

Szkolenie: Compendium CE
Testy penetracyjne: atakowanie i ochrona systemów informatycznych



Cel szkolenia:

Celem szkolenia "**Testy penetracyjne: atakowanie i ochrona systemów informatycznych**" jest wprowadzenie do tematyki **testów penetracyjnych**. Uczestnik zapozna się z aktualnymi technikami oraz narzędziami używanymi podczas **przeprowadzenia ataków na zdalne systemy**. Tematyka obejmuje m.in. pasywne i aktywne zbieranie informacji, techniki identyfikacji usług oraz systemów bezpieczeństwa. Uczestnik pozna anatomie ataku oraz metody umożliwiające przejmowanie kontroli nad zdalnym systemem. Przedstawione również zostanie oprogramowanie pozwalające na zautomatyzowane **wyszukiwanie luk bezpieczeństwa**, a także przeprowadzenie ataku.

Plan szkolenia:

- Podstawowe informacje
 - Wprowadzenie do tematyki testów penetracyjnych
 - Włamanie Audyt/Auydt/Test penetracyjny
 - Aspekty prawne
 - Metodologie i fazy testu penetracyjnego
 - Planowanie (Planning)
 - Rekonesans (Reconnaissance)
 - Skanowanie (Scanning)
 - Wtargnięcie (Gaining Access)
 - Utrzymanie dostępu (Maintaining Access)
 - Zatarcie śladów (Covering Tracks)
 - Raportowanie (Reporting)
- Footprinting i rekonesans
 - Pasywne i aktywne zbieranie informacji
 - Inżynieria społeczna
- Skanowanie
 - Skanowanie sieci
 - Skanery automatyczne
- Enumeracja podatności
 - Rodzaje podatności
 - Wyszukiwanie podatności

- Wtargnięcie
 - Rodzaje ataków
 - Łamanie haseł
 - Ataki na sieci LAN
- Utrzymanie dostępu
 - Backdoory i rootkity
- Zatarcie śladów
- Raportowanie
 - Dobre praktyki
- Omijanie systemów IDS oraz Firewall
- Honypoty
- Buffer Overflow i Fuzzing
- Metody ochrony systemów
 - Dobre praktyki
- Warsztaty
 - Rekonesans podmiotów, skanowanie sieci, serwerów, usług
 - Google Hacking
 - Enumeracja zasobów
 - Penetracja sieci
 - Ataki phishingowe

Wymagania:

- dobra znajomość środowiska sieci komputerowych (IP, TCP, UDP i ICMP)
- doświadczenie w pracy/konfiguracji urządzeń sieciowych takich jak router, hub/switch
- dobra znajomość systemów Windows oraz Unix

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują **certyfikat** wystawiony imiennie oraz na firmę, sygnowany przez **Compendium Centrum Edukacyjne**.

Prowadzący:

Wykładowca Compendium Centrum Edukacyjnego.

Informacje dodatkowe:

- **Każdy z uczestników tego szkolenia jest zobowiązany do podpisania oświadczenia (bezpośrednio przed jego rozpoczęciem), że zdobytą wiedzę będzie wykorzystywał w sposób etyczny i zgodny z obowiązującym prawem, wyłącznie w celu podnoszenia poziomu bezpieczeństwa sieci, systemów i zasobów, których on lub jego pracodawca jest właścicielem.**
- Punkty CPE (CISSP) za udział w szkoleniu:

Uczestnicy tego szkolenia, którzy posiadają aktualną **certyfikację System Security Certified Practitioner (SSCP)** lub **Certified Information Systems Security Professional (CISSP)** mogą zdobyć jeden punkt **Continuing Professional Education (CPE)** za każdą godzinę szkolenia (1 CPE za pełną godzinę edukacyjną, co daje 6 CPE za standardowy dzień szkolenia w Compendium CE - ale nie więcej niż 8 CPE dziennie). W celu przyznania punktów CPE członkowie (ISC) 2 muszą samodzielnie zgłosić udział w naszym szkoleniu do (ISC)2 i muszą zachować dowód udziału (certyfikat uczestnictwa w szkoleniu) w przypadku konieczności potwierdzenia tego faktu w (ISC)2. Więcej informacji pod adresem <https://www.isc2.org/cpes/default.aspx> (dostęp tylko dla członków (ISC)2).