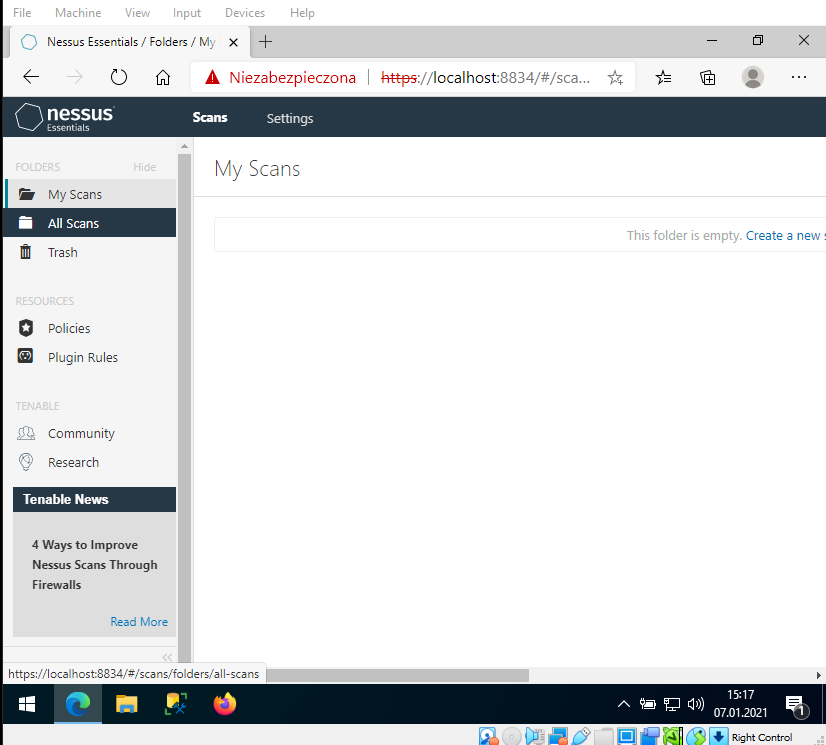
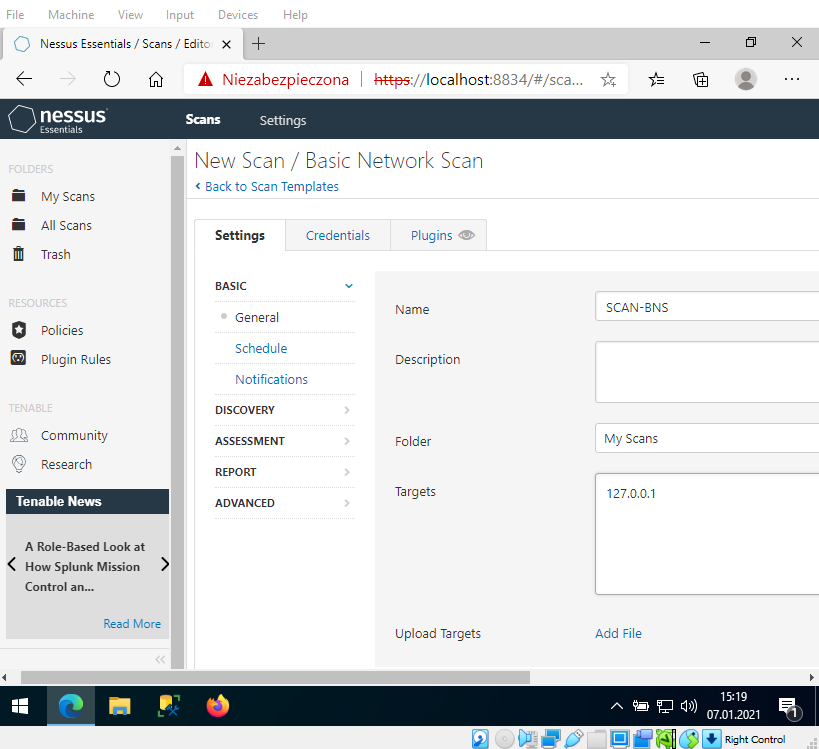
**Ogląd wszystkich skanerów**

