Załącznik nr 1b do SWZ

Szczegółowy Opis Przedmiotu Zamówienia Postępowanie **„Zakup sprzętu i oprogramowania serwerowego wraz z wdrożeniem w ramach realizacji projektu „Cyfrowa Gmina”**

1 Windows Server Standard 2022 - 16 Core (2szt.)
2 Windows Server Standard 2022 - 2 Core (1 szt.)
3 Windows Server CAL 2022 - Windows Server 2022 - 1 Device CAL (60 szt.)
4 Wdrożenie

Producent Microsoft*

Nazwa Ad 1 Windows Server Standard 2022 - 16 Core (2szt.)
Nazwa Ad 2 Windows Server Standard 2022 - 2 Core (1 szt.)
Nazwa Ad 3 Windows Server CAL 2022 - Windows Server 2022 - 1 Device CAL (60 szt.)

(Tekst oznaczony * Wypełnia Wykonawca)

Część 1. Licencje:

Lp.	Nazwa komponentu	Wymagane minimalne	Oferowany przez Wykonawcę *
1.	**System operacyjny**	Oprogramowanie Windows Server 2022 lub równoważne Opis równoważności dla licencji Windows Server 2022: 1. Współpraca z procesorami o architekturze x64. 2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym. 3. Możliwość budowania klastrów składających się z 64 węzłów. 4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 2 procesory oraz 16 rdzeni. 5. Praca w roli klienta domeny Microsoft Active Directory. 6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie Microsoft Windows Server 2012. 7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu. 8. Możliwość uruchomienia roli klienta i serwera czasu (NTP). 9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. 10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. 10. Możliwość uruchomienia roli serwera stron WWW. 11. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera. 12. W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych. 13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego. 14. Wszystkie wymienione parametry, role, funkcje, itp. systemu	Windows Server Standard 2022 - 16 Core (2szt.) Windows Server Standard 2022 - 2 Core (1 szt.) Windows Server CAL 2022 - Windows Server 2022 - 1 Device CAL (60 szt.)

		operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów). 15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. 17. Wbudowane wsparcie instalacji i pracy na wolumenach, które: 1) pozwalają na zmianę rozmiaru w czasie pracy systemu, 2) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, 3) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, 4) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 18. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość 19. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 20. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 21. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 22. Możliwość wykorzystania standardu http/2. 23. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 24. Dostępne dwa rodzaje graficznego interfejsu użytkownika: 1) klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, 2) dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 25. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. 26. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 27. Mechanizmy logowania w oparciu o: 1) login i hasło, 2) karty z certyfikatami (smartcard), 3) wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM). 28. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:	

		1) określonych grup użytkowników, 2) zastosowanej klasyfikacji danych, 3) centralnych polityk dostępu w sieci, 4) centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 29. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 30. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. 31. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. 32. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management). 33. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. 34. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: 1) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. 2) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: a. Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną; b. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania; c. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza; d. Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1; 3) Zdalna dystrybucja oprogramowania na stacje robocze. 4) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników. 5) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: a. Dystrybucję certyfikatów poprzez http,	

		b. Konsolidację CA dla wielu lasów domeny, c. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, d. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509 6) Szyfrowanie plików i folderów. 7) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec) 8) Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi 9) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. 10) Serwis udostępniania stron WWW 11) Wsparcie dla protokołu IP w wersji 6 (IPv6). 12) Wsparcie dla algorytmów Suite B (RFC 4869). 13) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows. 14) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. 15) Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 16) Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. 17) Mechanizmy wirtualizacji mające wsparcie dla: a. dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, b. obsługi ramek typu jumbo frames dla maszyn wirtualnych. c. obsługi 4-KB sektorów dysków, d. nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, e. możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. f. możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) g. możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego. 18) Możliwość uruchamiania kontenerów bazujących na	

