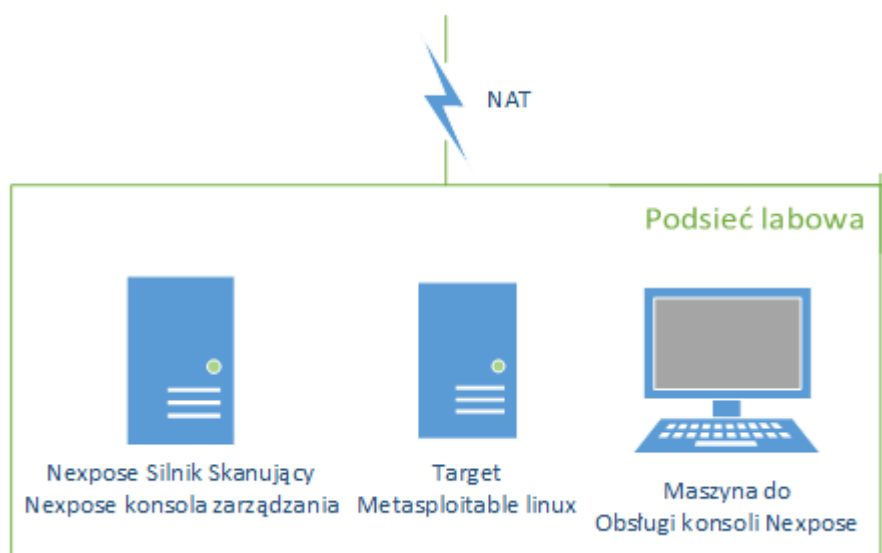


Dziś powracamy do serii o parze Nexpose i Metasploit. W dzisiejszym artykule zobaczycie jak poprawnie wpiąć w sieć, skonfigurować Nexpose oraz dodać „site” polecenie skanowania. Zapraszamy serdecznie!

## 1. Przyłączenie do sieci

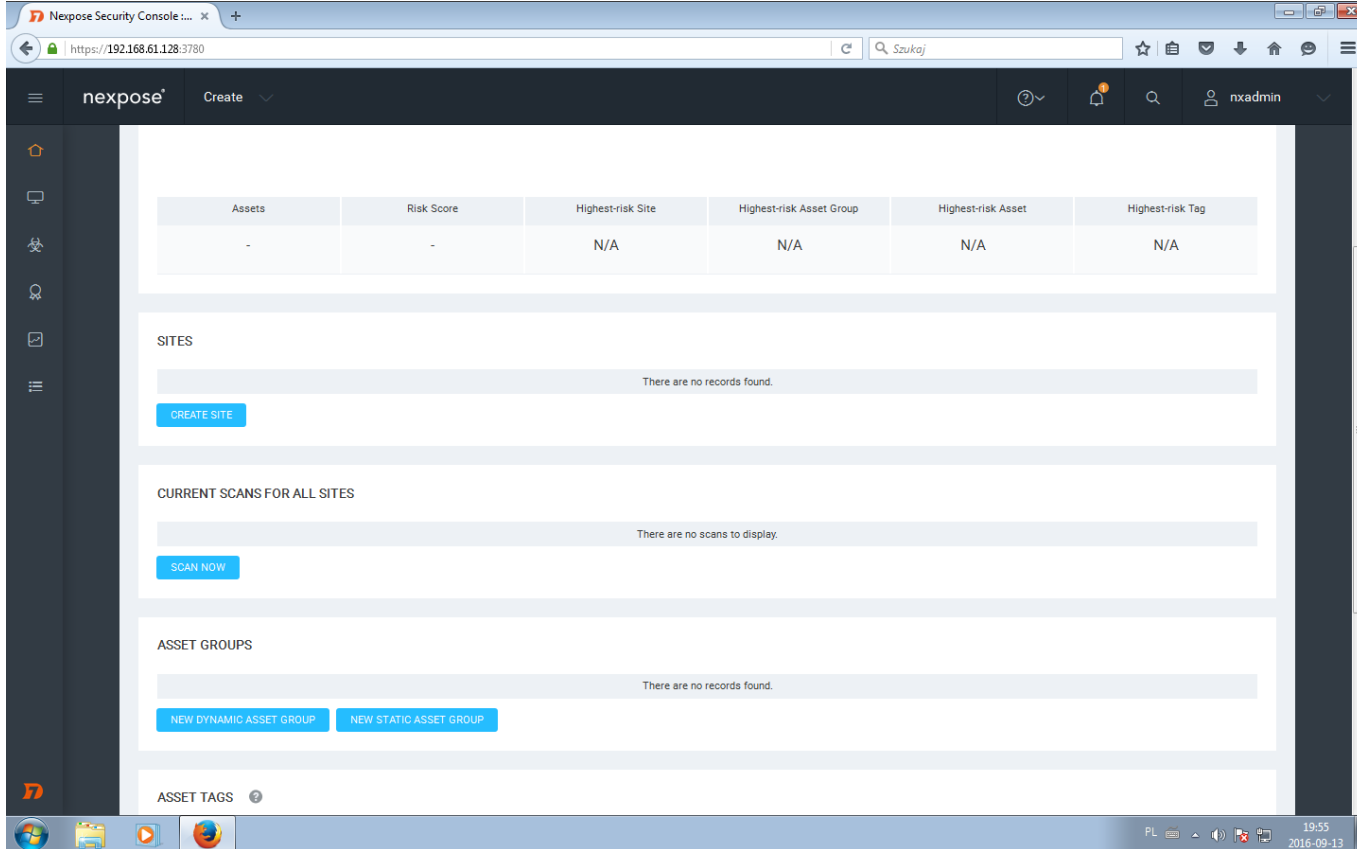
Pierwszą kwestią jaką rozważymy w tym miejscu, to to do jakich celów zamierzamy używać naszego skanera. Jeśli ma to być skaner wewnętrzny, w środowisku labowym do testowania pojedynczych maszyn możemy zastosować taki o to schemat sieci:



Alternatywą dla tego typu rozwiązania jest rozwiązanie produkcyjne. Przy tego typu sytuacjach musimy ustalić czy chcemy weryfikować mechanizmy bezpieczeństwa czuwające nad dostępem do maszyn czy też bezpieczeństwo samych maszyn. W przypadku gdy weryfikujemy bezpieczeństwo maszyn należy maszynie z Nexpose przydzielić bezpośredni dostęp do skanowanych maszyn oraz upewnić się, że po drodze nie ma żadnego mechanizmu blokującego. Dobrym pomysłem jest, na czas skanowania dodać naszą nexposową wirtualkę do [ACL](#) urządzeń sieciowych które są po drodze z Nexpose do targetu. Dzisiaj jednak zajmiemy się scenariuszem z testowaniem samych wirtualek w środowisku testowym.

