

# Wykrywanie zagrożeń i reakcja na incydenty

Laboratorium 9

Tomasz Jarząbek 272279  
Wiktoria Migasiewicz 272177

31.05.2025

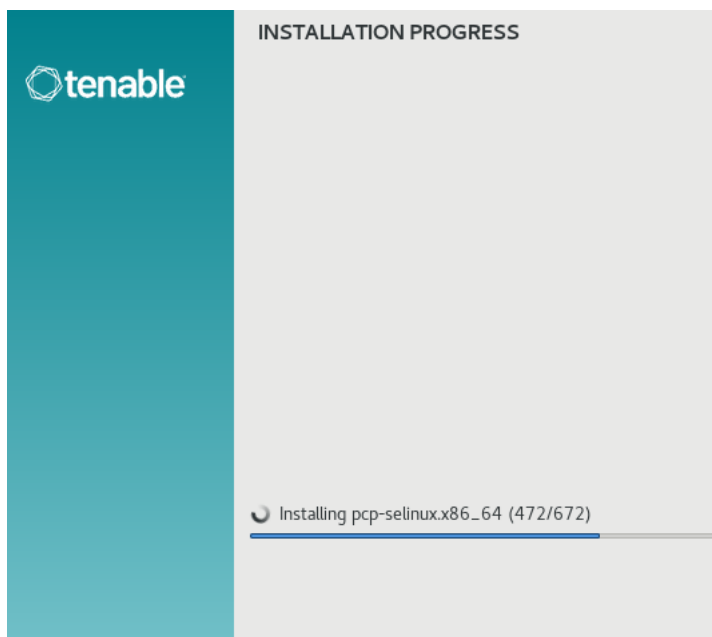
## Spis treści

<b>1</b>	<b>Rozwiązanie</b>	<b>3</b>
1.1	Tenable - instalacja . . . . .	3
1.2	Nessus - instalacja . . . . .	4
1.3	Skan hostów . . . . .	6
1.4	Skan sieci . . . . .	7
1.5	Skan uwierzytelniony . . . . .	9

# 1 Rozwiązanie

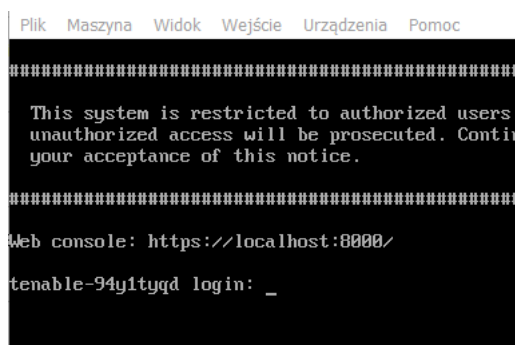
## 1.1 Tenable - instalacja

Przygotowano częściowo środowisko z poprzednich laboratoriów numer 6 i 7. Wykorzystano Alma Linux oraz Windows, pomijając Ubuntu. Zainstalowano za pomocą VirtualBox maszynę Tenable, umieszczając ją w tej samej sieci, co poprzednie dwie maszyny (10.0.3.0/24). Tenable dano odpowiednią ilość zasobów fizycznych i uruchomiono.