		Windows i Linux na tym samym hoście kontenerów. 19) Wsparcie dla rozwiązania Kubernetes. 20) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. 21) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). 22) Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB. 23) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 24) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. 25) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF 26) Mechanizm konfiguracji połączenia VPN do platformy Azure. 27) Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu. 28) Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów. 29) Zorganizowany system szkoleń i materiały edukacyjne w języku polskim. 30) Możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Enterprise). 35. W przypadku zaproponowania licencji równoważnych Wykonawca przeprowadzi na własny koszt instalację, konfigurację i integrację dostarczonego produktu. Wykonawca przeprowadzi migrację wszelkich danych i konfiguracji zapewniając identyczne funkcjonowanie całego środowiska w stosunku do aktualnego środowiska. Przerwa w działaniu aktualnie eksploatowanego środowiska produkcyjnego nie może wynieść więcej niż 7 godzin Dodatkowo w przypadku błędnego działania środowiska po instalacji licencji równoważnych Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania OPZ. 36. Ponadto zastosowanie rozwiązania równoważnego nie może ograniczyć funkcjonalności posiadanego systemu przez Zamawiającego i nie może powodować konieczności ponoszenia dodatkowych kosztów dla Zamawiającego.	

Formularz musi być również podpisany kwalifikowanym podpisem elektronicznym/podpisem zaufanym/podpisem osobistym

Część 2. Wdrożenie środowiska serwerowego:

1 Przedmiotem niniejszego postępowania jest:

1.1 Dostawa serwera typu Rack wraz z wykonaniem montażu w serwerowni Zamawiającego.

1.2 Dostawa NAS z 4 dyskami wraz z wykonaniem usługi montażu i konfiguracji w serwerowni Zamawiającego.

1.3 Dostawa 2 przełączników sieciowych wraz z wykonaniem usługi montażu i konfiguracji w serwerowni Zamawiającego.

1.4 Instalacja oprogramowania serwera w tym migracji środowiska serwerowego w serwerowni Zamawiającego.

1.5 Dostawa licencji:

Windows Server Standard 2022 - 16 Core (2szt.)
Windows Server Standard 2022 - 2 Core (1 szt.)
Windows Server CAL 2022 - Windows Server 2022 - 1 Device CAL (60 szt.)

1.6 Połączenie w klaster dostarczonego serwera z serwerami zamawiającego - klaster docelowo ma pracować w trybie zwirtualizowanym.

1.7 <u>Przygotowanie planu migracji - dostarczenie w ciągu 7 dni planu tej migracji z uwzględnieniem braków przestojów dla kluczowych usług.</u>

1.8 Montaż i przygotowanie NAS do działania w trybie zwirtualizowanego środowiska (w związku z klastrem).

1.9 Przygotowanie scenariusza wirtualizacji środowiska, na którym docelowo ma pracować utworzony klaster w trybie zwirtualizowanym jako rozwiązanie klastrowe z uwzględnieniem usług obecnie wdrożonych u zamawiającego - w ramach przygotowania tego scenariusza należy wykonać audyt obecnego środowiska pracy maszyn serwerowych z uwzględnieniem maszyn fizycznych i maszyn zwirtualizowanych, czego wynikiem ma być powstały **<u>scenariusz w terminie 7 dni.</u>**

1.10 Utworzenie na urządzeniu NAS dwóch oddzielnych wolumenów tak aby jeden działał w trybie storage, a drugi jako backup.

1.11 Wdrożenie kontrolera domeny (opis wdrożenia w **Załączniku nr 1**)

1.12 Montaż i konfiguracja switcha do poprawnej obsługi kontrolera domeny.

1.13 Konfiguracja switchy w trybie wysokiej dostępności sieci - (stackowanie po portach, które należy logicznie podzielić przy użyciu VLAN zgodnie z życzeniami klienta).

