Nexpose

https://docs.rapid7.com/

Rapid7 oferă două produse de bază pentru gestionarea vulnerabilităților:

- InsightVM (este complexa si se bazeaza pe Cloud - facilitati: Dashboards dinamic cu actualizări în timp real; sarcini de remediere în sistemele IT);
- - Nexpose (este o soluție locală pentru companii de orice dimensiune).

https://www.rapid7.com/products/nexpose/download/

Scanarea și analiza vulnerabilităților este procesul care detectează și evaluează vulnerabilitățile care există într-o infrastructură de rețea.

O vulnerabilitate este o caracteristică a unui activ pe care un atacator o poate exploata pentru a obține acces neautorizat la date sensibile.

Pentru a preveni breșele de securitate, este important să identificați și să remediați găurile de securitate și vulnerabilitățile care pot expune un activ la un atac.

Cu Nexpose se poate scana o rețea pentru vulnerabilități.

- Nexpose identifică serviciile active, porturile deschise și aplicațiile care rulează pe fiecare computer și încearcă să găsească vulnerabilități care pot exista pe baza atributelor serviciilor și aplicațiilor cunoscute.
- Nexpose dezvăluie rezultatele într-un raport de scanare, care vă ajută să prioritizați vulnerabilitățile pe baza factorului de risc și să determinați cea mai eficientă soluție de implementat.

Nexpose se integrează cu Metasploit Pro pentru a oferi un instrument de evaluare și validare a vulnerabilității care vă ajută

- să eliminați rezultatele fals pozitive,
- să verificați vulnerabilitățile,
- să testați modurile de remediere.

Observatie: Metasploit Pro oferă un conector care vă permite să adăugați o consolă Nexpose, astfel încât să puteți rula o scanare de vulnerabilitate direct din interfața web și să importați automat rezultatele scanării într-un proiect. De asemenea, puteți executa scanări din Nexpose și puteți importa rapoartele de scanare în Metasploit Pro pentru a efectua analiza și validarea vulnerabilității.

Care este mai bun Nessus vs Nexpose?

Nexpose și Nessus Professional sunt ambele instrumente excelente și pot fi folosite pentru a scana infrastructura IT.

- https://owasp.org/www-community/Vulnerability_Scanning_Tools
- https://allabouttesting.org/nexpose-vs-nessus-which-one-is-better/
- https://docs.rapid7.com/metasploit/vulnerability-scanning-with-nexpose/
- https://docs.rapid7.com/metasploit/installing-metasploit-pro

What is OWASP?

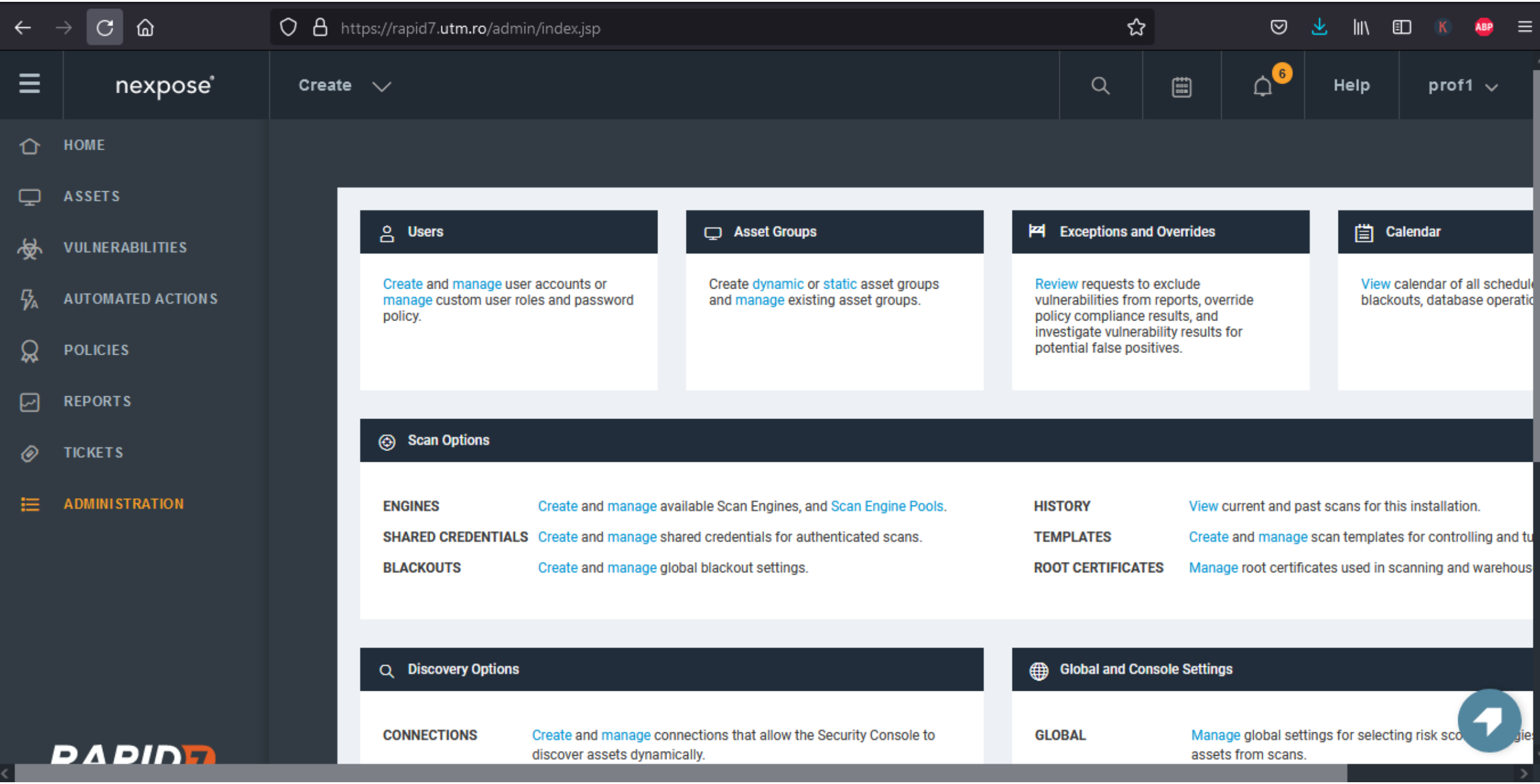
The Open Web Application Security Project (OWASP) is a worldwide nonprofit organization that focuses on improving software security. The main mission of OWASP is to ensure that software security is visible, and to provide insights and tools to help improve application security globally. through the top 10 lists for various categories, so that organizations can use the Top 10 lists to make informed decisions.

https://www.barracuda.com/glossary/owasp

Terminologie Nexpose:

- **Activ** - O gazdă într-o rețea.
- **Site** - Un grup logic de active care are un motor de scanare dedicat. Un site poate rula pe o perioadă lungă de timp și vă poate oferi date istorice, tendințe și este similar cu un proiect din Metasploit.
- **Scanare șablon** - Un șablon care definește nivelul de audit pe care Nexpose îl utilizează pentru a efectua o scanare a vulnerabilităților.

