Projekt

Wdrożenie systemu służącego do skanowania podatności opartego o narzędzie Nessus i implementacja skanów uwierzytelnionych dla platform Linux i Windows. Analiza raportu ze skanu bezpieczeństwa.

Autor:

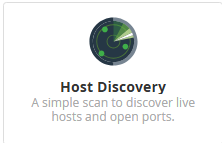
Wiktoria Migasiewicz

1. **Wprowadzenie**

Celem niniejszego sprawozdania jest zaprezentowanie procesu wdrożenia i konfiguracji systemu skanowania podatności opartego na narzędziu Nessus oraz analiza wyników zarówno skanów bez uwierzytelnienia, jak i skanów uwierzytelnionych na platformach Windows i Linux. W pierwszej części omówiono dostępne typy skanów w wersji Nessus Essential, w tym m.in. Host Discovery, Basic Network Scan, Web Application Tests oraz Credentialed Patch Audit. Druga część dokumentu przedstawia praktyczne zastosowanie tych skanów

1. **Opis skanów dostępnych w wersji Nessus Essential**

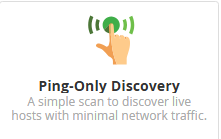
### 🔍 **Host Discovery**



Rysunek 1. Ikona skanu Host Discovery

Prosty skan mający na celu wykrycie aktywnych hostów w sieci oraz otwartych portów. Używany do wstępnego rozpoznania infrastruktury przed pełnym skanowaniem podatności.

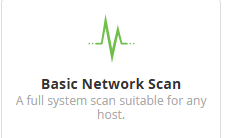
### 📶 **Ping-Only Discovery**



Rysunek 2. Ikona skanu Ping-Only Discovery

Minimalistyczny skan wykrywający tylko aktywne hosty na podstawie odpowiedzi na ping. Nie wykonuje żadnego dalszego zbierania informacji.

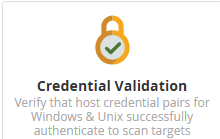
### 📈 **Basic Network Scan**



Rysunek 3. Ikona skanu Basic Network Scan

Pełne skanowanie podatności dla dowolnego hosta. Analizuje systemy pod kątem znanych luk bezpieczeństwa w oprogramowaniu, usługach i konfiguracjach.

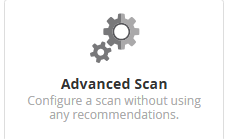
### 🧾 **Credential Validation**



Rysunek 4. Ikona skanu Credential Validation

Weryfikuje, czy podane dane uwierzytelniające do systemów (np. Windows lub Linux) są poprawne i umożliwiają zalogowanie się do systemu w trakcie skanowania.

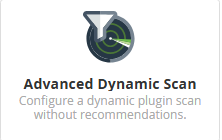
### ⚙️ **Advanced Scan**



Rysunek 5. Ikona skanu Advanced Scan

Zaawansowana konfiguracja skanu bez używania rekomendacji. Pozwala użytkownikowi pełną kontrolę nad zakresem i ustawieniami skanowania.

### 🧬 **Advanced Dynamic Scan**



Rysunek 6. Ikona skanu Advanced Dynamic Scan

Podobny do „Advanced Scan”, ale umożliwia tworzenie dynamicznych polityk skanowania, które dostosowują się do wykrytych systemów i usług – również bez rekomendacji.

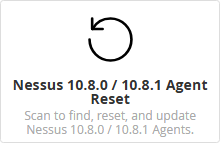
### 🛡️ **Malware Scan**



Rysunek 7. Ikona skanu Malware Scan

Wyszukuje oznaki infekcji złośliwym oprogramowaniem (malware) na systemach Windows i Unix. Przydatny do detekcji zainfekowanych urządzeń.