1.14 Wykonanie dokumentacji powykonawczej w zakresie opisowym oraz zwizualizowanym (szczegółowy opis w **Załączniku nr 3**)

Przedmiotem zamówienia jest dostawa i budowa nowej infrastruktury Data Center (określanego w dalszej części niniejszego dokumentu jako „**System**”) **wraz z usługą migracji** istniejącego środowiska Zamawiającego na dostarczany System

Przedmiot zamówienia obejmuje realizację następujących etapów:

Etap 1 – dostawa i uruchomienie infrastruktury technicznej dedykowanej wraz z dostarczeniem licencji na oprogramowanie tworzące System. Wykonawca dostarczy, skonfiguruje i uruchomi sprzęt, okablowanie oraz oprogramowanie niezbędne do zapewnienia stabilnego działania Systemu, jego wysokiej wydajności i zgodności z obowiązującymi przepisami prawa. Dostawa dotyczyć może zarówno nowego sprzętu, oprogramowania i licencji, jak i nowych lub dodatkowych komponentów. Licencje powinny umożliwiać uruchomianie wirtualizacji na dostarczanych serwerach fizycznych i obejmować pełne wykorzystanie procesorów i pamięci operacyjnej.

Etap 2 – uruchomienie środowiska testowego, końcowa konfiguracja Systemu,

Wykonawca uruchomi środowisko testowe poprzez przeniesie środowiska wdrożeniowego do infrastruktury Zamawiającego. Wykonawca w sposób uzgodniony z Zamawiającym na etapie Projektu Technicznego Wdrożenia wykona ostateczną konfigurację Systemu na środowisku testowym posiadającym pełną oczekiwaną funkcjonalność wskazaną w Opisie Przedmiotu Zamówienia (Klaster wraz z usługa migracji) tak aby umożliwić Zamawiającemu szczegółową weryfikację wdrożonego Systemu,

Etap 3 – uruchomienie środowiska produkcyjnego, dostawa dokumentacji technicznej Systemu, dostawa instrukcji obsługi Systemu.

Wykonawca wniesie korekty wynikające z audytu oraz testów przeprowadzonych przez Zamawiającego i uruchomi środowisko produkcyjne Systemu. Wykonawca wykona ostateczną konfigurację, testy i uruchomienie środowiska produkcyjnego Systemu spełniającego całość wymagań wskazanych w Opisie Przedmiotu Zamówienia. Wszelkie prace związane z instalacją i uruchomieniem elementów infrastruktury technicznej muszą zostać wcześniej uzgodnione z Zamawiającym i będą realizowane w ramach godzin pracy Zamawiającego. Realizacja tych prac nie mogą kolidować z działaniem innych systemów użytkowanych przez Zamawiającego

Infrastruktura techniczna Systemu

Wykonawca zobowiązany jest to dostarczenia oraz skonfigurowania i uruchomienia takich elementów infrastruktury technicznej, aby wypełnić wymagania postawione przed Systemem

Na potrzeby Systemu przewiduje się zastosowanie dwóch serwerów fizycznych, NAS i 2 przełączników sieciowych wraz z wymaganymi w OPZ licencjami, oraz wykonaniem usługi konfiguracji środowiska wirtualnego opartego o wymagany w postępowaniu wirtualizator Microsoft Hyper-V.

Jeżeli do osiągnięcia wszystkich zakładanych celów wdrożenia Systemu (funkcjonalnych, wydajnościowych, niezawodności) niezbędne okaże się zastosowanie również jakichś innych elementów infrastruktury technicznej, to Wykonawca zobowiązany jest do ich dostarczenia i uruchomienia. W tym przypadku wszystkie wymagania dotyczące opisanej w tym dokumencie infrastruktury technicznej mają zastosowanie również do tych dodatkowych elementów, w

szczególności wymóg, że Zamawiający nie dopuszcza uruchamiania jakichkolwiek funkcjonalności bezpośrednio na serwerach fizycznych, bez zastosowania wirtualizacji niezgodnej z Projektem Technicznym Wdrożenia.

Koncepcja wdrożenia

Koncepcja wdrożenia zakłada instalację serwera fizycznego, na których Wykonawca zobowiązany będzie do instalacji klastra wirtualizacyjnego opartego o rozwiązanie firmy Microsoft Hyper-V oraz do przeprowadzenia migracji obecnie istniejącego środowiska Zamawiającego również opartego o środowisko firmy Microsoft Hyper-V, na nowo utworzoną infrastrukturę.
Równolegle zakłada się prowadzenie prac wirtualizacji serwera systemu obiegu dokumentów na infrastrukturę klastra wysokiej dostępności.
Po skutecznym kroku migracji wirtualnych maszyn z serwera, Zamawiający wymaga instalacji będącego poza klastrem wysokiej dostępności, wirtualizatora Microsoft Hyper-V oraz instalacji wirtualnych maszyn oraz serwera plików.
Schemat działań przedstawiono w **Załączniku nr 2.**

Załącznik nr 1

Wdrożenie kontrolera domeny Active Directory z usługami:

Część 1. Założenia

W ramach wdrożenia serwera zostanie również przeprowadzona instalacja i wdrożenie kontrolera domeny umożliwiającego chociażby centralne zarządzanie znaczną liczbą użytkowników, urządzeń, możliwymi dostępami oraz przede wszystkim bezpieczeństwem.
Do głównych zalet posiadania domeny poza wyżej wymienionymi należy zaliczyć:

- zarządzanie hasłami i uprawnieniami użytkowników (np. RODO)
- automatyczne aktualizacje i instalacja oprogramowania w firmie
- prostsze uwierzytelnianie – wprowadzając usługi katalogowe administrator może dać użytkownikowi za pomocą jednego logowania dostęp do określonych zasobów – możliwość powiązania wielu programów z logowaniem domenowym skracającym czas i zwiększającym efektywność
- redukcję kosztów związaną z centralnym administrowaniem kontami użytkownika – czas pracy administratorów, zarządzanie ilością licencji/kont

Do wdrożenia Active Directory w pełnym zakresie funkcjonalności wymagane jest od Zamawiającego posiadanie komputerów z zainstalowanym systemem operacyjnym Windows w wersji Professional lub Enterprise.
Dodatkowo wraz z uruchomieniem kontrolera domeny wdrożone zostaną usługi terminalowe oraz DNS.

Część 2. Plan wdrożenia

Prace na serwerze:

- Instalacja na serwerze usługi AD
- Konfiguracja DNS i DHCP sieci lokalnej
- Przygotowanie - logiczny wygląd drzewa
- Wdrożenie - fizycznie las

Prace na stacjach roboczych:

- Migracja profili użytkownika z sieci lokalnej
- Dodanie AD na stacjach roboczych
- Konfiguracja użytkowników
- Opracowanie instrukcji migracji danych i przeprowadzenie 3 wspólnych migracji danych

Na serwerze AD przygotowanie środowiska do procesu synchronizacji / migracji lasu do Azure Active Directory.

Załącznik nr. 2

Zakres prac wdrożeniowych w kolejności wykonania

W ramach prac wdrożeniowych przeprowadzone zostaną następujące czynności:

- Projekt realizacyjny:
    - Analiza przedwdrożeniowa
    - Szczegółowa architektura wdrożenia
    - Dokumentacja projektowa
- Akceptacja Zamawiającego + naniesienie ewentualnych zmian
- Przygotowanie środowiska zgodnie z dokumentacją projektową:
    - Konfiguracja NAS i serwera w oparciu o środowisko Microsoft Hyper-V
    - Przygotowanie scenariusza migracji
- Migracja środowiska wirtualnego
    - Realizacja scenariusza migracji poprzez:
    - Migracja wirtualnych maszyn Zamawiającego na dostarczony NAS i serwer
    - Wirtualizacja serwera systemu obiegu dokumentów opartego na systemie Linux na dostarczony NAS i serwer
    - Weryfikacja poprawności migracji

- Usługi powdrożeniowe:
    - Przygotowanie serwera pod wirtualizację - instalacja 10 wirtualnych maszyn - zapasowego kontrolera domeny oraz serwera plików
- Dokumentacja powdrożeniowa wraz ze schematem połączeń
- Odbiór prac przez Zamawiającego