Ciclul de viață al programului de Securitate


https://rapid7.utm.ro/admin/index.jsp
nexpose
Create
6
Help
prof1
HOME
ASSETS
VULNERABILITIES
AUTOMATED ACTIONS
POLICIES
REPORTS
TICKETS
ADMINISTRATION
Users
Create and manage user accounts or manage custom user roles and password policy.
Asset Groups
Create dynamic or static asset groups and manage existing asset groups.
Exceptions and Overrides
Review requests to exclude vulnerabilities from reports, override policy compliance results, and investigate vulnerability results for potential false positives.
Calendar
View calendar of all schedul
blackouts, database operati
Scan Options
ENGINES
Create and manage available Scan Engines, and Scan Engine Pools.
SHARED CREDENTIALS
Create and manage shared credentials for authenticated scans.
BLACKOUTS
Create and manage global blackout settings.
HISTORY
View current and past scans for this installation.
TEMPLATES
Create and manage scan templates for controlling and tu
ROOT CERTIFICATES
Manage root certificates used in scanning and warehous
Discovery Options
CONNECTIONS
Create and manage connections that allow the Security Console to discover assets dynamically.
Global and Console Settings
GLOBAL
Manage global settings for selecting risk sco
assets from scans.

Ce este un site?

- Un site este o colecție de active care sunt vizate pentru o scanare. Trebuie să creați un site pentru a rula o scanare a mediului și pentru a găsi vulnerabilități.
- Un site este format din:
  - active țintă (opțional)
  - un șablon de scanare
  - unul sau mai multe motoare de scanare
  - alte setări legate de scanare, ar fi programări sau alerte

Diferite moduri de a adăuga active la un site

- Puteți specifica activele țintă în mai multe moduri:
  - după numele, adresa sau zona individuală
  - după numele grupului de active
  - printr-o conexiune dinamică de descoperire

Atentie: condiții precum lățimea de bandă a rețelei, latența și numărul de active incluse afectează în cele din urmă eficiența scanării.

Exemple de ținte de scanare

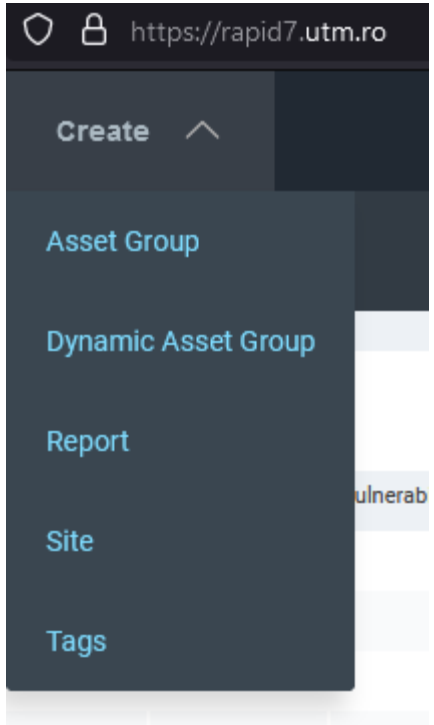
- Stația de lucru personală
- Un sistem de testare sau de laborator (non-production)
- Orice sistem pentru care aveți acreditări de administrator

Specificarea grupurilor de active vă permite să scanați pe baza grupărilor logice pe care le-ați creat anterior. În cazul scanării grupurilor dinamice de active, aveți posibilitatea să scanați în funcție de îndeplinirea anumitor criterii de către active. De exemplu, puteți scana toate activele al căror sistem de operare este Ubuntu. Pentru a afla mai multe despre grupurile de active, consultați Lucrul cu grupuri de active.

Adăugarea de active prin conexiune este ideală pentru un mediu țintă extrem de fluid, ar fi implementarea de active virtualizate. Nu este neobișnuit ca mașinile virtuale să sufere modificări continue, ar fi instalarea diferitelor sisteme de operare, susținerea de diferite bazine de resurse sau dezactivarea și dezactivarea acestora. Aveți posibilitatea să modificați apartenența la active într-un site care populează activele printr-o conexiune prin modificarea conexiunii de descoperire sau a filtrelor de criterii care determină ce active sunt descoperite.

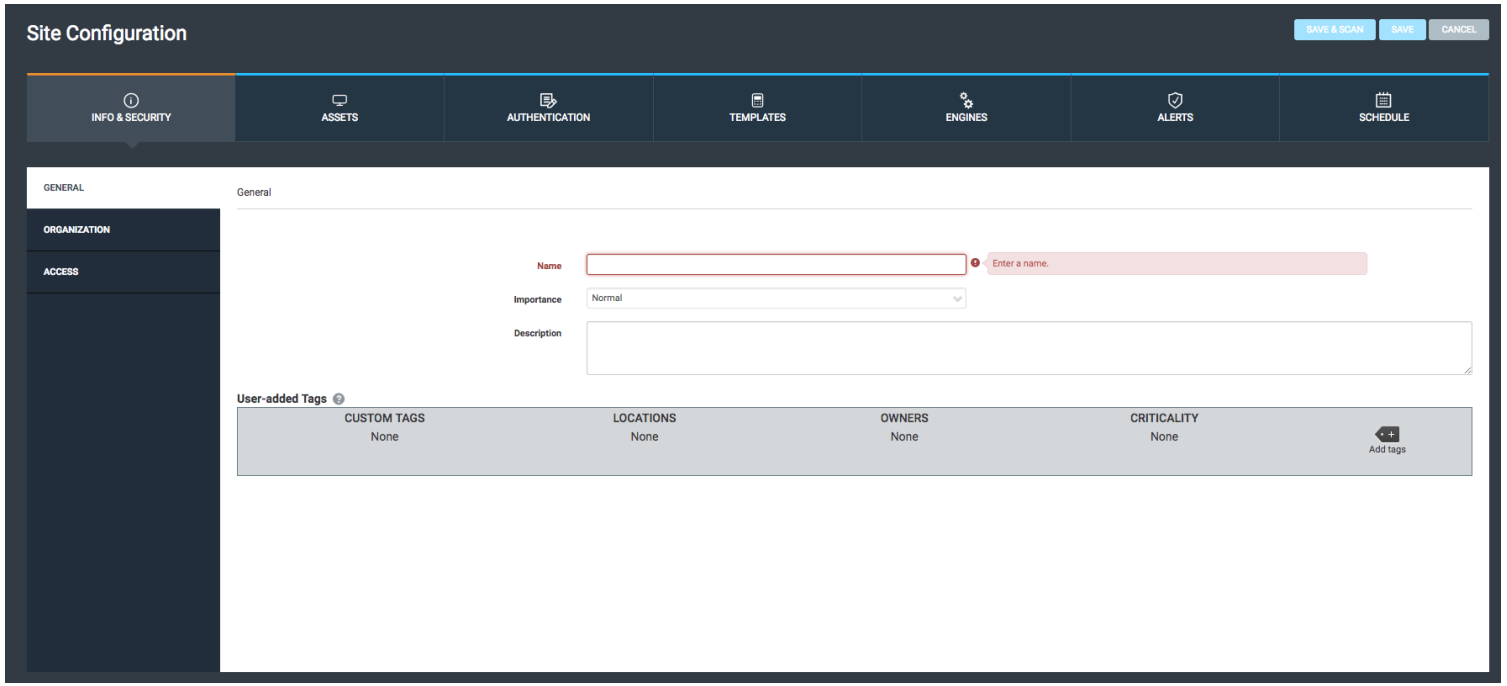
Prin ce diferă site-urile de grupurile de active?

