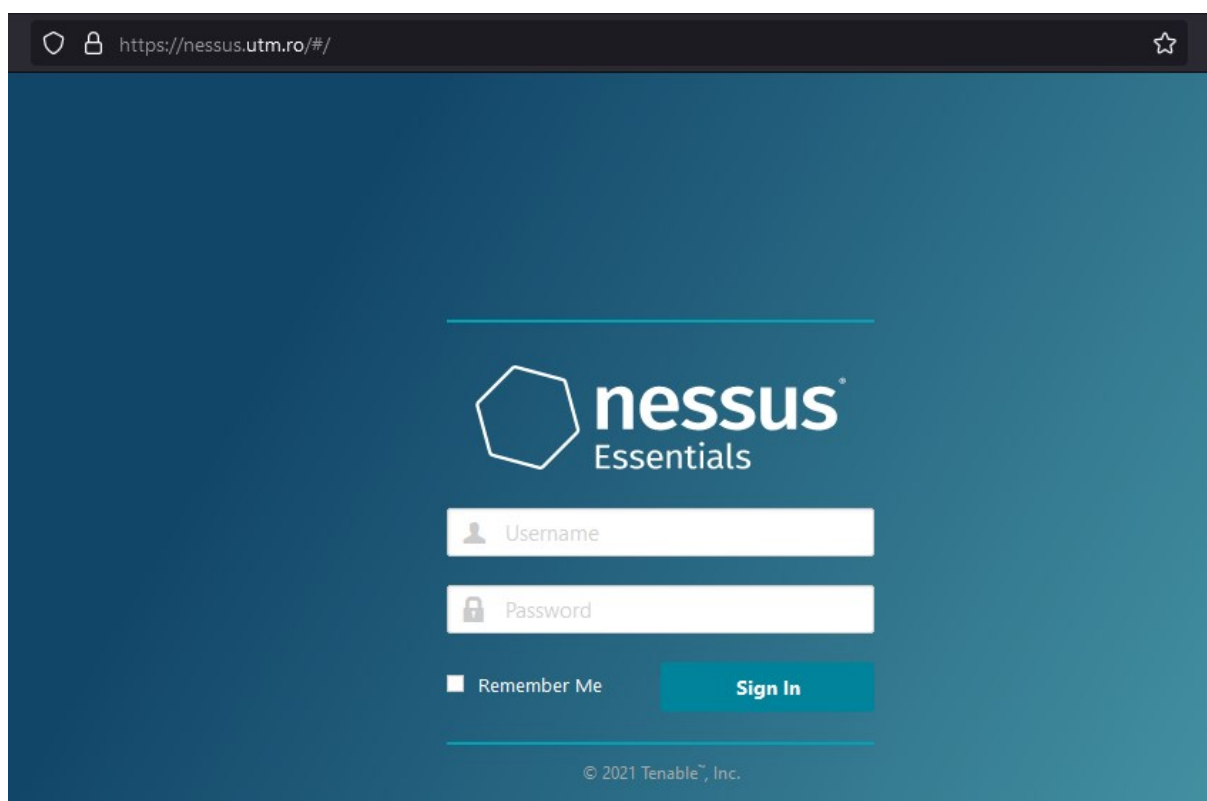


# Nessus Profesional

Nessus CyberX: <https://10.224.2.191:8834/#/>  
admin / CyberX01

- [https://owasp.org/www-community/Vulnerability\\_Scanning\\_Tools](https://owasp.org/www-community/Vulnerability_Scanning_Tools)
- <https://docs.tenable.com/nessus/Content/ScanAndPolicyTemplates.htm>
- <https://www.tenable.com/tenable-for-education/nessus-essentials>



**Nessus Profesional**, cea mai răspândită soluție de evaluare a vulnerabilităților din industrie vă ajută să reduceți suprafața de atac a organizației dvs. și să asigurați **conformitatea**. Nessus oferă descoperirea de mare viteză a activelor, auditarea configurației, profilarea țintei, detectarea malware-ului, descoperirea datelor sensibile etc.

**Nessus** acceptă multe tehnologii - sisteme de operare de scanare, dispozitive de rețea, hipervizoare, baze de date, servere web dar și infrastructura critică pentru vulnerabilități, amenințări și încălcări de conformitate.

Are cea mai mare **bibliotecă actualizată continuu** de verificări ale vulnerabilităților și configurației, și astfel Nessus stabilește standardul pentru viteză și acuratețe a scanării vulnerabilităților.

Obțineți vizibilitate deplină asupra vulnerabilităților dvs

Nota: **Nimic dintr-o rețea nu rămâne static foarte mult timp. Activele se schimbă, la fel și vulnerabilitățile care vă pot pune în pericol. Obținerea unei evaluări complete a mediului dumneavoastră este primul pas.....**

#### **Atentie:**

Trecerea **pe scară largă la munca de la distanță a atomizat suprafața de atac, creând noi provocări pentru profesioniștii în securitate.**

Deoarece majoritatea organizațiilor se așteaptă să mențină un model de lucru hibrid – în care angajații vor avea opțiunea de a lucra acasă sau la birou abordările tradiționale ale securității cibernetice sunt puse la încercare zilnic. Mediul dinamic și provocator de astăzi necesită o nouă abordare a evaluării vulnerabilității.