## 2. Konfiguracja „site’u”

Kolejnym krokiem jest konfiguracja site’u – czyli prosto mówiąc zadaniem skanowania. W tym dziale określamy jakie hosty chcemy skanować, jakich podatności szukać czy też jakich uwierzytelnień użyć



Assets	Risk Score	Highest-risk Site	Highest-risk Asset Group	Highest-risk Asset	Highest-risk Tag
-	-	N/A	N/A	N/A	N/A

SITES

There are no records found.

CREATE SITE

CURRENT SCANS FOR ALL SITES

There are no scans to display.

SCAN NOW

ASSET GROUPS

There are no records found.

NEW DYNAMIC ASSET GROUP NEW STATIC ASSET GROUP

ASSET TAGS

Aby skonfigurować site, należy przejść do kreatora site’ów za pomocą przycisku „Create Site”.



## Nexpose - dodajemy hosty i wykonujemy pierwsze skanowanie.

The screenshot shows the Nexpose Security Console interface. The browser address bar displays `https://192.168.61.128:3780/scan/config.jsp#/scanconfig/about`. The page title is "Site Configuration". The navigation menu includes "INFO & SECURITY", "ASSETS", "AUTHENTICATION", "TEMPLATES", "ENGINES", "ALERTS", and "SCHEDULE". The "GENERAL" tab is selected, showing the following configuration:

- Name: `pierwsze_skany` (with a green checkmark)
- Importance: `Normal` (dropdown menu)
- Description: `nasze pierwsze zadanie skanowania.`

The "User-added Tags" section is expanded, showing a table with the following columns: CUSTOM TAGS, LOCATIONS, OWNERS, and CRITICALITY. The table contains one row with the following values:

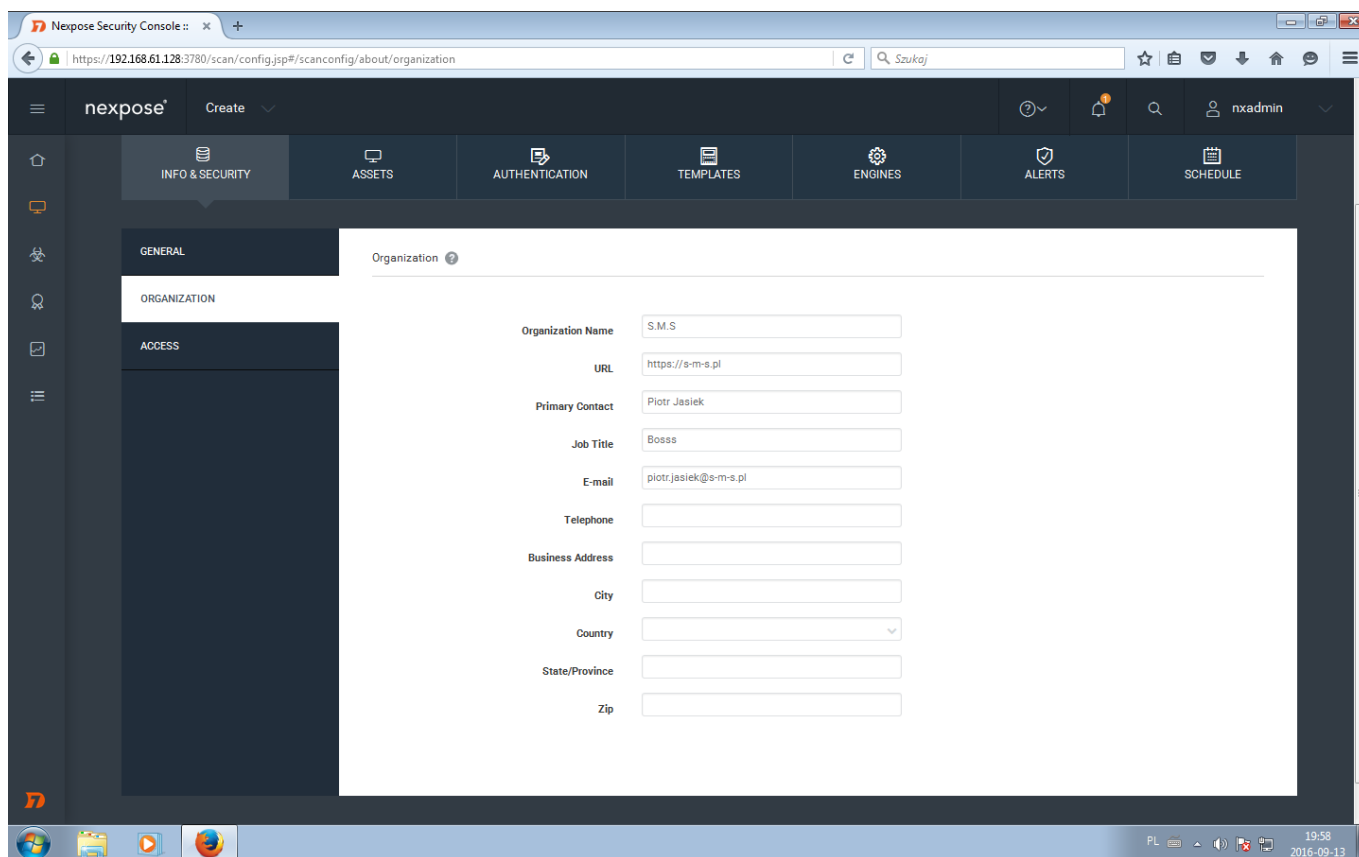
CUSTOM TAGS	LOCATIONS	OWNERS	CRITICALITY
None	biuro x	prezes x	Very High x

Below the table, there is a form to add a new tag. The "TAG NAME" field contains `pierwszy skan` and the "TAG COLOR" field shows a purple color swatch. An "ADD" button is visible.