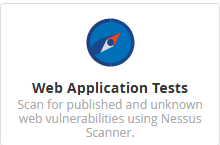
### 🔄 **Nessus 10.8.0 / 10.8.1 Agent Reset**



Rysunek 8. Ikona skanu Nessus 10.8.0 / 10.8.1 Agent Reset

Skanowanie w celu odnalezienia, ponownego przypisania i aktualizacji agentów Nessus w wersjach 10.8.0 i 10.8.1. Dotyczy środowisk wykorzystujących agentów zdalnych.

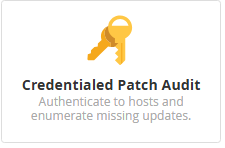
### 🌐 **Web Application Tests**



Rysunek 9. Ikona skanu Web Application Tests

Skanowanie aplikacji webowych w poszukiwaniu znanych podatności – zarówno tych opublikowanych, jak i nieudokumentowanych. Używa mechanizmu Nessus Scanner.

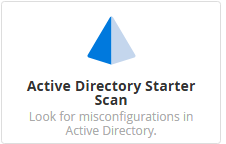
### 🛠️ **Credentialed Patch Audit**



Rysunek 10. Ikona skanu Credentialed Patch Audit

Skanowanie uwierzytelnione, które pozwala ocenić poziom aktualizacji systemu oraz wykryć brakujące poprawki bezpieczeństwa na podstawie logowania do hosta.

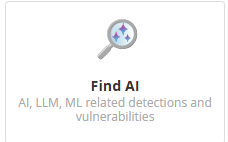
### 🧭 **Active Directory Starter Scan**



Rysunek 11. Ikona skanu Active Directory Starter Scan

Wyszukuje błędy i błędne konfiguracje w środowisku Active Directory. Przydatny do podstawowej analizy bezpieczeństwa domeny Windows.

