SZKOLENIE ŚREDNIO ZAAWANSOWANE

Active Directory pod ostrzałem – najczęstsze ataki i skuteczna obrona

SEC/ACTIVE-DIRECTORY

Czas trwania: 2 dni (16h)

Szkolenie prezentuje praktyczne podejście do bezpieczeństwa Active Directory, obejmujące najczęstsze ataki na AD, ochronę tożsamości, hardening kontrolerów domeny, wykrywanie zagrożeń, analizę uprawnień, bezpieczeństwo kont uprzywilejowanych, monitoring Windows i SIEM oraz ograniczanie ryzyka ransomware i przejęcia domeny

Cele szkolenia

- Szkolenie przygotowuje do identyfikowania błędów konfiguracji Active Directory, nadmiernych uprawnień i luk bezpieczeństwa zwiększających ryzyko przejęcia domeny, eskalacji uprawnień oraz nadużyć kont uprzywilejowanych
- Szkolenie uczy analizowania najczęstszych technik ataków na Active Directory, w tym ataków na Kerberos i NTLM, oraz oceniania ich wpływu na bezpieczeństwo tożsamości, usług katalogowych i infrastruktury Windows
- Szkolenie pokazuje, jak planować hardening Active Directory, kontrolerów domeny, kont administracyjnych, grup uprzywilejowanych i zasad bezpieczeństwa w celu ograniczania powierzchni ataku
- Szkolenie rozwija umiejętność monitorowania zdarzeń bezpieczeństwa, analizowania logów Windows i wykrywania anomalii, eskalacji uprawnień oraz podejrzanej aktywności wymagającej reakcji zespołów administracyjnych i SOC
- Szkolenie przygotowuje do przeprowadzania audytu bezpieczeństwa Active Directory, analizy ścieżek ataku, przeglądu uprawnień oraz opracowywania rekomendacji hardeningu ograniczających ryzyko ransomware i przejęcia domeny

Zalety

- Uczestnik analizuje konfigurację Active Directory pod kątem błędów bezpieczeństwa, nadmiernych uprawnień i podatności zwiększających ryzyko przejęcia domeny
- Uczestnik rozróżnia najczęstsze techniki ataków na Active Directory, w tym ataki na poświadczenia, Kerberos i NTLM, oraz ocenia ich wpływ na bezpieczeństwo środowiska domenowego
- Uczestnik monitoruje zdarzenia Windows, analizuje logi bezpieczeństwa i identyfikuje oznaki nadużyć, eskalacji uprawnień oraz ataków na konta użytkowników i administratorów
- Uczestnik planuje hardening kontrolerów domeny, wdraża zasady ochrony tożsamości i dobiera mechanizmy zabezpieczania kont uprzywilejowanych w Active Directory
- Uczestnik kontroluje uprawnienia, członkostwa w grupach, delegacje i zasady dostępu w środowisku AD, identyfikując niebezpieczne konfiguracje i potencjalne ścieżki ataku
- Uczestnik opracowuje rekomendacje audytowe i plan naprawczy wzmacniające bezpieczeństwo Active Directory oraz odporność infrastruktury na ransomware i przejęcie domeny

Dla kogo?

- Administratorzy Active Directory i Windows Server z podstawowym doświadczeniem w utrzymaniu domen, kont i polityk bezpieczeństwa
- Specjaliści cyberbezpieczeństwa oraz inżynierowie bezpieczeństwa analizujący ryzyka tożsamości, uprawnień i ochrony środowisk Windows
- Członkowie zespołów SOC i osoby monitorujące logi oraz incydenty bezpieczeństwa w infrastrukturze Microsoft
- Administratorzy infrastruktury IT odpowiedzialni za konta uprzywilejowane, dostęp administracyjny i hardening systemów
- Audytorzy bezpieczeństwa informacji oraz osoby realizujące przeglądy uprawnień, konfiguracji AD i zgodności z

wymaganiami organizacji
- Specjaliści IAM i PAM posiadający podstawową znajomość Active Directory, Windows Server i administracji użytkownikami

Wymagania

- Podstawowa znajomość Active Directory
- Podstawowa znajomość Windows Server
- Znajomość podstaw administracji użytkownikami i uprawnieniami
- Podstawowa wiedza dotycząca cyberbezpieczeństwa
- Podstawowa znajomość uwierzytelniania w Windows (Kerberos, NTLM) jest mile widziana