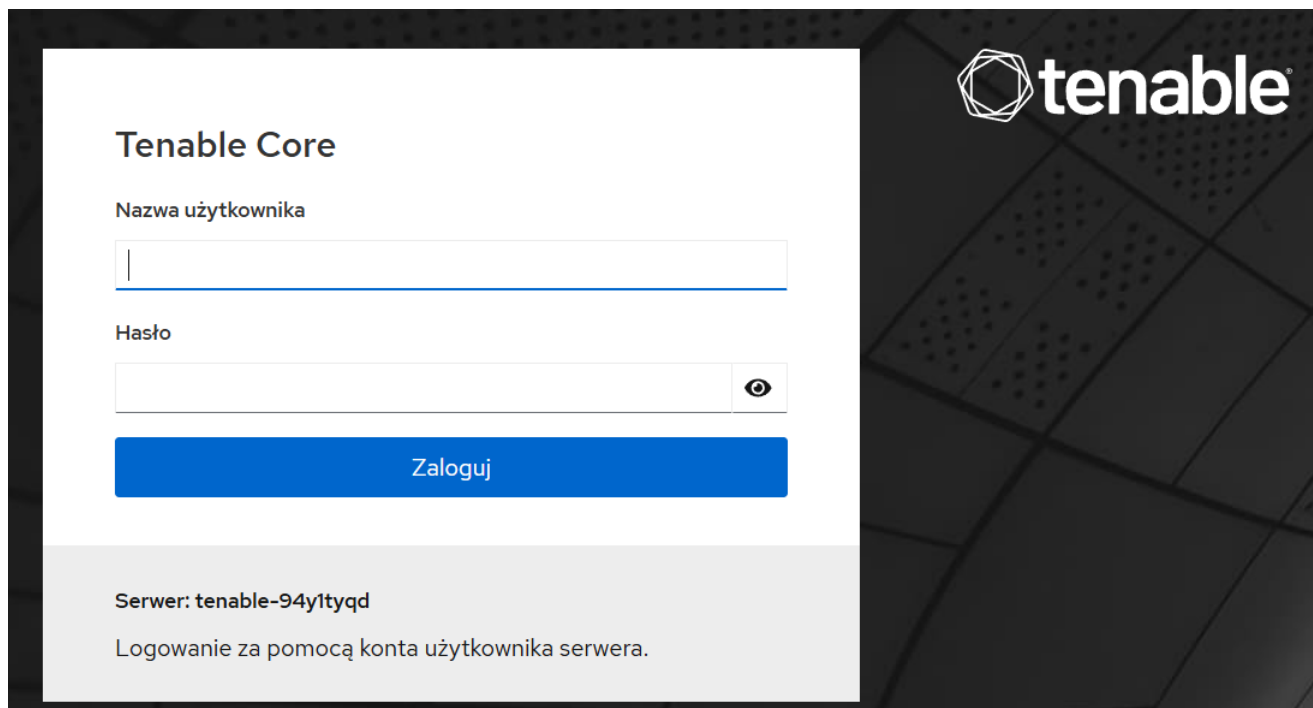
Rysunek 1: Instalacja Tenable.

Nadano odpowiedni adres IP (10.0.3.15) oraz stworzono konto użytkownika: **tenable**.



Rysunek 2: Zainstalowane Tenable.

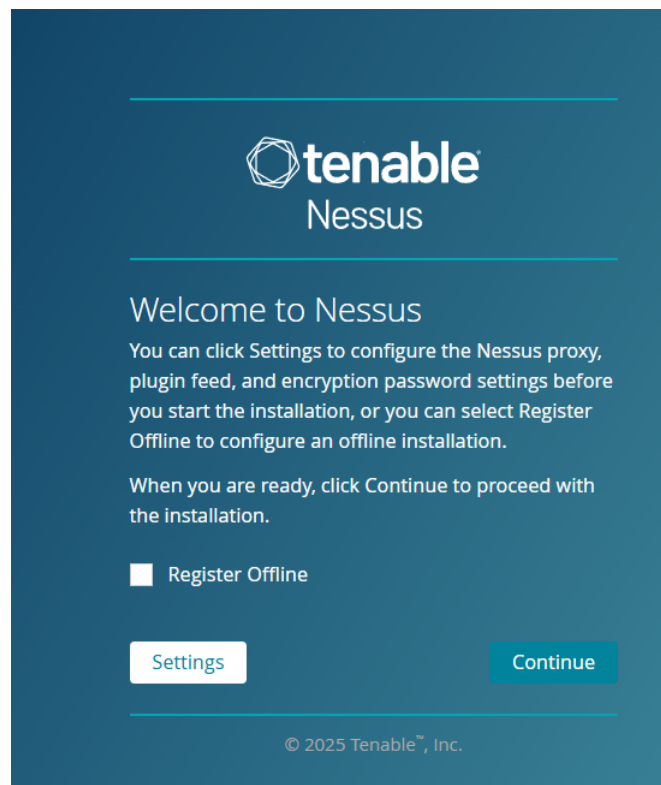
Tenable został uruchomiony, a po zarejestrowaniu się na stronie Nessusa, wygenerowany został klucz aktywacyjny. Działający Tenable operuje na porcie 8000, co dzięki przekierowaniu z VirtualBox można było zobaczyć na maszynie hosta:



Rysunek 3: Tenable - GUI.