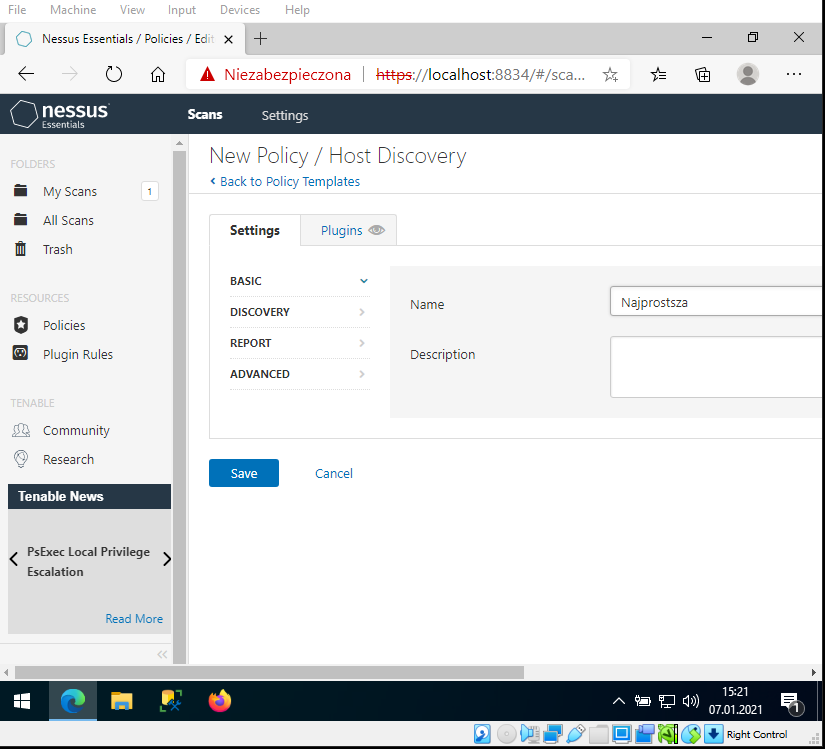
Wchodzimy na główną stronę Nessus Essentials na stronę wszystkich skanów.

**Tworzenia skanera**

Dalej tworzymy nowy skan typu Basic Network Scan. Wybieramy jakąś nazwę (naprzykład SCAN-BNS) i target jako nasz lokalny IP adres (127.0.0.1). Także możemy dodać opis do skanu opcjonalnie.

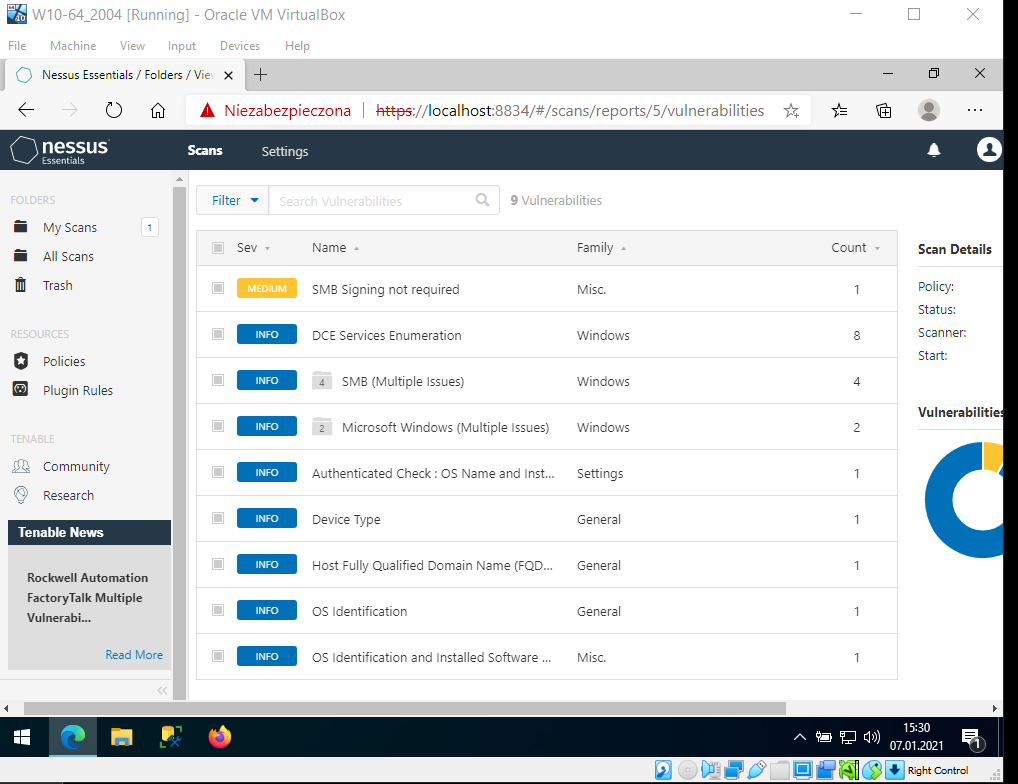
**Tworzenie Policy**

Możemy utworzyć nową Policy we wkladce „Policies”. Będziemy jej wykorzystywać dla tworzenia innego skanu.