Elemente cheie de luat în considerare atunci când vă adaptați strategia de evaluare a vulnerabilității aplicațiilor:

**Portabilitatea** - Un analist de securitate sau o echipă mare de securitate corporativă trebuie să fie gata să se deplaseze într-un mediu dispersat geografic. O forță de muncă dispersă implică faptul că, trebuie să existe un instrument de evaluare a vulnerabilităților care să fie ușor de portat, astfel încât utilizatorii să poată călători fără probleme între clienți sau medii.

**Eficiența** - găsirea rapidă a vulnerabilităților și identificarea cauzei lor, este o etapă esențială pentru a reduce riscul abordând rapid orice vector nou descoperit. Acest lucru necesită abilitatea de a efectua o scanare profundă care poate produce o analiză detaliată a întregului mediu. Pentru analiza în timp real, capturile de pachete joacă un rol cheie în îndeplinirea cerințelor criminalistice și de conformitate, oferindu-vă posibilitatea de a vă concentra până la nivelul pachetului. În plus, pentru a lua decizii bune sau pentru a demonstra conformitatea istorică cu regulile de reglementare sau politicile de securitate, este esențial să poți **folosi rapoartele potrivite.**

**Ușurința** în utilizare îmbunătățește eficiența. Dacă instrumentul dvs. de evaluare a vulnerabilităților are o experiență de utilizator cu care este dificil să lucrați, nu este intuitivă sau necesită dificultăți în învățare, utilizatorii vor avea probleme.

**Prioritizarea** remedierii îmbunătățește eficiența. Întotdeauna vor exista mai multe vulnerabilități decât poți face față. Pentru ca practicienii în securitate să acorde prioritate remedierii, organizațiile trebuie să fie capabile să înțeleagă

gravitatea unei anumite vulnerabilități în contextul a ceea ce înseamnă aceasta în mediul lor unic.

**Cercetarea** - Este esențial ca soluția dvs. de evaluare a vulnerabilităților să fie susținută de o echipă de cercetare dedicată descoperirii exploatărilor zero day și să ofere îndrumări de specialitate despre vulnerabilitățile cunoscute. Mai mult, o astfel de cercetare trebuie să fie încorporată în instrumentul dumneavoastră de evaluare a vulnerabilităților în timp real

Versiunea Nessus 10.0, lansată pe 28 octombrie 2021 și este acum disponibil pe **Raspberry Pi**. Acest lucru este util în mod special pentru testeri, consultanți și alții a căror funcție necesită mobilitate între locații.

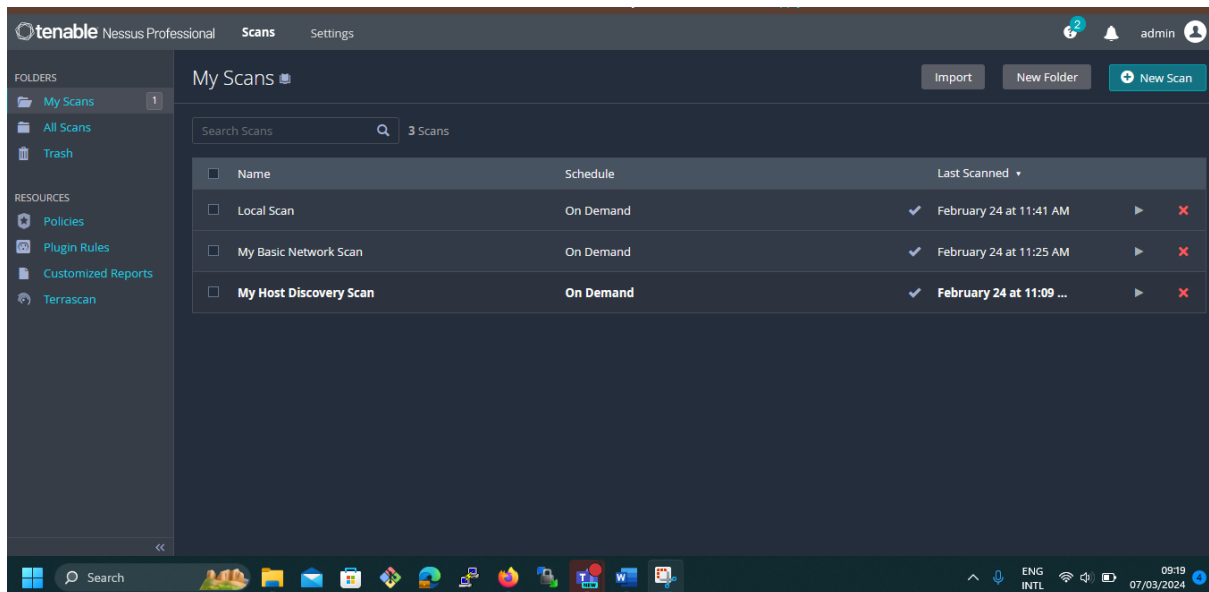
Pentru a îmbunătăți eficiența, Nessus 10.0, conține și o funcție de plug-in compilată dinamic, care reduce amprenta bazei de date Nessus Plugin cu până la 75%. Această nouă caracteristică mărește performanța de scanare, reducând în același timp supraîncărcarea memoriei scannerului.

Pentru ușurință în utilizare, Nessus a pus un accent mare pe îmbunătățirea experienței generale de raportare. Aceasta include un aspect actualizat și îmbunătățit al rapoartelor statice disponibile.

Pentru a ajuta la prioritizarea remedierii, Nessus vine cu o nouă funcție încorporată de captare a pachetelor, care permite o capacitate puternică de depanare a problemelor de scanare ale clienților.