Pierwszą zakładką jaka ukazuje się nam jest „Info & Security” W zakładce tej deklarujemy nazwę, tagi identyfikacyjne czy dostępy dla ewentualnych współpracowników. Dobrze prócz nazwy podać takie, które pozwolą nam później wygodniej segregować, czy też wyszukiwać maszyny w bazie danych. Opis site, może się okazać pomocny przy identyfikacji konkretnych sitów.



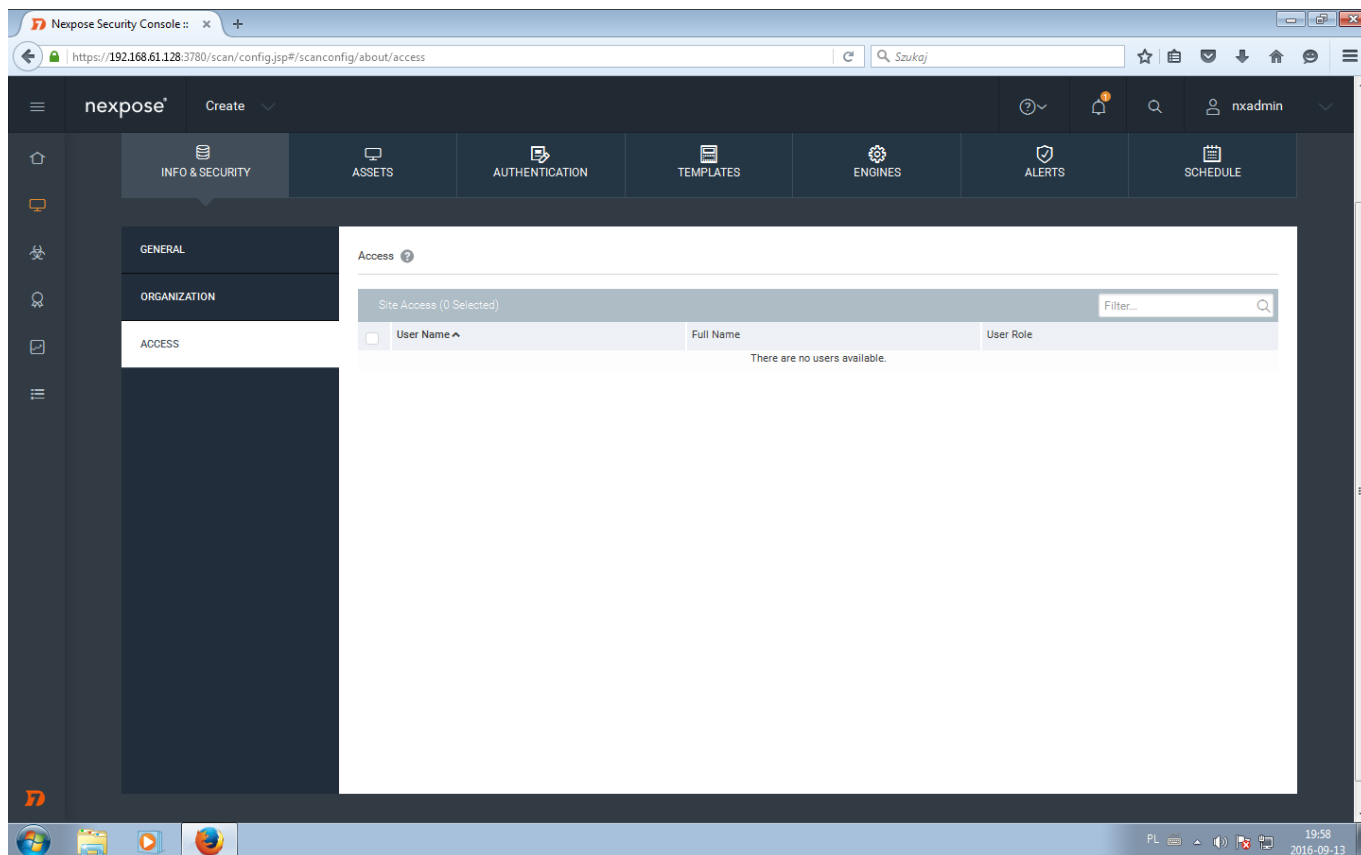
## Nexpose – dodajemy hosty i wykonujemy pierwsze skanowanie.



Dział „Organization” zawiera dane dotyczące organizacji do której należą dane maszyny. Dane te, dodawane są później do końcowego raportu. Nexpose może być używany do skanowania wielu oddzielnych infrastruktur, nawet oddzielonych od siebie fizycznie.