Program

1. Active Directory jako cel cyberataków
2. Dlaczego AD jest kluczowym elementem infrastruktury: domena, kontrolery domeny, las jako granica bezpieczeństwa
3. Konsekwencje przejęcia domeny
4. Typowa ścieżka napastnika w środowisku domenowym: rozpoznanie, zdobycie poświadczeń, eskalacja uprawnień, ruch boczny, utrwalenie dostępu, przejęcie domeny
5. Dlaczego napastnicy atakują tożsamość, a nie tylko systemy
6. Najczęstsze błędy konfiguracji Active Directory
7. Nadmierne uprawnienia i niebezpieczne członkostwa w grupach, w tym w grupach wbudowanych o wysokich uprawnieniach
8. Konta z przypisanymi nazwami SPN, konta, dla których nie jest wymagane wstępne uwierzytelnianie Kerberos, hasła niewygasające i konta nieużywane
9. Ustawienia domyślne ułatwiające atak, np. możliwość dołączania komputerów do domeny przez zwykłych użytkowników
10. Starsze protokoły i systemy: NTLMv1, SMBv1, nieaktualne wersje systemów
11. Błędy w zasadach grup (GPO) i w delegowaniu uprawnień
12. Ukryte ścieżki do uprawnień administracyjnych: dlaczego sama lista grup nie wystarcza
13. Ataki na poświadczenia i uwierzytelnianie
14. Jak działają Kerberos i NTLM – w zakresie potrzebnym do zrozumienia ataków (TGT, bilet usługowy, konto krbtgt, skrót hasła NT)
15. Zdobywanie haseł: password spraying, AS-REP Roasting, Kerberoasting
16. Przechwytywanie i przekazywanie uwierzytelnienia: NTLM relay, zatruwanie odpowiedzi LLMNR i NBT-NS, wymuszanie uwierzytelnienia (coercion)
17. Wykorzystanie zdobytych poświadczeń: Pass-the-Hash, Pass-the-Ticket, Overpass-the-Hash
18. Gdzie poświadczenia „leżą” na stacjach i serwerach: pamięć procesu LSASS, poświadczenia buforowane
19. Znaczenie i ograniczenia MFA: zwiększa bezpieczeństwo logowania, jeśli jest prawidłowo skonfigurowane i egzekwowane, ale samo nie eliminuje ryzyka wykorzystania wcześniej pozyskanych skrótów haseł lub biletów Kerberos (Pass-the-Hash, Pass-the-Ticket), ataków Kerberoasting ani nadużycia uprawnień replikacji (DCSync); dlatego trzeba je uzupełnić ochroną poświadczeń, ograniczaniem uprawnień, odpowiednią konfiguracją Kerberos i NTLM oraz monitoringiem
20. Eskalacja uprawnień i przejęcie domeny
21. Nadużycia ACL/DACL: prawa takie jak GenericAll, WriteDACL i WriteOwner oraz ich skutki
22. Delegacja Kerberos: unconstrained, constrained i delegacja oparta na zasobach (RBCD)
23. Usługi certyfikatów Active Directory (AD CS): błędnie skonfigurowane szablony i urzędy certyfikacji (klasyfikacja ESC; analizowane są wybrane scenariusze, m.in. ESC1, ESC4 i ESC8)
24. DCSync: nadużycie uprawnień replikacji katalogu w celu pozyskania skrótów haseł i innych wrażliwych danych uwierzytelniających, w tym dotyczących kont uprzywilejowanych
25. Fałszowanie biletów Kerberos: Golden Ticket i Silver Ticket oraz rola konta krbtgt
26. Utrwalanie dostępu po przejęciu domeny: ukryte zmiany w ACL i GPO, dodatkowe konta
27. Ścieżka od zwykłego konta użytkownika do administratora domeny – jak łączą się poszczególne techniki
28. Ochrona tożsamości i kont uprzywilejowanych
29. Model warstwowy (tiering) i Enterprise Access Model: wydzielenie najwyższej warstwy (Tier 0) oraz stacje administracyjne (PAW)
30. Osobne konta administracyjne, zasada najmniejszych uprawnień, dostęp na żądanie (just-in-time)
31. Ochrona kont wysokiego ryzyka: grupa Protected Users (w tym ograniczenia i wpływ na zgodność), silosy uwierzytelniania oraz mechanizm AdminSDHolder/SDProp – zasada działania, audyt i wykrywanie nadużyć
32. Windows LAPS: unikalne hasła lokalnych administratorów
33. Konta usług: zarządzane konta usług (gMSA) zamiast kont ze statycznymi hasłami, ograniczanie SPN i uprawnień
34. Cykl życia kont, regularne przeglądy uprawnień i separacja obowiązków
35. Hardening kontrolerów domeny i protokołów
36. Kontrolery domeny: minimalna instalacja, brak dodatkowych ról i oprogramowania, aktualizacje, dostęp administracyjny wyłącznie ze stacji administracyjnych
37. Podpisywanie LDAP (integralność komunikacji) i LDAP channel binding (powiązanie uwierzytelnienia z sesją TLS, ochrona przed atakami relay); podpisywanie SMB – domyślne wymagania zależą od wersji i edycji systemu oraz kierunku połączenia (zmiany w Windows 11 24H2 i Windows Server 2025), a ich znaczenie dla obrony przed atakami relay jest omawiane na przykładach