La baza tuturor se află munca Tenable Research, care urmărește fluxurile de informații despre amenințări și vulnerabilități pentru a se asigura că echipele de pluginuri pot oferi acoperire produselor cât mai curând posibil. Tenable Research se concentrează pe activități diverse care stau la baza managementului vulnerabilităților: dezvoltarea de noi detectări pentru active și vulnerabilități; dezvoltarea auditului și verificărilor de conformitate; îmbunătățirea automatizării gestionării vulnerabilităților pentru a accelera lansarea detectărilor de vulnerabilități și găsirea vulnerabilităților zero-day în produsele comune și critice.

## Interfata principala



**Atentie:** Cand creați și gestionați scanări trebuie să țineți seama de numărul de licențe folosite.

### Nota:

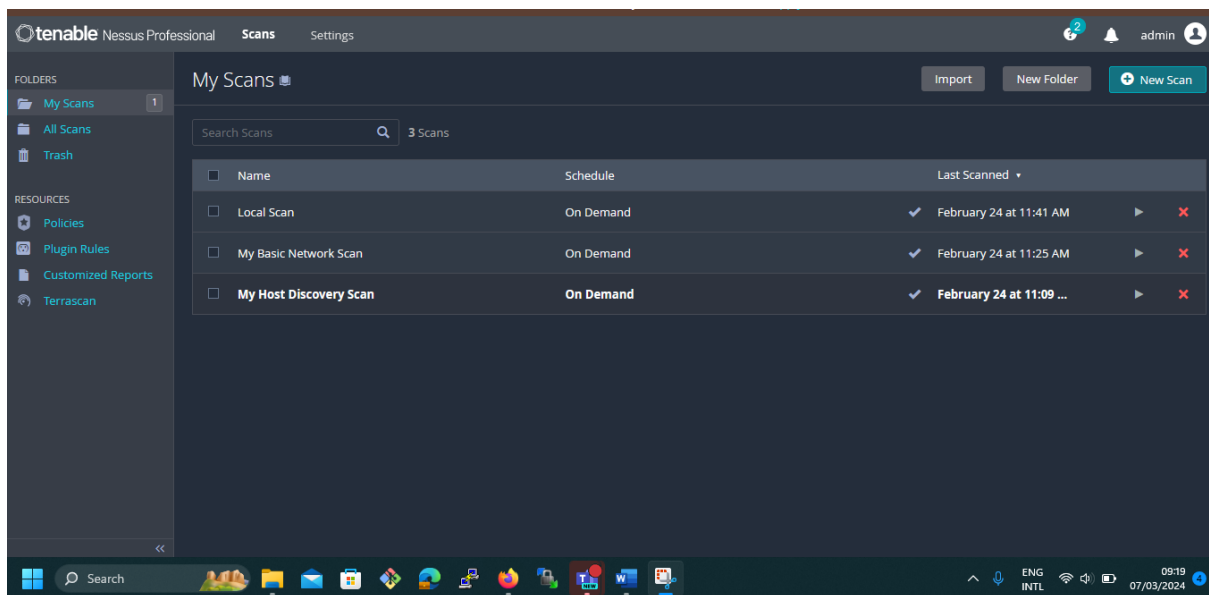
#### Create a User Account

This procedure can be performed by an administrator in Nessus Manager or Nessus Professional with legacy features. Multiple users are not available in Nessus Professional 7.0 and later.

**Atentie la pastrarea configurației aplicației.**

Interfata aplicației, conține următoarele sarcini disponibile pe pagina Scanări.

- Creați o scanare
- Importați o scanare
- Creați o scanare de agent
- Modificați setările de scanare
- Configurați o pistă de audit
- Ștergeți o scanare, etc.



## Exemplu: **Descoperirea gazdei**

A ști ce gazde sunt în rețeaua ta este primul pas către orice evaluare a vulnerabilităților. Lansați o scanare de descoperire a gazdei pentru a vedea ce gazde sunt în rețeaua dvs. și informațiile asociate, cum ar fi adresa **IP, sistemele de operare și porturile deschise, dacă sunt disponibile**. După ce aveți o listă de gazde, puteți alege ce gazde doriți să vizați într-o anumită scanare pentru identificare vulnerabilități.

Puteți lansa oricând o scanare de descoperire a gazdei sau o scanare ulterioară utilizând fluxul de lucru.

Creați și lansați o scanare de descoperire a gazdei:

1. .. click **Scans**.

The **My Scans** page appears.

2. In the upper right corner, click the **New Scan** button.

The **Scan Templates** page appears.


3. Under **Discovery**, click the **Host Discovery** template.

4. Configure the host discovery scan:

- For **Name**, enter a name for the scan.
- For **Targets**, enter targets as hostnames, IPv4 addresses, or IPv6 addresses.

**Tip:** For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0,192.168.0.1). For more information, see [Scan Targets](#).

- (Optional) Configure the remaining [settings](#).

