Oferta na przeprowadzenie testów penetracyjnych wewnętrznych i zewnętrznych usług sieciowych oraz aplikacji webowych

Oferujemy przeprowadzenie testów penetracyjnych wewnętrznych i zewnętrznych usług sieciowych oraz aplikacji webowych. Większość usług przeprowadzamy zdalnie. Testy penetracyjne usług sieciowych z wnętrza sieci możemy przeprowadzić również na miejscu u Klienta.

Proponowane usługi

Testy penetracyjne zewnętrznych usług sieciowych

Założenia podstawowe:

- Praca wykonywana jest zdalnie

Wynik końcowy:

- Przygotowany raport opisany w dalszej części
- Przeprowadzone testy zgodnie z opisem wskazanym poniżej – dla infrastruktury.

Wycena:

Wariant 1:
limit do 3 adresów IP lub 5 usług (typu poczta, strona www, usługa ftp, itp.): 6600 PLN netto
Wariant 2:
limit do 5 adresów IP lub 10 usług (typu poczta, strona www, usługa ftp, itp.): 8800 PLN netto
Wariant 3:
limit do 10 adresów IP lub 20 usług (typu poczta, strona www, usługa ftp, itp.): 12000 PLN netto

Testy penetracyjne usług sieciowych przeprowadzane z wnętrza sieci

Założenia podstawowe:

- Praca wykonywana jest zdalnie

Wynik końcowy:

- Przygotowany raport opisany w dalszej części
- Przeprowadzone testy zgodnie z opisem wskazanym poniżej – dla infrastruktury.

Wycena:

Wariant 1:
limit do 50 adresów IP: 8800 PLN netto
Wariant 2:
limit do 100 adresów IP: 14000 PLN netto
Wariant 3:
limit do 200 adresów IP: 20000 PLN netto

Testy penetracyjne usług sieciowych przeprowadzane z wnętrza sieci

Założenia podstawowe:

- Praca wykonywana jest na miejscu u Klienta

Wynik końcowy:

- Przygotowany raport opisany w dalszej części
- Przeprowadzone testy zgodnie z opisem wskazanym poniżej – dla infrastruktury.

Wycena:

Wariant 1:
limit do 50 adresów IP: 14000 PLN netto
Wariant 2:
limit do 100 adresów IP: 19000 PLN netto
Wariant 3:
limit do 200 adresów IP: 26000 PLN netto

Testy penetracyjne aplikacji webowej

Założenia podstawowe:

- Praca wykonywana jest zdalnie

Wynik końcowy:

- Przygotowany raport opisany w dalszej części
- Przeprowadzone testy zgodnie z opisem wskazanym poniżej – dla aplikacji webowych.

Wycena:

Wariant 1:
testowanie strony z zewnątrz + testy modułu logowania: 4800 PLN netto
Wariant 2:
limit do 3 różnych ról i maks 10 formularzy: 8800 PLN netto
Wariant 3:
limit do 3 różnych ról i maks 20 formularzy: 12000 PLN netto
Wariant 4:
limit do 5 różnych ról i maks 50 formularzy: 20000 PLN netto

Opis prac realizowanych dla infrastruktury

W ramach przeprowadzonych testów dla infrastruktury wykonywane są następujące prace:

Krok 1:

Ustalany zostaje z Zamawiającym, zakres infrastruktury, dla której przeprowadzone są testy

Krok 2:

Konsultanci zbierają samodzielnie informację na temat badanego środowiska i komponentów IT

Krok 3:

Zostają zidentyfikowane działające usługi, porty, typy i wersje działającego oprogramowania

Krok 4:

Przeprowadzona jest analiza znanych podatności z wykorzystaniem narzędzi automatycznych

Krok 5:

Przeprowadzona jest manualna weryfikacja wskazanych przez aplikacje podatności krytycznych. Potwierdzane lub odrzucane jest ich istnienie.

Krok 6:

Przeprowadzone są kontrolowane ataki na infrastrukturę teleinformatyczną i usługi w postaci:

- próby uzyskania dostępu do komponentów z wykorzystaniem domyślnych i słabych haseł oraz tych, które zostały stworzone na podstawie zapoznania się z infrastrukturą Klienta
- za zgodą Klienta wykonywane są próby wykorzystania krytycznych podatności przy użyciu narzędzi typu exploit

Prace te są wykonane w oparciu o wyżej wskazane metodyki i będą dotyczyły między innymi:

Zbierania informacji o badanym środowisku (Rekonesans)