### 🤖 **Find AI**

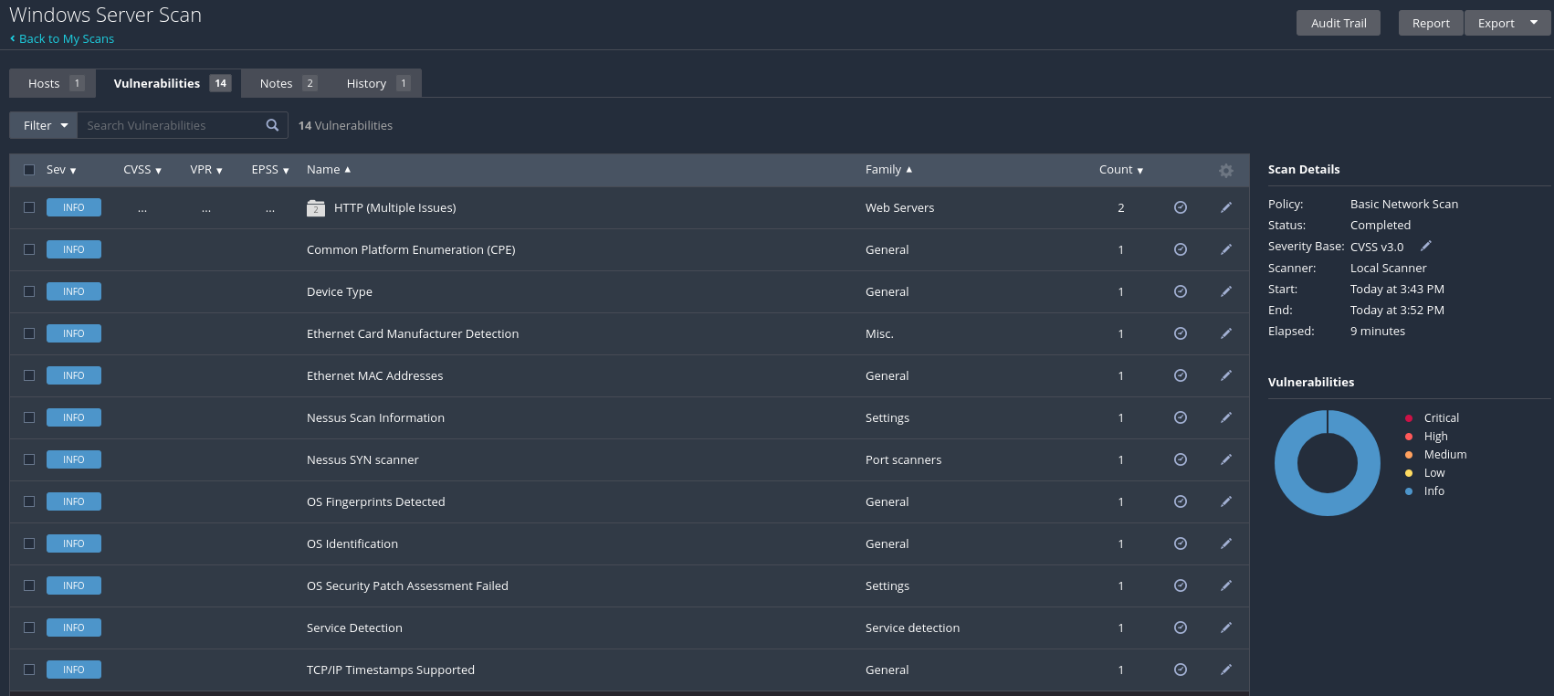


Rysunek 12. Ikona skanu Find AI

Wyszukuje podatności, błędy i detekcje powiązane ze sztuczną inteligencją (AI), uczeniem maszynowym (ML) i przetwarzaniem języka naturalnego (LLM). Nowa, eksperymentalna opcja.

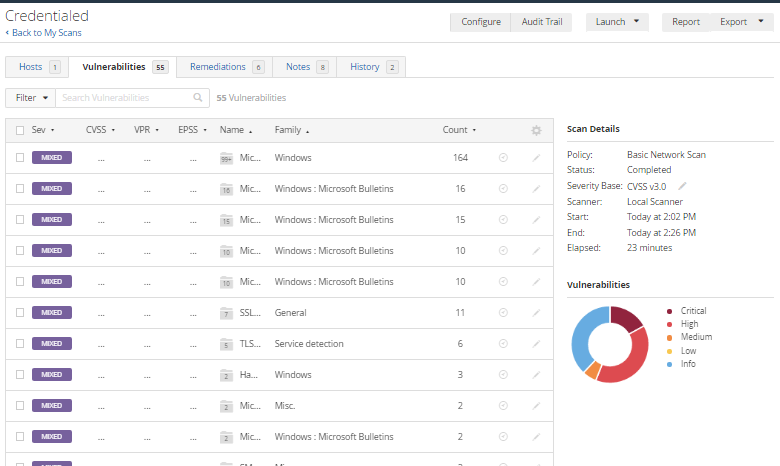
1. **Wdrożenie skanów na maszynie Windows Server 2022**

Wynik skanu *Basic Network Scan* bez uwierzytelnienia:



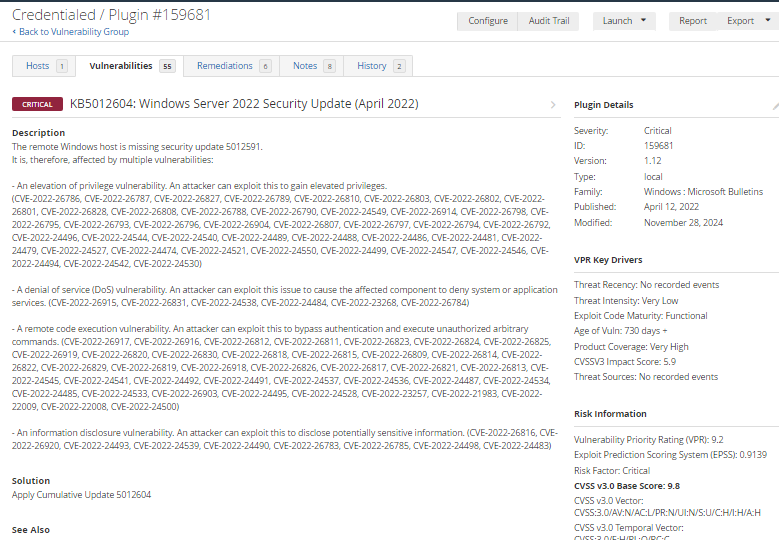
Rysunek 13. Wynik skanu bez uwierzytelnienia maszyny Windows

