SUNCAPITAL

TESTY
PENETRACYJNE

dla aplikacji webowych, aplikacji desktopowych, aplikacji mobilnych, infrastruktury.

OFERTA

Każdy test opieramy na poniższym scenariuszu (choć w każdym mogą istnieć różnice w zależności od potrzeb klienta, możliwości środowiska itp.):

- 1. Zdobywanie informacji (OSINT)
- 2. Identifykacja infrastruktury (domeny, adresy ip, vpn)
- 3. Enumeracja serwisów i zasobów (co dostarcza każdy element infrastruktury np. "wystawione" endpointy do api, aplikacje webowe, panele administracyjne, api dla aplikacji mobilnych, środowiska testowe, elementy infrastruktury ci/cd
- 4. Eksploitacja podatności i błędów konfiguracji na zidentyfikowanych serwisach
- 5. Podnoszenie uprawnień w skompromitowanych systemach
- 6. Backdooring - utrzymywanie zdobytych uprawnień
- 7. Lateral movement - zdobywanie kolejnych przyczółków dzięki wstępnej kompromitacji zasobów
- 8. Raport - podzielony na sekcję techniczną i dla managementu.

W ramach testów opieramy się na kategoriach podatności opisanych m.in. w OWASP Top 10, OWASP Mobile. Wykorzystuję techniki, taktyki i procedury opisywane m.in. w Mitre Att&ck. Monitoruję podatności opisane na listach CVE.

Nasi ludzie przeprowadzili już kilkadziesiąt testów bezpieczeństwa. Testerzy posiadają odpowiednie kwalifikacje.

W naszej pracy wykorzystujemy szereg narzędzi, w tym:
- skanery automatyczne (Owasp Zap, Nessus, OpenVas, BurpSuite)
- nmap, dirb, nikto, maltego.

Poruszamy się w językach programowania: python, c++, javascript, php, bash, powershell.

Czas realizacji każdego testu jest indywidualny - testy mogą trwać od 3-4 dni nawet do miesiąca. W ramach zlecenia stałego lub usługi długoterminowej podpisujemy umowy na wykonywaną usługę.
Cena usługi jest bardzo elastyczna i ustalamy ją indywidualnie po bezpłatnych konsultacjach.

ZAPYTAJ O OFERTĘ

+48 71 707-03-76
suncapital@suncapital.pl
suncapital.pl
Ołtaszyńska st. 92c/6
53-034 Wrocław