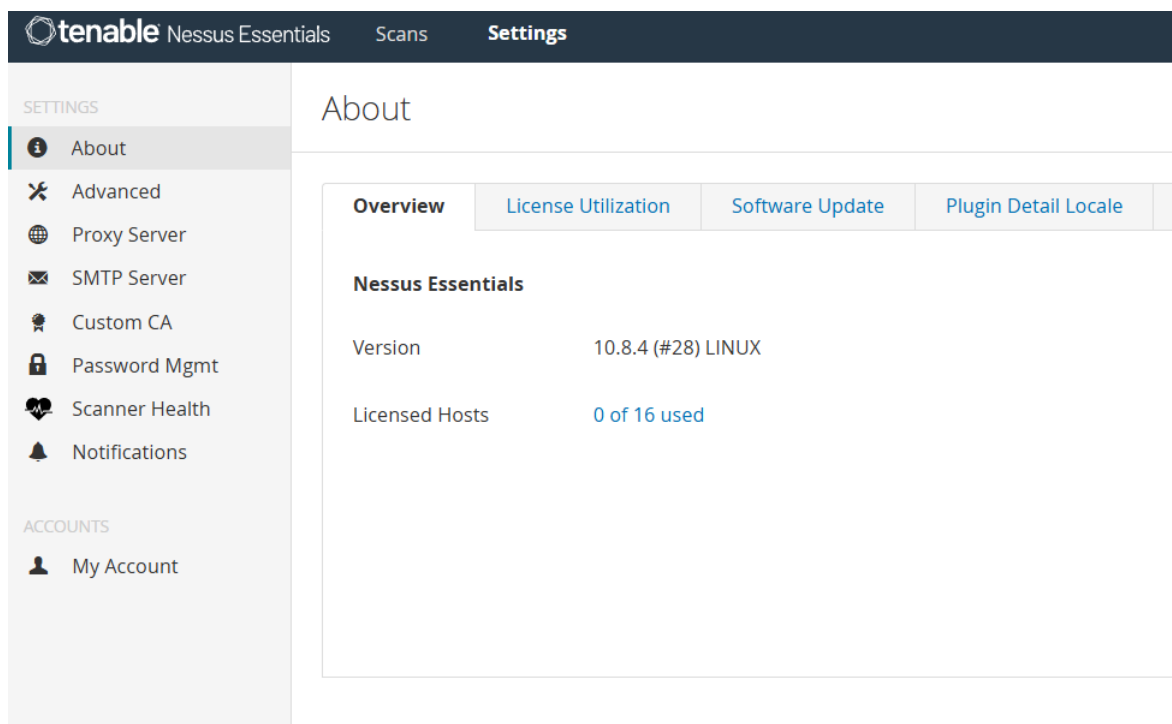
## 1.2 Nessus - instalacja

Następnie należało otworzyć port 8834, aplikację Nessus:



Rysunek 4: Nessus - rejestracja.

Stworzono użytkownika Nessus po wprowadzeniu klucza aktywacyjnego.

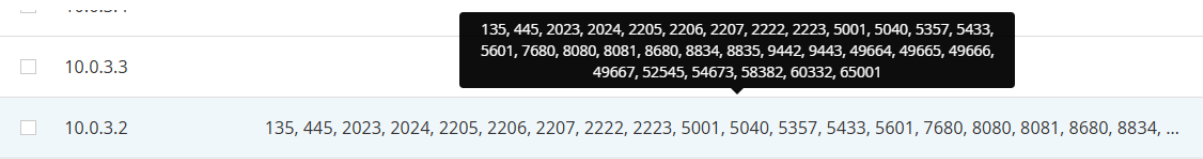


Rysunek 5: Nessus - GUI.

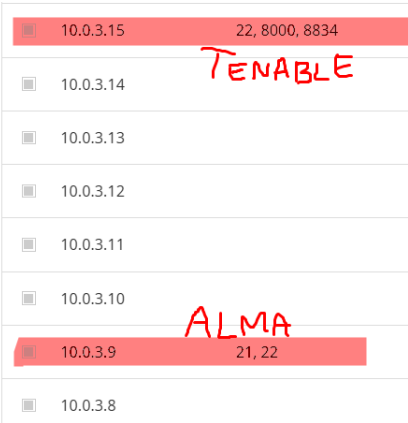
Należało odczekać moment, by wszystkie pluginy się zainstalowały. W tym czasie uruchomiono maszyny Alma linux oraz Windows.

1.3 Skan hostów

Następnie, w GUI Nessusa, po wejściu w zakładkę **Scans**, automatycznie poproszono użytkownika o wpisanie hostów lub zakresu sieci do przeskanowania (podano sieć 10.0.3.0/24). Rozpoczęto skanowanie sieci i znalezionych hostów.