Wynik skanu *Basic Network Scan* z uwierzytelnianiem:



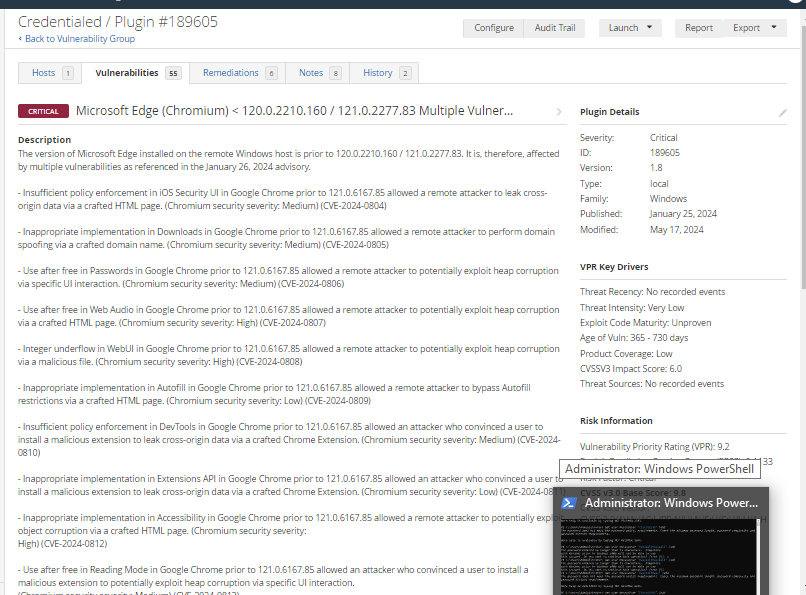
Rysunek 14. Wynik skanu z uwierzytelnieniem maszyny Windows

Sam test bez mis konfiguracji wykrył wiele podatności, między innymi brak aktualizacji bezpieczeństwa.



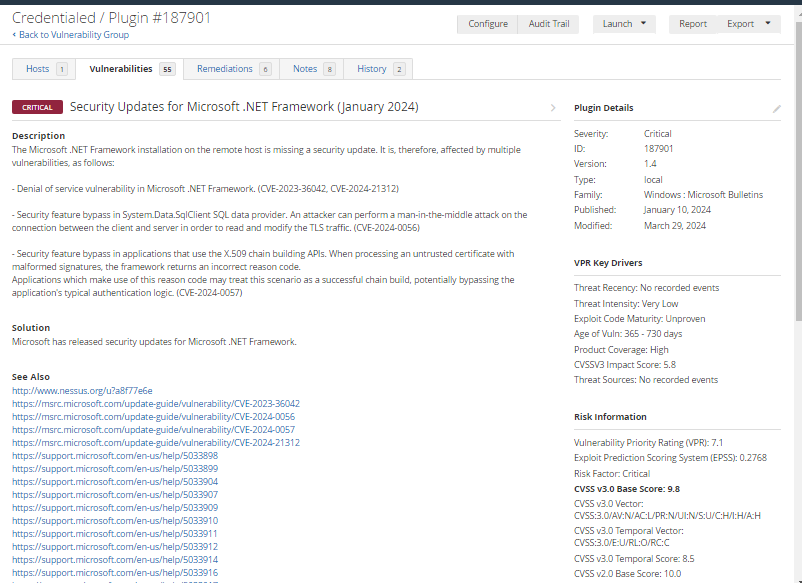
Rysunek 15. Szczegóły podatności o braku aktualizacji bezpieczeństwa

Wykryto także starą wersję Microsoft Edge.