- Grupurile de active oferă diferite modalități prin care membrii organizației pot acorda acces, vizualiza, scana și raporta informații despre active. Aveți posibilitatea să creați grupuri de active care conțin active pe mai multe site-uri.
- **Scenarii de creare a site-ului**



Create Your First Site

From the **Home** page of your Security Console, click the **Create** dropdown and select **Site**. The Security Console displays the “Site Configuration” screen.



https://docs.rapid7.com/nexpose/create-and-scan-a-site/

- **“Info & Security”**
- On the **General** tab, name and describe your site. While common names include department titles or office locations for the assets being scanned, you can name this site after your target asset or “sample site” for easy reference.
- **“Assets”**
- The **Assets** tab is where you specify which of your assets should be included in the site, and if necessary, which should be excluded as well. You can specify individual assets by their Fully Qualified Domain Name (FQDN) or IP address, but IP address ranges are the most effective method. Site configurations accept a variety of IPv4 and IPv6 range notations, including Classless Inter-Domain Routing (CIDR).

“Authentication”

The **Authentication** tab allows you to configure different sets of credentials depending on the type of asset you target for a scan.

Configure Credentials

Click the **Add Credentials** tab to configure a set of credentials for your site to use:

1. On the **General** sub-tab, name and optionally describe your credentials.

   This name will identify these credentials on the **Manage Authentication** tab when saved.

2. On the **Account** tab, select the authentication service you want to use.

While several options are available here for a variety of scenarios, Rapid7 recommends the following two services as a good starting point for authenticated scans:

- **Microsoft Windows/Samba (SMB/CIFS)** for Windows machines
- **Secure Shell (SSH)** for Linux and Mac machines

You can read more about authentication on the following pages:

- Authentication on Unix and related targets: best practices
- Authentication on Windows: best practices

Complete the username and password fields as required.

Default ports for SSH and SMB/CIFS

By default, Nexpose attempts SSH communication through port 22 and SMB/CIFS communication through port 445.

Click **Test Credentials** when finished.

Credential Test Results Explained

Successful credential tests show a green confirmation message. Failed tests appear in red and may show the following text:

- **Invalid credentials** - Your username and/or password were incorrect.
- **Connection refused** - You specified the wrong port number, the port is not open on the host, or a firewall actively blocked the connection.
- **Host not found** - The IP address or FQDN specified was not found on the network. This means that you entered the wrong address, the host network cannot be reached from the network subnet hosting the console, or the host is not connected.

After you've successfully tested your credentials, click **Create** to save them.

“Templates”

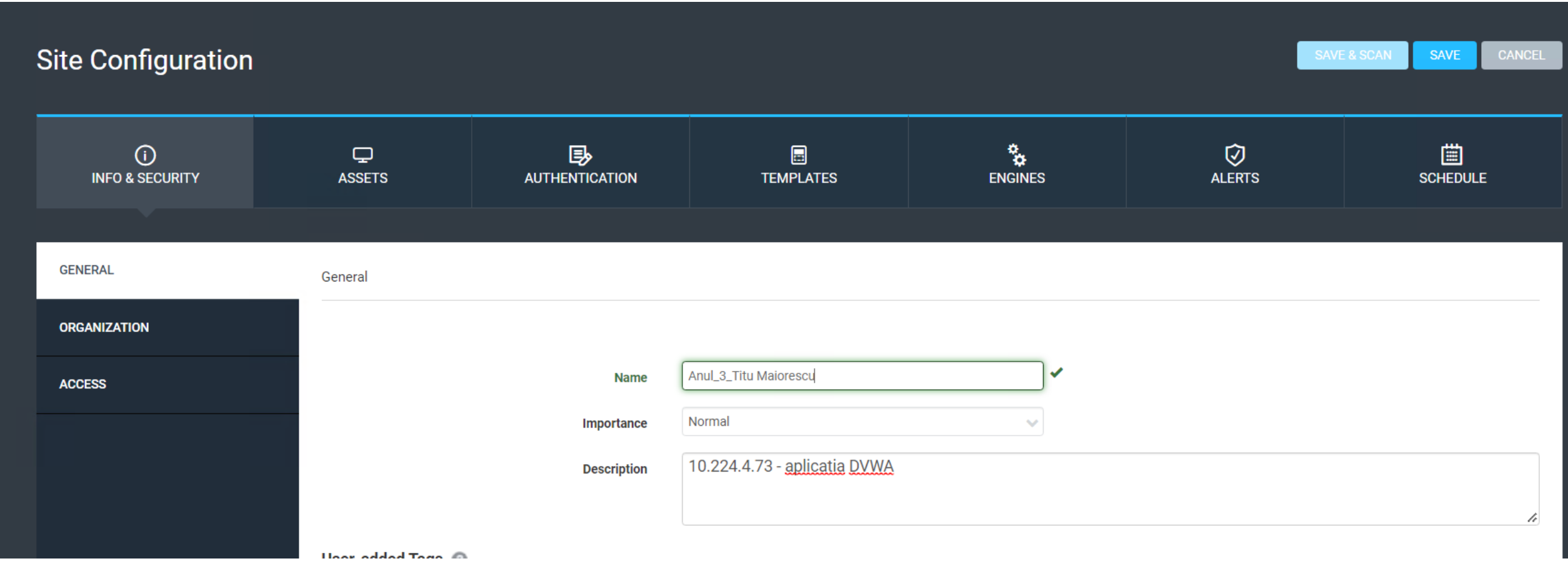
- Sites must be configured to use a specific Scan Template during the scanning process. You can think of the Scan Template as the method by which the Scan Engine probes your assets.
- On the **Select Scan Template** tab, select **Full Audit without Web Spider**.
- Generally considered as the default Scan Template for the Security Console, **Full Audit without Web Spider** has the following traits:
    - Performs only safe checks
    - Looks for network-based vulnerabilities
    - Checks for patches and hotfixes
    - Audits at the application layer
    - Scans only default ports

This template also excludes policy checking and web spidering, hence its name. As a consequence, it’s fast, broadly scoped, and reliable.

Save and Scan Your Site

- You should now have all the information required for your first basic site. Keep in mind that there are many other options for site configurations that were not covered here, but this basic configuration is suitable for your first scan.
- Click **Save & Scan** in the upper right corner of your screen to save your site configuration and scan it immediately.
- If you would like to learn more about site configuration capabilities, the Site creation scenarios page is a good place to start.
- **Scan Progress**
- After initiating your first scan, the Security Console displays the site details page. The “Scan Progress” section at the top gives you a live look at the progress of the ongoing scan as it runs.

Studiu de caz



Faceți clic pe filele din *Configurare site* pentru a configura diverse aspecte ale site-ului și scanează:

Assets

Specify assets by **Names/Addresses** | Connection

INCLUDE — 1 assets

1 **Assets** Alege fișierul | Nu ai al...ciun fișier

10.224.4.73 × Enter name, address, or range.

0 **Asset Groups**

Enter an asset group name.