Zbieranie informacji obejmuje zbieranie wszelkich możliwych informacji dotyczących badanych elementów środowiska. W większości przypadków głównym źródłem informacji jest Internet. Internet może dostarczyć informacji o celu przy użyciu kilku metod, zarówno technicznych (np. DNS / WHOIS) i nietechnicznych (wyszukiwarki, grupy dyskusyjne, listy mailingowe, itp.). Jest to wstępny etap każdego audytu bezpieczeństwa informacji, który jest często pomijany. Podczas wykonywania jakichkolwiek testów w systemie informacyjnym, zbieranie informacji i eksploracja danych jest niezbędna, i dostarcza wszystkich możliwych informacji w celu poprawnego realizowania prac. Informacje mogą być zbierane w następujący sposób:

- Zlokalizowanie obecności badanego elementu w sieci docelowej
- Uzyskanie informacji od rejestratora domeny np. w sposób:
- Sprawdzić obecność w DNS
- Zobaczyć więcej informacji w DNS
- Sprawdzić Spam przeglądania bazy danych
- Sprawdzić informacje w WHOIS

Analizy działających usług, otwartych portów

W dalszej części dla badanych elementów infrastruktury przeprowadzana jest analiza działających usług oraz otwartych portów. Podczas tego etapu realizacji prac dokonywana jest również enumeracja, to znaczy zdobywana jest informacja na temat działającego systemu, jego wersji, zdobywana jest wiedza na temat działających usług, ich nazw, oraz wersji. Prace te mogę być wykonywane przy wykorzystaniu poniższych metod:

- Sprawdzenie dostępności hosta skanem ICMP
- Skanowanie portów TCP
- Skanowanie portów UDP
- Skanowanie SYN, ACK, FIN, XMAS, UDP, NULL
- Skanowanie FIN/ACK

- Analiza odpowiedzi ARP
- Weryfikacja dostępnych ścieżek sieci - TRACEROUTE
- Fingerprinting – uzyskanie informacji o systemie oraz usługach jakie są zainstalowane
    - Banner grabbing,
    - Bogus Flag Probe test
    - ISN Sampling
    - Analiza czasu życia pakietu (Time To Live)
    - Analiza pakietów HTTP, TCP

Analizy znanych podatności

Celem tego etapu jest wykorzystanie informacji zebranych wcześniej do technicznej oceny rzeczywistego istnienia luk w zabezpieczeniach. Analiza podatności odbywa się za pomocą narzędzi automatycznych, wspierana jest pracami ręcznymi, i ma za zadanie zweryfikować ogólnie znane, opublikowane podatności, jak np. podatności XSS, SQL injection, Fuzzing, lokalizowania słabych haseł. Aplikacja automatyczna w krótkim czasie jest w stanie zweryfikować kilka tysięcy podatności dotyczących wielu popularnych usług jak np.:

- ftp
- telnet, SSH
- bazy danych sql
- aplikacje webowe
- system pocztowy
- zarządzanie przez SNMP, WMI
- usługi uwierzytelniania
- itp.

Penetracji słabości

Etap związany z penetracją słabości polega na próbie uzyskania nieautoryzowanego dostępu do usługi bądź badanego elementu. Realizuje się go np. poprzez obejście zastosowanych zabezpieczeń lub wykorzystaniu wcześniej wykrytych podatności. Etap penetracji polega na:

- Znalezieniu dowodu (proof of concept). To znaczy, polega na udowodnieniu możliwości nadpisania danego oprogramowania, wprowadzenia do niego zmian, otrzymania z serwisu danych niedostępnych dla danego użytkownika, uzyskania uprawnień autoryzowanego użytkownika, wykonania operacji niedozwolonej, itp.

Większość wymienionych wyżej zagrożeń możliwa jest do wykonania za pomocą programów (Exploitów) wykorzystujących podatności, takie jak m.in.:

- Niewłaściwe prawa dostępu - wykorzystanie niewłaściwych ustawień praw dostępu do usług i informacji,

- Atak na hasła (np. RAS, VPN) - próba uzyskania dostępu do systemu poprzez podawanie haseł w formie kolejnych kombinacji znaków (brute force), wykorzystanie słownika haseł, bądź tzw. słabych haseł (specyficznych dla określonych systemów),
- Przepełnienie bufora - doprowadzenie do przepełnienia bufora aplikacji połączone z wprowadzeniem do bufora odpowiedniego kodu (np. poleceń systemowych) i uruchomienie tego kodu
- Specyficzne Exploits - uzyskanie nieupoważnionego dostępu do usług i informacji serwera sieciowego poprzez wykorzystanie specyficznych błędów tego serwera,
- Niestabilność systemu (ang. race condition) - próba uzyskania dostępu do systemu poprzez wykorzystanie tymczasowej niestabilności systemu.

