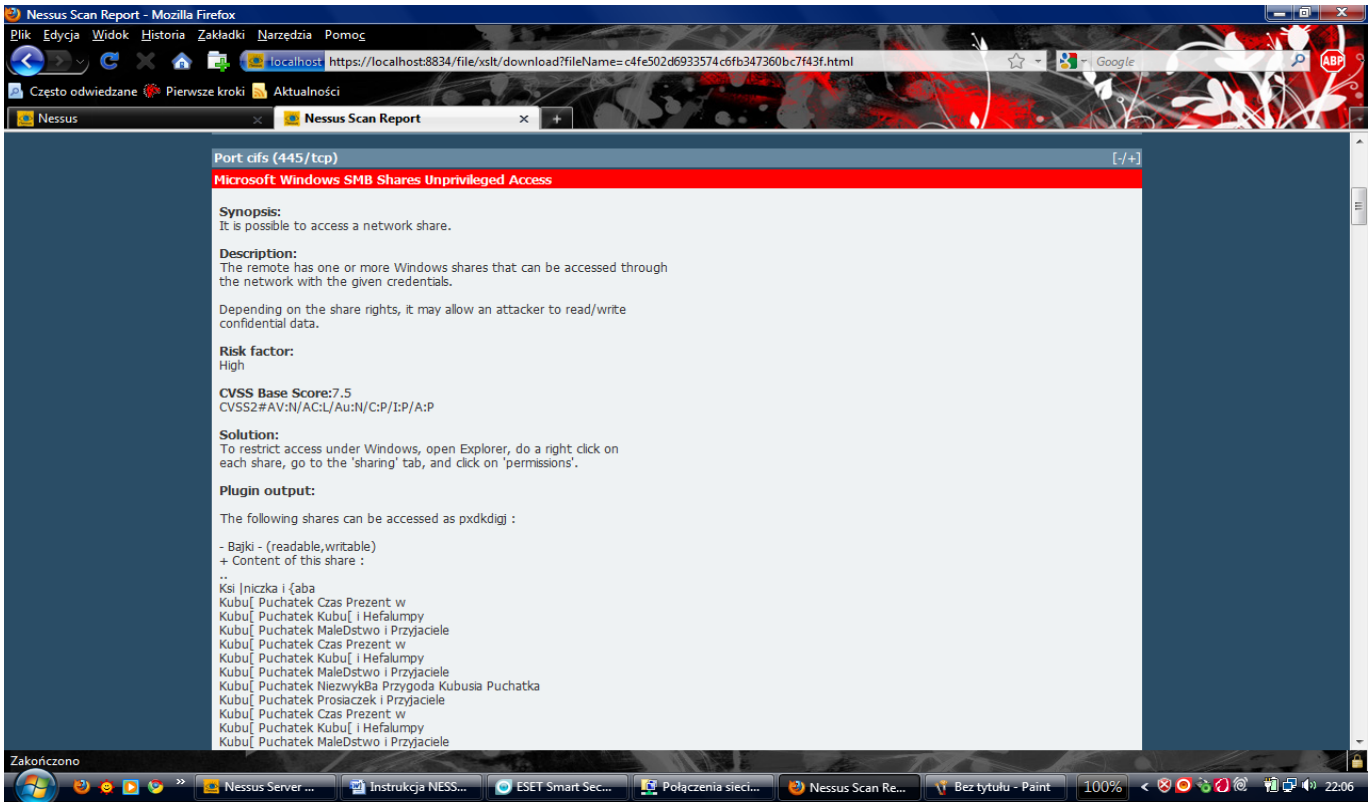


4. Zdalne skanowanie.

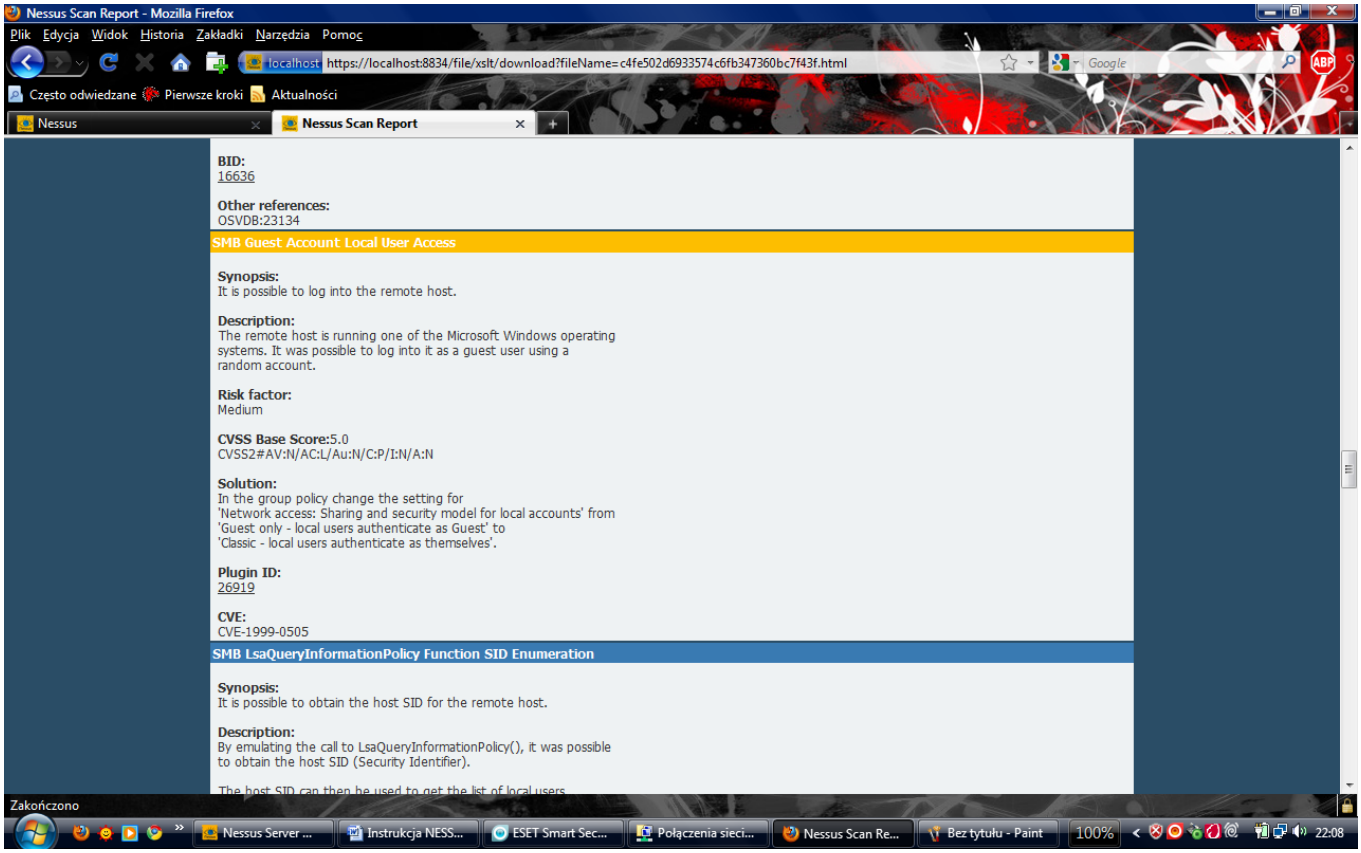
a.) W przypadku skanowania innego komputera w sieci lokalnej, różnica tkwi tylko w podaniu w polu „Scan targets” zamiast localhost adresu komputera który chcemy przeskanować. Skanowanie obcego komputera zazwyczaj trwa trochę dłużej.



b.) W tym przypadku dowiedzieliśmy się między innymi, że host 192.168.1.2 posiada udostępnione niechronione zasoby oraz ich listę.



c.) Dowiedzieliśmy się również, iż posiada aktywne konto guest oraz wiele innych informacji.



5. Informacje dodatkowe:

- Jeśli w polu „Scan target wpiszemu adres sieci wraz z maską, Nessus przeskanuje wszystkie aktywne komputery w sieci np. (192.168.1.0/24)

- Jeśli występuje problem ze skanowaniem komputerów, możliwą przyczyną może być zapora.