Rysunek 6: Nessus - skan znalezionych hostów w sieci Widnows.



Rysunek 7: Nessus - skan znalezionych hostów w sieci Alma oraz Tenable.

Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO				Ping the remote host	Port scanners	254
INFO				Nessus SYN scanner	Port scanners	6
INFO				Nessus Scan Information	Settings	3
INFO				Netstat Portscanner (SSH)	Port scanners	3

Rysunek 8: Nessus - skan znalezionych hostów w sieci.

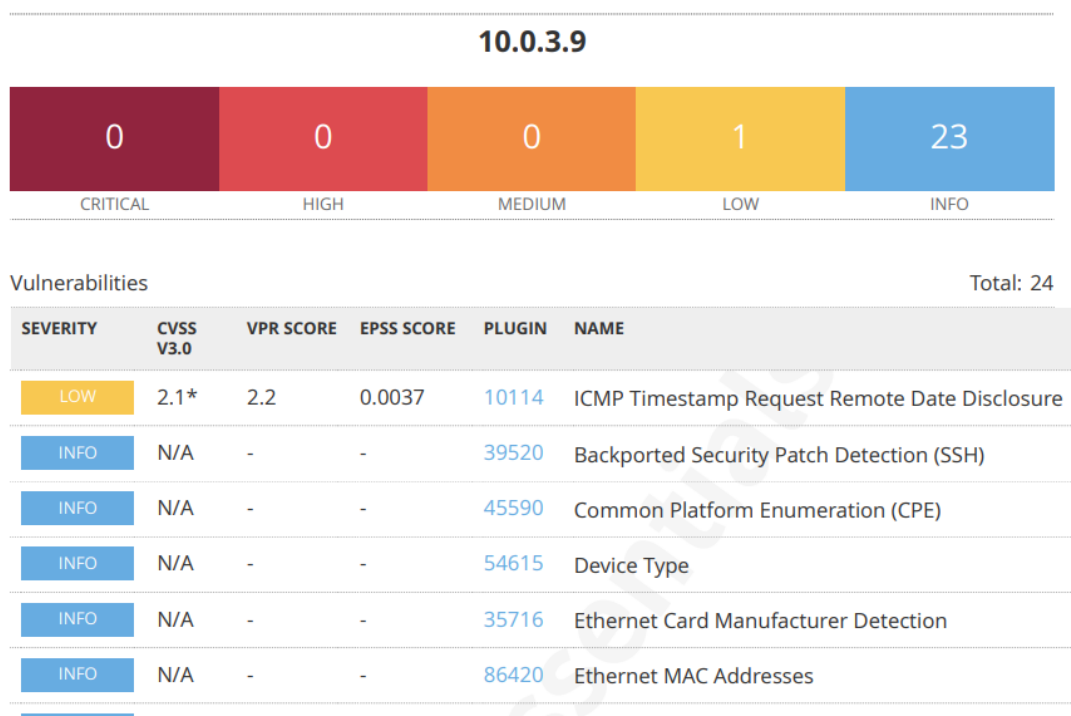
Nessus znalazł 4 aktywne maszyny - Alma, bramę domyślną (port 53), Windows oraz Tenable.

Występował również nieaktywnych hostów. Na Alma znalazł tylko dwa aktywne porty - 22 (SSH) i 21 (FTP). Natomiast znalazł ich znacznie więcej na Windows:

- |                     |                    |                         |
|---------------------|--------------------|-------------------------|
| • 21 / tcp / ftp    | • 5001 / tcp /     | • 9443 / tcp /          |
| • 22 / tcp / ssh    | • 5040 / tcp /     | • 49664 / tcp / dce-rpc |
| • 53 / tcp /        | • 5357 / tcp / www | • 49665 / tcp / dce-rpc |
| • 135 / tcp / epmap | • 5433 / tcp /     | • 49666 / tcp / dce-rpc |
| • 445 / tcp / cifs  | • 5601 / tcp /     | • 49667 / tcp / dce-rpc |
| • 2023 / tcp /      | • 7680 / tcp /     | • 52545 / tcp / dce-rpc |
| • 2024 / tcp / ssh  | • 8080 / tcp /     | • 54673 / tcp /         |
| • 2205 / tcp /      | • 8081 / tcp /     | • 58382 / tcp / www     |
| • 2206 / tcp /      | • 8680 / tcp /     | • 60332 / tcp / dce-rpc |
| • 2207 / tcp /      | • 8834 / tcp / www | • 65001 / tcp /         |
| • 2222 / tcp / ssh  | • 8835 / tcp / www |                         |
| • 2223 / tcp / ssh  | • 9442 / tcp /     |                         |