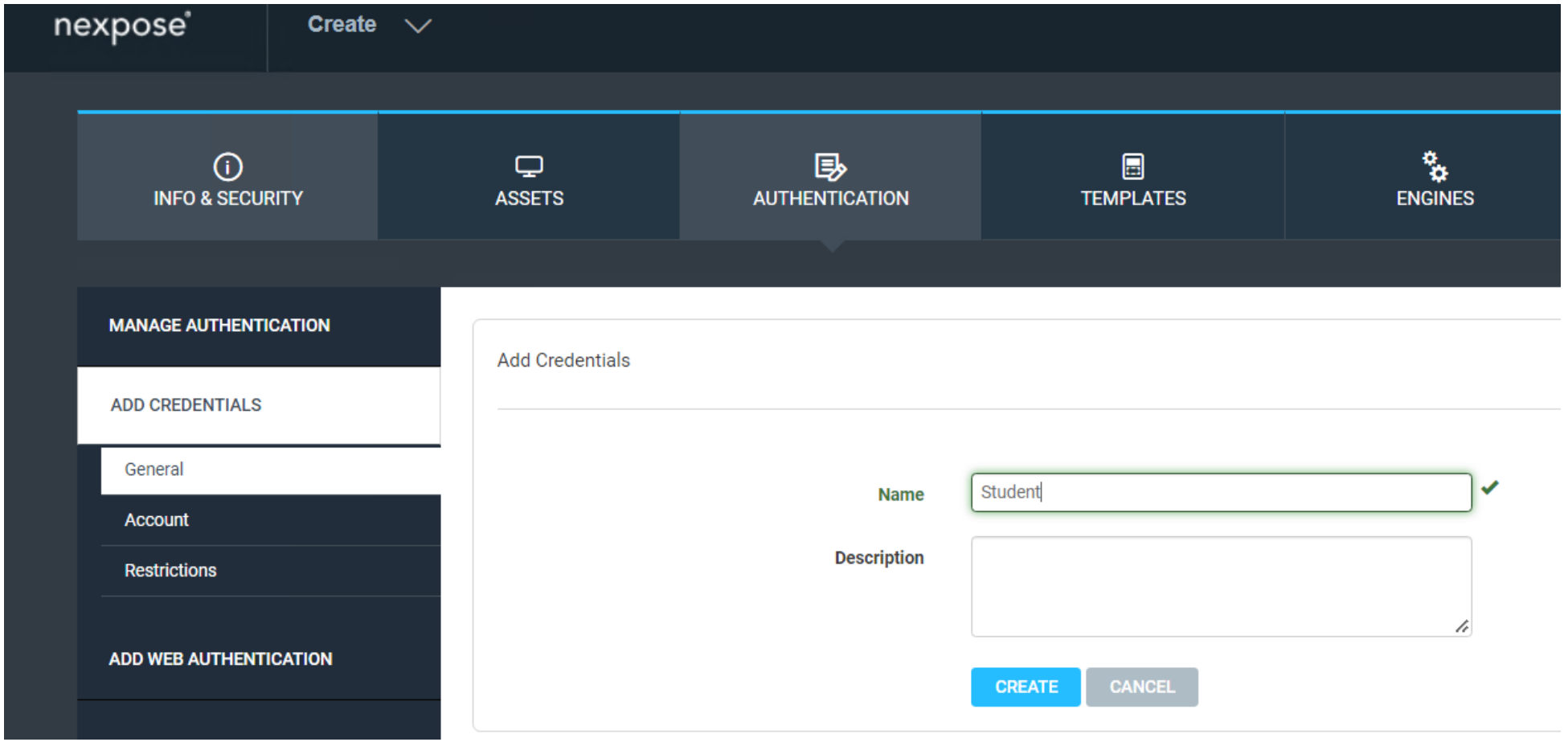
EXCLUDE — 0 assets

0 **Assets** Alege fișierul | Nu ai al...ciun fișier

Enter name, address, or range.

0 **Asset Groups**

Enter an asset group name.


nexpose
Create
INFO & SECURITY
ASSETS
AUTHENTICATION
TEMPLATES
ENGINES
MANAGE AUTHENTICATION
ADD CREDENTIALS
General
Account
Restrictions
ADD WEB AUTHENTICATION
Add Credentials
Name
Student
Description
CREATE
CANCEL

MANAGE AUTHENTICATION

General

Account

Restrictions

ADD CREDENTIALS

ADD WEB AUTHENTICATION

Edit Credential

SAVE CANCEL

Service: Microsoft Windows/Samba (SMB/CIFS)

Credential Management: Nexpose

Domain: 10.224.4.73

User Name: cyberx

Password: ••••••••

Confirm Password: ••••••••

Test Credentials

IP Address/Host Name: 10.224.4.73

Port:

TEST CREDENTIALS

Authentication succeeded on 10.224.4.73.

Site Configuration

SAVE & SCAN | SAVE | CANCEL

INFO & SECURITY | ASSETS | AUTHENTICATION | TEMPLATES | ENGINES | ALERTS | SCHEDULE

SELECT SCAN TEMPLATE

CREATE SCAN TEMPLATE

Selected Scan Template: Full audit without Web Spider

Scan Templates

Filter...

Name	Asset Discovery	Service Discovery	Checks	Source	Copy
DISA	ICMP, TCP	Custom TCP	Safe Only		
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	Custom		
FDCC	ICMP, TCP	Custom TCP	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 ...	Custom		

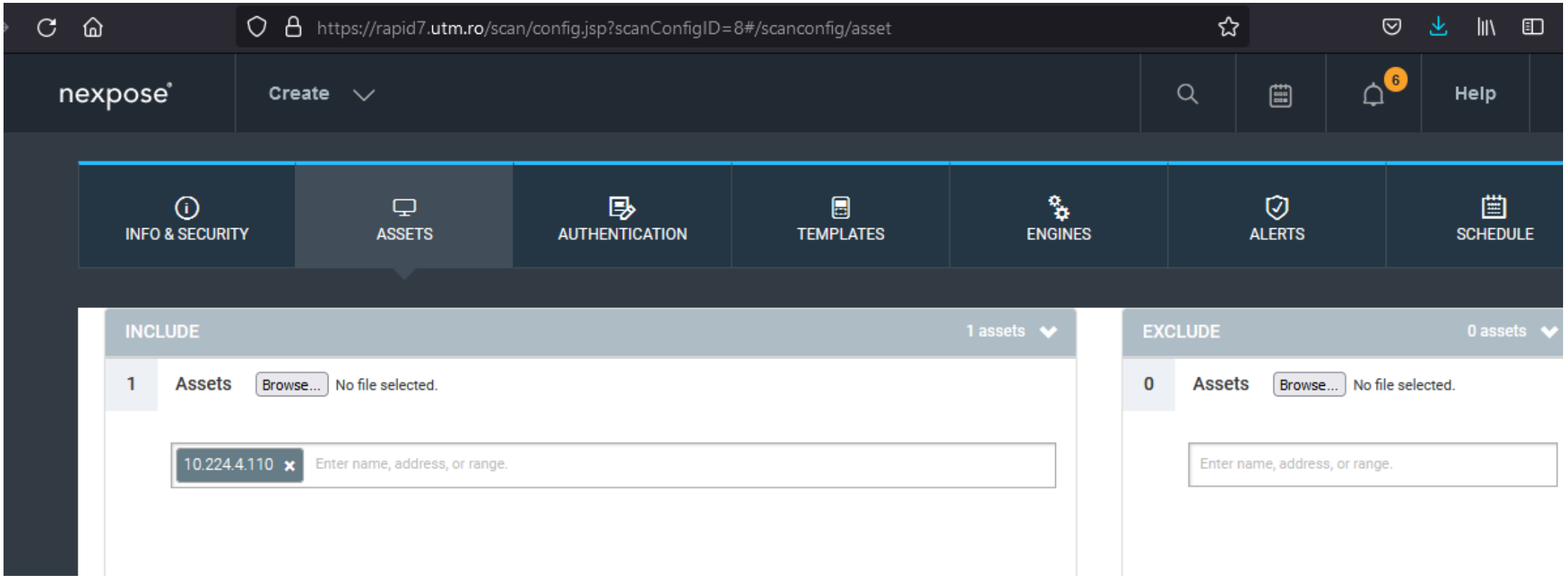
Student_Inf | View all sites
Full audit without Web Spider | View all scans