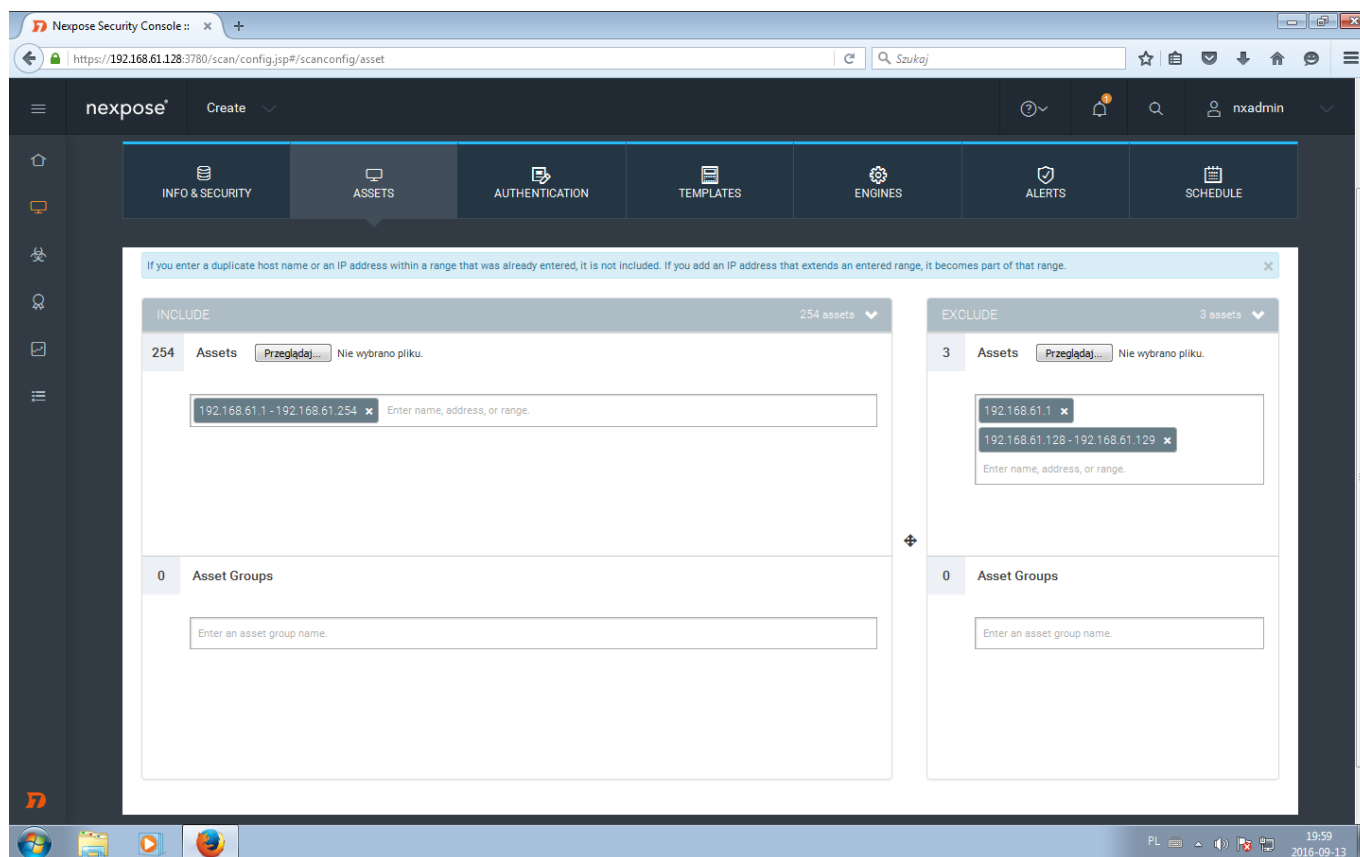
Nexpose - dodajemy hosty i wykonujemy pierwsze skanowanie.



W zakładce „Access” podajemy którzy użytkownicy mają mieć dostęp do naszego site’u.



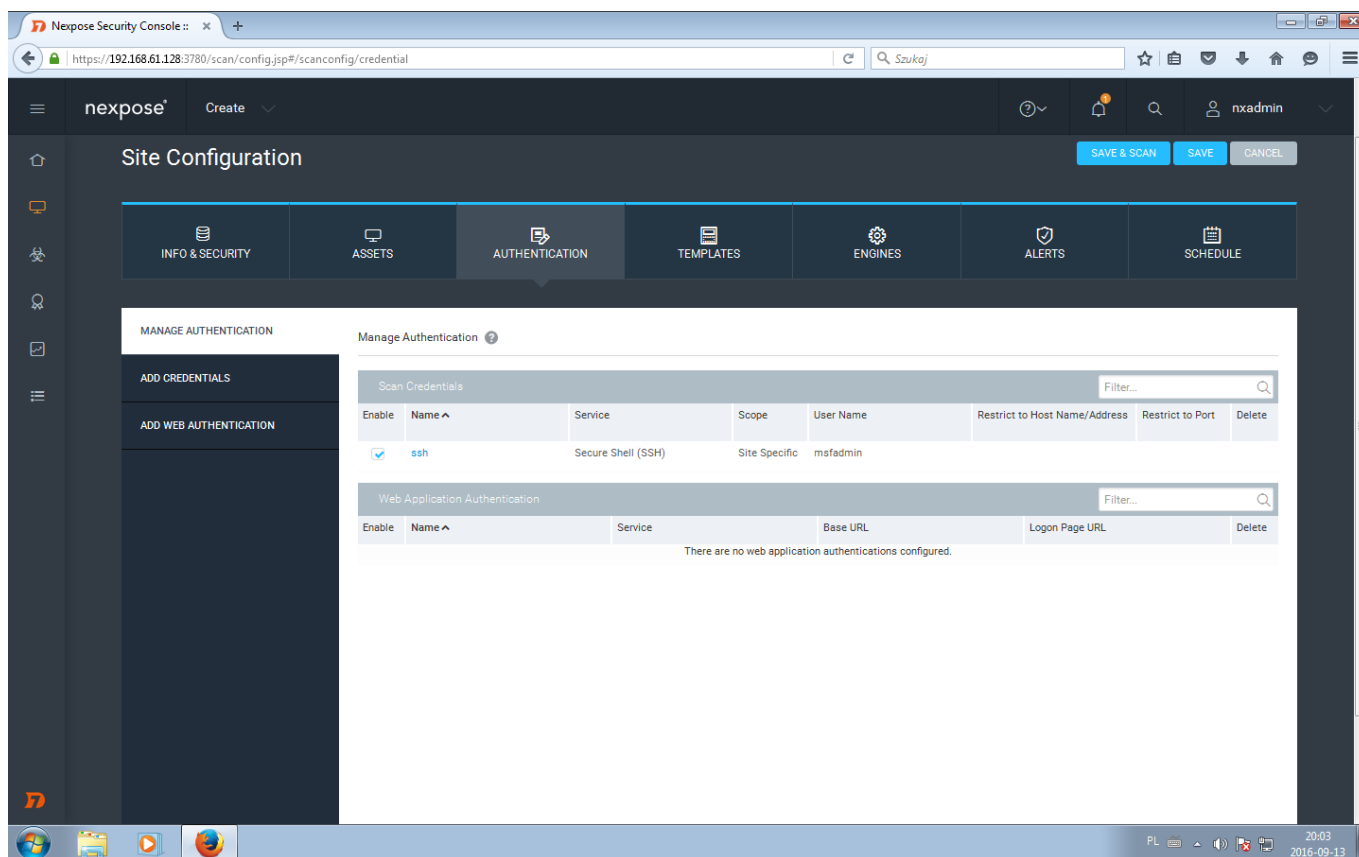
## Nexpose – dodajemy hosty i wykonujemy pierwsze skanowanie.