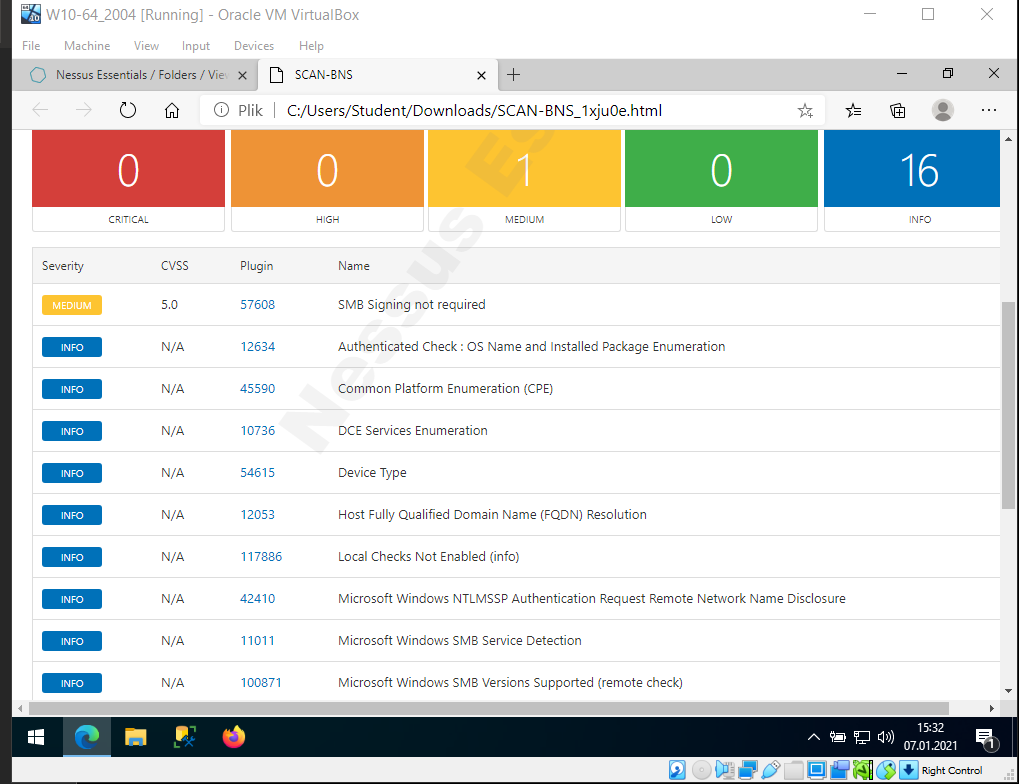


**Wynik skanowania i tworzenie raportów**

Po skończeniu skanowania otrzymujemy takie wyniki. Jak widać mamy tylko 1 wrażliwość typu MEDIUM i 16 typu INFO (nie grozi to niczym).



Mamy wygodniejszy widok o wynikach skanowania. Każdą wrażliwość można otworzyć w nowym oknie, żeby zobaczyć więcej informacji na jej temat. Żeby pobrać raport musimy wygenerować .html lub .csv plik, klikając na przycisk na gorze strony informacji. Dołączam raport odzielnym plikiem.



**Omówienie i Usuwanie wrażliwości**

Przy kliknięciu na którąkolwiek wrażliwość otrzymujemy dokładną informację.