SCAN PROGRESS

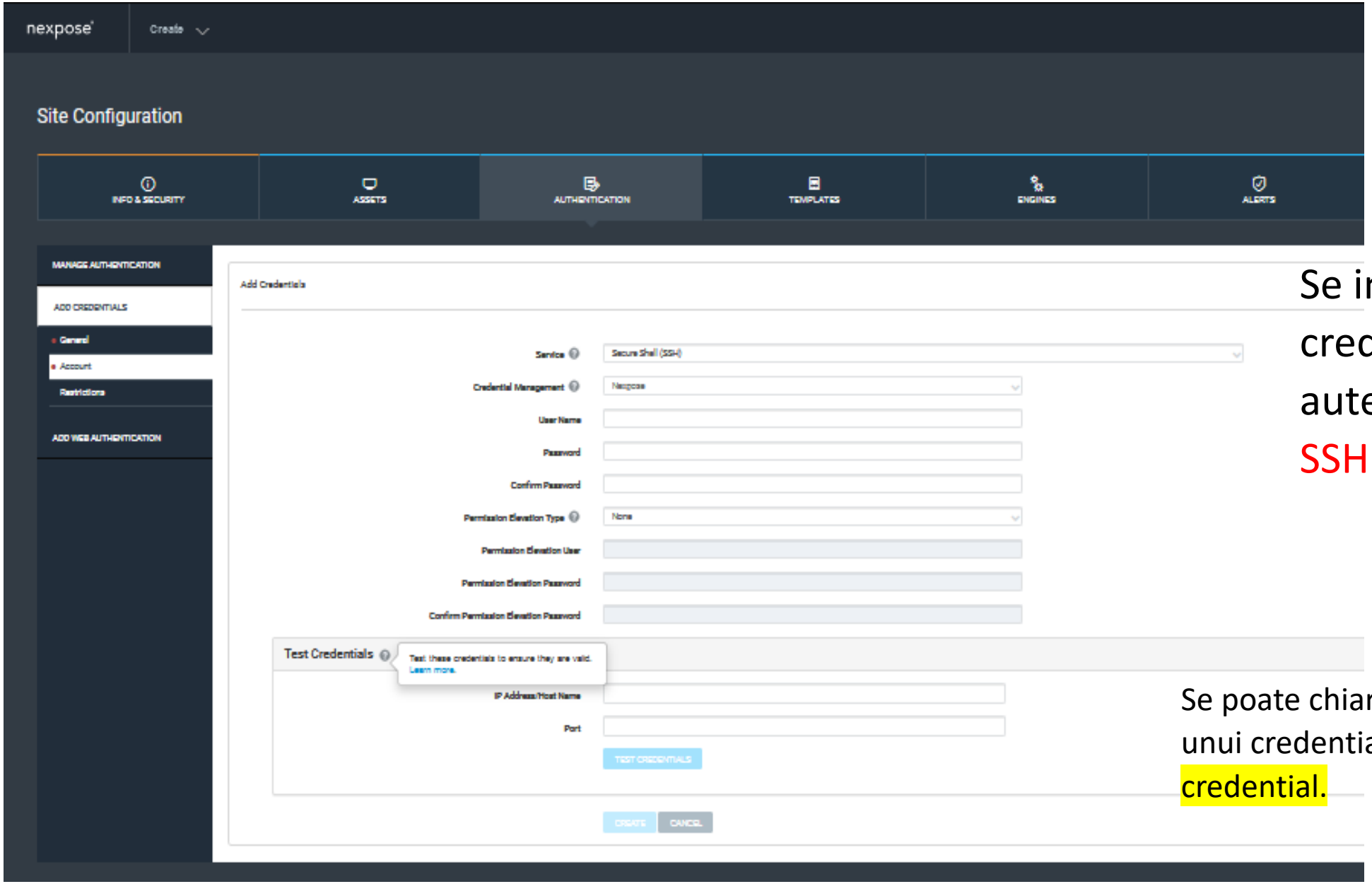
Scan Type	Started	Assets	Vulnerabilities	Total Elapsed Scan Time	Assets Scanned	Scan Engine
Manual	3/10/2022 10:54 PM	0	0	12 seconds	Asset discovery is in progress... Active: 0, Pending: 0, Complete: 0	Local scan engine