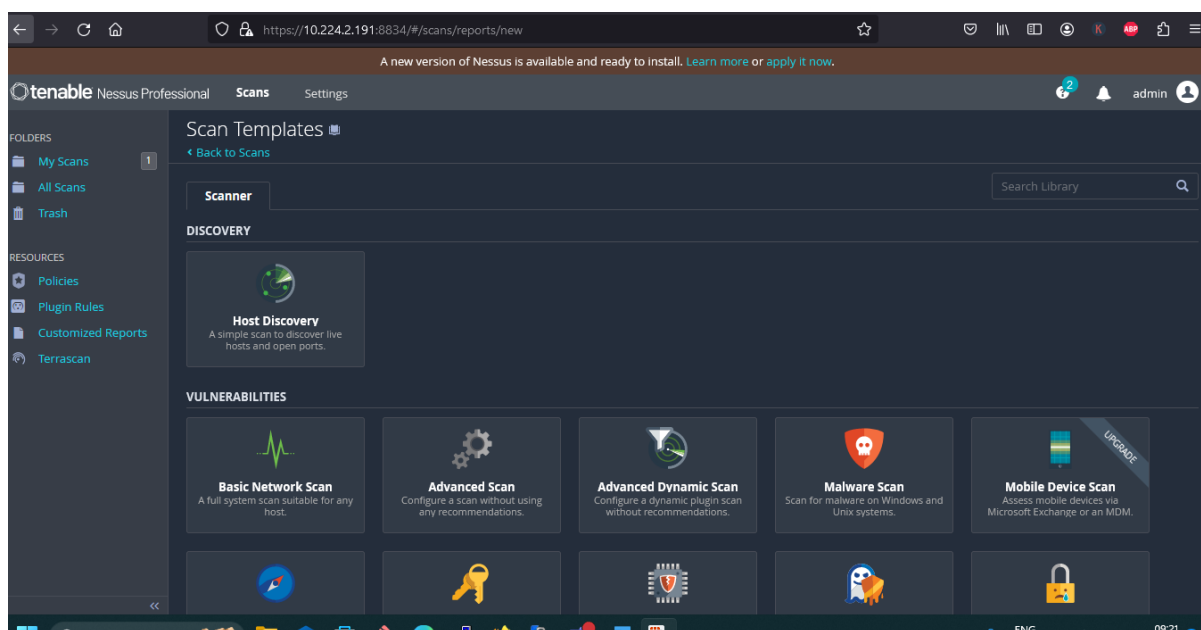
5. To launch the scan immediately, click the  button, and then click **Launch**.

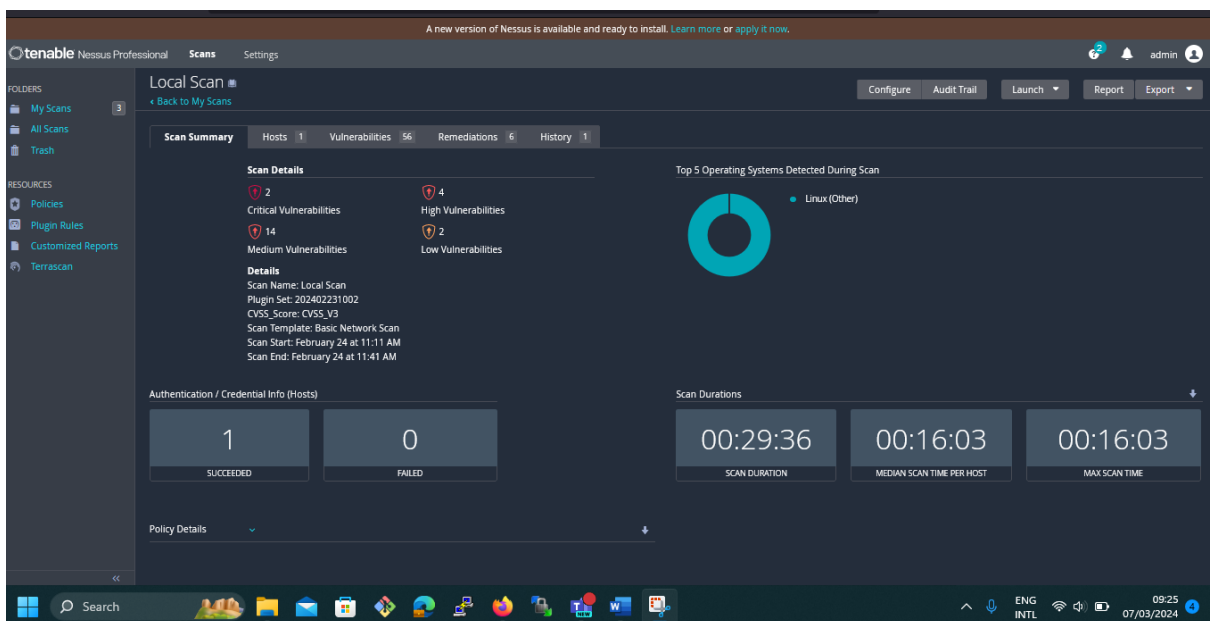
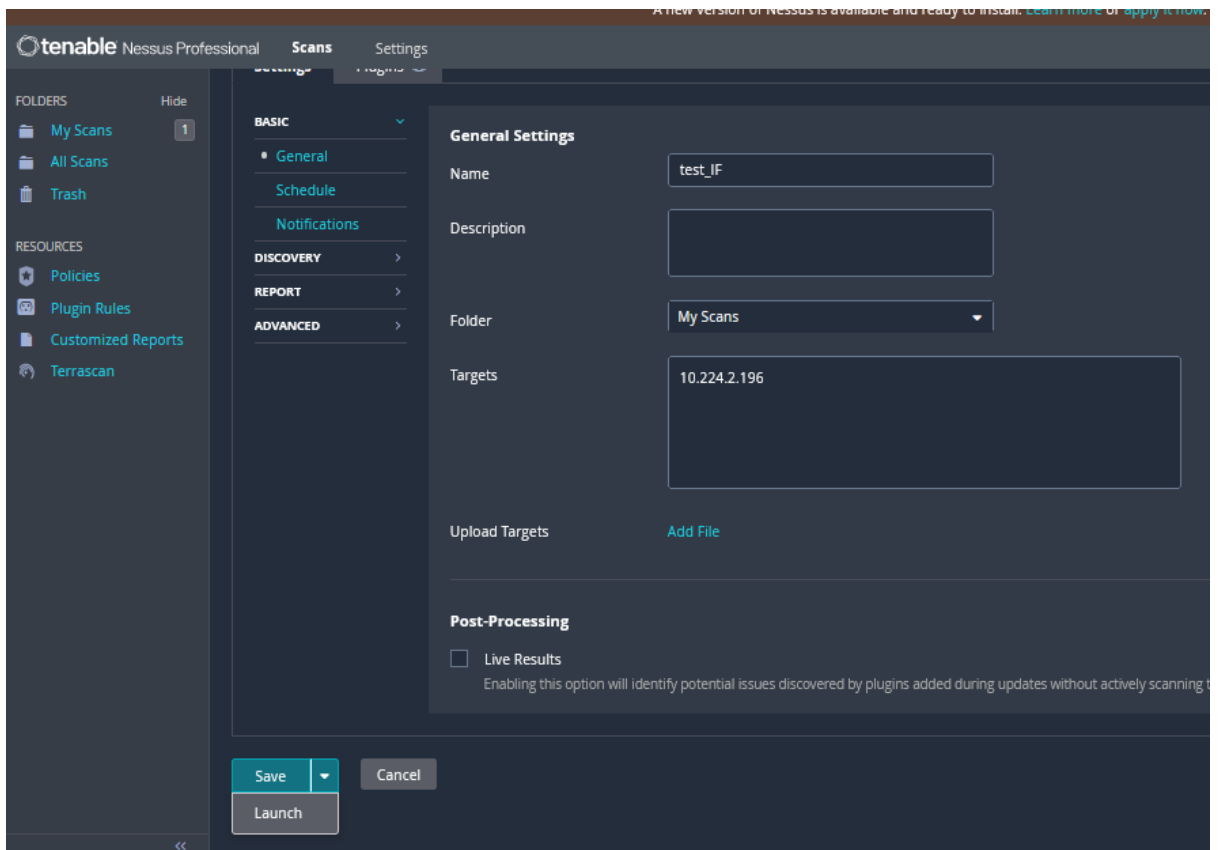
Nessus runs the host discovery scan, and the **My Scans** page appears.