Podczas realizowania prac Wykonawcy, Zlecający zapewni dostęp do audytowanych systemów do czasu zakończenia prac przez konsultantów strony Wykonującej. Zlecający zadba również o to, aby podczas realizowanych prac środowisko i aplikacje nie ulegało zmianom.

Opis prac realizowanych dla aplikacji webowych

Wszystkie testy aplikacji webowych przeprowadzane są w dwóch wariantach.

Pierwszy wariant zakłada, że osoby testujące nie posiadają danych do zalogowania się do aplikacji webowej i wykorzystują dostęp użytkownika bez uprawnień. Testują również moduł zabezpieczeń.

Drugi wariant zakłada, że testy realizowane są po zalogowaniu się użytkownika do aplikacji. Testy wykonane są z wnętrza aplikacji, w tym między innymi testowany jest sposób autoryzacji użytkowników, próba wykonania operacji przez użytkowników danej roli a możliwej do wykonania tylko dla użytkowników innej roli, itp.

Pełen zakres prac jakie realizujemy przedstawia opis OWASP dostępny pod adresem:
https://wiki.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

Wykonywane są wszystkie zalecenia tam przedstawione. Jest to bardzo szczegółowy opis, który między innymi zawiera takie prace jak:

- Zbieranie informacji o portalu ze źródeł zewnętrznych (Internet)
- Przegląd konfiguracji i sposobu zarządzania
- Test modułów zrządzania dostępem
- Testy autentykacji i autoryzacji
- Testowanie sesji użytkowników
- Próby wstrzyknięcia złośliwego kodu
- Sprawdzenie obsługi błędu i weryfikacja logiki działania portalu
- Błędy objawiające się po stronie klienta

Aplikacja webowa weryfikowana jest również pod względem posiadania podatności z listy OWASP TOP 10. https://owasp.org/www-project-top-ten/

Dodatkowo na życzenie Klienta - bez dodatkowych kosztów – wykryte zagrożenia przedstawione są w raporcie ASVS 3 dla wskazań aplikacji poziomu nr 1. Wskazane są informacje czy dana wytyczna została spełniona czy też nie jest jeszcze spełniona ze wskazaniem powodu, dlaczego.

Więcej informacji na temat standardu ASVS 3 dostępnych jest tutaj: https://www.owasp.org/images/d/d1/OWASP_Application_Security_Verification_Standard_3.0.1_PL.pdf

Wyniki przedstawiane są w postaci tabeli.

Raport

W wyniku przeprowadzonych prac sporządzony zostanie raport końcowy, zawierający wszystkie wyniki i wnioski zebrane podczas przeprowadzonego testu. Sporządzony dokument będzie zawierał:

- **Cel i zakres projektu** – określenie celu i zakresu audytu,
- **Podstawę formalną** – podstawę formalną, według której zostały przeprowadzone prace
- **Podsumowanie dla kierownictwa** - podsumowanie dla kierownictwa najważniejszych wyników i wniosków
- **Zakres prac** – wskazany zakres prac, jaki został przeprowadzone
- **Zastosowaną metodologię** – informacje na temat metodologii oraz sposobów, jakimi konsultanci realizowali prace
- **Rezultaty** - w postaci konwencji oceniania, opisu, w jaki sposób zostały przygotowane wyniki
- **Wyniki szczegółowe** - wyniki uzyskane w trakcie przeprowadzania testów z opisem, czterostopniowym poziomem zagrożenia oraz rekomendacjami ze strony Wykonawcy
- **Załączniki** – dokumenty i materiały uzyskane w trakcie wykonywania prac

Informacje o wykrytych błędach krytycznych infrastruktury lub procesu będą zgłaszane Zamawiającemu w trybie natychmiastowym.