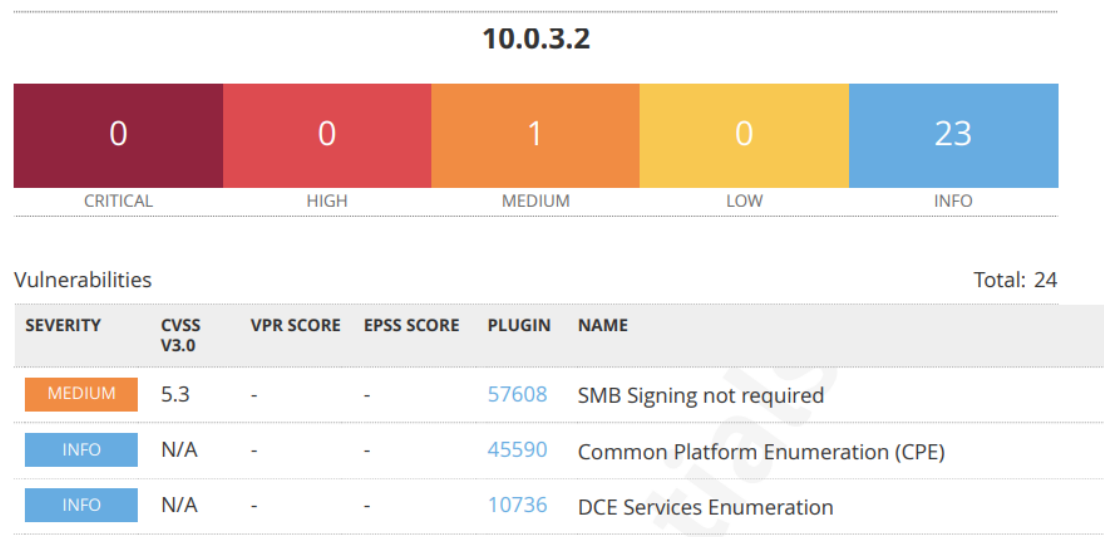
## 1.4 Skan sieci

Następnie przeprowadzono skan sieci (znalezionych hostów - Linux i Windows). Ponieważ z niewiadomych przyczyn po godzinie trwania skanu zawsze łączność z maszyną Windows się przerywała (po stronie Windowsa, jak wyczytano z logów Nessusa na Tenable - podejrzewane jest przeciążenie, zbyt duża ilość pakietów wysyłana do maszyny Windows i zapełnienie jej portów, dlatego mogłaby chcieć zamknąć połączenie. Nie tłumaczy to natomiast dlaczego Tenable w tym momencie zrywa łączność z bramą domyślną, a utrzymuje z Alma), skany przeprowadzono dla maszyn osobno. Pierwszy skan przeprowadzono dla maszyny Alma. Załączone zostały dwie wersje - z ogólnie znalezionymi zagrożeniami w postaci listy oraz w postaci wyszczególnionej.



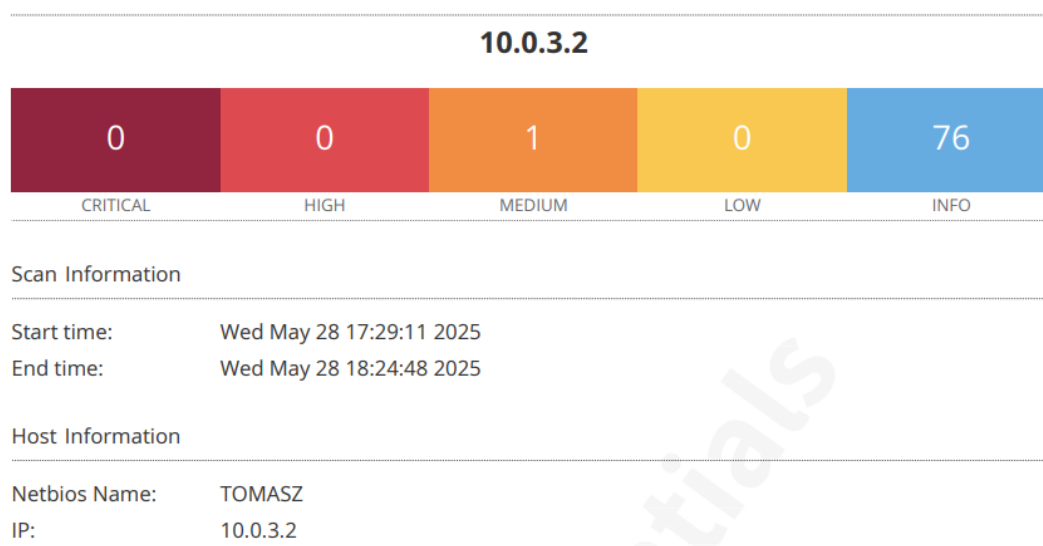
Rysunek 9: Nessus - skan znalezionych zagrożeń w Alma.