STOP SCAN | PAUSE SCAN

DOWNLOAD

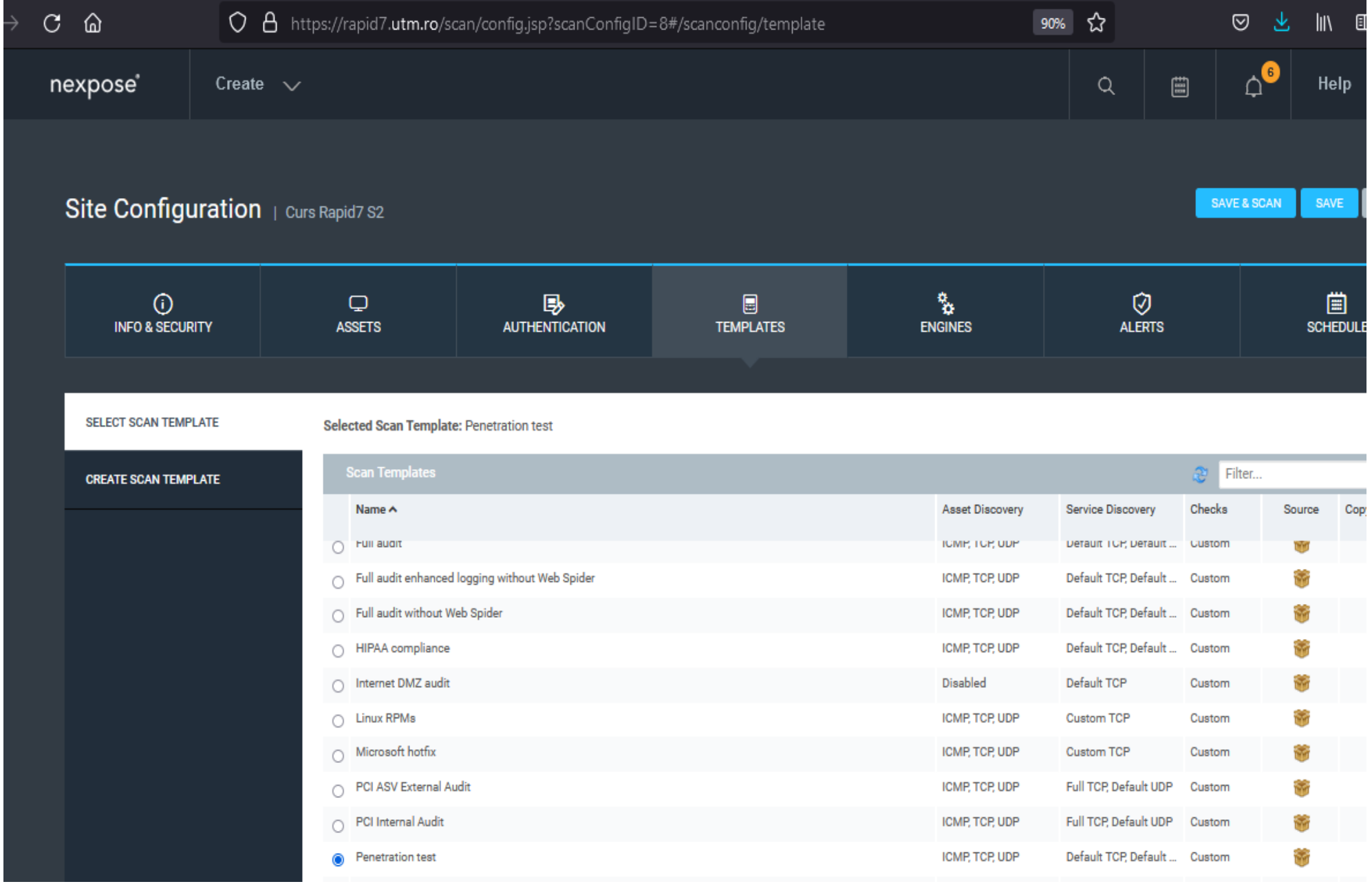


2. Se adauta “Assets”

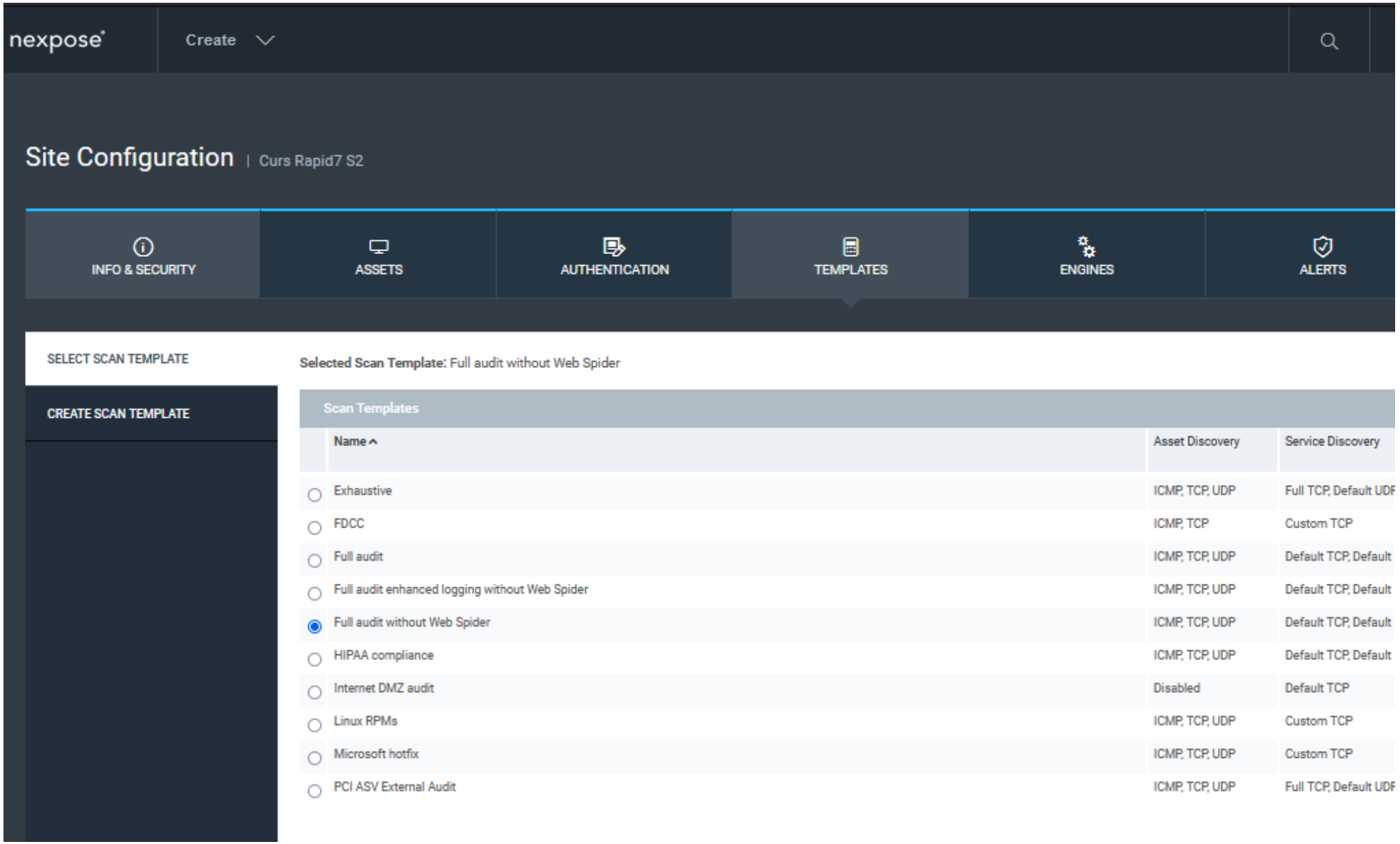


Se introduc credentialele de autentificare de tip SSH (ID / Pass)

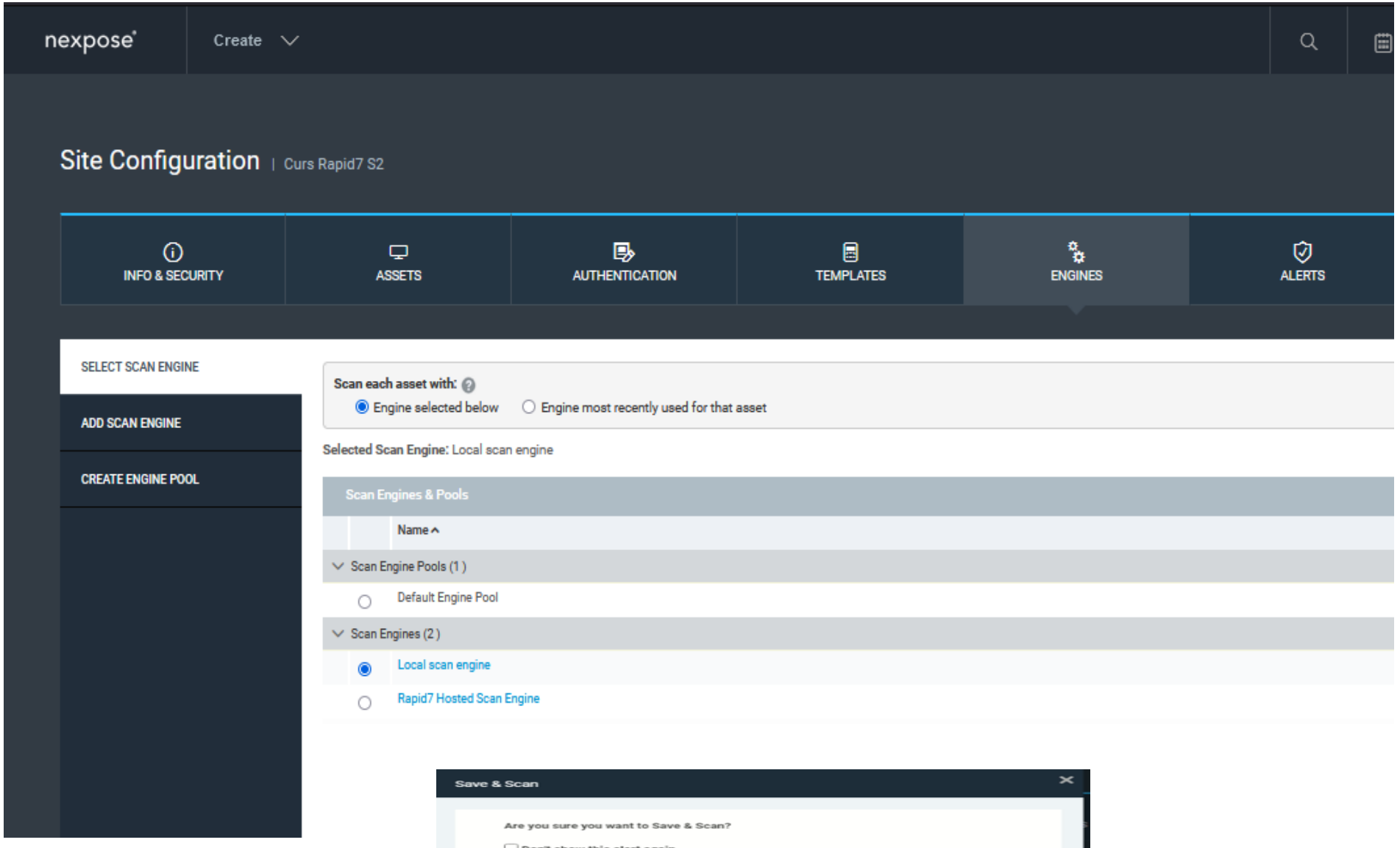
Se poate chiar testa corectitudinea unui credential. Apoi,…“Create” la credential.