Kategoryzacja wyników i konwencje oceniania

Główną częścią składową raportu będzie lista wykrytych podatności w systemie wraz ze wskazaniem sugerowanych rekomendacji. Wyniki uzyskane w trakcie przeprowadzania testów podzielone zostaną zgodnie z czterostopniową skalą zagrożenia, wyrażoną w kolorach:

Critical (Krytyczna)	Podatność łatwa do wykorzystania i o bardzo dużym wpływie na bezpieczeństwo, może ją wykorzystać każdy użytkownik mający dostęp do badanego elementu.
High (Wysoka)	Podatność trudniejsza do wykorzystania lub wymagająca wykonania dodatkowej akcji po stronie użytkownika, administratora, systemu ale o bardzo dużym wpływie na bezpieczeństwo.
Medium (Średnia)	Podatność o średnim prawdopodobieństwie wykorzystania lub średnim wpływie na bezpieczeństwo.
Low (Niska)	Podatność o niskim prawdopodobieństwie wykorzystania lub niskim wpływie na bezpieczeństwo, często jednak pozwalająca atakującemu poznać informacje pozwalające dobrać odpowiednie wektory ataku służące dalszej penetracji usługi
Info (Informacyjna)	Wiadomość informacyjna, niemająca wpływu na bezpieczeństwo

Każda ze znalezionych podatności otrzyma numer identyfikacyjny. Podatności zostaną dokładnie opisane, wskazane zostaną zagrożenia wraz z dowodem potwierdzającym wystąpienie błędu. Dla wszystkich poziomów zagrożeń wskazane zostaną rekomendacje, przy czym dla niskiej podatności można będzie je odbierać, jako wskazówka do tworzenia przyszłych środowisk o podobnym charakterze. Podatności zostaną umieszczone w tabelce według wzoru:

Skala zagrożenia	ID 1. Błąd opisany w temacie
	Opis podatności:
	Informacje o miejscu występowania podatności:
	Dowód istnienia podatności:
	Rekomendacje usuwające podatność:

Wskazane w opiniach rekomendacje mają charakter pomocniczy. Organizacje przed ich wdrożeniem muszą się upewnić, że zalecane rozwiązanie jest tym rozwiązaniem, które będzie najlepsze. Dokonaną zmianę zalecamy najczęściej wykonać na środowisku testowym i dopiero po przeprowadzonych testach, gdy wyniki działania będą prawidłowe wdrożyć je na systemach produkcyjnych.

Standardy i zasady pracy konsultantów

Realizując prace dla naszych Klientów bierzemy zawsze pod uwagę obowiązujące standardy i dobre praktyki bezpieczeństwa IT opisane w międzynarodowych metodykach:

- ISO 27000 (norma międzynarodowa standaryzująca systemy zarządzania bezpieczeństwem informacji)
- PCI DSS (Payment Card Industry Data Security Standard)
- OSSTM Manual (Open Source Security Testing Methodology Manual)
- ISSAF (OISSG Penetration Testing Framework)
- NIST (National Institute of Standards and Technology)
- SANS Information Security Reading Room
- The Social Engineering Framework

Do najważniejszych z nich możemy zaliczyć:

- Konsultant przestrzega bezpieczeństwa, prywatności zdobytych danych
- Konsultant działa zawsze zgodnie z obowiązującym lokalnym prawem
- Konsultant zawiadamia osoby wskazane o rozpoczęciu przeprowadzania prac
- Konsultant przeprowadza testy w pierwszej kolejności bez jakikolwiek uprawnień, nawet, gdy posiada takowe przed rozpoczęciem testów.
- Konsultant wykorzystuje narzędzia tak, aby nie wprowadzić szkód w badanym środowisku
- Konsultant w przypadku wykonania testów, które mogą spowodować uszkodzenie działania usługi lub jej unieruchomienie, wykonuje je uzyskując wcześniej zgodę Zlecającego

Na każdym etapie prac postępujemy według obowiązujących u Klienta standardów biorąc pod uwagę dostępność, integralność oraz poufność przetwarzanych informacji przez testowane systemy.

- **Poufność** (confidentiality) - właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
- **Integralność** (integrity) - właściwość zapewnienia dokładności i kompletności aktywów.
- **Dostępność** (availability), zwana też dyspozycyjnością - jest zdefiniowana, jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne

Przeprowadzając testy socjotechniczne wykorzystujemy wiedzę z zakresu psychologii społeczne, a w szczególności reguł:

- reguła wzajemności (otrzymaliśmy coś za darmo, powinniśmy się odwdzięczyć)

- reguła konsekwencji (kiedyś obiecywałeś, że tak zrobisz w takiej sytuacji)
- reguła sympatii (osoby które znamy, które darzymy zaufaniem)
- wpływ autorytetu (wysokie stanowiska w firmie, w Państwie)
- społeczny dowód słuszności (bo wszyscy tak robią)
- reguła niedostępności (jeżeli coś jest trudno osiągalne, to na pewno jest dobre)
- reguła zaangażowania i konsekwencji (jeżeli coś już tyle czasu robiliśmy, należy do ukończyć)

Nasze doświadczenie pozwala przeprowadzić prace na najwyższym możliwym poziomie.