Taki sam typ testu wykonany został dla Windows. Co ciekawe, skrócona lista pokazuje jedynie 23 informacyjne alerty, ale lista szczegółowa aż 76.



Rysunek 10: Nessus - skan znalezionych zagrożeń w Windows ogólny.





Rysunek 11: Nessus - skan znalezionych zagrożeń w Windows szczegółowy.

W każdym razie, jest tylko jedno wykryte zagrożenie, które nie kategoryzuje się jako informacyjne. Ostrzegają, że:

- Alma - Low - "ICMP Timestamp Request Remote Date Disclosure" ostrzega, że możliwe jest dokładne określenie czasu, który posiada host (pozwala na omijanie protokołów zabezpieczających przed brakiem synchronizacji czasu).
- Windows - Medium - "Signing is not required on the remote SMB server." ostrzega, iż możliwe do przeprowadzenia są ataki typu MitM na serwerze SBM

## 1.5 Skan uwierzytelniony

Na Alma Linux dodano nowego użytkownika **tenacc** oraz nadano mu uprawnienia root-a. W konfiguracji skanu dodano użytkownika tenacc i nadano mu eskalację uprawnień sudo.

SSH

Authentication method

password

Username

tenacc

Password (unsafe!)

.....

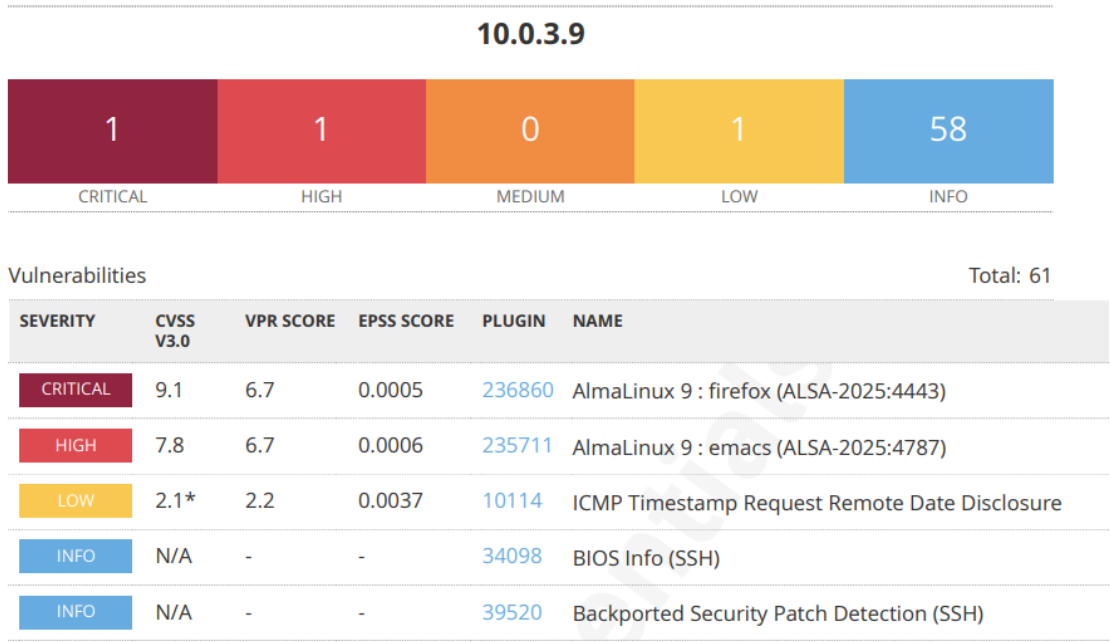
This password could be compromised if Nessus connects to the host with a known\_hosts file in the "Global Settings" section.