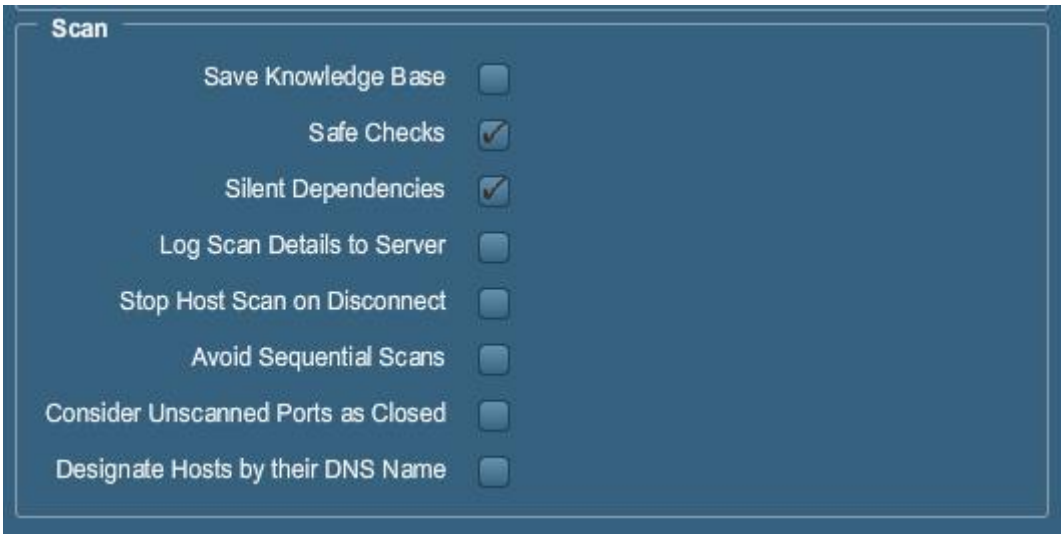
- Aby przeskanować kilka komputerów w sieci wystarczy wpisać ich adresy oddzielone „ , ”(przecinkiem).

6. Opis opcji Policies (tworzenie zasady skanowania)
General

Zakładka składa się z kilku sekcji:

- Basic – zawiera pola Name (nazwa polityki), Visibility (Private jeśli zbiór zasad ma być dostępny tylko dla użytkownika który ją tworzy, lub Shared gdy może być dostępna dla innych) oraz Description (krótki opis dotyczący danego zbioru zasad).

- Scan – zawiera kilka możliwych trybów skanowania:

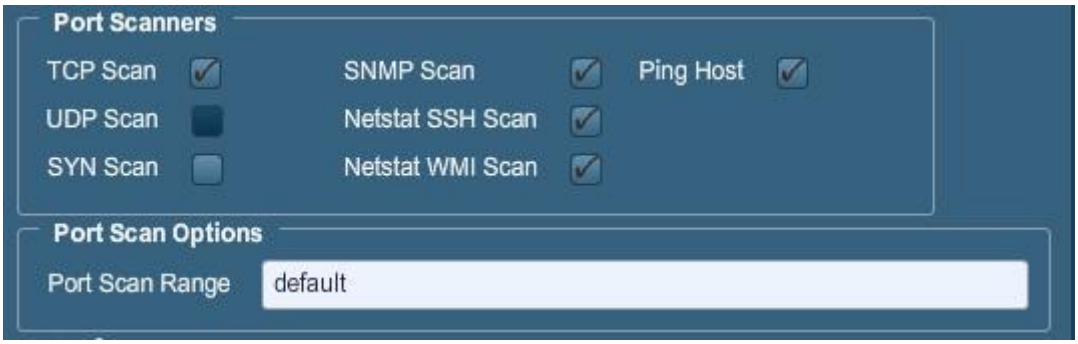


Save Knowledge Base – po zaznaczeniu zapisze informacje o skanowaniu w bazie danych aby ułatwić późniejsze skanowaniu.(przydatne gdy co jakiś czas mamy powtarzać to skanowanie)
Safe Checks – zablokuje wtyczki mogące zaszkodzić skanowanemu komputerowi
Silent Dependencies – informacje wywołane przez wtyczki uruchamiane automatycznie nie zostaną dodane do raportu końcowego.
Log Scan Details to Server – zapisuje dodatkowe informacje o skanowaniu
Stop Host Scan on Disconnect – zatrzyma skanowanie jeśli skanowany komputer przestanie odpowiadać.
Avoid Sequential Scans – domyślnie Nessus skanuje komputery po kolei jak zostaną wpisane na liste, zaznaczając tę opcję skanuje w kolejności losowej.
Consider Unscanned Ports as Closed – uważa nie przeskanowane porty za zamknięte
Designed Hosts by their DNS name – uważaj hosty po ich DNS'owych nazwach.

- Network Congestion – informacje o ruchu w sieci

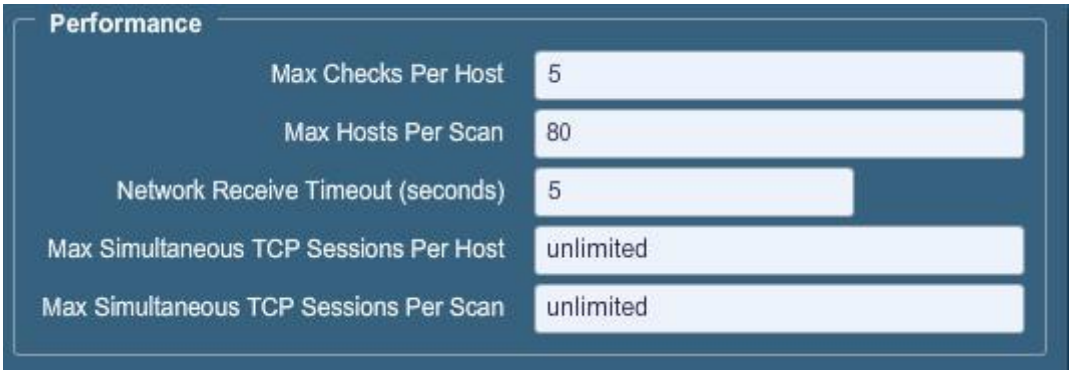
Reduce Parallel Connections on Congestion – po zaznaczeniu, jeśli Nessus wykryje że badany host wysyła zbyt dużo pakietów, przystosuje tempo skanowania aby nie przeciążać łącza, gdy będzie taka możliwość automatycznie powróci do poprzedniej prędkości.
Use Kernel Congestion Detection (Linux Only) – dotyczy tylko systemów z rodziny Linux, umożliwia Nessus'owi monitorowanie dostępnych zasobów i wykorzystanie ich w maksymalnym stopniu.

- Port Scanners i Port Scan Options – zawierają opcje dotyczące portów.



TCP Scan, UDP Scan, SYN Scan– umożliwia ustawienie jakiego typu portu mają być skanowane, odpowiednio TCP,UDP, SYN.
SNMP Scan – umożliwia skanowanie w poszukiwaniu włączonych usług SNMP (więcej o SNMP: http://pl.wikipedia.org/wiki/Simple_Network_Management_Protocol).
Netstat SSH Scan, Netstat WMI Scan – umożliwia używania funkcji netstat w poszukiwaniu otwartych portów, oparte jest w oparciu o komendy dostępne poprzez użycie SSH (dotyczy Linuxa) i WMI (dotyczy Windows). Więcej o WMI i SSH: http://pl.wikipedia.org/wiki/WMI, http://pl.wikipedia.org/wiki/SSH.
Ping Host – umożliwia „pingowanie" zdalnego hosta na wielu portach aby ocenić czy jest dostępny.
Port Scan Range – definiuje zakres portów podlegających skanowaniu. Im więcej tym dłużej potrwa skanowanie np. 21-23,25,80 umożliwia skanowanie portów od21 do23 oraz 25 i 80. Im węższa grupa do skanowania tym proces ten trwa krócej.