Rysunek 16. Szczegóły podatności o przestarzałej wersji Microsoft Edge

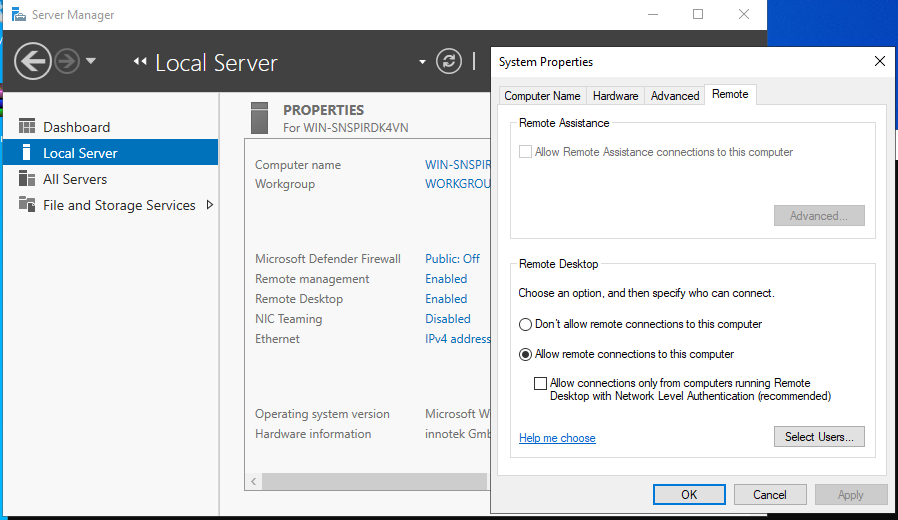
Wykryto brak aktualizacji dla framework’u .NET.



Rysunek 17. Szczegóły podatności o braku aktualizacji dla framework’u NET

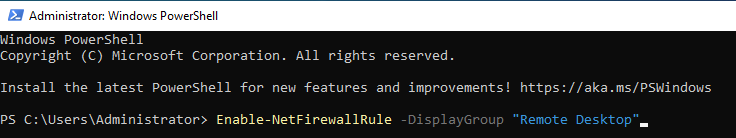
**Następnie celowo wprowadzono poniższe podatności:**

W aplikacji Server Manager włączono opcję pozwalającą na RDP.



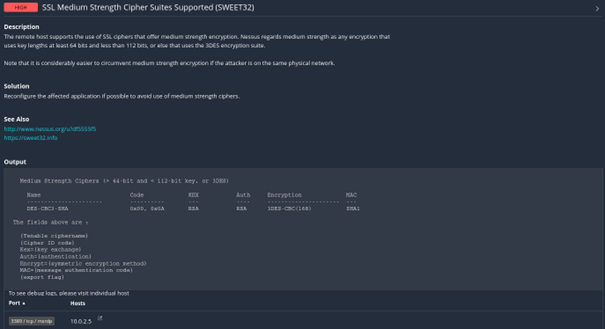
Rysunek 18. Włączenie usługi RDP

Otworzono port zezwalający na RDP.



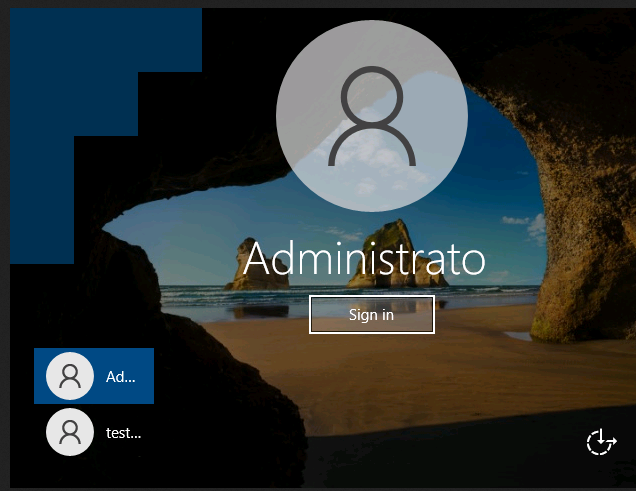
Rysunek 19. Otworzenie portu dla usługi RDP

