Szkolenie: Mile2
C)PTC - Certified Penetration Testing Consultant

DOSTĘPNE TERMINY

2024-10-14 | 4 dni | Kraków / Wirtualna sala
2024-10-14 | 4 dni | Virtual Classroom

Cel szkolenia:

Neutralne produktowo szkolenie Mile2 **C)PTC Certified Penetration Testing Consultant** jest przeznaczony dla tych **specjalistów ds. bezpieczeństwa**, **administratorów systemów sieciowych**, **pentesterów**, którzy są zainteresowani głębszym spojrzeniem na konkretne techniki penetracji w odniesieniu do systemów operacyjnych.

Kurs ten uczy niezbędnych umiejętności związanych z pracą w charakterze członka zespołu testerskiego na etapie eksploatacji/wykorzystywania odkrytych podatności np. jak przeprowadzić atak typu przepełnienie bufora przeciwko programom działających w systemach Windows i Linux, jednocześnie podważając funkcje takie jak DEP czy ASLR. Kurs ten też poprowadzi przez Top 10 OWASP, uczy, jak tworzyć programy w powłoce pozwalające na uzyskanie możliwości zdalnego wykonywanie kodu, a także jak analizować i testów wykorzystujących debuggera exploity pobierane z exploit-db.

Kurs w szczególności zawiera takie elementy jak:

- omówieniem zasad, którymi powinniśmy się kierować budują kompetentny zespół testerski
- techniki skanowanie za pomocą NMAP
- wprowadzenie do fuzzing z wykorzystaniem Spike
- pisanie kodu, którego celem jest atak typu przepełnienie bufora
- bezpieczeństwo aplikacji webowych
- Linux Stack Smashing
- obchodzenie zabezpieczeń anty exploitowych
- pisanie raportów po testowych

Kurs **C)PTC** - **Certified Penetration Testing Consultant** jest nastawiony na dogłębne ćwiczenia laboratoryjne przygotowanych dla większości modułów. Uczestnicy mogą spędzić ponad 16 godzin wykonując laboratoria, które bazują na realnych przykładach z prawdziwych **testów penetracyjnych** i procesów tworzenia exploitów. Po ukończeniu szkolenia:

- absolwenci szkolenia **Certified Penetration Testing Consultant** posiadają wiedzę i umiejętności pozwalające im na przeprowadzenie **testów penetracyjnych** zgodnych z

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

aktualnymi standardami i najlepszymi praktykami. Są również w sposób kompetentny przygotowani do **egzaminu certyfikacyjnego CPTC**.

Kurs **C)PTC** skierowany jest do:

- testerów bezpieczeństwa
- etycznych hackerów
- audytorów systemów sieciowych
- specjalistów ds. bezpieczeństwa systemów informatycznych
- kierowników działów bezpieczeństwa
- kierowników działów informatycznych

Akredytacje i wyróżnienia:

Mile2® jest:

- AKREDYTOWANE przez NSA CNSS 4011-4016
- WSKAZANE przez NIST / Homeland Security NICCS's Cyber Security Workforce Framework
- ZAAKCEPTOWANE przez FBI Cyber Security Certification Requirement list (Tier 1-3)

Plan szkolenia:

- Budowanie zespołu pentesterskiego
  - Zarządzanie projektem
  - Metryki
  - Role w zespole, obowiązki i korzyści
  - Ćwiczenia laboratoryjne - Skills Assessment
- Automatyzacja skanowania NMAP
  - Podstawy NMAP
  - Automatyzacja skanowania NMAP
  - Raport z wyników skanowania NMAP
  - Ćwiczenie laboratoryjne – Automation Breakdown
- Proces eksploatacji
  - Cel, powód
  - Środki zaradcze
  - Unikanie
  - Precyzyjne uderzenie
  - Dostosowywanie eksploatacji
  - Dopasowane exploity

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Zero Day Angle
- Przykładowe drogi ataku
- Ogólny cel procesu eksploatacji

- Fuzzing z wykorzystaniem Spike
  - Vulnserver
  - Konfiguracja Spike Fuzzing
  - Fuzzing aplikacji TCP
  - Dostosywanie skrypt Fuzzing
  - Ćwiczenia laboratoryjne - Fuzzing with Spike
- Proste przepełnienie bufora
  - Exploit-DB
  - Immunity Debugger
  - Python
  - Shellcode
  - Ćwiczenie laboratoryjne - Let’s Crash and Callback
- Stack Based Windows Buffer Overflow
  - Debugger
  - Poszukiwanie podatności
  - Kontrolowanie EIP oraz awarii
  - Instrukcja JMP ESP
  - Znajdowanie przesunięcia
  - Wykonywanie kodu
  - Czy exploit działa?
  - Ćwiczenie laboratoryjne - MiniShare for the Win
- Bezpieczeństwo aplikacji internetowych i ich eksploatacja
  - Aplikacje internetowe
  - OWASP Top 10 -2017
  - Zap
  - Scapy
- Linux Stack Smashing & Scanning
  - Wykorzystywanie stosu w systemie Linux
  - Ćwiczenia labolatoryjne - Stack Overflow. Did we get root?
- Losowe ułożenie przestrzeni adresowej (ASLR) w Linux
  - Stack Smashing to the Extreme
  - Ćwiczenie laboratoryjne - Defeat Me and Lookout ASLR
- Windows Exploit Protection

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Wprowadzenie do Windows Exploit Protection
- Strukturalne zarządzanie wyjątkami
- Zapobieganie wykonywaniu danych (ang. Data Execution Prevention, DEP)
- SafeSEH / SEHOP

- SEH i ASLR
  - Konfiguracja podatnego serwera
  - Czas na testowanie
  - "Vulnserver" spotyka się z Immunity
  - Demo VulnServer
  - Ćwiczenia labolatoryjne - Time to overwrite SEH and ASLR
- Pisanie raportu z wykonanego pentestu
  - Raportowanie

Wymagania:

Posiadanie dowolnego **certyfikatu** z zakresu **przeprowadzania testów penetracyjnych** np. **CPTE Certified Penetration Testing Engineer** lub równoważnej wiedzy.

Poziom trudności

Certyfikaty:

Uczestnicy szkolenia otrzymują **certyfikat** ukończenia szkolenia wystawiony imiennie oraz na firmę sygnowany przez firmę **Mile2**. Ponadto kurs ten przygotowuje uczestników do **certyfikowanego egzaminu Certified Penetration Testing Consultant**, który jest realizowany za pośrednictwem systemu egzaminacyjnego Mile2 (Mile2 Assessment & Certification System "MACS"),

Egzamin trwa 2 godziny i składa się z 100 pytań wielokrotnego wyboru.

Każdy uczestnik autoryzowanego szkolenia C)PTC - Certified Penetration Testing Consultant otrzymuje bezpłatny voucher na egzamin CPTC.

Prowadzący:

Autoryzowany instruktor Mile2 (Certified Mile2 Instructor).

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Informacje dodatkowe:

Uczestnikom tego szkolenia w szczególności polecamy również szkolenia i dalszą certyfikację z zakresu:

- **C)IHE** - **Certified Incident Handling Engineer**
- **C)DRE** - **Certified Disaster Recovery Engineer**

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001