W zakładce „Assets” definiujemy jakie hosty chcemy skanować. Ważnym by odpowiednio skonfigurować tą część, jeśli zrobimy to błędnie możemy otrzymać fałszywe wyniki i stracić czas na przeglądaniu wyników które nas nie interesują. Na powyższym przykładzie do skanowania został podany zakres adresów 192.168.61.1-254, jest to zakres naszej sieci. W przedziale „exclude” umieszczamy hosty które chcemy pominąć przy skanowaniu. W tym przypadku umieściłem tam ip maszyny z nexposem, bramy oraz maszyny która służy mi za wirtualny desktop.



Nexpose – dodajemy hosty i wykonujemy pierwsze skanowanie.



Nexpose pozwala nam na skanowanie nie tylko zewnątrz maszyny, ale również na skanowanie wewnątrz maszyny. W ten sposób możemy określić czy rozwiązania które wdrożyliśmy są poprawnie zaimplementowane. Pozwala nam również to, zweryfikować czy możliwy jest atak cybernetyczny od wewnątrz.

Zakładka „authentication” daje nam możliwość zadeklarowania sposobu połączenia z skanowaną maszyną. Dla tego konkretnego przykładu wybrałem ssh.



Nexpose - dodajemy hosty i wykonujemy pierwsze skanowanie.

The screenshot shows the Nexpose Security Console interface in a web browser. The browser's address bar displays the URL: `https://192.168.61.128:3780/scan/config.jsp#/scanconfig/credential/new`. The interface features a dark sidebar on the left with navigation icons and a main content area. The top navigation bar includes tabs for 'INFO & SECURITY', 'ASSETS', 'AUTHENTICATION', 'TEMPLATES', 'ENGINES', 'ALERTS', and 'SCHEDULE'. The 'AUTHENTICATION' tab is active, and the 'ADD CREDENTIALS' option is selected in the sidebar. The main content area displays a form titled 'Add Credentials' with the following fields:

- Name:** A text input field containing the value 'ssh', which is highlighted in green with a checkmark to its right.
- Description:** A text input field containing the value 'dostęp ssh do maszyny testowej'.

At the bottom of the form, there are two buttons: 'CREATE' (highlighted in blue) and 'CANCEL' (greyed out). The Windows taskbar at the bottom of the screen shows the system tray with the date '2016-09-13' and time '20:00'.





# Nexpose - dodajemy hosty i wykonujemy pierwsze skanowanie.

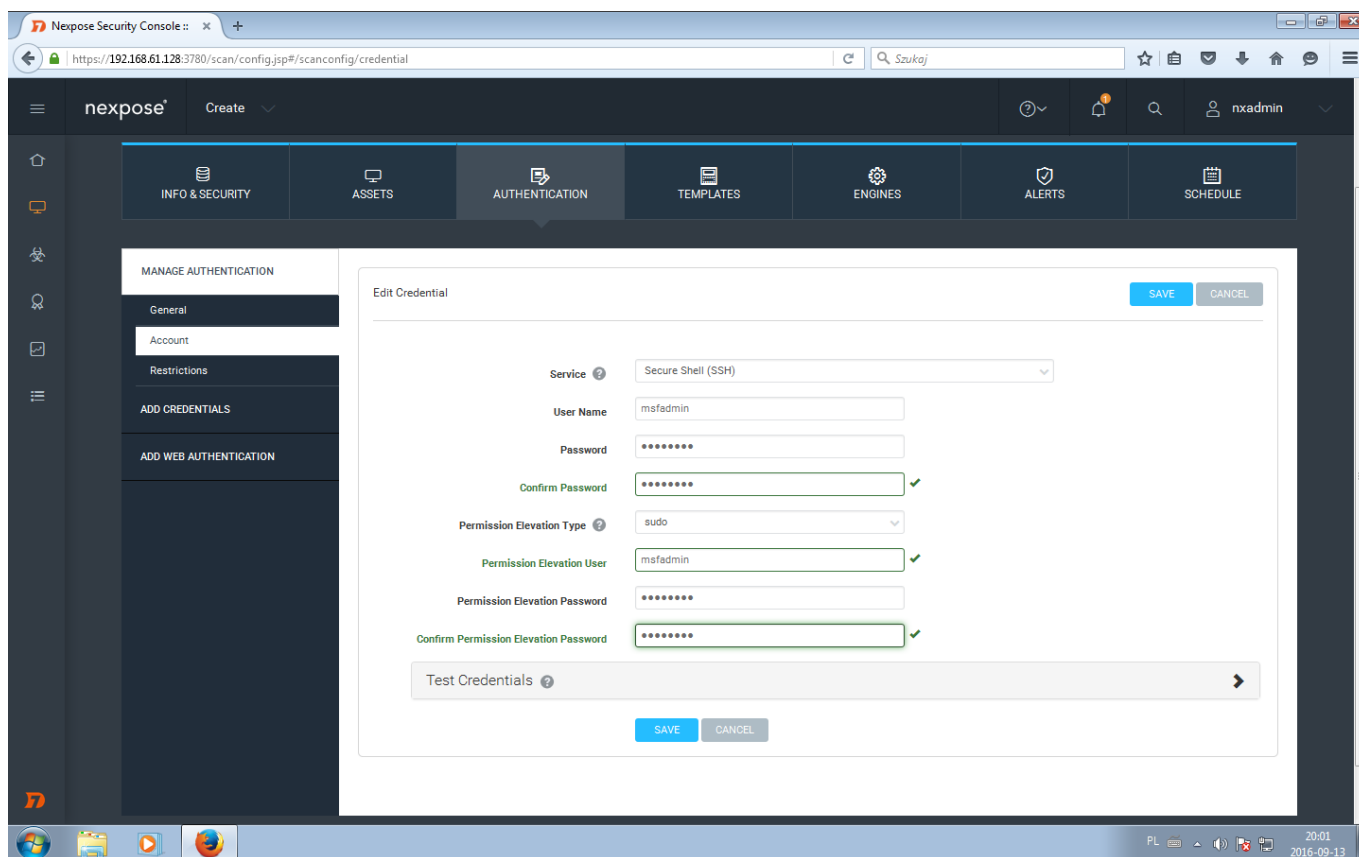
The screenshot displays the Nexpose Security Console interface. The browser address bar shows the URL: `https://192.168.61.128:3780/scan/config.jsp#/scanconfig/credential`. The main navigation bar includes tabs for INFO & SECURITY, ASSETS, AUTHENTICATION, TEMPLATES, ENGINES, ALERTS, and SCHEDULE. The left sidebar contains options for MANAGE AUTHENTICATION, ACCOUNT, RESTRICTIONS, ADD CREDENTIALS, and ADD WEB AUTHENTICATION. The central area is titled 'Edit Credential' and features a dropdown menu for selecting a service. The dropdown list includes the following options:

- Microsoft Windows/Samba (SMB/CIFS)
- Concurrent Versioning System (CVS)
- DB2
- File Transfer Protocol (FTP)
- IBM AS/400
- Lotus Notes/Domino
- Microsoft SQL Server
- Microsoft Windows/Samba (SMB/CIFS)
- Microsoft Windows/Samba LM/NTLM Hash (SMB/CIFS)
- MySQL Server
- Oracle
- Post Office Protocol (POP)
- PostgreSQL
- Remote Execution
- Secure Shell (SSH)
- Secure Shell (SSH) Public Key
- Simple Network Management Protocol v1/v2c
- Simple Network Management Protocol v3
- Sybase SQL Server
- TELNET
- Web Site HTTP Authentication

The 'Test Credentials' button is visible at the bottom of the dialog box. The system tray at the bottom right shows the time as 20:00 and the date as 2016-09-13.



Nexpose – dodajemy hosty i wykonujemy pierwsze skanowanie.



Po wprowadzeniu danych uwierzytelniających możemy przetestować je na wybranym przez siebie serwerze. W tym celu uzupełniamy zakładkę „Test credentials”.



Nexpose - dodajemy hosty i wykonujemy pierwsze skanowanie.

The screenshot shows the 'Edit Credential' interface in the Nexpose Security Console. The main form is for a 'Secure Shell (SSH)' service. The user name is 'msfadmin'. The password and confirmation password fields are filled with masked characters and have green checkmarks. The permission elevation type is set to 'sudo' and the permission elevation user is 'msfadmin', both with green checkmarks. The permission elevation password and its confirmation are also filled and checked. A 'Test Credentials' dialog is open, showing the IP address '192.168.61.130' and port '22', both with green checkmarks. Below the dialog, a message states 'Authentication succeeded on 192.168.61.130.' The interface includes a sidebar with navigation options like 'General', 'Account', 'Restrictions', 'ADD CREDENTIALS', and 'ADD WEB AUTHENTICATION'. The top navigation bar shows 'Create' and 'nxadmin'.



## Nexpose – dodajemy hosty i wykonujemy pierwsze skanowanie.

The screenshot shows the Nexpose Security Console interface. The browser address bar indicates the URL: `https://192.168.61.128:3780/scan/config.jsp#/scanconfig/credential`. The main navigation bar includes 'nexpose' and 'Create'. The 'Site Configuration' page has tabs for 'INFO & SECURITY', 'ASSETS', 'AUTHENTICATION', 'TEMPLATES', 'ENGINES', 'ALERTS', and 'SCHEDULE'. The 'AUTHENTICATION' tab is active, showing 'MANAGE AUTHENTICATION' options: 'ADD CREDENTIALS' and 'ADD WEB AUTHENTICATION'. The 'Scan Credentials' table has one entry:

Enable	Name	Service	Scope	User Name	Restrict to Host Name/Address	Restrict to Port	Delete
<input checked="" type="checkbox"/>	ssh	Secure Shell (SSH)	Site Specific	msfadmin			

The 'Web Application Authentication' section is empty, with the message: 'There are no web application authentications configured.'

Gdy już mamy uzupełnione dane autoryzacyjne pozwalające nam na skanowanie od wewnątrz, należy wybrać odpowiedni schemat skanowania. W przypadkach, gdy wykonujemy skanowanie sieci produkcyjnej, lub po prostu chcemy zweryfikować, czy nasze maszyny nie posiadają podatności należy wybrać „Full audit without Web Spider”. Opcja ta, wykona pełne skanowanie pomijając zbieranie linków z stron www.



Nexpose – dodajemy hosty i wykonujemy pierwsze skanowanie.

The screenshot shows the Nexpose Security Console interface. The browser address bar displays `https://192.168.61.128:3780/scan/config.jsp#/scanconfig/template`. The main navigation bar includes tabs for INFO & SECURITY, ASSETS, AUTHENTICATION, TEMPLATES, ENGINES, ALERTS, and SCHEDULE. The 'TEMPLATES' tab is active, showing a 'SELECT SCAN TEMPLATE' dialog. The 'Selected Scan Template' is 'Full audit without Web Spider'. Below this, a table lists various scan templates with columns for Name, Asset Discovery, Service Discovery, Checks, and Source.