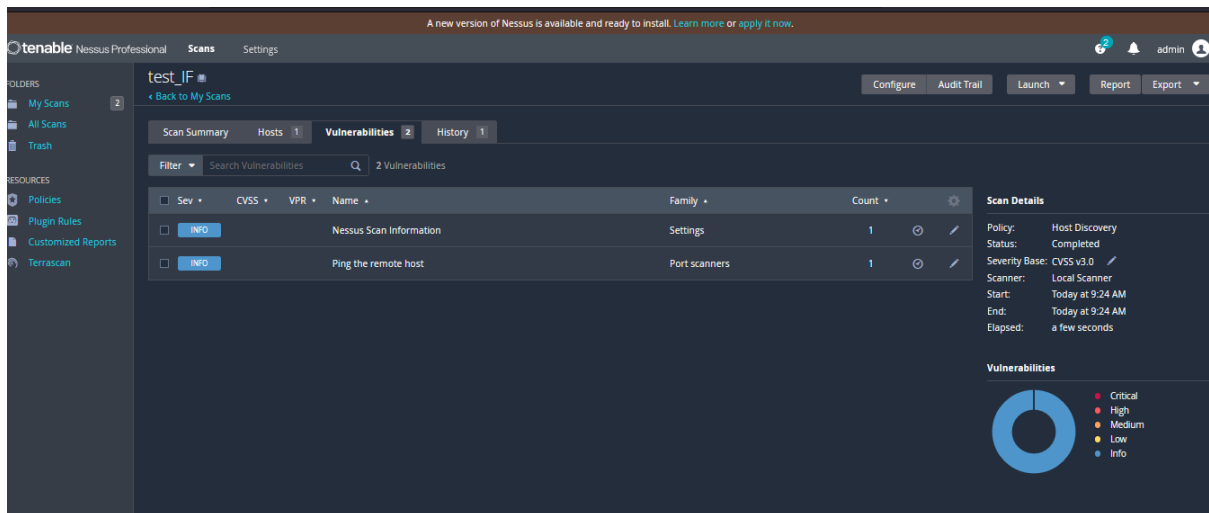
6. In the scans table, click the row of a completed host discovery scan.

The scan's results page appears.

7. În fila **Hosts**, vizualizați gazdele pe care Nessus le-a descoperit și orice informații asociate disponibile, cum ar fi adresa IP, FQDN, sistemul de operare și porturile deschise.







## Creai și lansezi o scanare pe una sau mai multe gazde descoperite:

1. In the top navigation bar, click **Scans**.

The **My Scans** page appears.

2. In the scans table, click the row of your completed host discovery scan.

The scan's results page appears.

3. Click the **Hosts** tab.

Nessus displays a table of scanned hosts.

4. Select the check box next to each host you want to scan in your new scan.

At the top of the page, the **More** button appears.

5. Click the **More** button.

A drop-down box appears.


6. Click **Create Scan**.

The **Scan Templates** page appears.

7. Select a [scan template](#) for your new scan.

Nessus automatically populates the **Targets** list with the hosts you previously selected.



8. Configure the rest of the scan settings, as described in [Scan and Policy Settings](#).
9. To launch the scan immediately, click the  button, and then click **Launch**.

