

Zadanie: Testy penetracyjne systemów informatycznych

Założenia ogólne

A)

1. Przedmiotem zamówienia jest przeprowadzenie 5 testów dedykowanych penetracyjnych dla wybranych przez zamawiającego usług on-line świadczonych przez Urząd, 1 zewnętrzny test penetracyjny horyzontalny black-box dla całej zewnętrznej adresacji IP, którą dysponuje Zamawiający oraz 1 testu horyzontalnego white-box dla wybranej przez Zamawiającego wewnętrznej infrastruktury teleinformatycznej.
2. Test dedykowany ma przyjąć postać zasymulowania zachowania realnego atakującego próbującego złamać zabezpieczenia pojedynczej usługi on-line świadczonej przez urząd.
3. Test horyzontalny black-box ma przyjąć postać zasymulowania zachowania realnego atakującego wykonującego rekonesans dostępnych usług świadczonych przez Zamawiającego mający na celu wykrycie luk bezpieczeństwa we wszystkich usługach udostępnionych przez Zamawiającego.
4. Test horyzontalny white-box ma przyjąć postać zasymulowania zachowania realnego atakującego, który uzyskał dostęp do wewnętrznej infrastruktury teleinformatycznej Zamawiającego.
5. Testy będą wykonywane do 31.05.2026 r. zgodnie z ustalonym po podpisaniu umowy harmonogramem realizacji usług.
6. Harmonogram realizacji Usług musi w szczególności określać terminy wykonywania testów oraz skład zespołu testerów.
7. Usługa będzie realizowana na podstawie zawartej umowy.

B) Dedykowany test penetracyjny

1. Pojedynczy dedykowany test penetracyjny usługi on-line świadczonej przez Zamawiającego obejmować będzie symulację zachowania prawdziwego atakującego które ma na celu wykrycie i wykorzystanie znalezionych luk bezpieczeństwa do przełamania zabezpieczeń bezpieczeństwa i infiltracji środowiska IT Zamawiającego.
2. Test musi umożliwić wykrycie:
 - obecności znanych błędów i luk w urządzeniach sieciowych i oprogramowaniu,
 - możliwości omijania wdrożonych systemów zabezpieczeń,
 - podatności systemu na rozpowszechnianie złośliwego oprogramowania,
 - możliwości uzyskania nieautoryzowanego dostępu do przetwarzanych informacji,
 - możliwości manipulacji świadczonymi usługami,

- podatności związanych z zastosowanymi technologiami i architekturą aplikacji webowych, a także z zastosowanymi serwerami aplikacyjnymi oraz bazodanowymi,
 - podatności związanych z mechanizmami uwierzytelniania oraz walidacją danych wejściowych.
3. Zamawiający określi Wykonawcy adres www pod którą dostępna jest usługa.
 4. Przedmiotem pojedynczego dedykowanego testu penetracyjnego będą wszystkie ewentualne moduły usługi świadczonej pod wskazanym adresem
 5. Wskazane aplikacje oraz/lub strona www zostaną przetestowane automatycznymi narzędziami służącymi do poszukiwania podatności w sposób nie wpływający na ich ciągłość pracy.
 6. Testy wskazanej usługi zostaną uzupełnione o testy manualne poszukiwania błędów umożliwiających dostęp do infrastruktury lub bazy danych oraz nieautoryzowaną publikację treści. Uzupełnienie manualne nie powinno przekroczyć 7 dni.
 7. Wyniki skanowania zostaną przedstawione w postaci raportu zawierającego:
 - opis wykonanych testów,
 - klasyfikację i szczegółowy opis istniejących podatności oraz zagrożeń z nimi związanych. Opracowanie takie należy stworzyć dla podatności sklasyfikowanych jako średnie, krytyczne i wysokie wg. metodologii CVSSv3.
 - określenie w sposób szczegółowy sugerowanych sposobów usunięcia wykrytych podatności
 8. Wykonawca przedstawi raport i omówi go w sposób techniczny w siedzibie zamawiającego lub za zgodą Zamawiającego w formie telekonferencji.
 9. Zamawiający oczekuje ponownych testów określających skuteczność usunięcia wykrytych podatności w czasie określonym umową.
 10. Po wykonaniu ponownych testów sprawdzających Wykonawca w kolejnej wersji raportu określi skuteczność usunięcia podatności.

C) Horyzontalny test penetracyjny black-box

1. Pojedynczy horyzontalny test penetracyjny black-box obejmować będzie symulację zachowania prawdziwego atakującego wykonującego skanowanie zewnętrznej adresacji IP Zamawiającego, które ma na celu wykrycie i wykorzystanie znalezionych luk bezpieczeństwa do przełamania zabezpieczeń bezpieczeństwa i infiltracji środowiska IT Zamawiającego.
2. Zamawiający przekaze Wykonawcy pulę adresacji IP która ma stanowić zakres testu
3. Atak na wewnętrzną sieć Zamawiającego będzie prowadzony w wariancie otwartym, co oznacza, że Wydział IT Zamawiającego będzie wiedział o teście i nie będzie próbował aktywnie przeciwdziałać atakowi. Strony będą wzajemnie informować się o ryzykach związanych z zakłóceniem ciągłości działania procesów Zamawiającego.