Narzędzie Nessus wykryło tę podatność:



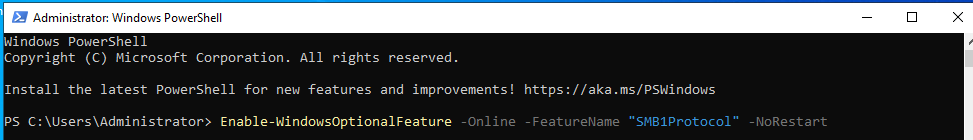
Rysunek 20. Szczegóły podatności o usłudze RDP

Ponadto w raporcie ze skanu znajdował się załącznik, przedstawiajacy próbę logowania do systemu przez RDP.



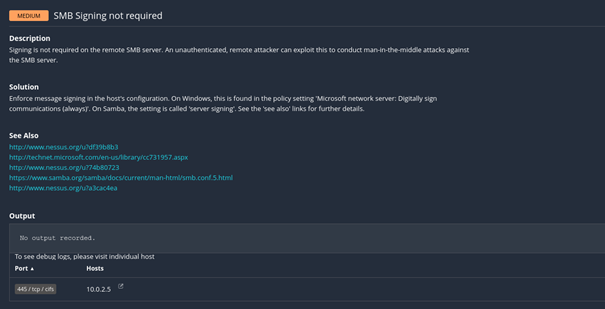
Rysunek 21. Próba logowania przez protokół RDP

Następną wprowadzoną podatnością było uruchomienie przestarzałego protokołu SMBv1.



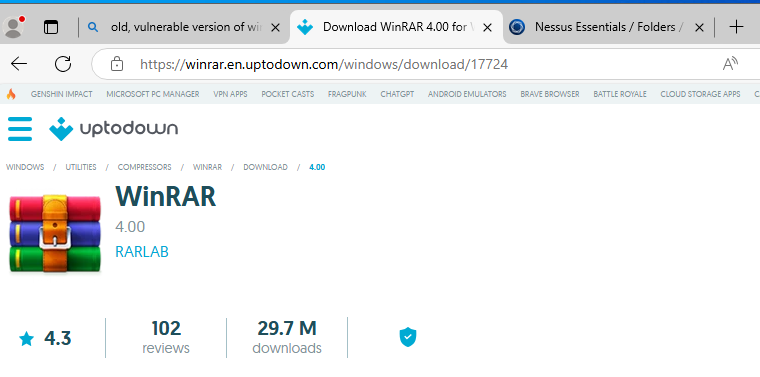
Rysunek 21. Proces uruchomienia protokołu SMBv1

Podatność została wykryta.



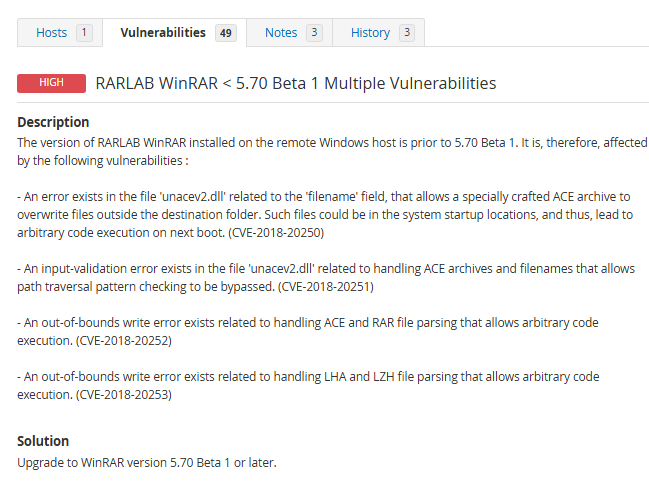
Rysunek 21. Szczegóły podatności o braku wymogu podpisu SMB

Ostatnią wprowadzoną podatnością na maszynie Windows było pobranie starej wersji WinRAR z 2012 roku.