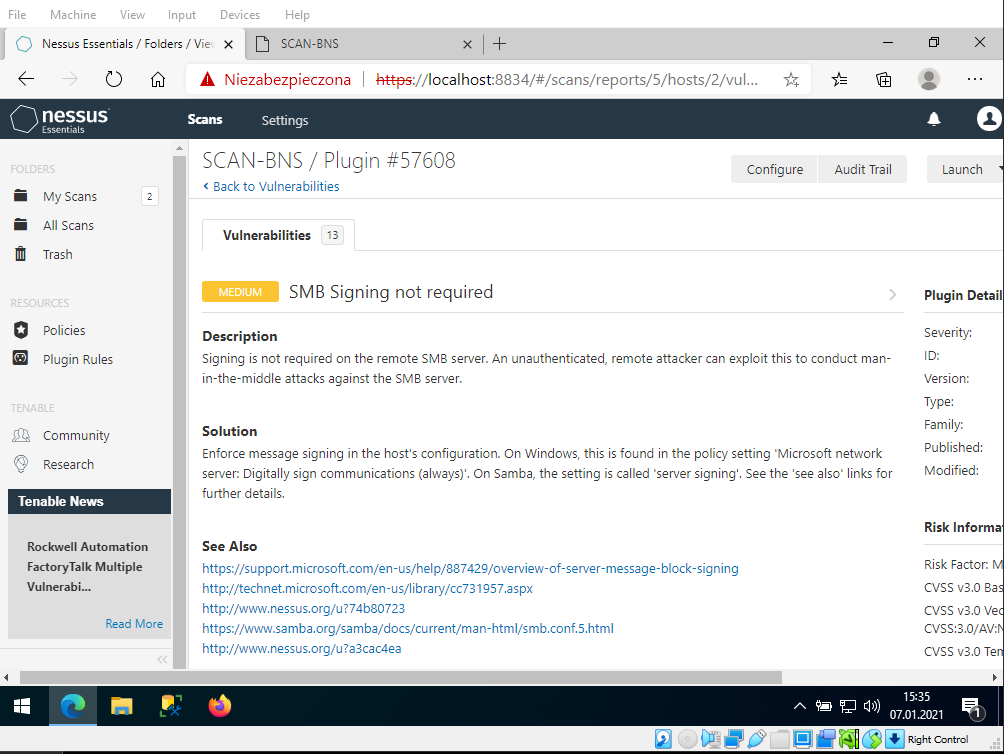
Dla przykładu weźmemy wrażliwość typu MEDIUM „SMB Signing not required”. W pukcie opisu mamy dokłady opis, który pozwala nam zrozumieć co jest nie tak, a punkt „Solution” da nam możliwość poprawienia tej wrażliwości.

**Opis wrażliwośći brzmi tak:**

*Podpisywanie nie jest wymagane na zdalnym serwerze SMB. Nieuwierzytelniona, zdalna osoba atakująca może to wykorzystać do przeprowadzenia ataków typu man-in-the-middle na serwer SMB.*

**Żeby poprawić wrażliwość musimy:**

- Wymusić podpisywanie wiadomości w konfiguracji hosta. W systemie Windows można to znaleźć w ustawieniu zasad „Serwer sieciowy Microsoft: podpisuj cyfrowo komunikację (zawsze)”. W Sambie ustawienie to nosi nazwę „podpisywania serwera”.



**Wniosek i trochę o firmie Tenable**

Tenable to najbardziej wszechstronna w branży platforma zarządzania lukami w zabezpieczeniach oparta na ryzyku (RBVM), umożliwiająca:

* przeglądanie wszystkich zasobów i słabych punktów na całej powierzchni ataku - w tym w chmurze, OT i środowiskach kontenerowych
* przewidywanie, co ma znaczenie, poprzez zrozumienie słabych punktów w kontekście ryzyka biznesowego, a także krytyczności aktywów, na które mają one wpływ
* działanie w odniesieniu do każdej podatności o wysokim priorytecie, aby skutecznie zarządzać ryzykiem i mierzyć KPI, aby skutecznie komunikować skuteczność

Tenable zapewnia najbardziej kompleksowe dostępne rozwiązanie do zarządzania lukami w zabezpieczeniach, oparte na ryzyku, które pomaga określić priorytety działań naprawczych, dzięki czemu można podjąć zdecydowane działania w celu zmniejszenia największego ryzyka biznesowego przy jak najmniejszym wysiłku.

Produkt zapewnia doskonałe dane na temat podatności, systemów, których dotyczy problem, oraz informacje dotyczące środków zaradczych. W przeciwieństwie do innych rozwiązań do zarządzania wrażliwościami najbardziej podoba mi się to, że śledzi postępy w miarę przeprowadzania nowych skanów, pokazuje, jakie wrażliwości w zabezpieczeniach załatałeś od czasu poprzednich skanowań, aby pokazać postęp. Najlepsze graficzne reprezentacje środowiska, jakie kiedykolwiek widziałem, i raportowanie można w pełni dostosować, aby szybko zmienić dane i skoncentrować się na bardziej szczegółowych problemach.

**Kilka przykładów skanowania**

Przykład skanowania typu Advanced:

