9. Zadania logiczne: Przygotuj zadania, które wymagają logicznego myślenia i zastosowania wiedzy, np. "Jakie kroki podjąć, aby zlokalizować adres IP na podstawie FQDN?"

Kilka przykładowych zadań logicznych związanych z tematyką DNS i Active Directory:

1. **Zadanie: Lokalizacja adresu IP na podstawie FQDN** Jakie kroki podjąć, aby zlokalizować adres IP na podstawie pełnej nazwy domeny (FQDN)? Opisz proces od momentu wpisania FQDN w przeglądarkę do uzyskania adresu IP.

2. **Zadanie: Bezpieczeństwo w dynamicznych aktualizacjach DNS** Dlaczego zabezpieczenia w dynamicznych aktualizacjach DNS są istotne? Wyjaśnij, jakie zagrożenia mogą wystąpić, jeśli nie ma odpowiednich mechanizmów zabezpieczeń w procesie aktualizacji rekordów DNS.

3. **Zadanie: Różnice między rekordami DNS a rekordami AD** Porównaj i skontrastuj rekord DNS typu A z rekordem SRV w kontekście Active Directory. Jakie informacje przechowują te rekordy i w jaki sposób są wykorzystywane?

4. **Zadanie: Korzyści płynące z hierarchicznej struktury DNS** Dlaczego hierarchiczna struktura DNS jest istotna dla efektywnego zarządzania nazwami domenowymi w skali globalnej? Przedstaw co najmniej dwie korzyści wynikające z tej struktury.

5. **Zadanie: Rola DNS w procesie autentykacji w Active Directory** Jak DNS wpływa na proces autentykacji użytkowników w środowisku Active Directory? Wyjaśnij, dlaczego dostępność i poprawna konfiguracja serwerów DNS jest kluczowa dla udanej autentykacji.

6. **Zadanie: Integracja DNS z usługami AD** Wyjaśnij, w jaki sposób rekordy SRV w DNS są wykorzystywane do integracji z usługami Active Directory. Dlaczego takie rekordy są istotne dla lokalizacji różnych usług w domenie?

7. **Zadanie: Różnice między DNS a WINS** Porównaj różnice między systemem DNS a systemem WINS w kontekście rozwiązywania nazw w sieci. Jakie są zalety korzystania z DNS w porównaniu do WINS?

8. **Zadanie: Rekurencyjny resolver w DNS** W jaki sposób działa rekurencyjny resolver w procesie odpytywania DNS? Wyjaśnij, dlaczego ten element jest kluczowy dla skutecznego przekształcania nazw domenowych na adresy IP.

9. **Zadanie: Konfiguracja stref DNS w środowisku AD** Jakie są trzy główne typy stref DNS w kontekście Active Directory? Opisz, jakie informacje przechowują i jaka jest ich rola w obszarze zarządzania nazwami w sieci.

10. **Zadanie: Wykorzystanie DNS poza AD** Przedstaw scenariusz, w którym osoba korzysta z DNS do uzyskania adresu IP dla danej witryny internetowej. Opisz, jakie kroki podejmuje serwer DNS, aby dostarczyć adres IP na podstawie wpisanej nazwy domenowej.

Oczywiście, poniżej znajdują się rozwiązania do przykładowych zadań logicznych:

1. **Zadanie: Lokalizacja adresu IP na podstawie FQDN** Aby zlokalizować adres IP na podstawie pełnej nazwy domeny (FQDN), należy wykonać następujące kroki:

   a. Przeglądarka wysyła zapytanie DNS do lokalnego rekurencyjnego resolvera.

   b. Resolver odpytuje serwery DNS, zaczynając od serwerów korzenia, aby zlokalizować serwer odpowiedzialny za daną domenę.

   c. Serwer DNS odpowiedzialny za daną domenę zwraca adres IP odpowiadający podanej FQDN.

   d. Resolver przekazuje adres IP do przeglądarki, która nawiązuje połączenie z danym adresem.

2. **Zadanie: Bezpieczeństwo w dynamicznych aktualizacjach DNS** Zabezpieczenia w dynamicznych aktualizacjach DNS są istotne, aby zapobiec fałszerstwom i nieautoryzowanym modyfikacjom rekordów DNS. Bez odpowiednich zabezpieczeń, atakujący może zmieniać rekordy DNS, co prowadziłoby do przekierowania ruchu na fałszywe serwery. Mechanizmy zabezpieczeń, takie jak mechanizmy kluczy TSIG lub DNSSEC, pomagają weryfikować autentyczność aktualizacji DNS.

3. **Zadanie: Różnice między rekordami DNS a rekordami AD** Rekord DNS typu A przechowuje mapowanie pomiędzy nazwą domenową a adresem IPv4. Rekord SRV (Service) w kontekście Active Directory przechowuje informacje o usługach i ich dostępności w domenie. Rekord SRV jest wykorzystywany do lokalizacji usług, takich jak kontrolery domeny, serwery poczty czy serwery autoryzacji.

4. **Zadanie: Korzyści płynące z hierarchicznej struktury DNS** Hierarchiczna struktura DNS pozwala na efektywne zarządzanie nazwami domenowymi w skali globalnej. Korzyści to m.in.:

- Skalowalność: Nowe domeny można dodawać bez konieczności ingerencji w istniejącą strukturę.
- Redundancja: W razie awarii jednego serwera DNS, inne serwery mogą obsłużyć zapytania.
- Rozproszenie obciążenia: Serwery DNS mogą obsługiwać zapytania z różnych regionów.
- Lokalizacja: Hierarchia ułatwia zlokalizowanie serwera obsługującego daną domenę.

5. **Zadanie: Rola DNS w procesie autentykacji w Active Directory** DNS jest kluczowym elementem w procesie autentykacji w Active Directory. Użytkownik komputera z AD komunikującego się z kontrolerem domeny wysyła zapytanie DNS w celu zlokalizowania kontrolera domeny. Poprawna konfiguracja DNS jest niezbędna do poprawnego przeprowadzenia procesu autentykacji i dostępu do zasobów w domenie.

6. **Zadanie: Integracja DNS z usługami AD** Rekordy SRV w DNS są wykorzystywane do integracji z usługami Active Directory. Te rekordy informują o dostępności usług, takich jak autentykacja, usługi katalogowe czy usługi Kerberos. Dzięki nim można zlokalizować serwery odpowiedzialne za te usługi w danej domenie.

7. **Zadanie: Różnice między DNS a WINS** Różnice między DNS a WINS obejmują:

- Adresy IP vs. nazwy NetBIOS: DNS tłumaczy nazwy domenowe na adresy IP, podczas gdy WINS przyporządkowuje nazwy NetBIOS do adresów IP.
- Hierarchiczna struktura vs. płaska przestrzeń nazw: DNS ma hierarchiczną strukturę, a WINS używa płaskiej przestrzeni nazw.
- Internet vs. lokalna sieć: DNS jest szeroko wykorzystywany w Internecie i wewnątrz firm, a WINS jest bardziej ograniczony do lokalnych sieci Windows.

8. **Zadanie: Rekurencyjny resolver w DNS** Rekurencyjny resolver to serwer DNS, który odpytuje inne serwery DNS w celu znalezienia odpowiedzi na zapytanie. Gdy otrzymuje zapytanie od klienta, rekurencyjny resolver może skonsultować się z serwerami korzenia, serwerami górnej poziomej domeny itd., aby znaleźć odpowiedni adres IP dla danej nazwy domenowej.

9. **Zadanie: Konfiguracja stref DNS w środowisku AD** Trzy główne typy stref DNS w kontekście Active Directory to: strefa podstawowa (primary zone), strefa dodatkowa (secondary zone) i strefa wejściowa (stub zone). Strefa podstawowa przechowuje podstawowe informacje o domenie. Strefa dodatkowa jest repliką strefy podstawowej, służy jako backup. Strefa wejściowa zawiera informacje o serwerach DNS innych domen w celu rozpoznawania ich nazw.

10. **Zadanie: Różnice między plikami hosts a rekordami DNS** Różnice między plikami hosts a rekordami DNS obejmują:

- Zastosowanie: Plik hosts służy do lokalnego mapowania nazw na adresy IP, podczas gdy rekordy DNS obsługują globalne mapowanie.
- Zakres: Plik hosts działa tylko na jednym komputerze, a rekordy DNS obsługują całą sieć.

- Zarządzanie: Aktualizacje pliku hosts muszą być ręcznie wprowadzane, podczas gdy rekordy DNS mogą być dynamicznie aktualizowane.
- Skalowalność: Plik hosts jest niepraktyczny w większych sieciach, a rekordy DNS są skalowalne.

11. **Zadanie: Rola DNS w lokalizacji zasobów sieciowych** DNS przypisuje nazwy czytelne dla ludzi (FQDN) do adresów IP, co ułatwia lokalizację zasobów sieciowych. Dzięki temu użytkownicy nie muszą pamiętać adresów IP, a zamiast tego mogą używać nazw domenowych do odnajdywania serwerów, drukarek i innych zasobów w sieci.

12. **Zadanie: Znaczenie konfiguracji stref DNS w AD** Poprawna konfiguracja stref DNS w środowisku Active Directory ma ogromne znaczenie. Właściwie skonfigurowane strefy DNS zapewniają poprawne funkcjonowanie procesów autentykacji, lokalizacji zasobów i komunikacji w środowisku AD. Nieprawidłowa konfiguracja może prowadzić do problemów z dostępem do zasobów i usług.

13. **Zadanie: Wykorzystanie rekordów MX w DNS** Rekordy MX (Mail Exchanger) w DNS są używane do kierowania ruchu pocztowego w sieci. Określają, które serwery są odpowiedzialne za obsługę poczty elektronicznej dla danej domeny. Rekordy MX zawierają informacje o priorytetach serwerów, które pomagają określić, który serwer zostanie użyty w pierwszej kolejności.

14. **Zadanie: Rola DNSSEC w zabezpieczeniach DNS** DNSSEC (DNS Security Extensions) to zestaw rozszerzeń zapewniających zabezpieczenia dla rekordów DNS. Głównym celem DNSSEC jest zapewnienie autentyczności i integralności rekordów DNS, aby zapobiec atakom typu cache poisoning i spoofing. Rekordy DNSSEC zawierają cyfrowe podpisy, które mogą być weryfikowane przez klientów DNS.

15. **Zadanie: Wpływ błędnej konfiguracji DNS na AD** Błędna konfiguracja DNS może mieć poważne skutki dla funkcjonowania Active Directory. Może prowadzić do problemów z autentykacją, lokalizacją zasobów, replikacją danych i dostępem do usług. Niewłaściwa konfiguracja DNS może skutkować błędnymi danymi w procesach AD, co może znacząco wpłynąć na stabilność i bezpieczeństwo środowiska.

16. **Zadanie: Wpływ braku rekordów PTR na e-mail** Rekordy PTR (Pointer) w DNS służą do mapowania adresu IP na nazwę domenową. Brak rekordów PTR może mieć negatywny wpływ na dostarczanie poczty elektronicznej, ponieważ wiele serwerów poczty korzysta z odwrotnej weryfikacji DNS, aby potwierdzić, że serwer wysyłający pocztę jest autentyczny. Brak rekordów PTR może skutkować odrzuceniem lub oznaczeniem poczty jako spam.

17. **Zadanie: Jakie informacje zawierają rekordy SOA w DNS?** Rekordy SOA (Start of Authority) w DNS zawierają informacje o dominie, takie jak:

- Nazwa głównej strefy.
- Adres e-mail osoby odpowiedzialnej za strefę.
- Numer wersji strefy.
- Czas wygaśnięcia strefy.
- Czas odświeżania strefy.
- Inne informacje administracyjne.

18. **Zadanie: Jakie są główne cele DNS w kontekście Active Directory?** Główne cele DNS w kontekście Active Directory to:

- Rozpoznawanie nazw: DNS umożliwia przypisywanie nazw czytelnych dla ludzi (FQDN) do adresów IP.
- Lokalizacja kontrolerów domeny: DNS pomaga w odnajdywaniu kontrolerów domeny w celu przeprowadzenia autentykacji i dostępu do zasobów.
- Autorytatywna usługa domenowa: DNS jest wykorzystywane do przechowywania informacji o zasobach w domenie.
- Integracja z usługami AD: DNS jest integralną częścią procesów autentykacji i komunikacji w środowisku Active Directory.