- Performance – zawiera opcje dotyczące wydajności

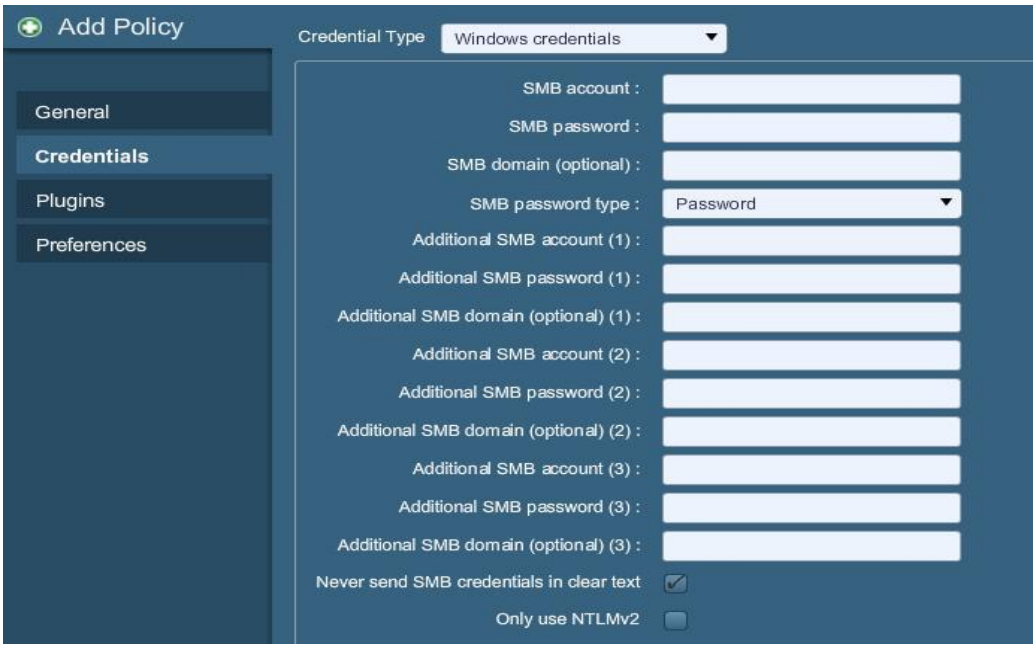


Max Checks Per Host – zawiera liczbę maksymalnych sprawdzań jednego hosta w jednym czasie.
Max Hosts Per Scan – określa maksymalną liczbę hostów skanowanych w tym samym czasie.
Network Receive Timeout(seconds) – jest to czas wyrażony w sekundach określający okres oczekiwania na odpowiedź skanowanego hosta, jeśli skanowanie odbywa się po wolnym łączu należy zwiększyć ten czas.
Max Simultaneous TCP Sessions Per Host – określa maksymalną ilość sesji TCP dla jednego hosta
Max Simultaneous TCP Sessions Per Scan - określa maksymalną ilość sesji TCP dla jednego skanowania.

Credentials

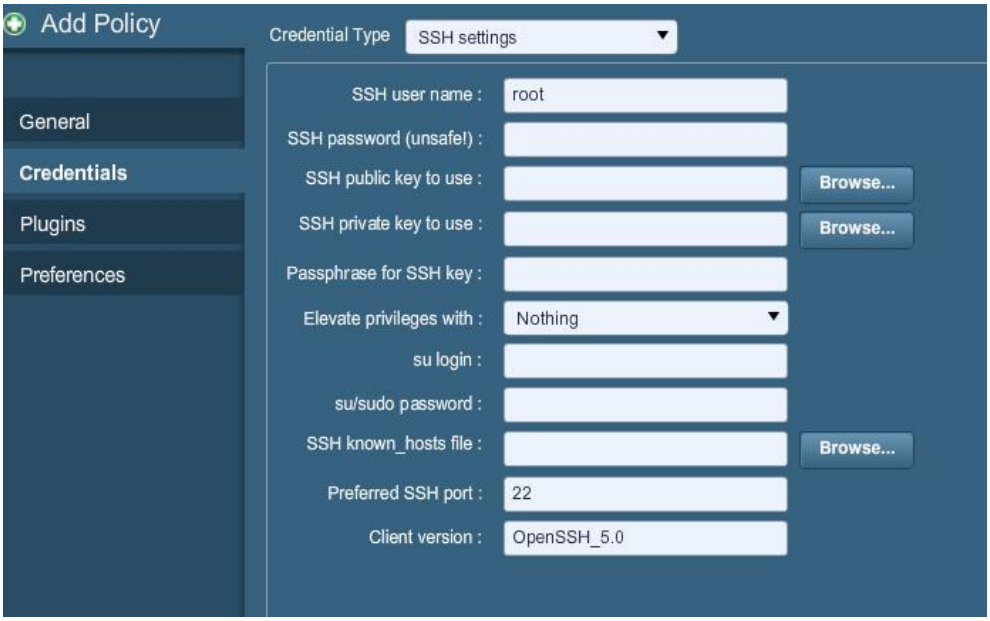
Umożliwia ustawienia opcji związanych z uwierzytelnianiem w różnych usługach od SMB, SSH, Kerberos aż po czysty tekst.

- Windows Credentials:



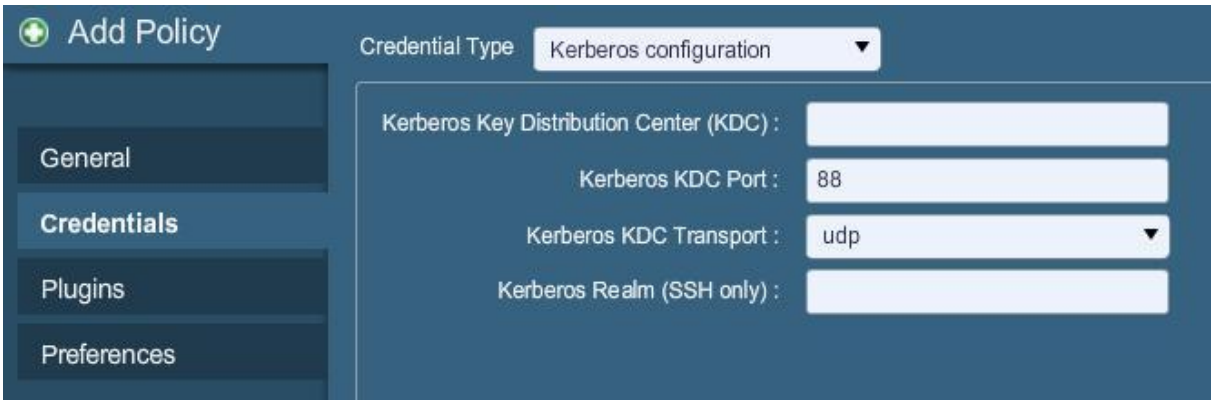
Dotyczy konfiguracji protokołu SMB (rodzina Windows) zawiera okna w które należy wpisać login (*SMB account*) oraz hasło (*SMB password*) dla głównego użytkownika, opcjonalnie dodając nazwę domenową. Można ustawić również szyfrowanie hasła poprzez wybranie odpowiedniej opcji w *SMB password type*. Opcjonalnie można zdefiniować jeszcze trzech dodatkowych użytkowników do tego celu służą pola *Additional SMB account*, *Additional SMB password*, *Additional SMB domain* oznaczone odpowiednio liczbami porządkowymi kolejnych użytkowników *(1-3)* . Dokładny opis tego protokołu: http://pl.wikipedia.org/wiki/SMB
Ostatnie możliwe do zaznaczenia opcje to jest:
Never Send SMB Credentials In clear text – po zaznaczeniu zapewniają że dane nie będą wysyłane w postaci nie szyfrowanej (czystego tekstu)
Only use NTLMv2 - zapewnia używanie tylko tego standardu szyfrowania które jest dosyć bezpieczne, więcej http://en.wikipedia.org/wiki/NTLM#NTLMv2

- SSH settings:



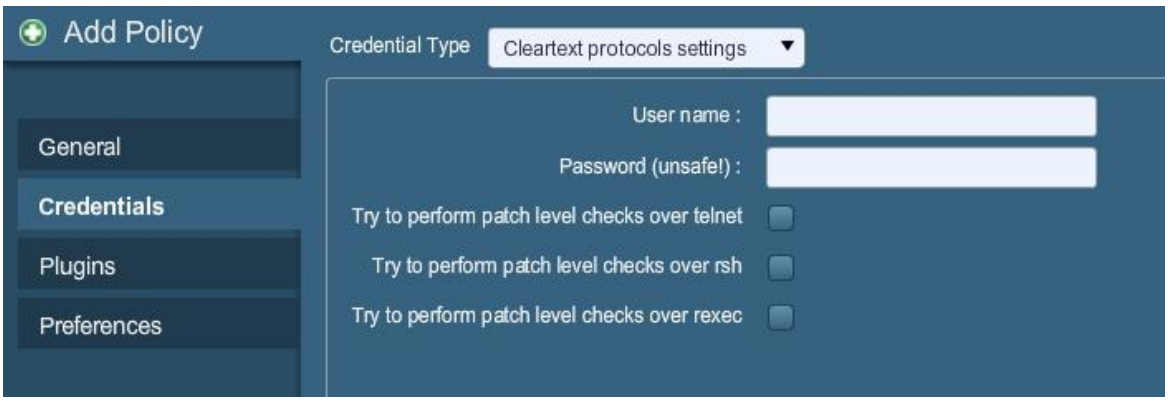
Dotyczy konfiguracji protokołu SSH (rodzina Linux) zawiera okna w które należy wpisać nazwę użytkownika (*SSH user name*) oraz hasło (*SSH password*) dla uprzywilejowanego użytkownika (root). Pierwsza różnica od razu rzucająca się w oczy w porównaniu do poprzedniego protokołu to fakt że wysyłane hasło nie jest szyfrowane. Komunikacja za pomocą tego protokołu jest gwarantuje bezpieczeństwo za pomocą mechanizmu kluczy: prywatnych i publicznych, aby możliwa była komunikacja należy uzupełnić pola *SSH public key to use* oraz *SSH private key to use* wskazując miejsce na dysku gdzie pliki reprezentujące te informacje są przechowywane w tym celu klikamy *Browse* (przeglądaj).
Passphrase for SSH key - w tym polu należy wpisać hasło dostępowe składające się minimum z 8 znaków, znaków specjalnych, dużych i małych liter oraz cyfr.
Elevate privilige with – określa stopień uprzywilejowania od *sudo* przez *su* aż po *su+sudo*.
Po wybraniu jednej z tych opcji należy podać login i hasło dla konta o takich uprawnieniach (*su login* oraz *su/sudo password*).
SSH known_hosts file – umożliwia wczytanie z pliku listy hostów do komunikacji za pomocą protokołu SSH, podobnie jak wyżej należy wskazać plik poprzez *Browse.*
Preferred SSH port – określa port do komunikacji SSH
Client version – określa wersje klienta za pomocą którego nastąpi komunikacja.