Załącznik nr 3

Wykonanie dokumentacji powykonawczej w zakresie opisowym oraz zwizualizowanym

Etap 1. Wykonanie pełnego skanu infrastruktury wraz z raportem przy użyciu narzędzia do eksploracji sieci i skaner portów/zabezpieczeń Nmap:
Opis narzędzia:

Nmap (ang. „Network Mapper") jest narzędziem open source do eksploracji sieci i audytów bezpieczeństwa. Został zaprojektowany do szybkiego skanowania dużych sieci, ale również działa dobrze w stosunku do pojedynczych adresów. Nmap wykorzystuje niskopoziomowe pakiety IP do wykrywania, które adresy są dostępne w sieci, jakie udostępniają usługi (nazwa aplikacji i wersja), na jakich systemach operacyjnych pracują (wersja systemu), jakie typy systemów zaporowych (firewall) są wykorzystywane i dziesiątek innych cech. Nmap jest powszechnie wykorzystywany do audytów bezpieczeństwa, również wielu administratorów sieci i systemów wykorzystuje go wykonywania rutynowych czynności, takich jak inwentaryzacja zasobów sieci, zarządzanie aktualizacjami oprogramowania i monitorowania systemów oraz ich czasu działania (uptime). Wynikiem działania Nmapa jest lista przeskanowanych adresów z dodatkowymi informacjami zależnymi od wykorzystanych opcji. Jedną z głównych informacji jest „lista interesujących portów". Zawiera ona numery portów wraz z protokołami, nazwami usługi i wykrytym stanem. Stan może zostać opisany jako otwarty, filtrowany, zamknięty, lub niefiltrowany. Otwarty oznacza, że aplikacja na badanym adresie oczekuje na połączenia/pakiety przychodzące na ten port. Filtrowany oznacza, że system zaporowy lub inne urządzenie blokujące ruch sieciowy nie dopuszcza komunikacji do tego portu i z tego powodu Nmap nie jest w stanie określić czy badany port jest otwarty czy zamknięty. Zamknięty port nie posiada aplikacji, która obsługuje komunikację sieciową. Porty sklasyfikowane jako niefiltrowane odpowiadały na zapytania Nmapa, jednak nie było możliwe określenie, czy były one otwarte czy zamknięte. Nmap raportuje kombinacje stanów otwarty|filtrowany i zamknięty|filtrowany jeśli nie jest w stanie określić, który z dwóch podanych stanów lepiej opisuje stan portu. Lista portów może również zawierać informacje o wykrytych wersjach oprogramowania, jeśli została włączona detekcja wersji. Jeśli została wybrana opcja skanowania dostępnych protokołów (-sO), Nmap zamiast listy portów dostarczy informacji na temat dostępności poszczególnych protokołów IP.
Poza listą interesujących portów, Nmap może dostarczyć dodatkowych informacje na temat badanych adresów, takich jak odwrotne nazwy DNS, prawdopodobne systemy operacyjne, typu urządzeń i adresy sprzętowe MAC.
Opcje oprogramowania Nmap:
Skrócona lista opcji jest wyświetlana przy uruchomieniu Nmapa bez dodatkowych parametrów, a jej najnowsza wersja jest zawsze dostępna pod adresem https://nmap.org/data/nmap.usage.txt.

