Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

COMARCH
Szkolenia

Bezpieczeństwo Windows

Ataki i ochrona środowiska Microsoft Windows w firmie

Cele szkolenia

Szkolenie ma na celu przybliżenie zagadnień związanych z bezpieczeństwem systemów Microsoft Windows ze szczególnym uwzględnieniem aspektów ich atakowania i ochrony. W ramach szkolenia omówione i zaprezentowane zostaną metody ataków na typowo skonfigurowane systemy Microsoft Windows oraz sposoby zabezpieczania ich przed popularnymi atakami lokalnymi i zdalnymi.

Umiejętności

Dzięki szkoleniu uczestnik będzie:

- Wykorzystywać model “Cyber Kill Chain” w kontekście bezpieczeństwa infrastruktury Windows,
- Określać obszary ataku na systemy Microsoft Windows,
- Wykorzystywać słabe punkty systemu Windows przy dostępie lokalnym,
- Identyfikować systemy Windows w sieci komputerowej, oraz określać oferowane przez nie usługi za pomocą narzędzi do skanowania sieci komputerowych,
- Prawidłowo przeprowadzać skanowanie podatności w sieci LAN,
- Wykorzystywać podatności poprzez sieć komputerową, przy dostępie zdalnym,
- Umieć przejąć kontrolę nad systemem operacyjnym Windows,
- Eskalować uprawnienia w środowisku Active Directory w celu przejęcia kontroli nad usługą,
- Poprawnie zabezpieczać środowisko stacji roboczych przed omawianymi zagrożeniami,
- Wdrażać zabezpieczenia Active Directory w celu utrudnienia skompromitowania usługi.

Profil uczestników

Szkolenie przeznaczone jest dla osób odpowiedzialnych za utrzymanie i obsługę środowiska Microsoft Windows oraz osoby odpowiedzialne za bezpieczeństwo infrastruktury IT.

Szkolenie dla: administratorów usługi Active Directory, administratorów stacji roboczych, pentesterów, pracowników działów bezpieczeństwa (red/blue team).

Przygotowanie uczestników

Szkolenie wymaga dobrej znajomości systemów Microsoft Windows w wersji od Windows 7 / Windows 2012 wzwyż, rozumienia i umiejętności posługiwania się usługami Active Directory, rozumienia dokumentacji

technicznej w języku angielskim, sprawnego poruszania się obszarze sieci komputerowych. Koniecznym jest przynajmniej podstawowa umiejętność posługiwania się systemem Linux (optymalnie dystrybucją Kali Linux).

Szczegółowy program szkolenia

1. Model “Cyber Kill Chain”
2. Wektory ataków na system Windows
   - 2.1. Ataki lokalne
   - 2.2. Ataki zdalne
   - 2.3. Ataki socjotechniczne, wykorzystujące błędy ludzkie
3. Ogólny model ataków na infrastrukturę opartą na Windows
   - 3.1. Przejęcie kontroli nad kontem lokalnym
   - 3.2. Lokalna eskalacja uprawnień
   - 3.3. Ustanowienie persystencji
   - 3.4. Rekonesans i ruch boczny („lateral movement”)
   - 3.5. Eskalacja uprawnień w strukturze Active Directory
4. Ochrona poświadczeń w systemie Windows
   - 4.1. Pliki: SAM, NTDS.DIT
   - 4.2. Rejestr
   - 4.3. Proces lsass.exe
   - 4.4. Mechanizmy ochrony haseł: LM Hash i NTLM Hash
   - 4.5. Łamanie skrótów haseł
5. Ochrona systemu w sieci:
   - 5.1. Użycie skanera Network Mapper („Nmap”)
   - 5.2. Analizator komunikacji sieciowej Wireshark
   - 5.3. Skaner podatności OpenVAS
   - 5.4. Platforma Metasploit i wykorzystywanie wykrytych podatności (np. EternalBlue, PrintNightmare, Zerologon)
6. Rozszerzanie wpływu:
   - 6.1. Pass-the-hash (PtH)
   - 6.2. Local System impersonation
   - 6.3. Ochrona sekretów LSA
   - 6.4. Przywileje i prawa użytkowników
7. Ochrona lokalna
   - 7.1. Bitlocker, TPM, PIN, klucz startowy
   - 7.2. Firewall systemowy
   - 7.3. Aktualizacje
   - 7.4. Ochrona kont wysoceuprzywilejowanych
8. Ochrona w sieci
   - 8.1. Managed Service Accounts (MSA)
   - 8.2. Group Managed Service Accounts (gMSA)
   - 8.3. Local Administrator Password Solution (LAPS)
   - 8.4. Bastion Forest
   - 8.5. Modele Just Enough Administration (JEA) oraz Just In-Time (JIT)
9. Podsumowanie.

Centrum Szkoleniowe Comarch
ul. Prof. Michała Życzkowskiego 33
31-864 Kraków

Metoda realizacji szkolenia

Szkolenie realizowane jest w formie stacjonarnej lub zdalnej. Każdy z uczestników ma do dyspozycji własne środowisko składające się z kilku maszyn wirtualnych odzwierciedlających typowe rzeczywiste środowisko Active Directory, które najpierw próbuje skutecznie zaatakować a następnie zabezpieczyć.

Liczba dni, liczba godzin szkoleniowych

4 dni po 8 godzin lekcyjnych.

Ścieżka rozwoju po szkoleniu

- Autoryzowane szkolenie „Course 20744-C: Securing Windows Server 2016" – dla osób zainteresowanych ochroną infrastruktury opartej na Microsoft Windows,
- Szkolenia, egzaminy I certyfikacja „Certified Ethical Hacker" (CEH) albo "Offensive Security Certified Professional" (OSCP).

Informacje dodatkowe o szkoleniu:

Poziom szkolenia: ☐podstawowy ☐średnio zaawansowany ☒zaawansowany

Szkolenie w formie: ☒stacjonarnej ☒zdalnej

Język szkolenia: ☒polski ☒angielski

Liczebność grupy - szkolenie stacjonarne: min: 4 max: 8

Liczebność grupy - szkolenie zdalne: min: 4 max: 8

Wymagania techniczne: Każdy uczestnik musi mieć dostęp do środowiska w którym będzie w stanie uruchomić do 6 VM jednocześnie w oparciu o platformę Hyper-V, w przypadku szkoleń stacjonarnych – PC wyposażony przynajmniej w procesor 8-rdzeniowy, 32GB RAM i 120GB SSD albo maszyna wirtualna w Azure o analogicznych parametrach. Wymagany dostęp do internetu.

O trenerze:

Kajetan Miś