- Kerberos configuration



Umożliwia konfiguracje kolejnego protokołu uwierzytelnienia i autoryzacji, tym razem zwanej o polsku Cerberem.
Kerberos Key Distribution Center (KDC) – należy podać identyfikator (ip jednego z serwerów KDC) Centrum Dostarczania Klucza z którego zasobów (użytkownicy jak i usługi) będziemy korzystać.
Kerberos KDC Port – określa numer portu po którym ma następować łączenie za pomocą tego protokołu.
Kerberos KDC Transport – określa sposób połączenia UDP lub TCP.
Kerberos Realm (SSH only) – umożliwia łączenie się za pomocą odpowiednika nazw domenowych, jednak tylko w momencie gdy mamy do czynienia z SSH.

- Cleartext protocls settings



Zawiera ustawienia dla protokołów przesyłających dane czystym (nie szyfrowanym tekstem).
User name – pole do wpisania nazwy użytkownika
Password(unsafe!) – nieszyfrowane (podczas wysyłania) pole hasła dla użytkownika
Try to perform patch level checks over telnet
Try to perform patch level checks over rsh
Try to perform patch level checks over rexec

Zaznaczenie jednej z powyższych opcji umożliwia próbę wykonania połączenia za pomocą jednego z protokołów: telnet, rsh, rexec.

Plugins
Umożliwia dołączenie wtyczek które podczas skanowania testuja komputer pod danym kątem. Wtyczek jest około 40 tys podzielone zostały na kategorie. Najbardziej istotne i popularne zostaną przedstawione. Jednak pewne zasady ogólne są dla wszystkich podobne to znaczy a by dowiedzieć się czegoś więcej o danej wtyczce wystarczy wybrać ją z rodziny dostępnych następnie Na interesujące nas kryterium testowania np.:

z rodziny *Peer-to-Peer File Sharing* odnalazłem wtyczkę dotyczącą używania usługi eDonkey. gdyby taka usługa została wykryta na komputerze skanowanym uzyskalibyśmy następujące informacje:

eDonkey Detection

Synopsis
There is a peer-to-peer file sharing application listening on the remote host.

Description
The remote host appears to be running eDonkey or one of its variants,
which is commonly used for sharing music, films, and software.

Solution
Make sure this service agrees with your organization's security
and acceptable use policies.

See Also
http://en.wikipedia.org/wiki/EDonkey_network

Informacje odczytane w opisie podsuwają nam streszczenie wtyczki (*Synopsis*) jej opis (*Description*) oraz sposób rozwiązania(*Solution*). W tym wypadku z racji że opisywana wtyczka dotyczyła sieci P2P (wymiany plików) rozwiązanie sprowadza się jedynie do upewnienia czy współdzielone pliki są zgodne z polityka organizacji ochrony praw autorskich.

Opis ważniejszych rodzin wtyczek:
- Backdoors – zawiera wtyczki testujące oprogramowanie komputera pod względem luk w aplikacjach, przez które możliwe byłyby włamania do takiego hosta, lub pod względem obecności złośliwego oprogramowania to umożliwiające tzw Trojany. Przykładowe wtyczki:

Bagle.B Detection wykrywa robaki w systemie informacje:

Bagle.B Detection

Synopsis
A worm was detected on the remote host.

Description
The remote host has the Bagle.B worm installed. This is a variant of the Bagle worm which spreads via email and has a backdoor that listens on port 8866.

Solution
Use an anti-virus product to remove the worm.

Z zamieszczonych informacji widać że aby pozbyć się problemu wystarczy przeskanować komputer antywirusem.

Agobot.FO Backdoor Detection

Agobot.FO Backdoor Detection

Synopsis
The remote host has a backdoor installed.

Description
The remote host has the Agobot.FO backdoor installed. This backdoor is known to:
- Scan local networks for common Microsoft vulnerabilities.
- Scan local networks for exploitable DameWare systems.
- Brute force local Microsoft machine User accounts.
- Connect to an IRC channel and setup a BOT for remote command execution.

Solution
This backdoor should be immediately removed from the network and manually cleaned.

W tym wypadku postępowanie sprowadza się do odnalezienia w systemie aplikacji i jej usunięcia ręcznie.

Microsoft IIS Download.Ject Trojan Detection

Microsoft IIS Download.Ject Trojan Detection

Synopsis
The remote host is infected by a Trojan Horse.

Description
Download.Ject is a Trojan that infects Microsoft IIS servers. The Trojan's dropper sets it as the document footer for all pages served by IIS Web sites on the infected computer.

Solution
Use an Anti-Virus to clean machine.

Opisywana złośliwa aplikacja sprowadza się do aplikacji serwera produkcji Microsoftu. Tak naprawde z racji dużej popularności programów tego producenta bardzo często pada ofiarą złośliwego kodu. Aby nie paść jego ofiarą należy na bieżąca aktualizować swoje aplikacje.

W tym akurat przypadku po raz kolejny wystarczy użyć antywirusa.

- Rodzina wtyczek CGI dotyczy błędów zagrożeń związanych z komunikacją serwera WWW z innymi aplikacjami znajdującymi się na serwerze. Np.

/doc Directory Browsable - jest związana z możliwością przeglądania zawartości folderu /doc a więc jest to dość krytyczny błąd. Solucją jest zmiana polityki uprawnień na takie aby ten folder nie był dostępny z zewnątrz.

Wtyczki z biblioteki CGI abuses: XSS dotyczą zabezpieczeń elementów dynamicznych które znajdują się na stronach WWW. Poprzednia wtyczka pochodziła z biblioteki CGI abuses która dotyczyła elementów statycznych. Z CGI abuses: XSS pochodzi między innymi wtyczka:

ATutor 1.5.1 Multiple Script XSS – jest ona związana z wrażliwością kodu php a więc tym samym wrażliwością na tzw CrossScript czyli uruchamianie zewnętrznych skryptów w miejscu w którym nie powinno to mieć miejsca. Przykładem takiego ataku może być np. usunięcie bazy danych.

- CISCO ta rodzina wtyczek zawiera testy sprawdzające konfiguracje urządzeń firmy CISCO. I tak np.
wtyczka Cisco 675 Router Default Unpassworded Account sprawdza czy użytkownik uprzywilejowany ma ustawione hasło,
Cisco Catalyst 5000 Series Frame STP Port Broadcast DoS (CSCdt62732) sprawdza czy nie występuje luka w oprogramowaniu umożliwiająca przeprowadzenia ataku typu DoS.

- Databases zawiera wtyczki testujące serwery baz danych różnych producentów m.in. MS SQL Server, IBM solidDB, MySQL, Oracle…

- Debian Local Security Check sprawdza system operacyjny z rodziny Debian pod kątem brakujących uaktualnień bez których system jest podatny na ataki pze względu na występujące w nim luki.

- Denial of Service rodzina wtyczek sprawdzająca podatność hosta na ataki tego typu. Jest to zbiór naprawdę rozbudowanych wtyczek sprawdzających dany host pod róznymi kątami od zawieszania się modemu przez luki w aplikacjach aż po fragmentacje paczek w sieciach TCP/IP

- FTP sprawdza serwery hosty pełniące role FTP w poszukiwaniu ewentualnych luk mogących stwarzać ryzyko ataku.

- Fedora Local Security Check podobnie jak ww Debian Local Security Check sprawdza bezpieczeństwo system, tym razem Fedory.

- Firewalls niezmiernie ważna rodzina wtyczek nie można o niej zapomnieć skanując dany host gdyż sprawna zapora to podstawa bezpieczeństwa systemu komputerowego.

- FreeBSD, Gentoo, MacOS X, Mandriva, RedHat, Slackware, Solaris, SuSE, Ubuntu, VMWare ESX, Windows Local Security Check jak ww dotyczące systemów operacyjnych.