Nessus salvează și lansează scanarea

## Import a Scan

You can import a scan that was [exported](#) in Nessus (.nessus) or Nessus DB (.db) format. With an imported scan, you can view scan results, export new reports for the scan, rename the scan, and update the description. You cannot launch imported scans or update policy settings.

You can also import .nessus files as policies. For more information, see [Import a Policy](#).

### To import a scan:

1. In the top navigation bar, click **Scans**.

The **My Scans** page appears.

2. In the upper-right corner, click **Import**.

Your browser's file manager window appears.

3. Browse to and select the scan file that you want to import.

**Note:** Supported file types are exported Nessus (.nessus) and Nessus DB (.db) files.

The **Scan Import** window appears.

4. If the file is encrypted, type the **Password**.
5. Click **Upload**.

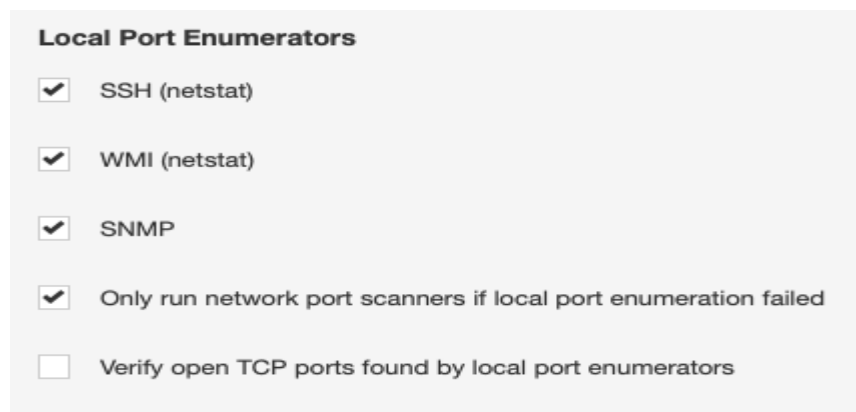
Nessus importă scanarea și datele asociate acesteia.

## Impactul scanării complete a porturilor asupra unui firewall de rețea

Este posibil ca unii utilizatori să fie nevoiți să efectueze scanarea completă a porturilor în scopuri de audit de rețea. Dacă traficul de scanare va trece printr-un firewall de rețea, asigurați-vă că planificați cu atenție și monitorizați sesiunea și utilizarea resurselor infrastructurii dvs.

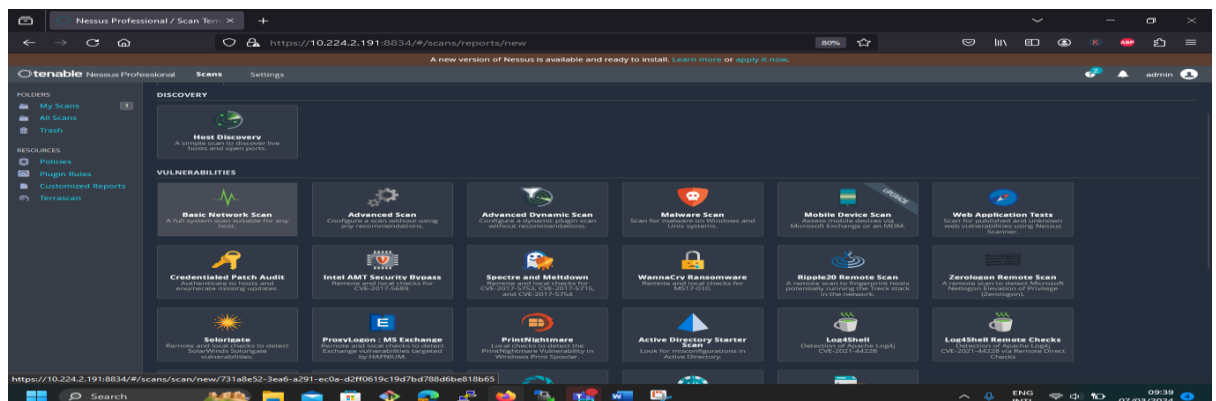
## Configurarea unei scanări de acreditări