Skrócona lista pozwala łatwiej zapamiętać najpopularniejsze opcje, ale nie zastąpi wgłębienia sie w resztę tej dokumentacji. Wiele z pozostałych opcji nie jest nawet zawartych na liście skróconej.
Użycie: nmap [Typ(y) skanowania] [Opcje] {specyfikacja celu}
SPECYFIKACJA CELU:
  Można podać nazwy hostów, adresy IP, sieci, itp.
  Przykłady: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <plik_wejściowy>: Odczytanie listy hostów/sieci z pliku
  -iR <ilość hostów>: Wybranie losowych adresów
  --exclude <host1[,host2][,host3],...>: Wyłączenie hostów/sieci
  --excludefile <plik_wyłączeń>: Wyłączenie listy hostów/sieci z pliku
WYKRYWANIE HOSTÓW:
  -sL: Lista skanowania - tylko wyświetla listę hostów do skanowania
  -sP: Skanowanie Ping - tylko wykrywanie dostępności hostów
  -P0: Traktuj wszystkie hosty jako dostępne - pomijanie wykrywania
  -PS/PA/PU [lista_portów]: Wykrywanie TCP SYN/ACK lub UDP na wybranych portach
  -PE/PP/PM: Zykrywanie za pomocą ICMP echo, timestamp, zapytania o maskę sieci
  -n/-R: Nie używaj zapytań DNS/Zawsze odpytuj DNS [domyślnie: czasami]
  --dns-servers <serv1[,serv2],...>: Używaj określonych serwerów DNS
  --system-dns: Używaj systemowych ustawień DNS
TECHNIKI SKANOWANIA:
  -sS/sT/sA/sW/sM: Skanowania TCP SYN/Connect()/ACK/Window/Maimon
  -sN/sF/sX: Skanowania TCP Null, FIN i Xmas
  --scanflags <flagi>: Ręczne narzucanie flag TCP
  -sI <host zombie[:port]>: Idlescan
  -sO: Skanowanie protokołów IP
  -b <host pośredni ftp>: Skanowanie FTP bounce
SPECYFIKACJA PORTÓW I KOLEJNOŚCI SKANOWANIA:
  -p <zakres portów>: Skanuj tylko podane porty
    Przykład: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
  -F: Szybkie skanowanie - tylko porty zawarte w pliku nmap-services
  -r: Skanuj porty kolejno - wyłączenie losowania kolejności
DETEKCJA USŁUG/WERSJI:
  -sV: Wykrywaj wersję usługi na otwartych portach
  --version-intensity <poziom>: Od 0 (tylko niektóre) do 9 (Używaj wszystkich testów)
  --version-light: Limituj do najpopularniejszych testów (poziom 2)
  --version-all: Używaj wszystkich testów (poziom 9)
  --version-trace: Pokazuj dokładne informacje podczas skanowania (do usuwania błędów)
DETEKCJA OS:
  -O: Włączenie wykrywania systemu operacyjnego
  --osscan-limit: Limitowanie wykrywania OS do obiecujących hostów
  --osscan-guess: Zgaduj wersję OS bardziej agresywnie
WYDAJNOŚĆ I ZALEŻNOŚCI CZASOWE:
  -T[0-5]: Ustaw szablon (wyższy jest szybszy)
  --min-hostgroup/max-hostgroup <rozmiar>: Rozmiary grup do równoległego skanowania
  --min-parallelism/max-parallelism <ilość_prób>: Zrównoleglenie testów
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <msec>: Specyfikuje czas testów
  --max-retries <ilość>: Ustala ilość możliwych powtórzeń testu