-General sprawdza dane takie jak możliwość odczytywania BIOSu, dostęp do pamięci, dostęp do system operacyjnego, udostępnione pliku, wykrywane sieci wifi

- Netware wtyczki sprawdzające stabilność I bezpieczeństwo aplikacji internetowych

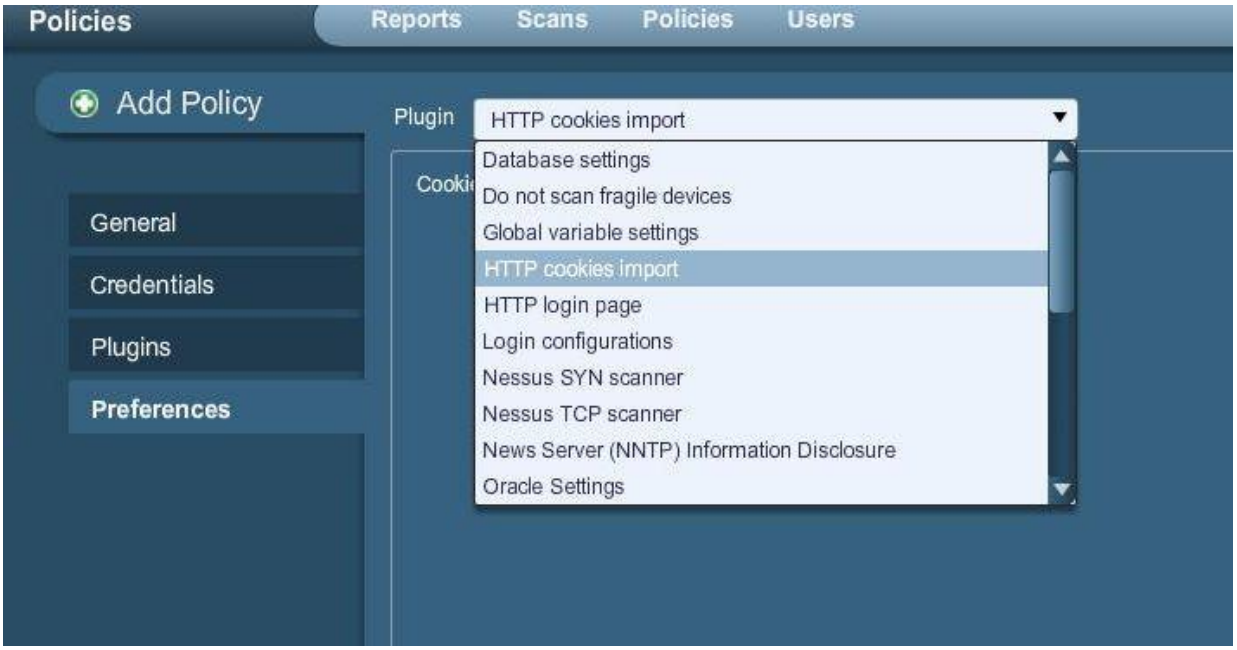
- Peer-to-Peer sprawdza bezpieczeństwo wymiany w sieciach P2P

- SMTP problems – sprawdza problemy występujące z protokołem SMTP.

- SNMP - sprawdza czy usługa jest włączona i czy działa poprawnie

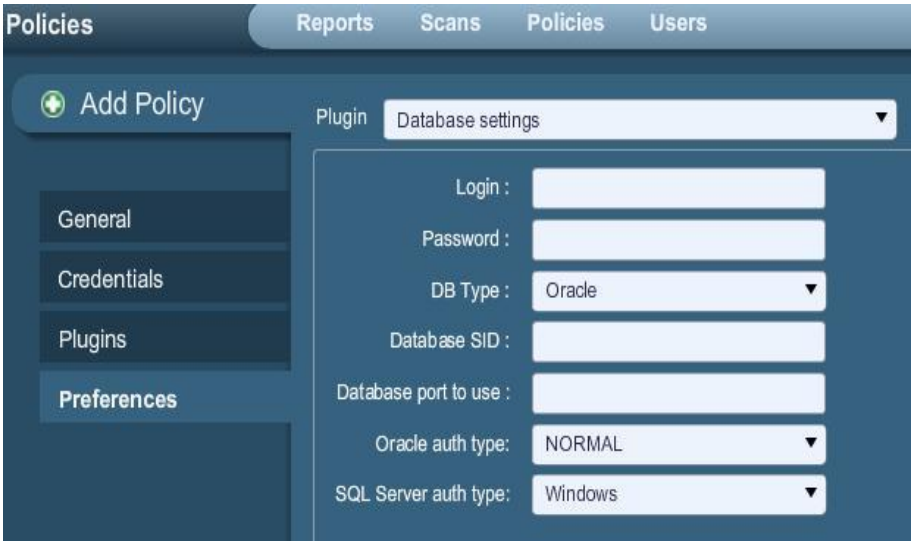
- Service Detection – sprawdza uruchomione w systemie usługi

Preferences



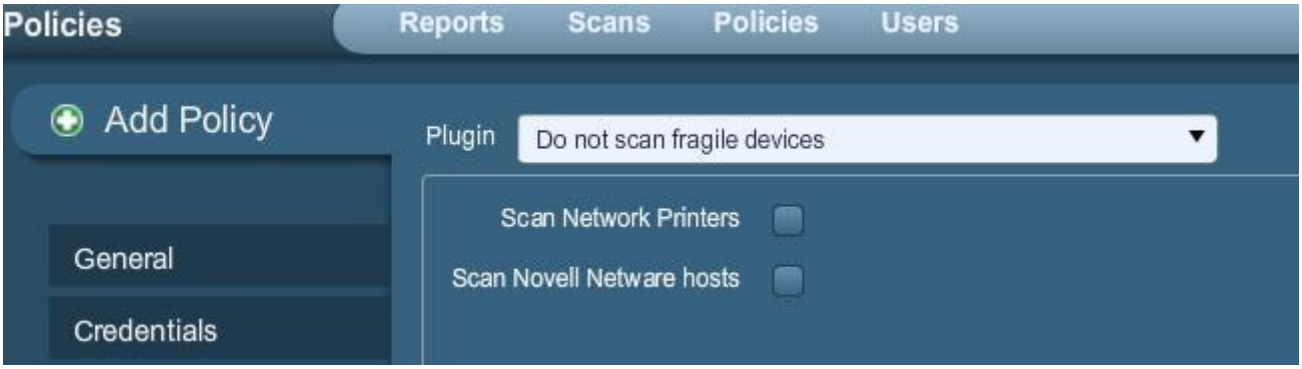
Zakładka ta zawiera różnego rodzaju opcje ogólne związane z programem i skanowaniem czy ustawieniami niektórych własności które należy uwzględnić podczas skanowania np. czy firewall ma być wykrywany czy blokowany oraz np. dane potrzebne do logowania do bazy danych. Lista dostępnych opcji zależy od tego jakie wtyczki są dostępne.

- Database settings



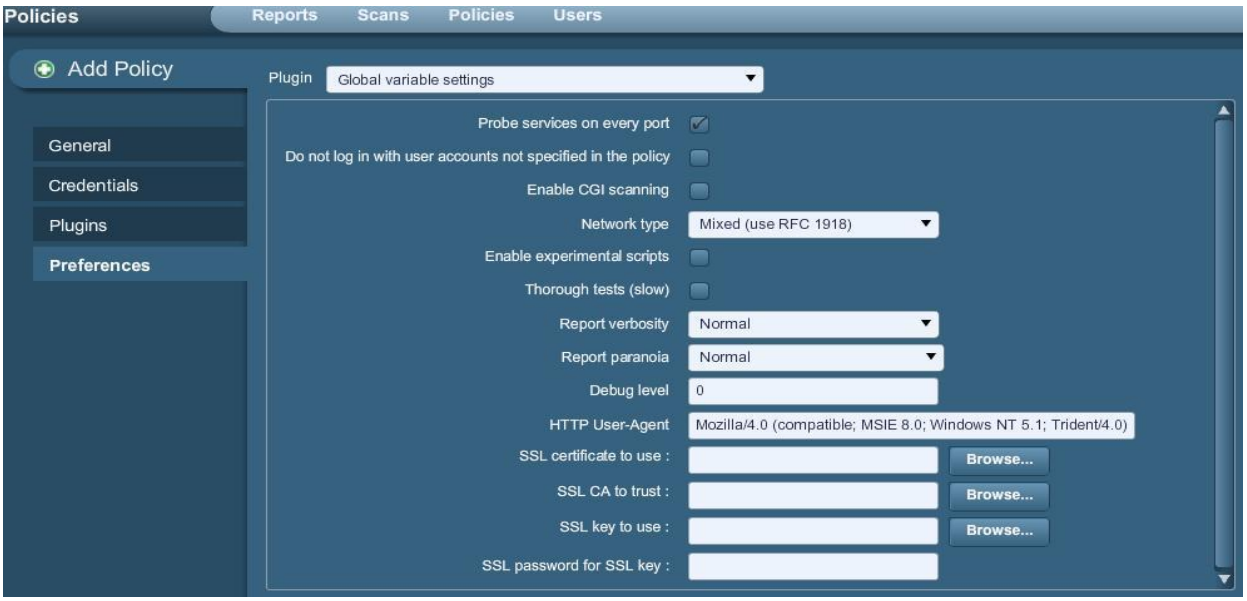
Jeśli chcemy przeskanować bazę danych należy ustawić widoczne pola. Oczywiście to czy będziemy mogli wykonać takie skanowanie zależy od tego czy mamy odpowiednie wtyczki aktywne.
Login – należey podać login do bazy danych
Password – hasło dla użytkownika o podanym wyżej loginie
DB Type – z listy wybieramy typ bazy danych, do wyboru są: Oracle, SQL Server, MySQL, DB2, PostgreSQL.
Database SID – należy podać identyfikator systemu bazy danych do audytu
Database port to use – numer portu na którym nastąpi skanowanie bazy danych
Oracle Auth Type – typ uwierzytelniania w przypadku baz Oracle, dostępne opcję to: NORMAL, SYSOPER, SYSDBA.
SQL Server Auth Type – typ uwierzytelniania serwera bazy SQL, dostępne opcje to Windows lub SQL.