Name	Asset Discovery	Service Discovery	Checks	Source
Discovery Scan	ICMP, TCP, UDP	Custom TCP, Custo...	Disabled	👑
Discovery Scan - Aggressive	ICMP, TCP, UDP	Custom TCP, Custo...	Disabled	👑
Exhaustive	ICMP, TCP, UDP	Full TCP, Default UDP	Safe Only	👑
FDCC	Disabled	Default TCP, Default ...	Safe Only	👑
Full audit	ICMP, TCP, UDP	Default TCP, Default ...	Custom	👑
Full audit enhanced logging without Web Spider	ICMP, TCP, UDP	Default TCP, Default ...	Custom	👑
Full audit without Web Spider	ICMP, TCP, UDP	Default TCP, Default ...	Custom	👑
HIPAA compliance	ICMP, TCP, UDP	Default TCP, Default ...	Safe Only	👑
Internet DMZ audit	Disabled	Default TCP	Custom	👑
Linux RPMs	ICMP, TCP, UDP	Custom TCP	Custom	👑

Następnym krokiem jest wybranie silnika skanującego. Jest to wybór maszyny na której zainstalowany jest moduł skanera. Silniki skanujące możemy mieć zainstalowane na maszynie na której skanujemy, lub też zdalnie. Rozdzielenie instalacji konsoli zarządzania i silnika skanującego daje nam możliwość przemieszczania się z konsolą (np na laptopie) i wykonywanie skanowań w wielu miejscach. Licencjonowanie dotyczy w tym przypadku konsoli zarządzającej.



Nexpose – dodajemy hosty i wykonujemy pierwsze skanowanie.

The screenshot displays the Nexpose Security Console interface. The top navigation bar includes tabs for INFO & SECURITY, ASSETS, AUTHENTICATION, TEMPLATES, ENGINES, ALERTS, and SCHEDULE. The main content area is titled "SELECT SCAN ENGINE" and contains the following elements:

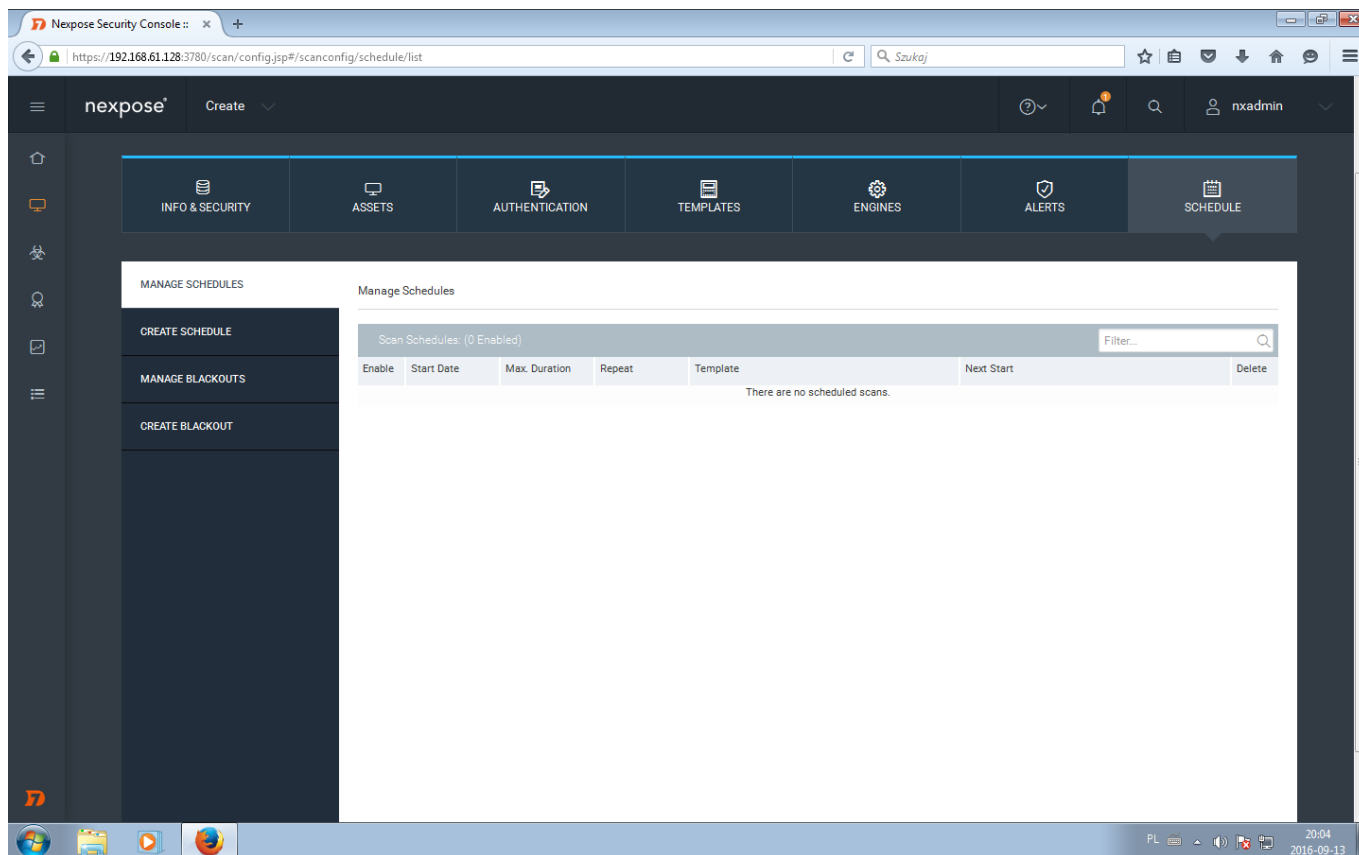
- A section "Scan each asset with:" with two radio buttons: "Engine selected below" (selected) and "Engine most recently used for that asset".
- A "Selected Scan Engine: Local scan engine" label.
- A "Scan Engines & Pools" table with a search filter.
- A table listing scan engine pools and engines:

Scan Engines & Pools		Filter...
Name	Status	
Scan Engine Pools (1)		
<input type="radio"/> Default Engine Pool		
Scan Engines (2)		
<input checked="" type="radio"/> Local scan engine	Active	
<input type="radio"/> Rapid7 Hosted Scan Engine	Pending authorization	

Ostatnim krokiem jest ustawienie kalendarza. Skanowania możemy ustawić systematycznie



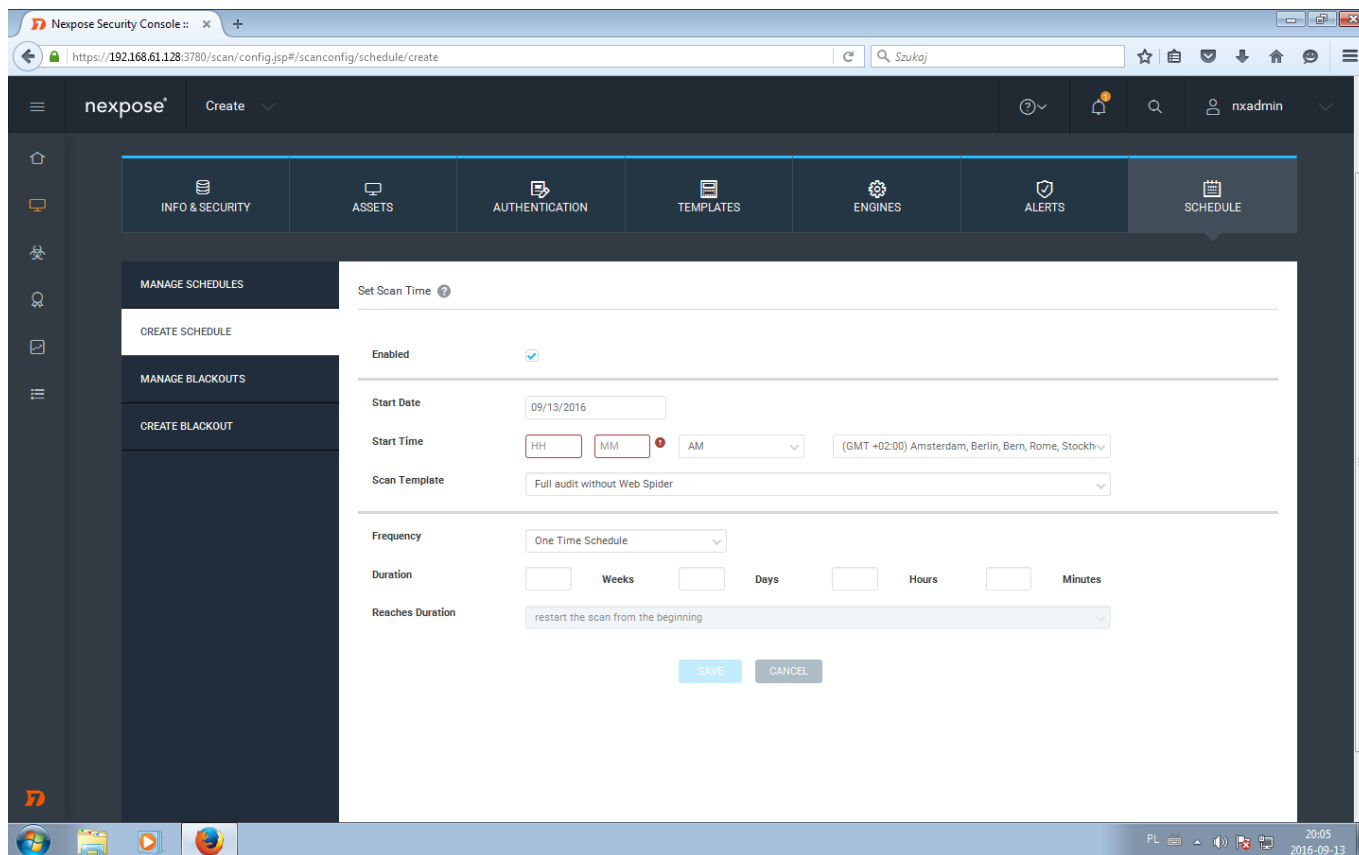
Nexpose – dodajemy hosty i wykonujemy pierwsze skanowanie.



Podążając za instrukcjami ustawiamy odpowiednio czas startu skanowania, częstotliwość oraz co program ma zrobić jeśli poprzedni skan się nie zakończył.



Nexpose – dodajemy hosty i wykonujemy pierwsze skanowanie.



Teraz, gdy mamy wypełnione wszystkie zakładki, lub tylko te, które są nam potrzebne klikamy „save”.





## Nexpose – dodajemy hosty i wykonujemy pierwsze skanowanie.

The screenshot shows the Nexpose Security Console interface. At the top, there is a navigation bar with the Nexpose logo and a 'Create' dropdown. Below the navigation bar, there is a main content area with a dark sidebar on the left. The main content area displays a table with the following data:

Assets	Risk Score	Highest-risk Site	Highest-risk Asset Group	Highest-risk Asset	Highest-risk Tag
-	-	<a href="#">pierwsze_skanuj</a> ▲ 0.0 (was N/A)	N/A	N/A	N/A

Below the table, there is a section titled 'SITES' with a table listing the sites:

Name	Assets	Vulnerabilities	Risk	Scan Engine	Type	Scan Status	Scan	Edit	Delete
<a href="#">pierwsze_skanuj</a>	0	0	0.0	Local scan engine	Static	Not scanned			

Below the 'SITES' table, there is a section titled 'CURRENT SCANS FOR ALL SITES' with a message: 'There are no scans to display.' and a 'SCAN NOW' button.

At the bottom of the interface, there is a section titled 'ASSET GROUPS'.

Po zapisaniu szablonu skanu zostajemy przekierowani do głównego panelu Nexpose, aby rozpocząć skanowanie klikamy w ikonkę radaru odpowiadającą interesującemu nas site'owi. I to tyle jeśli chodzi o planowanie i wykonywanie skanowania. Już niedługo instrukcje jak analizować wyniki skanowania.