19. **Zadanie: Jakie są podobieństwa między DNS a WINS?** Zarówno DNS, jak i WINS (Windows Internet Name Service) są używane do przypisywania nazw komputerów do adresów IP, ale istnieją różnice:

- DNS jest bardziej rozbudowanym systemem i obsługuje nie tylko komputery Windows.
- WINS jest bardziej ograniczony do środowisk Windows i obsługuje starsze systemy oparte na protokole NetBIOS.
- DNS ma hierarchiczną strukturę, a WINS działa na zasadzie przeszukiwania lokalnych baz danych.

20. **Zadanie: Wpływ braku rekordu SRV w DNS na AD** Brak rekordów SRV (Service Location) w DNS może mieć negatywny wpływ na Active Directory. Rekordy SRV zawierają informacje o usługach w domenie, takie jak lokalizacja kontrolerów domeny, serwerów plików, serwerów poczty itp. Brak tych rekordów może skutkować trudnościami w lokalizacji i dostępie do usług AD.

21. **Zadanie: Jakie jest znaczenie rekurencyjnego resolvera w procesie DNS?** Rekurencyjny resolver DNS odgrywa kluczową rolę w procesie odpytywania DNS. Gdy klient (np. przeglądarka internetowa) wysyła zapytanie o nazwę domenową, rekurencyjny resolver przeszukuje hierarchicznie drzewo DNS, odwiedzając kolejne serwery DNS, aż znajdzie docelowe IP. Następnie przekazuje odpowiedź klientowi.

22. **Zadanie: Jakie są zalety dynamicznych aktualizacji DNS w AD?** Zalety dynamicznych aktualizacji DNS w środowisku Active Directory to:

- Automatyczna aktualizacja: Komputery w sieci mogą automatycznie rejestrować i aktualizować swoje rekordy DNS.
- Łatwiejsze zarządzanie: Eliminuje konieczność ręcznej aktualizacji, co ułatwia zarządzanie dużymi sieciami.
- Zapobieganie błędom: Pomaga uniknąć błędów związanych z ręcznym wprowadzaniem rekordów DNS.

23. **Zadanie: W jaki sposób DNS i Active Directory są zintegrowane?** DNS i Active Directory są ściśle zintegrowane w procesach autentykacji, lokalizacji zasobów i komunikacji. Kontrolery domeny w AD są również serwerami DNS, a rekordy DNS przechowują informacje o zasobach i usługach w domenie. DNS jest niezbędny do prawidłowego funkcjonowania procesów AD.

24. **Zadanie: Jakie są korzyści korzystania z nazw domenowych (FQDN) zamiast adresów IP?** Korzyści korzystania z nazw domenowych (FQDN) to:

- Łatwiejsza zapamiętywalność: Nazwy domenowe są czytelne dla ludzi, co ułatwia zapamiętywanie w porównaniu do adresów IP.
- Elastyczność: Adresy IP mogą się zmieniać, ale nazwa domenowa może pozostać stała.
- Skalowalność: Nazwy domenowe pozwalają na przenoszenie zasobów bez zmiany ich adresów IP.
- Łatwiejsze zarządzanie: Rekordy DNS mogą być aktualizowane w celu przekierowania ruchu na inne serwery.

25. **Zadanie: Jakie są potencjalne zagrożenia związane z DNS spoofing?** Zagrożenia związane z DNS spoofing obejmują:

- Cache poisoning: Fałszywe informacje DNS wprowadzone do pamięci podręcznej serwera DNS mogą kierować ruch do nieautoryzowanych miejsc.
- Man-in-the-middle: Atakujący może podszyć się pod serwer DNS i przekierowywać ruch w celu przechwycenia danych.

- Phishing: Atakujący może tworzyć fałszywe strony internetowe z wykorzystaniem podszytych nazw domenowych w celu oszukania użytkowników.

To są kolejne zestawy zadań i pytań, które mogą być wykorzystane do przetestowania wiedzy uczniów na temat DNS i Active Directory. Możesz dostosować je do potrzeb swojej lekcji.