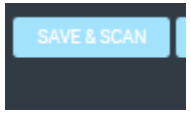
Se aleg “Template”-ul/ sabloanele de scanare

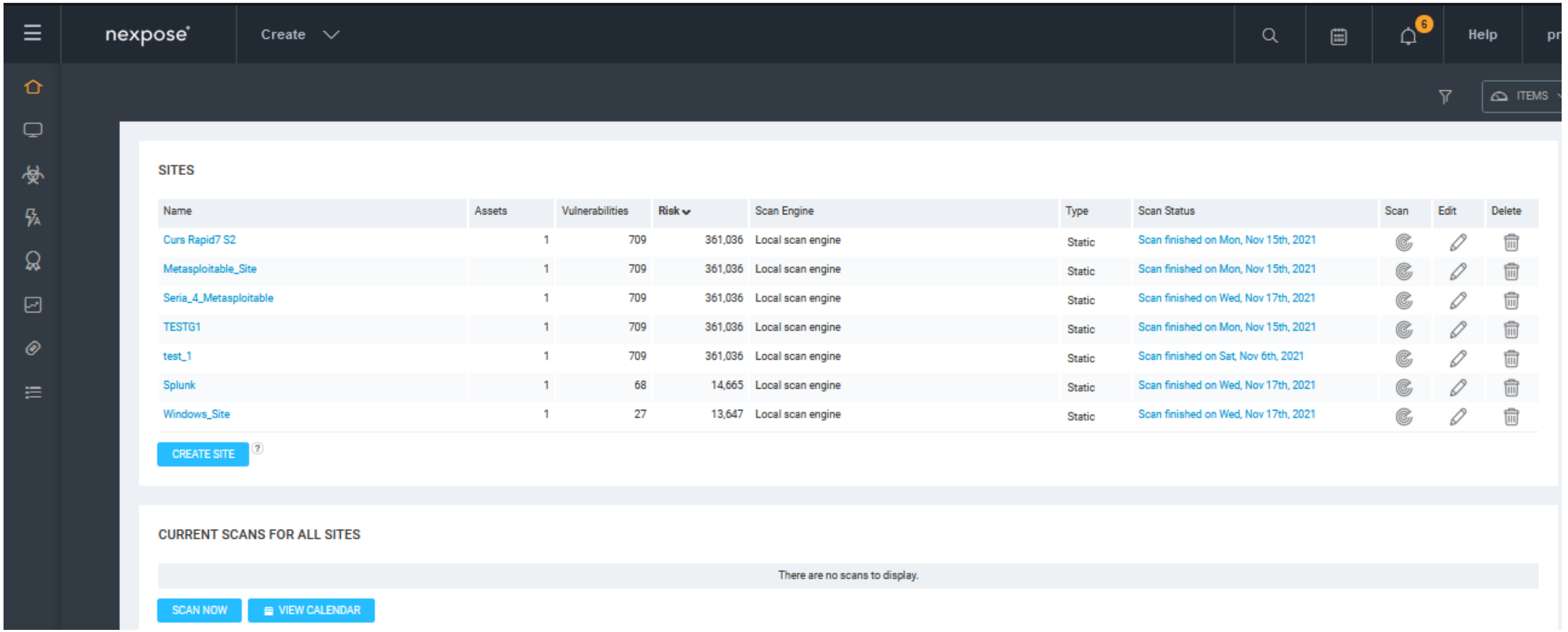


Se aleg “Template”-ul/ sabloanele de scanare


nexpose
Create
Site Configuration | Curs Rapid7 S2
INFO & SECURITY
ASSETS
AUTHENTICATION
TEMPLATES
ENGINES
ALERTS
SELECT SCAN ENGINE
ADD SCAN ENGINE
CREATE ENGINE POOL
Scan each asset with:
Engine selected below
Engine most recently used for that asset
Selected Scan Engine: Local scan engine
Scan Engines & Pools
Name
Scan Engine Pools (1)
Default Engine Pool
Scan Engines (2)
Local scan engine
Rapid7 Hosted Scan Engine

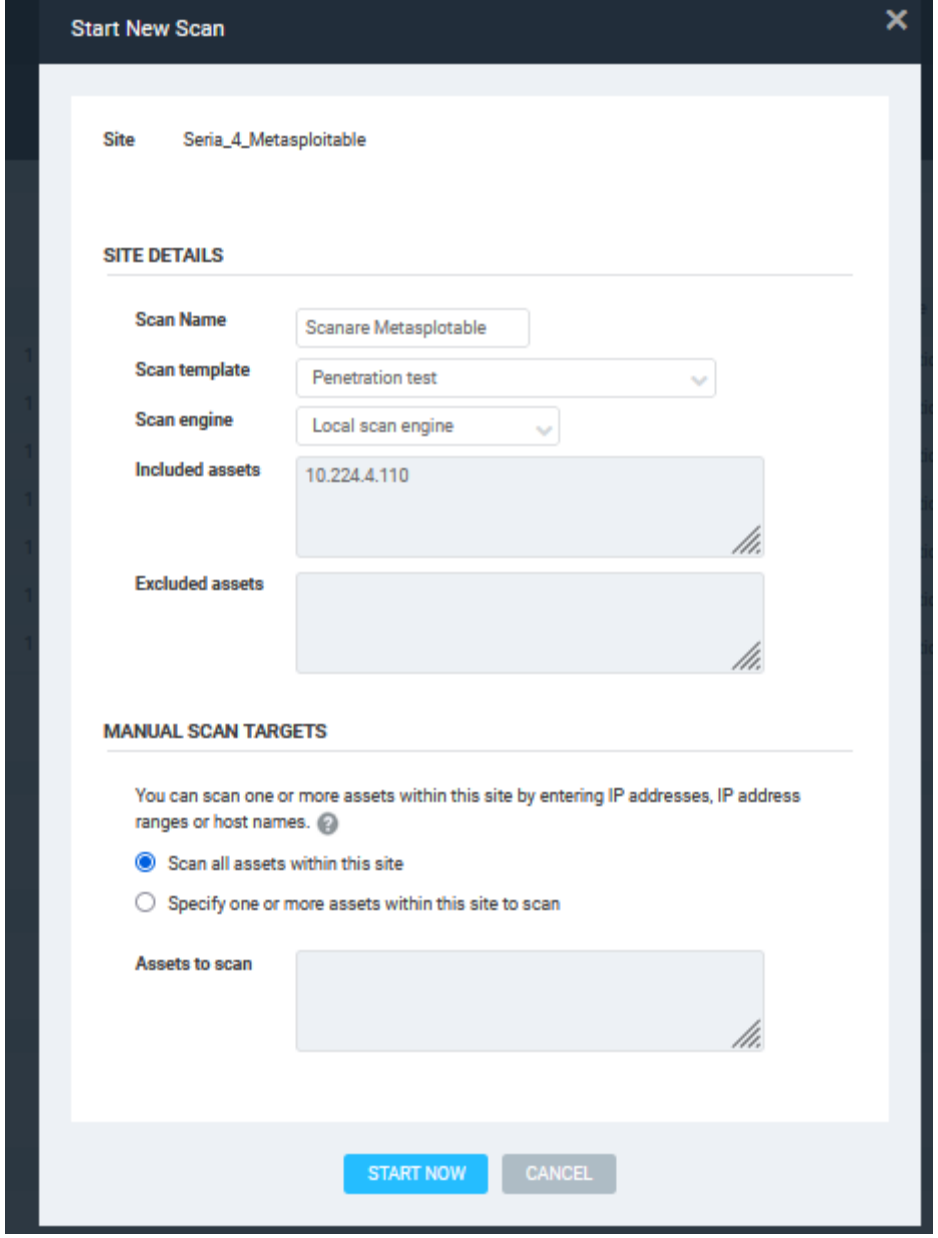
Save & Scan
Are you sure you want to Save & Scan?
Don't show this alert again.
SAVE & SCAN
SAVE ONLY


