Szkolenie: Mile2
C)PSH - Certified PowerShell Hacker

Cel szkolenia:

Kurs **C)PSH - Certified PowerShell Hacker** to cztery intensywne dni nauki poświęcone kluczowym zagadnieniom związanym z wykorzystaniem PowerShell jako narzędzia do hakowania. Jest powszechnie wiadomo, że większość firm w swojej infrastrukturze wykorzystuje Active Directory w celach zarządza procesem uwierzytelnianiem i autoryzacją urządzeń, użytkowników i obiektów w swoich organizacjach. Wiele z nich używa również PowerShell do przyspieszenia i uproszczenia zarządzania usługami.

Czy wiesz, że w wielu z pośród udanych włamań hackerskich z ostatnich lat wykorzystane zostały ataki oparte na PowerShell?

Aby się dowiedzieć, jak to wyglądało i dlaczego było to możliwe, zastało przygotowane właśnie to 4 dniowe szkolenie. Zawarty w kursie materiał uczy, jak wykorzystywać narzędzia, które są bezpośrednio wbudowane w systemach Windows lub też dostępne jako open source dla systemów Mac i Linux. Kurs opiera się zarówno na rzeczywistych implementacjach infrastruktury Windows jak i rzeczywistych technikach stosowanych podczas realnych testów penetracyjnych. Ukończysz szkolenie z prawdziwym zestawem umiejętności, pozwalającymi na testowanie pod katem bezpieczeństwa środowisk Windows, jak nigdy dotąd. A przede wszystkim zdobędziesz również umiejętności pozwalające na zapobieganie atakom. W szczególności podczas kursu C)PSH będziesz miał do swojej dyspozycji:

- szczegółowy podręcznik z opisem laboratorium
- środowisko szkoleniowe oparte o maszyny wirtualne do samodzielnego wykonywania podczas ćwiczeń laboratoryjnych
- wskazów dotyczące ja testować własną infrastrukturę AD
- przykłady ataków, które możesz realnie wykorzystać podczas swoich testów
- dowiesz się jak zabezpieczyć się przed atakami PowerShell

Absolwent szkolenia Certified PowerShell Hacker poza zdobyciem wcześniej wskazanej wiedzy i umiejętności jest w sposób kompetentny przygotowany do egzaminu certyfikacyjnego CPSH.

Kurs skierowany jest szczególnie do:

- etycznych hackerów
- testerów bezpieczeństwa (Pen Testerów)
- administratorów systemów Microsoft
- inżynierów ds. bezpieczeństwa

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

- administratorom Active Directory
- tych wszystkich, którzy chcą się więcej dowiedzieć na temat bezpieczeństwa

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:

- Wprowadzenie do PowerShell
  - Różne opcje narzędzi
  - Instalowanie wszystkiego, co będzie potrzebne
  - Podstawy języka
  - Korzystanie z Windows API i WMI
  - Interakcja z rejestrem
- Wprowadzenie do Active Directory i Kerberos
  - Omówienie protokołu Kerberos
  - Kerberos/Cerber – trzygłowy pies
  - Centrum dystrybucji kluczy
  - Protokołu Kerberos w szczegółach
  - Dlaczego Kerberos jest ważny dla hakera
  - Przegląd Active Directory
  - Zrozumienie koncepcji AD
  - Obiekty i atrybuty AD
- Metodyka testów penetracyjnych – przypomnienie
  - Wprowadzenie do metodyki
  - Plan!
  - Identyfikacja podatności
  - Ataki skierowane na klienta z wykorzystaniem i bez wykorzystania PowerShell
- Zbieranie informacji i enumeracja
  - Co może zobaczyć użytkownik domeny?
  - Enumeracja domeny
  - Mapowanie zaufania i uprawnień
  - Co mamy po skutecznym ataku

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

- Eskalacja uprawnień
  - Eskalacja uprawnień lokalnych
  - Ataki oparte na metodzie powtórzeń (Credential Replay Attacks)
  - Eskalacja uprawnień domeny
  - Zrzut systemu i tajemnice domeny
  - PowerShell i urządzenia do wprowadzania danych przez człowieka (Human Interface Devices)
- Ataki ukierunkowane - ruchy poziome (Lateral Movements) i nadużywanie zaufania
  - Ataki na Kerberos (Złote, Srebrne bilety i inne)
  - Problemy związane z delegowaniem uprawnień
  - Ataki poprzez zaufane domeny
  - Nadużywanie zaufania lasów domen
  - Nadużywanie zaufania serwera SQL
  - Atak typu Pivoting
- Trwałe utrzymywanie kontroli i omijanie obrony
  - Nadużywanie list ACL Active Directory
  - Trwałe utrzymywanie kontroli
  - Omijanie obronne
  - Atakowanie usługi Azure Active Directory
- Obrona przed atakami PowerShell
  - Ochrona infrastruktury Active Directory
  - Wykrywanie ataków
  - Logowanie
  - Transcripts
  - Korzystanie z certyfikatów
  - Korzystanie z Bastion Hosts
  - Korzystanie z AppLocker

Wymagania:

- Minimum 12 miesięcy doświadczenia z technologiami sieciowymi
- Dobra znajomość protokołu TCP / IP
- Znajomość produktów firmy Microsoft w tym w szczególności Active Directory
- Ogólna wiedza i umiejętności związane z przeprowadzaniem testów penetracyjnych
- Ogólna wiedza i umiejętności związane z programowaniem w językach skryptowych

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

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 PowerShell Hacker, 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)PSH - Certified PowerShell Hacker otrzymuje bezpłatny voucher na egzamin CPSH.

Prowadzący:

Autoryzowany instruktor Mile2 (Certified Mile2 Instructor).

Informacje dodatkowe:

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

- C)PTC - Penetration Testing Consultant
- C)IHE - Incident Handling 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