

**Załącznik Nr 2C**

**do Formularza ofertowego**

**CZĘŚĆ III – Przeprowadzenie testów penetracyjnych infrastruktury IT**

**OPIS ZAOFEROWANEGO SPRZĘTU**

**Dokument należy złożyć wraz z ofertą w formie elektronicznej**

**TESTY PENETRACYJNE**

**Zakres testów bezpieczeństwa infrastruktury**

1. Analiza konfiguracji i bezpieczeństwa serwerów na poziomie systemu operacyjnego i usługowego
2. sprawdzenie aktualności oprogramowania, obecności łatek systemowych,
3. dostępność domyślnych kont użytkowników, bezpieczeństwo kont administratorskich, zgodność   
   z polityką haseł,
4. uruchomione usługi, ich celowość,
5. zarządzanie systemami plików, polityka kopii zapasowych,
6. zarządzanie ruchem sieciowym, zdalny dostęp, członkostwo w domenie,
7. obecność i aktualność oprogramowania antywirusowego,
8. logowane zdarzeń systemowych,
9. zgodność konfiguracji z zewnętrznymi oraz wewnętrznymi standardami
10. Analiza konfiguracji i bezpieczeństwa na poziomie aktywnych urządzeń sieciowych
11. aktualność oprogramowania, obecność łatek systemowych,
12. dostępność domyślnych kont użytkowników, bezpieczeństwo kont, administratorskich, zgodność   
    z polityką haseł,
13. uruchomione usługi, ich celowość,
14. logowane zdarzeń systemowych, podłączenie do systemów korelacji zdarzeń
15. Analiza konfiguracji i bezpieczeństwa na poziomie kanałów komunikacji pomiędzy poszczególnymi komponentami :
16. weryfikacja ruchu sieciowego na poziomie aktywnych urządzeń sieciowych oraz usług udostępnionych na serwerach,
17. weryfikacja użytych protokołów i ich konfiguracji,
18. weryfikacja zabezpieczenia komunikacji pomiędzy poszczególnymi komponentami systemu informatycznego
19. Testy penetracyjne typu GreyBox obejmujące :
20. aktywne urządzenia sieciowe (routery, drukarki, dyski i inne),
21. potencjalne luki w systemach uwierzytelnienia,
22. poziom bezpieczeństwa haseł,
23. obecność kont typu “gość” oraz domyślnych haseł,
24. identyfikację urządzeń dostępnych z poziomu Internetu
25. analizę topologii sieci z wewnątrz i z poziomu Internetu,
26. analizę bezpieczeństwa systemów operacyjnych i oprogramowania używanego przez pracowników,
27. analizę bezpieczeństwa zapory sieciowej,
28. oszacowanie stopnia ryzyka wykrytych podatności
29. **Przygotowanie raportu końcowego z przeprowadzonych testów bezpieczeństwa ze szczegółowym opisem wykrytych zagrożeń oraz rekomendacjami co do implementacji mechanizmów obronnych.**

**Etapy wykonywania testów penetracyjnych sieci – pentestów**

1. **Konsultacja:**

Na początek omówienie zakresu i termin przeprowadzenia testów penetracyjnych zabezpieczeń sieci.

1. **Automatyczne testy penetracyjne sieci:**

W ramach testów penetracyjnych będzie symulowany atak hakerski, mający na celu uzyskać dostęp do sieci urzędu. Mają zostać wykorzystane profesjonalne skanery umożliwiającymi szybkie przetestowanie sieci pod kątem znanych metod ataków. Techniki testowania, podatność zasobów informatycznych na rozmaite działania cyberprzestępców – pod tym względem podczas testu penetracyjnego zabezpieczeń IT analizujemy m.in. otwarte porty, w celu uzyskania nieautoryzowanego dostępu do zasobów urzędu. Po testach urząd ma pewność bezpieczeństwa sieci i bezpieczeństwa systemów, wiedząc, czy są odporne na wszelkiego rodzaju techniki, technologie i narzędzia wykorzystywane do ataków hakerskich.

1. **Manualne testy penetracyjne sieci:**

W ramach testów manualnych weryfikujemy wykryte zagrożenia oraz wykonamy dodatkowe symulacje ataków, niedostępne z poziomu automatycznego skanowania.

1. **Analiza ryzyka:**

W ramach analizy ryzyka wykonane zostaną kompleksowe testy penetracyjne sieci, na ich podstawie oszacujemy poziom bezpieczeństwa systemu, stopień ryzyka wykrytych podatności oraz ustalimy priorytet naprawy poszczególnych błędów. Ta informacja, pozwoli na odpowiednią hierarchizację działań, tak aby najpoważniejsze nieprawidłowości usunąć na samym początku, a najmniej istotne na końcu.

1. **Przekazanie raportu wraz z rekomendacjami:**

Po wykonaniu testów penetracyjnych sieci raport ze szczegółowym opisem wykorzystywanych technik ataku i wykrytych zagrożeń oraz rekomendacjami co do implementacji mechanizmów obronnych. Ta instrukcja, w której zawarte są gotowe do wdrożenia rozwiązania, a wszelkie nieprawidłowości zostają szczegółowo opisane. Przykładowy raport po testowaniu zabezpieczeń będzie zawierać dużą ilość dokładnych, ale czytelnie zaprezentowanych danych i rekomendacji.

1. **Restety:**

Po tym, jak prace zostały wykonane, zalecamy powtórzenie testów penetracyjnych sieci w celu upewnienia się, że wykryte podatności zostały usunięte. Dzięki temu można uzyskać stuprocentową gwarancję prawidłowości i skuteczności wdrożonych zabezpieczeń i bezpieczeństwa sieci i zasobów IT.

*Dokument należy podpisać kwalifikowanym podpisem*

*elektronicznym lub podpisem zaufanym lub*

*elektronicznym podpisem osobistym*