- Do not scan fragile devices



Mamy możliwość wybrania czy podczas skanowania uwzględnione zostaną sieciowe drukarki (*Scan Network Printers*) oraz urządzenia sieciowe firmy Novell (*Scan Novell Netware hosts* inne opcję pojawiły by się gdyby zainstalowano więcej wtyczek).
Dodano możliwość wyboru czy skanować te urządzenia gdyż są one dosyć łatwe do zablokowania, tzn gdyby skanowanie odbywało się w godzinach pracy jest duża szansa że te urządzenia byłyby wyłączone z użycia na ten czas.

- Global variable settings

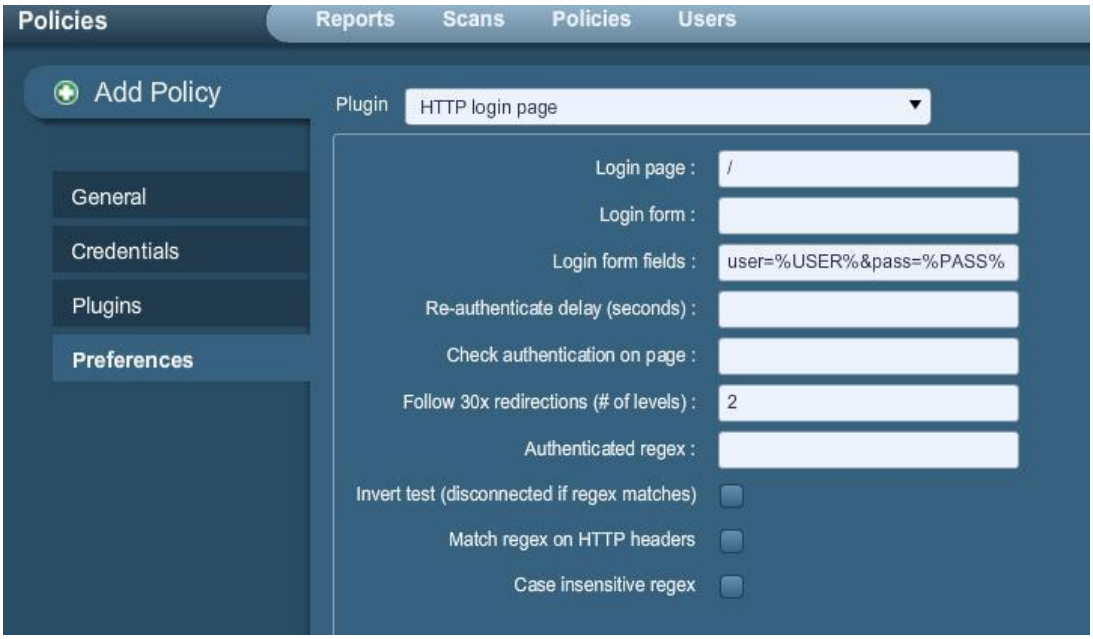


Zawiera różne opcje z szerokiego zakresu dostępnych możliwości oferowanych przez serwer Nessus'a.
Probe services on etery port – testuje usługi dostępne poprzez otwarte porty, należy mieć na uwadze że takie działanie może doprowadzić do niestabilności tych usług.
Do not log In with user account not specified in the policy – zablokuje możliwość logowanie się za pomocą konta użytkownika nie wymienionego w zasadzie skanowania.
Enable CGI Canning – zaznaczenie tej opcji włączy skanowanie usług CGI czyli związanych z komunikacją między serwerem WWW a innym aplikacjami dostępnymi na serwerze. Gdy ta opcja jest nie zaznaczona skanowanie odbywa się szybciej.
Network type – pozwala określić z jakiej puli adresów IP składa się nasza sieć z publicznych (*Public WAN Internet*), prywatnych (*Private LAN*) czy różnych (*Mixed use RFC 1918*).
Enable experimental scripts – pozwala używać wtyczek rozwijanych (nie wersji finalnych)
Thorough test (slow) – uruchamia testowanie gruntowne, każda z dostępnych wtyczek będzie pracowała w trybie o najwyższej dokładności np. skanowanie usług SMB będzie się składać z trzech poziomów a nie z jednego. Znacznie zwalnia skanowanie.
Report verbosity – ilość informacji zamieszczanych w raporcie im wyższy poziom tym ich będzie więcej. *Quiet* najniższy, *Normal* normalny, *Verbose* najwyższy najwięcej informacji.
Report paranoia – określa wrażliwość Nessus'a na zagrożenia które będą zamieszczanie w raporcie końcowym. Dostępne opcję: *Paranoid* zamieści stosowną informacje gdy tylko zwątpi w poprawność testu (nie zalecane, dużo fałszywych alarmów), *Normal* jest to kompromis, *Avoid false alarm* najbardziej pobłażliwa z możliwych poziomów (nie zalecane może ominąć poważne zagrożenie).
Debug level – po ustawieniu 1 proces debugowania zostanie włączony.
HTTP User Agent – określa jakie przeglądarki współpracują (oparte o jaki silnik) z klientem serwera Nessus.
SSL certificate to use – umożliwia połączenie ze zdalnym hostem poprzez SSL wymagany do tego certyfikat należy wskazać z dysku (*Browse*).
SSL CA to trust – określa Centrum Autoryzacji któremu Nessus może zaufać (należy wskazać z dysku).
SSL key to use –podobnie jak wyżej należy wskazać klucz do komunikacji.
SSL password for SSL key – hasło umożliwiające użycie klucze ww.

- HTTP Cookies Import

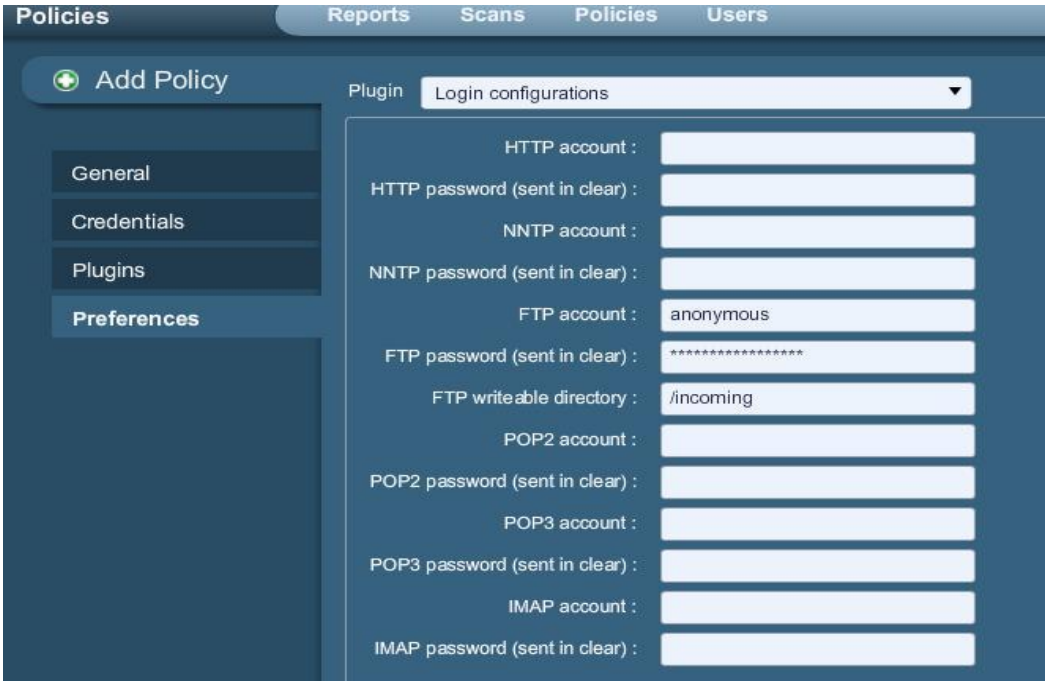
Po wybraniu tej opcji Nessus może zaimportować pliki *Cookies* y innego rodzaju oprogramowania np. przegldarki internetowej jest to potrzebne przy testowaniu niektórych serwerów WWW. Format wczytywanego pliku musi być zgodny z Netscape.

-HTTP login page



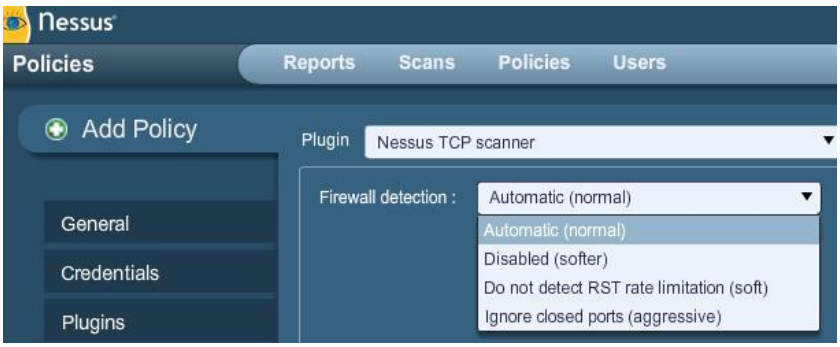
Zawiera opcję dotyczące kontroli nad aplikacjami webowymi.
Login page – należy podać adres serwisu internetowego
Login form – określa parametr „akcji" formularza, czyli w jaki sposób zostają przekazywane dane np.: <form method="POST" action="/login.php"> należy wpisać "/login.php".
Login form fields – zamiast zmiennych %USER% i %PASS% należy podać login i hasło jakie są wymagane do dostępu do serwisu.
Re-authenticate delay (seconds) – określa opóźnienie czasowe po jakim można ponowić próbe zalogowania (dotyczy nie udanej autoryzacji).
Follow 30x redirections (# of levels)- jeśli 30 razy zostanie wywołane żądanie przekserowania z przeglądarki nastąpi ono do adresu podanego w tym polu.
Authenticated regex - wyrażenie regularne na podstawie którego ma być sprawdzana autoryzacja.
Invert test (disconnected if regex matches) – odwrotność poprzedniego czyli wyrazenie regularne na podstawie którego określamy że zalogowanie nie zostało potwierdzone.
Match regex on http headers – dopasowanie do wzorca (wyr regularnego) na podstawie nagłówka http.
Case insensitive regex - umożliwia włączenie wrażliwości na wielkość znaków (duże małe litery).

- Login configurations



Zawiera dane logowania (login i hasło) różnych usług: HTTP, NNTP, FTP, POP2, POP3, IMAP.

- Nessus SYN scanner oraz Nessus TCP scanner

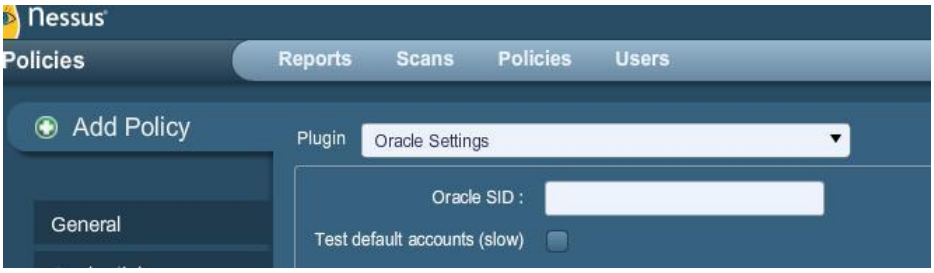


umożliwia wybór traktowania napotkanego podczas skanowania firewall'a dla różnych protokołów (TCP lub SYN):
Automatic – sprawdzi czy występuje firewall pomiędzy serwerem Nessus'a a skanowanym hostem.
Disabled – nie będzie tego sprawdzał
Do not detect RST rate limitation - ??
Ignore closed ports (aggressive) – Nessus uruchomi wtyczki skanujące porty pomimo iż są zamknięte przed zaporę.

- News Server (NNTP) Information Disclosure

Pozwala określić czy są testowane serwery informacyjne mogą rozsyłać spam.
From address – zawiera adres którego Nessus użyje aby wysłać wiadomość, jeśli serwer odpowie spamem to z racji fikcyjnego adresu nic na tym nie ucierpi.
Test group name regex - zawiera wyrażenie regularne które określa grupe odbiorców wiadomości.
Max crosspost – maksymalna liczba serwerów wiadomości jaka można wysłać wiadomości testowe.
Local distribution – jeśli zaznaczone Nessus ograniczy sprawdzanie serwerów wiadomości do lokalnych.
No archive – po zaznaczeniu Nessus sprawdzi czy wiadomości testowe są usuwane przez serwer.

- Oracle settings



zawiera ustawienia baz Oracle ich identyfikator systemowy (*Oracle SID*) oraz czy Nessus powinien skanować również konta domyślne co znacznie przedłuży test (*Test default accounts*).

- Ping a remote host

Zawiera opcję dotyczące skanowania komputera za pomocą „pingowania”.
TCP ping destination port(s) – określa porty jakie będą testowane za pomocą ping’a TCP, ARP, ICMP w zależności od wybrania opcji(*Do an ARP ping, Do a TCP ping, Do a ICMP ping*). Zaleca się pozostawienie domyślnej wartości *butli-in*.
Number of Retries (ICMP) – ustala ilość sygnałów pingujących dla ICMP.
Do an applicative UDP –użyje ping’a zgodnego ze specyfikacją aplikacji UDP tzn na portach 53 (DNS), 1111 (RPC),123 (NTP), 520 (RIP).
Make the dead hosts appear In the report – hosty nie odpowiadające na ping zostaną zamieszczone w raporcie.
Log live hosts in the report – do raportu zostanie dołączony log z przeprowadzenia ping’a z dostępnymi hostami.
Test the local Nessus host – po zaznaczeniu komputer na którym jest uruchamiany Nessus będzie również zeskanowany. Jest to przydatne w przypadku zdalnego skanowania i komputer z Nessus’em nie jest w zakresie sieci będącej skanowanej.
Fast Network Discovery – podczas pingowania Nessus sprawdza czas po jakim nastąpiła odpowiedź dodatkowo sprawdzając czy nie komunikacja host a serwer Nessus’a nie odbywa się poprzez jakiś serwer Proxy zajmuje to jakiś czas. Jeśli więc nie zależy nam na tym po prostu zaznaczmy tę opcje.

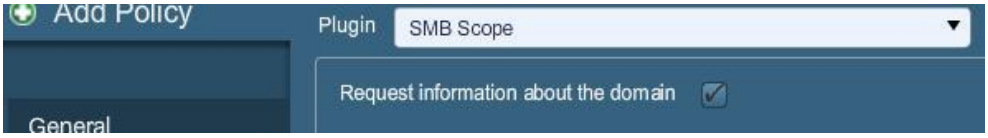
- Port scanner settings

Zawiera opcje dotyczące skanowania portów.
Check open TCP ports found by local port enumerators – jeśli lokalny numerator portów (WMI lub netstat) znjadzie otwarty port, Nessus zdalnie również go zweryfikuje. Pozwala to sprawdzić czy używane są zabezpieczenia typu firewall.
Only run network port scanners if local port enumeration failed – po zaznaczeniu tej opcji Nessus będzie polegał tylko na „opinii” lokalnego numeratora portów.