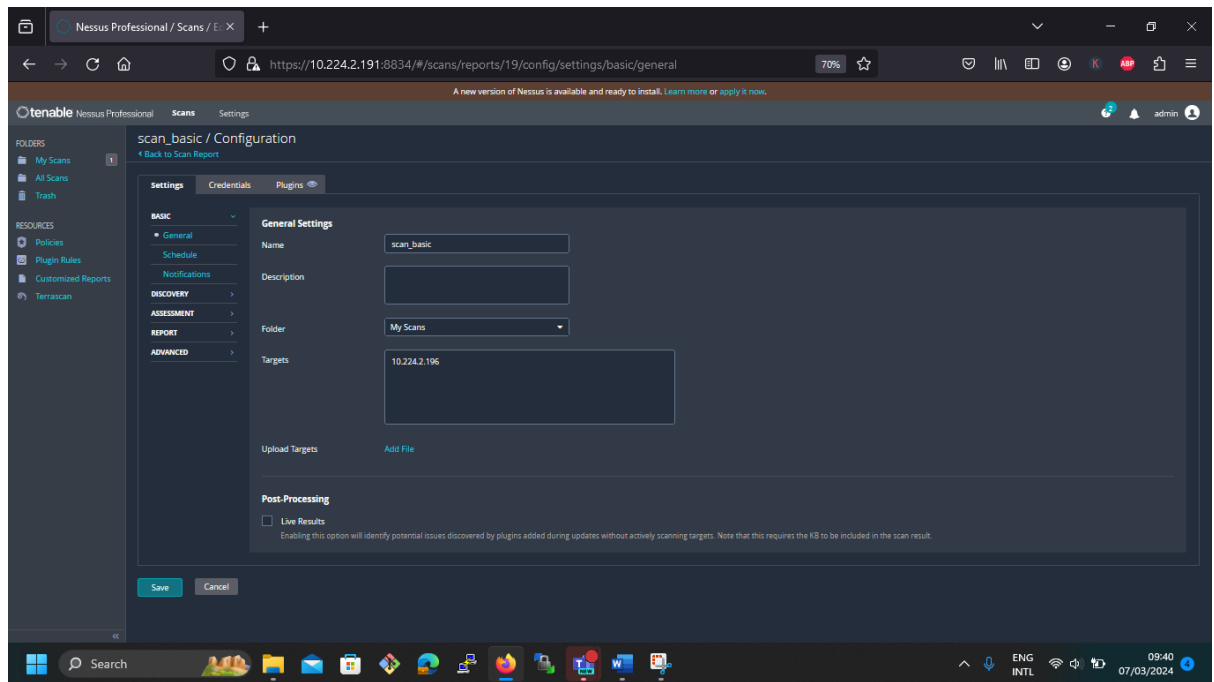
Scanerile de porturi locale sunt activate în mod implicit și vor rula atât timp cât Nessus se poate autentifica cu succes la țintă.



## Aplicatie practica

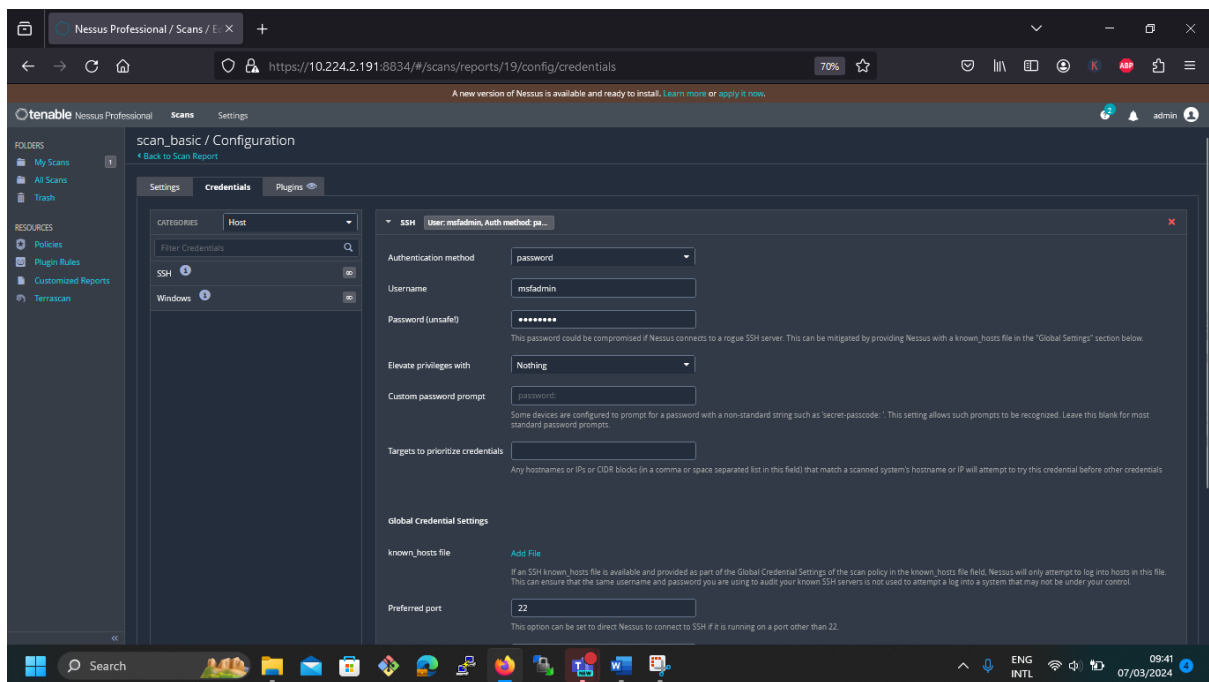
My Scans → New Scan → Basic Network Scan → si efectuati o operatie de **New Scan** completand campurile corespunzatoare

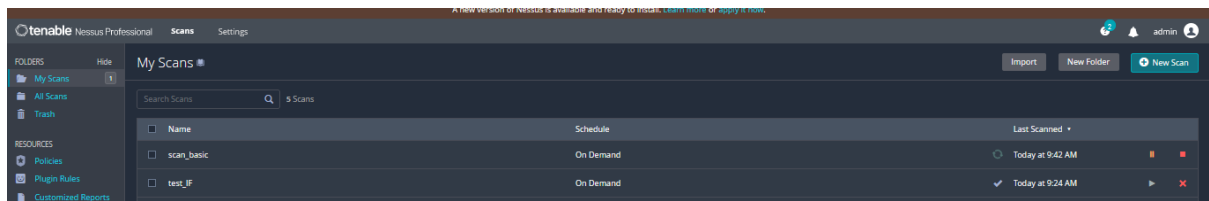
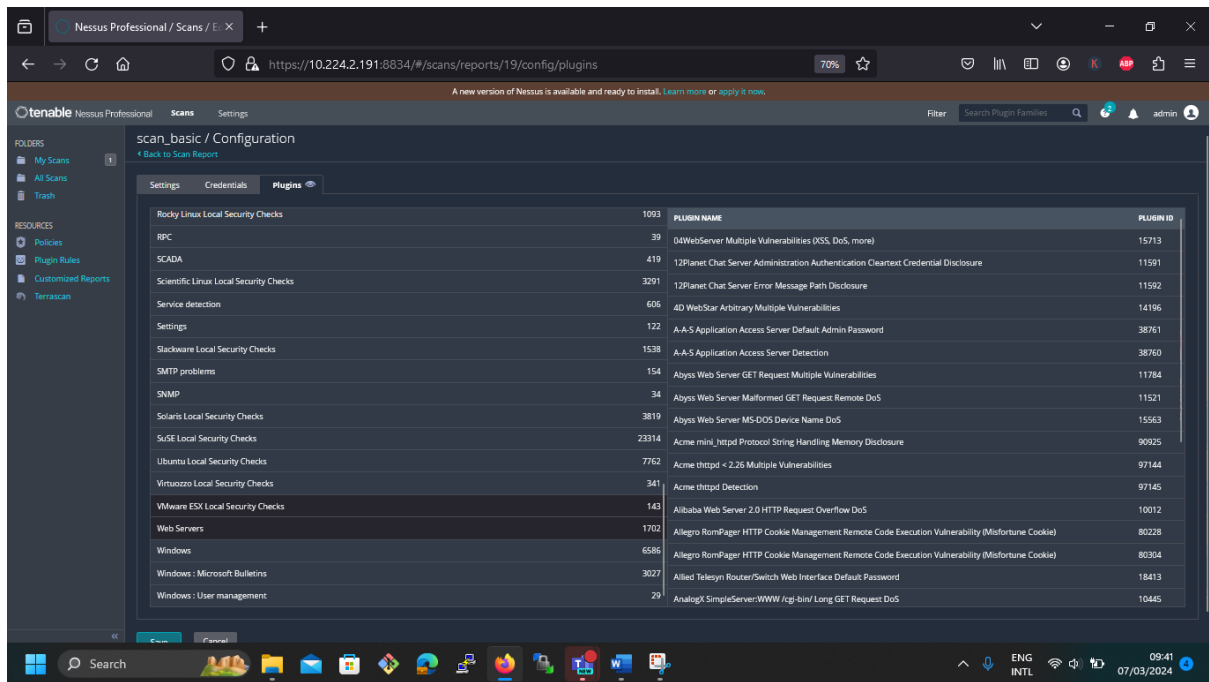




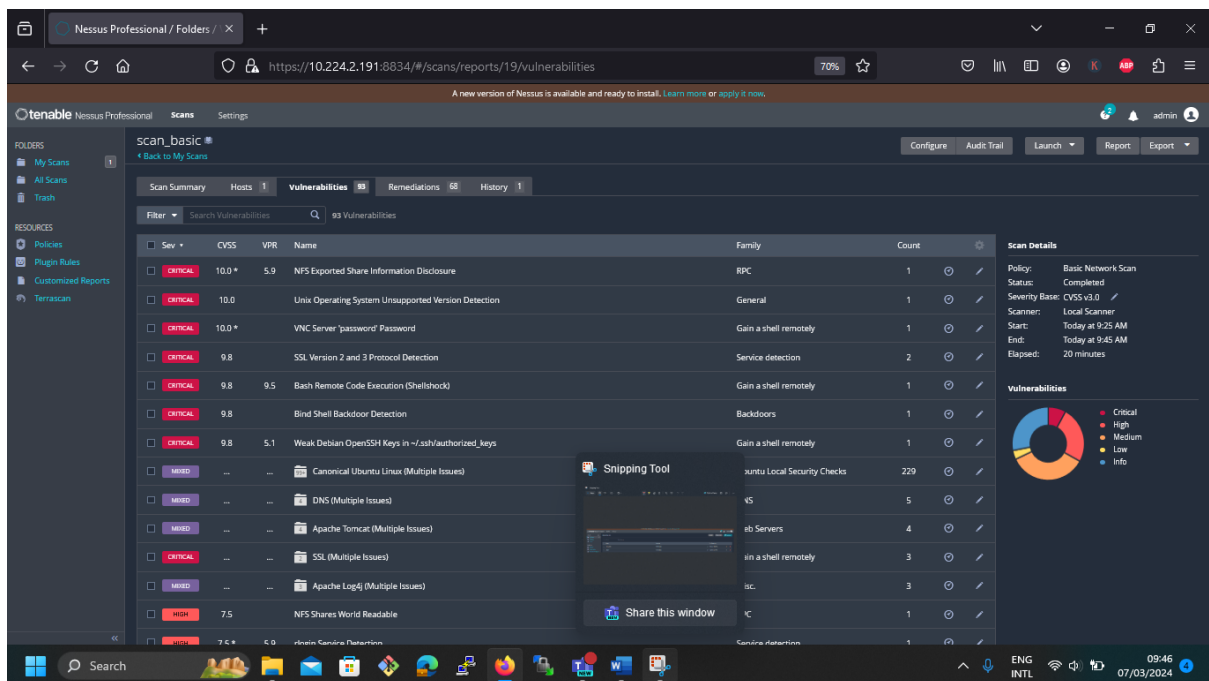
Metasploitable (SSH) 10.224.2.196/

- Un: msfadmin
- Pw: msfadmin





Discutati principalele vulnerabilitati identificate in urma procesului de scanare.



Sa se genereze un raport de vulnerabilitati.