Elevate privileges with

sudo

Rysunek 12: Nessus - konfiguracja skanu z uprawnieniami.

Następnie ponownie przeskanowano maszynę Alma Linux.



Rysunek 13: Nessus - wyniki skanu Almy z sudo.

Skan znalazł 61 podatności, czyli aż o 37 podatności więcej. Co więcej, wykryło jedną podatność krytyczną i jedną o zagrożeniu wysokim.

- Podatność krytyczna - "The remote AlmaLinux host is missing one or more security updates.- host Alma posiada paczki, które posiadają wiele podatności, co zostało opisane w Nessus (np. \* firefox: thunderbird: Privilege escalation in Firefox Updater (CVE-2025-2817)\* firefox: thunderbird: Unsafe attribute access during XPath parsing (CVE-2025-4087))

- Podatność wysoka - "The remote AlmaLinux host is missing a security update. więcej paczek posiadających podatności (np. arbitrary code execution via Lisp macro expansion (CVE-2024-53920))

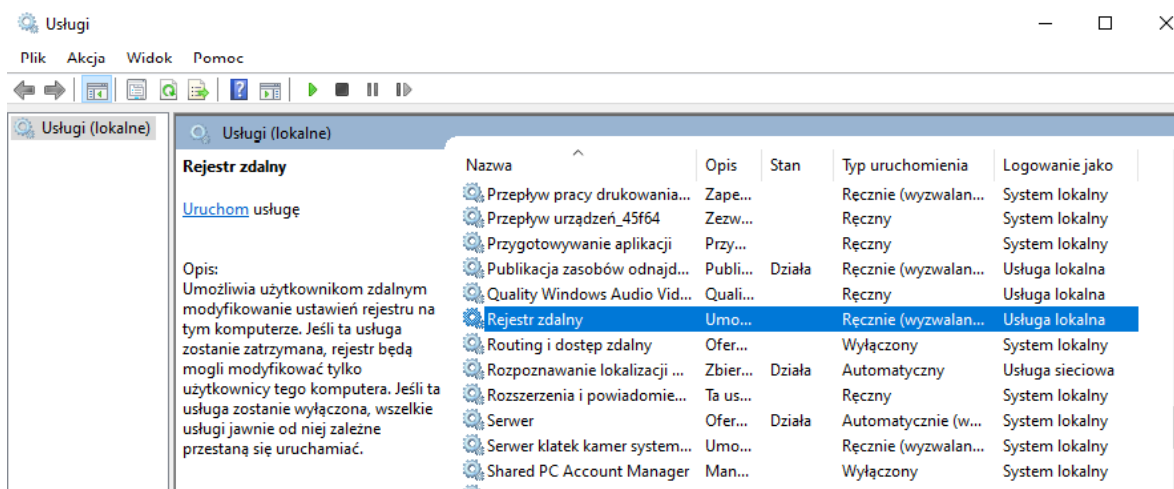
Skan uprzywilejowany (uwierzytelniony) był znacznie bardziej skuteczny w porównaniu do skanu zewnętrznego, znajdując więcej podatności o różnym stopniu zagrożenia. W *ScanNet1 / Plugin #19506 - Nessus Scan Information* sprawdzono, czy skan był uwierzytelniony.

```
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : yes, as 'tenacc' via ssh
Attempt Least Privilege : no
Patch management checks : None
Display superseded patches : yes (supersedence plug
```

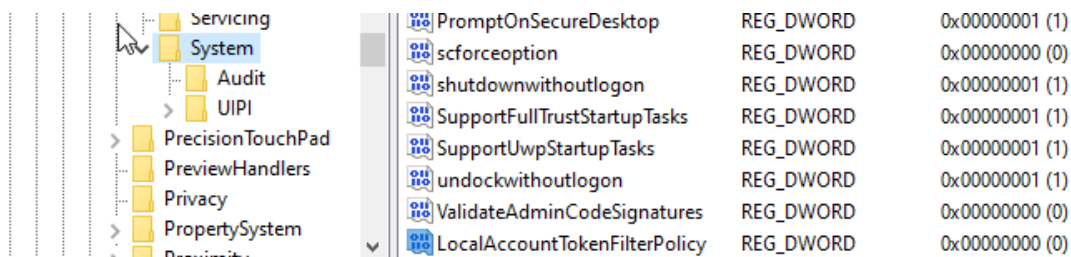
Rysunek 14: Nessus - Check - yes.

Jak widać, skan został uwierzytelniony.