Rysunek 22. Proces instalacji narzędzia WinRAR

Podatność została wykryta.



Rysunek 23. Szczegóły podatności WinRAR

1. **Wdrożenie skanów na maszynie Linux Kali 2025.1**

**Proces instalacji narzędzia Nessus**

Narzędzie Nessus zostało zainstalowane w wersji 10.8.4 dla dystrybucji systemu Linux Debian.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 24. Proces pobierana narzędzia Nessus

**Uruchomienie usługi Nessus**

Obraz zawierający tekst, Czcionka, zrzut ekranu

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 25. Proces uruchomienia usługi Nessus

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, System operacyjny

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 26. Uruchomienie narzędzia Nessus w przeglądarce na porcie 8834

**Skany podatności**

Przed instalacją jakichkolwiek usług na maszynie wirtualnej, przeprowadzony został pierwszy skan podatności w trybie ‘Basic Network Scan’.

Wynik skanu:

Obraz zawierający tekst, zrzut ekranu, Czcionka, krąg

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 27. Wynik pierwszego skanu podatności narzędziem Nessus

Obraz zawierający zrzut ekranu, tekst, oprogramowanie, Oprogramowanie multimedialne

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 28. Szczegóły pierwszego skanu podatności narzędziem Nessus

To zestawienie pokazuje, że Nessus znalazł przede wszystkim zbiór podatności w środowisku Node.js i Java (OpenJDK), krytyczną lukę w Pandas oraz kilka ogólnych problemów związanych z konfiguracją SSL i SSH.

**Skan uwierzytelniony**

Następnie został przeprowadzony uwierzytelniony skan w trybie ‘Advanced Network Scan’.Nie zostały wykryte dodatkowe podatności, lecz w tym rodzaju skanów Nessus zaproponował rozwiązania podatności w zakładce Remediations.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 29. Konfiguracja ustawień skanu uwierzytelnionego

Obraz zawierający tekst, oprogramowanie, Oprogramowanie multimedialne, zrzut ekranu

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 30. Wynik skanu uwierzytelnionego

**Obraz zawierający tekst, zrzut ekranu

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.**

Rysunek 31. Rekomendacje w skanie uwierzytelnionym

**Wprowadzenie podatności**

W następnym etapie celowo wprowadzono podatności, by zweryfikować skuteczność narzędzia Nessus.

**1. Słabe konfiguracje systemowe t.j.:**

- puste hasła użytkowników

- hasło w pliku .bashrc

- pliki z nadanymi uprawnieniami 777

Narzędzie Nessus nie poradziło sobie ze zidentyfikowaniem podatności wynikających ze słabych konfiguracji systemowych. Jest to być może specyfika działania tego programu lub zależność wynikająca z użycia podstawowej, darmowej wersji.

**2. Przestarzała biblioteka jQuery < 3.5.0** (plugin 136929, Severity MEDIUM, CVSS 6.1)

Zainstalowano podatną aplikację, która używa biblioteki jQuery w wersji 1.1.2.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 32. Weryfikacja wersji biblioteki jQuery

Program Nessus zidentyfikował możliwość licznych ataków XSS w skryptach front-endowych.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Strona internetowa

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 33. Szczegóły podatności przestarzałej biblioteki jQuery

**3. Aktywny moduł Apache mod\_status** (plugin 10677, Severity MEDIUM, CVSS 5.3)

Moduł mod\_status został załadowany do konfiguracji i aktywowany.

