Analiza SWOT rozwiązań niekomercyjnych

OpenVAS

Zalety	Wady
Mocne strony: • Darmowy • Open-source • Możliwość skanowania lokalnego oraz sieciowego • Wsparcie wielu protokołów – możliwość skanowania różnych typów systemów i aplikacji • Możliwość generowania szczegółowych raportów z wynikami skanu – ułatwienie analizy	**Słabe strony:** • Dość skomplikowany interfejs • Skany bywają czasochłonne
Szanse: • Aktywna społeczność – ciągły rozwój narzędzia, nowe funkcje • Integracja z innymi narzędziami i platformami – lepsze wykorzystanie i integracja z istniejącą infrastrukturą	**Zagrożenia:** • Ograniczenie popularności oraz rozpowszechniania przez konkurencję na rynku • Wymaganie ciągłych aktualizacji i śledzenia nowych podatności, aby utrzymać skuteczność

OWASP ZAP

Zalety	Wady
Mocne strony: • Open-source • Darmowy • Aktywnie rozwijany przez społeczność • Interaktywny interfejs użytkownika – łatwiejsze korzystanie z narzędzia • Możliwość dostosowania kodu do konkretnych potrzeb • Bogaty w funkcje	**Słabe strony:** • Zdalne sterowanie aplikacji webowych może być czasochłonne oraz generować duże ilości danych, co może wpłynąć na wydajność • Wymagane doświadczenie i wiedza techniczna, aby w pełni wykorzystać zaawansowane funkcje skanowania i poprawnie interpretować wyniki
Szanse: • Potencjalne zwiększenie wartości i skuteczności dzięki społeczności • Możliwość skanowania aplikacji i wdrażania poprawek w czasie rzeczywistym	**Zagrożenia:** • Ograniczenie popularności oraz rozpowszechniania przez konkurencję na rynku • Wymaganie ciągłych aktualizacji i śledzenia nowych podatności, aby utrzymać skuteczność

Nikto

Zalety	Wady
Mocne strony: • Bogata baza danych ze znanymi podatnościami i lukami w zabezpieczeniach • Darmowe narzędzie - dostępne dla każdego • Prosty w obsłudze i intuicyjny • Stałe aktualizacje i poprawki do skanera – w celu uwzględnienia nowych podatności i poprawy wydajności	**Słabe strony:** • Możliwość pominięcia najnowszych lub nieznanych podatności, które mogą być wykorzystywane przez atakującego • Skoncentrowany tylko na protokołach HTTP i HTTPS – nie jest skuteczny w wykrywaniu podatności w innych protokołach • Możliwość zgłaszania fałszywie pozytywnych wyników - sygnalizowanie istnienia podatności, które w rzeczywistości nie istnieją
Szanse: • Potencjalny rozwój i dodawanie nowych funkcji do skanera takich jak wsparcie dla innych protokołów, integracja z innymi narzędziami • Możliwość integracji z innymi narzędziami i frameworkami bezpieczeństwa - zwiększa to użyteczność i skuteczność	**Zagrożenia:** • Rosnąca ilość narzędzi i technologii defensywnych może spowodować, ze atakujący będzie omijać skaner Nikto - może to ograniczyć jego skuteczność • Ewolucja technik ataku – opracowywanie nowych technik ataku • Skoncentrowany głównie na statycznych stronach internetowych, możliwość trudności z wykrywaniem podatności w bardziej dynamicznych aplikacjach internetowych, takich jak aplikacje oparte na JavaScript

W3af

Zalety	Wady
Mocne strony: • Open-Source • Szeroki zakres funkcji skanowania aplikacji webowych • Interfejs graficzny • Możliwość dodania własnych wtyczek i skryptów – dostosowanie do indywidualnych potrzeb	**Słabe strony:** • Interfejs wymaga nauki – może być skomplikowany dla początkujących użytkowników • Ograniczony zakres funkcji - mniej wszechstronny niż komercyjne narzędzia
Szanse: • Potencjał do dalszego rozwoju dzięki społeczności • Możliwość skanowania aplikacji i wdrażania poprawek w czasie rzeczywistym	**Zagrożenia:** • Ograniczenie popularności oraz rozpowszechniania przez konkurencję na rynku • Wymaganie ciągłych aktualizacji i śledzenia nowych podatności, aby utrzymać skuteczność