4. Podczas testu wszystkie systemy bezpieczeństwa posiadane przez Zamawiającego pozostaną włączone
5. Wykonawca przygotowuje raport z przeprowadzonego testu z pełną inwentaryzacją stanu usług świadczonych w badanej adresacji, wykrytych podatności, wraz z technicznym opisem problemu oraz określeniem poziomu zagrożenia, a także rekomendacjami, jak je usunąć.
6. Wykonawca przedstawi raport i omówi go w sposób techniczny w siedzibie zamawiającego lub za zgodą Zamawiającego w formie telekonferencji.

D) Horyzontalny test penetracyjny white-box

1. Pojedynczy horyzontalny test penetracyjny white-box obejmować będzie symulację zachowania prawdziwego atakującego, np. operatora ransomware, który uzyskał dostęp do wewnętrznej infrastruktury teleinformatycznej Zamawiającego.
2. Zamawiający przygotowuje środowisko do testu na jednej maszynie w wybranej przez siebie sieci wewnętrznej i utworzy konto dla Wykonawcy (Pentestera), który uruchomi dedykowany do ataku „implant”, adekwatny do celów, ograniczeń i wyłączeń, o których mowa w ust. 3 poniżej.
3. Zakres ataku w wewnętrznej sieci Zamawiającego zostanie wspólnie uzgodniony przez Strony (cele, wyłączenia, ograniczenia).
4. Wykonawca rozpocznie test od najmniejszych uprawnień i dążyć będzie do uzyskania dostępu do innych maszyn, zidentyfikowania „istotnych” danych i informacji oraz znalezienia podatności, które pozwolą na eskalację uprawnień i ostatecznie do przejęcia całkowitej kontroli nad siecią lub środowiskiem Active Directory. W przypadku przejęcia kontroli nad siecią Wykonawca (Pentester) zobligowany będzie do dalszej analizy dostępnej infrastruktury w celu ustalenia możliwych ścieżek ataku mogących skutkować całkowitym przejęciem sieci Zamawiającego (innych niż wybranej przez Zamawiającego).
5. Atak na wewnętrzną sieć Zamawiającego będzie prowadzony w wariantcie otwartym, co oznacza, że Wydział IT Zamawiającego będzie wiedział o teście i nie będzie próbował aktywnie przeciwdziałać atakowi. Strony będą wzajemnie informować się o ryzykach związanych z zakłóceniem ciągłości działania procesów Zamawiającego.
6. Zamawiający, jak również Wykonawca ma prawo do przerwania testu w każdym momencie w związku z wystąpieniem wspomnianego wyżej ryzyka.
7. W przypadku przejęcia przez Pentestera użytkownika o odpowiednio wysokich uprawnieniach Wykonawca (Pentester) sprawdzi (potwierdzi) możliwość pobrania materiału kryptograficznego z hasłami użytkowników.
8. Wykonawca przygotowuje raport z przeprowadzonego testu z listą podatności, wraz z technicznym opisem problemu oraz określeniem poziomu zagrożenia, a także rekomendacjami, jak je usunąć.
9. Wykonawca przedstawi raport i omówi go w sposób techniczny w siedzibie zamawiającego lub za zgodą Zamawiającego w formie telekonferencji.

Warunki udziału w postępowaniu

- 1.** Zamawiający wymaga, aby Wykonawca dysponował oraz skierował do realizacji zamówienia zespół testowy składający się z co najmniej 1 osoby (członka), albo osobę, posiadającą wiedzę i doświadczenie popartą co najmniej jednym z niżej wymienionych certyfikatów:
 - 1)** OffSecurity Experienced Penetration Tester (OSEP);
 - 2)** Certified Ethical Hacker (CEH);
 - 3)** CompTIA Pentest+;
 - 4)** Certified Information Systems Auditor (CISA);
 - 5)** GIAC Penetration Tester (GPEN);
 - 6)** Certified Information Systems Security Professional (CISSP).
- 2.** Zamawiający dopuszcza certyfikaty równoważne do wymienionych powyżej, przy czym za certyfikat równoważny uważany będzie certyfikat potwierdzający zakres wiedzy i doświadczenia tożsamy z oficjalnym sylabusem egzaminu, którego równoważność jest wskazywana przez Wykonawcę. Wykonawca, który powołuje się na certyfikaty równoważne jest zobowiązany wykazać, że wskazywane przez niego certyfikaty potwierdzają zakres wiedzy i doświadczenia tożsamy z oficjalnym sylabusem egzaminu, którego równoważność jest wskazywana.
- 3.** Zamawiający wymaga, aby Wykonawca wykazał przeprowadzenie testów zgodnych z zakresem niniejszego zamówienia w okresie ostatnich 2 lat u minimum 3 zleceniobiorców zatrudniających min 100 pracowników.

Kary

Wykonawca za odstąpienie od umowy, niewykonanie lub nienależyte wykonanie zapisów umowy przewiduje zastosowanie kar powszechnie stosowanych dla zamówień tego typu.