SAVE & SCAN



Lista site-uri pentru scanare

Pornirea ulterioara a unei scanari



Seria_4_Metasploitable	1	709	361,036	Local scan engine	Static	In Progress	

- https://docs.rapid7.com/nexpose/creating-reports-based-on-sql-queries/

- https://docs.rapid7.com/nexpose/understanding-the-reporting-data-model-overview-and-query-design/
- https://docs.rapid7.com/nexpose/fingerprint-certainty/
- https://www.rapid7.com/try/metasploit-pro/

Fingerprint certainty

Certitudinea amprentei este o măsurare a preciziei estimate corespunzatoare unei scanări de a identifica trăsăturile unui activ.

Certitudinea amprentei este punctată conform unei scale de la 0 la 1,0. Scorurile de certitudine ale amprentei determină ???/de vulnerabilitate sunt efectuate împotriva activului.

Multe verificări de vulnerabilitate vor rula numai dacă amprenta sistemului îndeplinește un scor minim necesar. Scorurile de certitudine a amprentei de 1,0 sunt aproape întotdeauna produse de scanări autentificate.

Asset detail view

1. On the **Assets** tab of your Security Console, browse to the “Scanned” table.
2. Open the scanned asset you would like to inspect.
3. On the asset detail page, expand the **Items** dropdown in the upper right corner of your screen. Select **Fingerprints**.

- This will add the “Fingerprints” table to your asset detail page.

4. Scroll down to the “Fingerprints” table to examine fingerprint records and their corresponding certainty scores.

Completed scan view

1. On the **Home** tab of your Security Console, browse to the “Sites” table.
2. Open a completed scan by clicking a corresponding link under “Scan Status”.
3. In the “Completed Assets” table, open the scanned asset you would like to inspect.
4. Scroll down to the “Node Fingerprints” table to examine fingerprint records and their corresponding certainty scores.

NODE FINGERPRINTS

Vendor	Family	Device Class	Architecture	Product	Version	Source	Certainty
Ubuntu	Linux		x86	Linux	8.04	Configured Credentials	1
Ubuntu	Linux		x86	Linux	8.04	Unix System Fingerprinter	1
Ubuntu	Linux			Linux	8.04	SSH	0.85
Ubuntu	Linux			Linux		HTTP	0.8
Ubuntu	Linux			Linux		SMTP	0.8
Ubuntu	Linux			Linux		MySQL	0.75
Linux	Linux	General		LINUX 2.6.9 - 2.6.33	2.6.9	IP stack analysis	0.7
Linux	Linux			Linux		UDP IP ID Zero	0.6

UPDATED VULNERABILITY COVERAGE

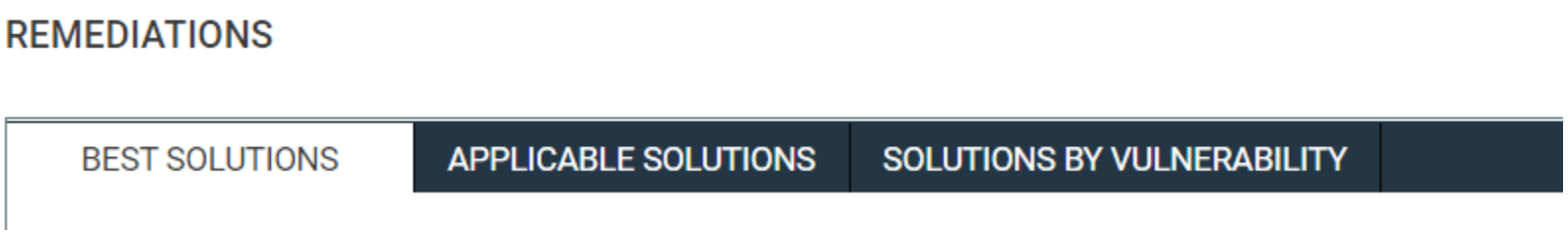
Content updates may include new and revised checks for vulnerabilities, patch verification, and security policy compliance. They may also include improvements to accuracy, fingerprinting, and scanning. Click the link for any vulnerability listed in the following table for more information.

Displaying new and modified content within the last 7 days. Last content update: 3672488004 (Friday, March 11, 2022 5:21:24 PM GMT)

Title	CVSS	Risk	Modified On
Debian: CVE-2022-26847: spip -- security update	4.4	104.6	Fri, Mar 11th, 2022
Debian: CVE-2022-26381: firefox-esr, thunderbird -- security update	4.4	104.6	Fri, Mar 11th, 2022
Debian: CVE-2022-26384: firefox-esr, thunderbird -- security update	4.4	104.6	Fri, Mar 11th, 2022
Debian: CVE-2022-26386: firefox-esr, thunderbird -- security update	4.4	104.6	Fri, Mar 11th, 2022
Debian: CVE-2022-26846: spip -- security update	4.4	104.6	Fri, Mar 11th, 2022
Debian: CVE-2022-26383: firefox-esr, thunderbird -- security update	4.4	104.6	Fri, Mar 11th, 2022
Debian: CVE-2022-26387: firefox-esr, thunderbird -- security update	4.4	104.6	Fri, Mar 11th, 2022
Red Hat: CVE-2022-24464: Important: .NET 6.0 security and bugfix update (Multiple Advisories)	4.4	104.94	Fri, Mar 11th, 2022
Centos Linux: CVE-2022-26381: Critical: firefox security update (Multiple Advisories)	4.4	104.94	Fri, Mar 11th, 2022

Studiu de caz

- Pentru Asset-ul 10.224.2.196 identificati sectiunea→FINGERPRINTS
- Pentru fiecare subcategorie din Remediatos analizati cel putin 2



- Analizati raportul cu vulnerabilitati obtinut in urma operatiei de scanare.