38. Ograniczanie użycia NTLM: audyt i analiza zależności, stopniowe eliminowanie wyjątków, migracja do Kerberos tam, gdzie to możliwe; status NTLMv1 (usunięty w Windows 11 24H2 i Windows Server 2025) i NTLMv2 oraz plany Microsoft dotyczące domyślnego wyłączania NTLM w kolejnych wydaniach
39. Kerberos: ograniczanie i wycofywanie RC4 na rzecz AES – zmiany domyślnego zachowania KDC związane z aktualizacjami z 2026 r., identyfikacja zależności od starszych systemów i kont usług oraz bezpieczna migracja do AES
40. Rotacja hasła konta krbtgt: zasady i skutki
41. Bezpieczne wprowadzanie zmian: tryby audytu przed egzekwowaniem, wdrażanie etapami, wzorcowe konfiguracje (Microsoft Security Baselines, CIS Benchmarks)
42. Ograniczanie powierzchni ataku: zbędne usługi na kontrolerach domeny (np. Print Spooler), segmentacja sieci, reguły zapory
43. Środowiska hybrydowe: Active Directory i Microsoft Entra ID
44. Zależności między AD a Entra ID: synchronizacja tożsamości (Entra Connect Sync, Cloud Sync), synchronizacja skrótów haseł, uwierzytelnianie przekazywane, federacja
45. Serwer synchronizacji i jego konta jako zasób najwyższej wrażliwości (Tier 0)
46. Konto Seamless SSO (AZUREADSSOACC$): ochrona konta, szyfrowanie AES zamiast RC4, rotacja klucza Kerberos oraz wpływ zmian zachowania KDC z 2026 r. na działanie uwierzytelniania
47. Ścieżki ataku między środowiskiem lokalnym a chmurą – w obu kierunkach
48. Konta administracyjne w chmurze rozdzielone od kont lokalnych (konta tylko w chmurze)
49. Wykrywanie nadużyć: Microsoft Defender for Identity i logi Entra ID
50. Monitoring i wykrywanie zagrożeń
51. Konfiguracja zaawansowanej polityki audytu oraz zbieranie odpowiednich zdarzeń z kontrolerów domeny, stacji roboczych i serwerów; przekazywanie logów do SIEM
52. Kluczowe zdarzenia: logowania i uwierzytelnianie Kerberos (m.in. 4624, 4625, 4768, 4769, 4771, 4776), zmiany w grupach i obiektach, dostęp do replikacji katalogu (4662 – przy odpowiednio skonfigurowanym audycie i wpisach SACL)
53. Wykrywanie technik z poprzednich modułów: password spraying, Kerberoasting, DCSync, nietypowe użycie biletów, zmiany ACL i AdminSDHolder
54. Narzędzia i mechanizmy: Microsoft Defender for Identity, reguły w SIEM, konta i obiekty-pułapki (honeytokens), które pozwalają wykryć podejrzaną aktywność
55. Rola zespołu SOC i przekazywanie sygnałów do zespołu reagowania na incydenty
56. Odporność Active Directory: kopie zapasowe i odtwarzanie po przejęciu
57. Rola AD w atakach ransomware od strony technicznej: dlaczego przejęcie domeny pozwala szybko szyfrować całe środowisko
58. Kopie zapasowe AD: stan systemu kontrolerów domeny, ochrona i izolacja kopii, testy odtwarzania
59. Plan odtwarzania lasu (forest recovery) według zaleceń Microsoft: kiedy jest potrzebny, wybór kopii sprzed kompromitacji, odtworzenie pierwszego kontrolera domeny, role FSMO, pozostałe kontrolery
60. Działania po odtworzeniu: dwukrotny reset hasła konta krbtgt z zachowaniem wymaganego odstępu czasowego między resetami, reset haseł kont uprzywilejowanych i innych poświadczeń objętych ryzykiem, reset haseł kont komputerów zgodnie z procedurą odtwarzania, przegląd GPO, ACL i usług certyfikatów oraz – w środowiskach z Seamless SSO – rotacja klucza Kerberos; kolejność działań zależy od skali kompromitacji i architektury lasu
61. Dokumentacja i ćwiczenia: instrukcja odtwarzania dostępna offline, testy w odizolowanym środowisku
62. Audyt bezpieczeństwa Active Directory
63. Zakres i metodyka audytu: konfiguracja, uprawnienia, ścieżki ataku, usługi certyfikatów, integracja hybrydowa
64. Narzędzia do oceny stanu bezpieczeństwa AD (np. PingCastle, Purple Knight, BloodHound) – stosowane wyłącznie za zgodą właściciela środowiska
65. Analiza wyników, ocena ryzyka i ustalanie priorytetów
66. Plan naprawczy: szybkie poprawki a zmiany długofalowe, ryzyko wpływu na działanie usług
67. Przygotowanie do audytów zewnętrznych i wymagań regulacyjnych (np. KSC/NIS2)
68. Warsztaty praktyczne
69. Analiza przykładowej konfiguracji Active Directory i wskazanie ścieżek ataku
70. Ocena uprawnień: grupy, ACL, delegacje Kerberos i szablony usług certyfikatów
71. Analiza scenariusza przejęcia domeny na podstawie przygotowanych logów i konfiguracji: od konta użytkownika do DCSync i Golden Ticket, wraz z wykryciem kolejnych etapów
72. Przygotowanie rekomendacji hardeningu i planu naprawczego z uwzględnieniem priorytetów
73. Szkic planu odtwarzania Active Directory po przejęciu