Lynis

Zalety	Wady
Mocne strony: • Szeroki zakres funkcjonalności modułów do analizy bezpieczeństwa - skanowanie podatności, konfiguracja systemu, monitorowanie integralności plików • Zaprojektowany w sposób modułowy - pozwala to na elastyczne dostosowanie i konfigurację narzędzi do konkretnych potrzeb i środowiska • Wieloplatformowy i obsługuje różne systemy operacyjne np. Linux, macOS, BSD – użyteczny dla wielu środowisk • Zaawansowane opcje konfiguracyjne, które umożliwiają dostosowanie skanera do specyficznych wymagań	**Słabe strony:** • Złożoność dla niedoświadczonych użytkowników • Proces analizy może być czasochłonny ze względu na szeroki zakres skanowania w szczególności dużych środowisk
Szanse: • Potencjał do dalszego rozwoju dzięki społeczności • Możliwość skanowania aplikacji i wdrażania poprawek w czasie rzeczywistym	**Zagrożenia:** • Ograniczenie popularności oraz rozpowszechniania przez konkurencję na rynku • Wymaganie ciągłych aktualizacji i śledzenia nowych podatności, aby utrzymać skuteczność

Wapiti

Zalety	Wady
Mocne strony: • Open-source • Prosty interfejs • Łatwa składnia • Możliwość skanowania aplikacji webowych • Dostosowanie do potrzeb poprzez parametryzowanie skanu i filtrowanie wyników	**Słabe strony:** • Ograniczony zakres funkcji - mniej wszechstronny niż komercyjne narzędzia • Mniejsza automatyzacja – wymaganie większego zaangażowania użytkownika • Możliwość generowania fałszywie pozytywnych wyników
Szanse: • Potencjał do dalszego rozwoju dzięki społeczności • Możliwość skanowania aplikacji i wdrażania poprawek w czasie rzeczywistym	**Zagrożenia:** • Ograniczenie popularności oraz rozpowszechniania przez konkurencję na rynku • Wymaganie ciągłych aktualizacji i śledzenia nowych podatności, aby utrzymać skuteczność

OpenSCAP

Zalety	Wady
Mocne strony: • Open-source • Wsparcie dla wielu standardów – możliwość kompleksowej oceny zabezpieczeń systemów • Możliwość skanu systemów operacyjnych, aplikacji i konfiguracji • Możliwość generowania szczegółowych raportów z wynikami skanu – ułatwienie analizy i podjęcia odpowiednich działań	**Słabe strony:** • Skomplikowany interfejs • Czasochłonna konfiguracja i dostosowanie do wymagań i środowisk
Szanse: • Potencjał do dalszego rozwoju dzięki społeczności • Możliwość skanowania aplikacji i wdrażania poprawek w czasie rzeczywistym • Zwiększające się zapotrzebowanie organizacji na narzędzia pomagające w audytach i identyfikacji podatności	**Zagrożenia:** • Ograniczenie popularności oraz rozpowszechniania przez konkurencję na rynku • Wymaganie ciągłych aktualizacji i śledzenia nowych podatności, aby utrzymać skuteczność

Nmap

Zalety	Wady
Mocne strony: • Wszechstronny - różnorodne tryby skanowania • Skalowalność i wydajność - skalowalność zarówno małych jak i dużych sieci • Wieloplatformowy i obsługuje różne systemy operacyjne np. Linux, macOS, Windows – użyteczny dla wielu środowisk • Rozwijany – aktualizacja narzędzia, dodawanie nowych funkcjonalności i rozwijanie problemów	**Słabe strony:** • Złożoność dla niedoświadczonych użytkowników • Wykrywany prze niektóre systemu obronne - niektóre systemy zabezpieczeń sieciowych mogą wykrywać aktywność skanowania Nmap i podejmować działania w celu utrudnienia lub zablokowania skanowania
Szanse: • Potencjał do dalszego rozwoju dzięki społeczności • Możliwość integracji z innymi narzędziami i frameworkami bezpieczeństwa - zwiększa to użyteczność i skuteczność	**Zagrożenia:** • Ewolucja technik obronnych - systemy zabezpieczeń sieciowych i oprogramowanie firewall rozwijają się, aby lepiej wykrywać i blokować aktywność skanowania • Korzystanie z Nmap w sposób nielegalny lub nieetyczny może narazić użytkownika na odpowiedzialność prawną i negatywną opinię publiczną.