- SMB Registry: Start the Registry Service during the scan
- SMB Scope

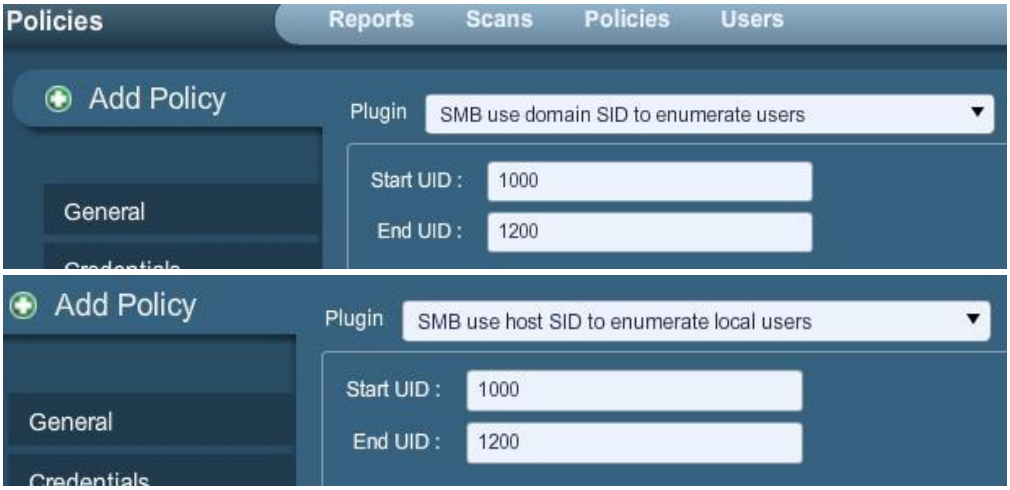
zawiera opcje dotyczące usług SMB.

Pierwsza umożliwia podczas skanowania uruchomienie usług nie korzystający z SMB.



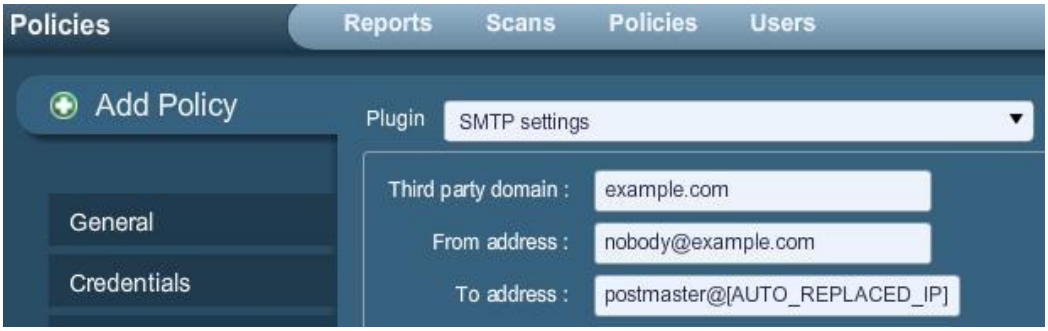
Druga umożliwia skanowanie użytkowników domenowych zamiast lokalnych.

- SMB use domain SID to enumerate users
- SMB use host SID to enumerate local users



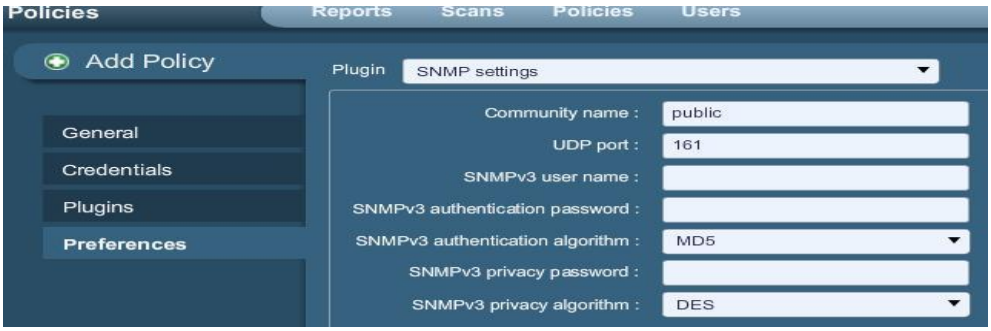
Pierwsza określa zasięg identyfikatora system do przeszukiwania wstecznego użytkowników na domenach, druga w obrębie lokalnych. Zaleca się zostawienie wartości domyślnych.

- SMTP settings



Zawiera ustawienia konfiguracji usługi SMTP
Nessus spróbuje przetestować tę usługę w obrębie domeny podanej w *Third party domain.* Jeśli wiadomość wysłana do adresów należących do ww, zarejestrowana na adres podany w *To address* zostanie odrzucona będzie oznaczać nieudaną próbe spamu. W przeciwnym razie oznacza że serwer SMTP jest używany do przekazywania spamu. Pole *From address* tworzy wirtualne konto aby zabezpieczyć się przed atakiem spamu wywołanym przez serwer.

- SNMP settings

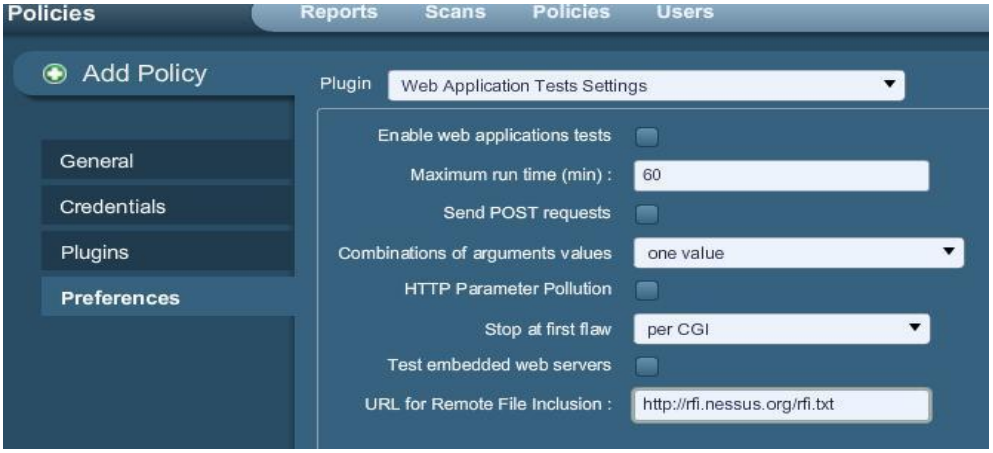


Pozwala skonfigurować Nessusa do połączenia i autentykacji z serwisami SNMP.
Community name – nazwa połączenia
UDP port – numer portu po którym ma się odbywać komunikacja
SNMPv3 user name – nazwa użytkownika dla protokołu SNMPv3
SNMPv3 authentication password – hasło uwierzytelniające użytkownika
SNMPv3 authentication algorithm – algorytm szyfrujący uwierzytelniania do wyboru: MD5 i SHA1
SNMPv3 privacy password – hasło używane do szyfrowania komunikacji
SNMPv3 privacy alorithm – algorytm używany do ww danych.

- Service Detection

Kontroluje jak Nessus będzie testował usługi oparte na SSL. Opcje *Known SSL port* oznacza skanowanie po znanym porcie SSL a więc 443, *All* po wszystkich, *None* po żadnym.

- Web Applications Tests Settings



Zawiera opcje związane z testowaniem aplikacji webowych.
Enable web applications tests – umożliwia sprawdzanie czy badany serwis jest odporny na ataki cross-scripting, sprawdza czy jakieś pliki nie posiadają zbyt pobłażliwych uprawnień etc. (w oparciu o dostępne wtyczki).
Maximum run time (min) – określa czs jak długo może odbywać się test.
Send POST requests – umożliwia testowanie serwisu za pomocą *POST-request.* Umożliwia to sprawdzenie poprawności danych wysyłanych przez formularze np. poprzez polecenie POST.
Combinations of arguments values – sprawdza kombinacje wartości agumentów http. Możliwe są trzy opcje: *One value* (zalecana), *All pairs*(wolna),*All combinations*(bardzo wolna).
HTTP Paramete Pollution – sprawdza czy adresy http nie zawierają nie potrzebnych informacji.
Stop at first flaw – zatrzymuje test po napotkaniu pierwszej usterki serwisu. Do wyboru są do jakiego typu usterki ma być przeprowadzany test. Do wyboru: *per CGI,* czyli do wystąpienia błędu

związanego z CGI(wspominanie kilka stron wcześniej), *per port (quicker)* do natrafienia na błędny otwarty port, *per parameter (slow)* do natrafienia na błąd parametru CGI, *look for all flaws (slower)* sprawdzi wszysteki usterki.
Test Embedded web Server – po zaznaczeniu przeskanowane zostaną również wbudowane serwery webowe.

- Web Mirroring

Umożliwia konfiguracje natywnego serwera webowego Nessusa zawierającego lustrzane użyteczne funkcje. Polega na tym że Nessus będzie przeglądał (testował) strony offline.
Number of pages to mirror – określa maksymalną liczbe stron do przechowania(testowania)
Maximum depth – limit poziomów (głebokości) linków ile Nessus będzie przechowywał
Start page –adres strony głównej od której zacznie się „lustracja”.
Excluded items Regen – wyrażenie regularne reprezentujące dane które mają nie zostać zlustrowane.
Follow dynamic pages – umożliwia Nessusowi łączenie się z linkami nie zważając na limity ustawione powyżej.

Pracę wykonali:

Przemysław Michalczyk

Bartosz Połaniecki