Obraz zawierający tekst, Czcionka, zrzut ekranu, Grafika

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 34. Weryfikacja konfiguracji Apache

Wykryta została podatność, gdzieEndpoint /server-status ujawnia szczegóły pracy serwera (listę wątków, przetwarzane żądania itp.), co może pomóc atakującemu w późniejszym planowaniu ataku.

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 35. Szczegóły podatności aktywnego modułu Apache

**4. Deafultowa konfiguracja Remote Desktop Protocol Server**

Zainstalwoano narzędzie xrdp w przestarzałej wersji i otwarto port 3389.

Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

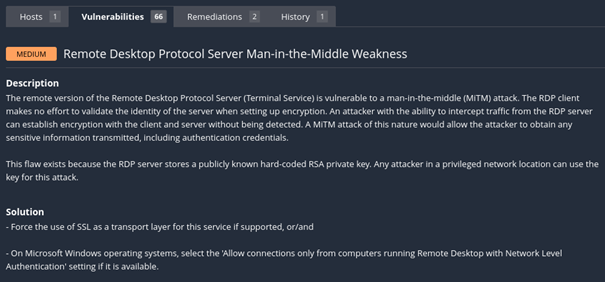
Rysunek 36. Weryfikacja stanu portu 3389

Obraz zawierający tekst, zrzut ekranu, Czcionka

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 37. Dalsza weryfikacja stanu portu 3389

Nessus wykrył podatność wynikająca z faktu, że serwer RDP jest domyślnie skonfigurowany



Rysunek 38. Szczegóły podatności RDP

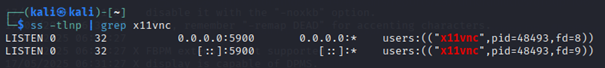
Niektóre z istotnych podatności nie zostały wykryte.

**Niewykryte podatności:**

1. **Podatność dającą zdalne wykonanie kodu (RCE)**

“RCE” w kontekście x11vnc to bypass uwierzytelnienia VNC, który pozwala atakującemu:

Połączyć się bez hasła, wysłać do serwera X11 dowolne polecenia, mieć pełną kontrolę nad pulpitem, czyli zdalne wykonanie kodu.



Rysunek 39. Proces weryfikujący stan portu 5900

1. **EICAR Test File**

EICAR to standardowy, bezpieczny plik testowy wykrywany przez wszystkie rozwiązania antywirusowe. Zawiera on specjalną sygnaturę prawdziwego złośliwego kodu.

Obraz zawierający tekst, Czcionka, zrzut ekranu

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Rysunek 40. Proces pobierania pliku EICAR Test File

1. **Repozytorium theZoo**

Repozytorium theZoo to zbiór realnych próbek malware – Nessus w standardowym Advanced Scan go nie „fingerprintuje” jako całości, tylko bada pojedyncze pliki pod kątem sygnatur antywirusowych.



Rysunek 41. Proces klonowania repozytorium theZoo

Powyższe podatności nie zostały wykryte najprawdopodobniej przez brak aktywowanych niektórych pluginów. W wykorzystanej podczas testów wersji apliakcji **Nessus Essentials 10.8.4** nie udostępniono między innymi pluginów **Discovery** oraz **Antivirus and Malware Detection**.

**5. Wnioski**

Wersja Essentials (10.8.4) oferuje pełne host‐ i port‐scanning oraz wykrywanie wielu krytycznych podatności na Windows i Linux. Brakuje jednak kluczowych grup pluginów.

Zidentyfikowany został nieaktualny software, webowe luki oraz ogólne problemy z SSL/SSH. Dodatkowo skan Adanced Network Scan pozwolił na wygenerowanie Remediations, ułatwiając planowanie działań naprawczych. Brak wykrycia pseudo-malware i RCE w x11vnc wynikał nie z błędów konfiguracji środowiska, lecz z ograniczeń edycji Essentials.

W celu dokładnej weryfikacji działania narzędzia Nessus niezbędny byłby dostęp do płatnej wersji Professional.