Na maszynie Windows utworzone zostało konta 'admin' i przypisano je do grupy administratorów. Przy pomocy narzędzia services.msc ustawiono sposób uruchamiania usługi „RemoteRegistry” na ręczny, a w edytorze rejestru dodano typu DWORD o nazwie „LocalAccountTokenFilterPolicy” w lokalizacji „HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System” o wartości równej 1.

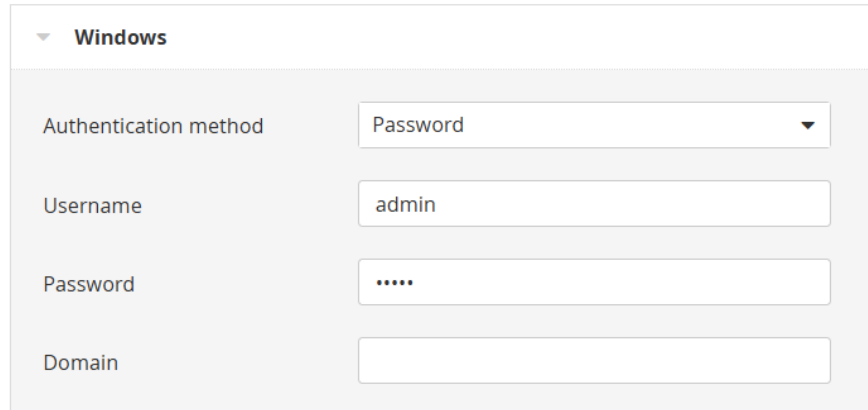


Rysunek 15: Ustawienia rejestru zdalnego



Rysunek 16: Zmienne edytora rejestru

Następnie uruchomiono skan uwierzytelniony. Zweryfikowano poprawność poświadczeń poprzez wgląd w wynik z plugini 19506.



▼ Windows

Authentication method Password ▼

Username admin

Password .....

Domain

Rysunek 16: Konfiguracja skanu z uprawnieniami - Windows

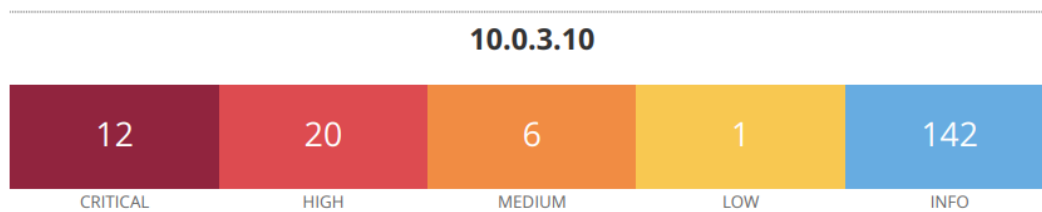
Skan uwierzytelniony okazał się znacznie skuteczniejszy, wykryto bowiem 12 krytycznych, 20 wysokich, 6 średnich i 1 niskich podatności. Porównując wynik do skanu niewierzytelzonego, gdzie wykryto jedynie 1 podatność, rezultat skanu jest o wiele dokładniejszy.

Przykładowe wykryte krytyczne podatności to:

- KB5027215: Windows 10 Version 21H2 / Windows 10 Version 2Security Update (June 2023)
- Security Updates for Microsoft .NET Framework (January 2024)
- KB5040427: Windows 10 Version 21H2 / Windows 10 Version 2Security Update (July 2024)

```
Optimize the test : yes
Credentialed checks : yes, as '10.0.3.10\admin' via SMB
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
```

Rysunek 17: Zawartość wyniku z pluginu 19506



Vulnerabilities Total: 181

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.2	0.1431	177252	KB5027215: Windows 10 Version 21H2 / Windows 10 Version Security Update (June 2023)
CRITICAL	9.8	9.4	0.8054	178159	KB5028166: Windows 10 Version 21H2 / Windows 10 Version Security Update (July 2023)
CRITICAL	9.8	10.0	0.9307	179497	KB5029244: Windows 10 Version 21H2 / Windows 10 Version Security Update (August 2023)
CRITICAL	9.8	8.4	0.9443	182854	KB5031356: Windows 10 Version 21H2 / Windows 10 Version Security Update (October 2023)
CRITICAL	9.8	9.5	0.9066	185585	KB5032189: Windows 10 Version 21H2 / Windows 10 Version Security Update (November 2023)

Rysunek 18: Wynik skanu uwierzytelnionego - Windows