--host-timeout <msec>: Pomijaj po zadanym czasie
--scan-delay/--max-scan-delay <msec>: Ustalenie opóźnienia pomiędzy testami
OPCJE FIREWALL/IDS:
-f; --mtu <wartość>: fragmentacja pakietów (opcjonalnie z podanym MTU)
-D <decoy1,decoy2[,ME],...>: Ukrywaj skanowanie za pomocą innych hostów
-S <Adres_IP>: Podmieniaj adres nadawcy
-e <interfejs>: Używaj podanego interfejsu
-g/--source-port <portnum>: Używaj podanego portu źródłowego
--data-length <num>: Dodawaj losowe dane do wysyłanych pakietów
--ttl <wartość>: Ustaw czas życia pakietów
--spoof-mac <adres mac/prefix/producent>: Podmieniaj adres MAC
--badsum: Wysyłaj pakiety z nieprawidłową sumą kontrolną TCP/UDP
WYJŚCIE:
-oN/-oX/-oS/-oG <plik>: Zapisz wyniki w podanym pliku normalnie, w XML, s|<rIpt kIddi3
i formacie grepowalnym
-oA <nazwabazowa>: Zapisz wyniki w trzech formatach jednocześnie
-v: Podwyższenie poziomu raportowania (podwójne użycie powiększa efekt)
-d[poziom]: Ustaw lub podwyższ poziom debugowania (do najwyższego 9)
--packet-trace: Pokazuj wszystkie wysyłane i odbierane pakiety
--iflist: Wyświetl listę interfejsów i routingu (do wykrywania błędów)
--append-output: Dołącz nowe wyniki do już istniejących w pliku
--resume <nazwapliku>: Wznów przerwane skanowanie
--stylesheet <ścieżka/URL>: plik styli XSL do konwersji wyników w XML do formatu HTML
--webxml: Domyślny styl z Insecure.Org
--no-stylesheet: Wyłączenie dodawania styli do plików z wynikami XML
RÓŻNE:
-6: Włączenie skanowania IPv6
-A: Włączenie detekcji OS i wersji usług
--datadir <katalog>: Podanie katalogu z plikami danych Nmapa
--send-eth/--send-ip: Wysyłaj za pomocą ramek ethernet lub pakietów IP
--privileged: Zakładaj, że użytkownik ma odpowiednie uprawnienia
-V: Wyświetl numer wersji Nmapa
-h: Wyświetl stronę pomocy
PRZYKŁADY:
nmap -v -A scanme.nmap.org
nmap -v -sP 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -P0 -p 80
Specyfikacja portów i kolejności skanowania
Poza wszystkimi metodami skanowania opisanymi wcześniej, Nmap oferuje opcję pozwalającą na podanie numerów portów do skanowania i określenie czy skanowanie ma przebiegać w kolejności sekwencyjnej czy losowej. Domyślnie Nmap skanuje wszystkie porty do 1024 włącznie oraz wyższe porty wyszczególnione w pliku nmap-services.
-p <zakres portów> (Skanuj tylko wybrane porty)
Opcja pozwala na zdefiniowanie listy portów do skanowania, zamiast domyślnej. Możliwe jest podanie pojedynczych portów jak i zakresów oddzielonych myślnikiem (np. 1-1023). Zakres można również pominąć, co spowoduje użycie całego zakresu (1-65535). Można więc po prostu podać opcję -p- do przeskanowania wszystkich portów od 1 do 65535 włącznie. Można również podać

port zero, ale trzeba to zrobić jawnie. W przypadku połączenia tej opcji ze skanowaniem protokołów (-sO), określa ona numery protokołów do sprawdzenia (0-255).
Przy jednoczesnym skanowaniu portów TCP i UDP możliwe jest oddzielne zdefiniowanie portów dla obu protokołów poprzez poprzedzenie numerów znakami odpowiednio T: i U:. Jako argument opcji przyjmowany jest ciąg znaków aż do następnej opcji. Na przykład, podanie -p U:53,111,137,T:21-25,80,139,8080 spowoduje przeskanowanie portów UDP o numerach 53,111 i 137 oraz podanych portów TCP. Przy skanowaniu zarówno portów TCP jak i UDP, nie można zapomnieć podać odpowiednich typów skanowania: -sU oraz przynajmniej jednego TCP (np. -sS, -sF czy -sT). Jeśli nie podano protokołu skanowania, na czas skanowania numery portów zostaną dodane do domyślnej listy portów.
-F (Skanowanie Fast (ograniczona ilość portów))
Pozwala na określenie, że mają być skanowane tylko porty zawarte w pliku nmap-services z pakietu Nmapa (lub z pliku protokołów dla opcji -sO). Opcja ta pozwala na szybsze skanowanie niż w przypadku wszystkich 65535 portów. Ponieważ lista ta zawiera tylko nieco ponad 1200 portów, różnica w szybkości w porównaniu do typowego skanowania TCP (około 1650 portów) nie jest duża. Różnica może być większa, jeśli zostanie podany własny, mały plik nmap-services za pomocą opcji --datadir.
-r (Nie używaj losowej kolejności)
Domyślnie Nmap skanuje porty w kolejności losowej (poza niektórymi najczęściej wykorzystywanymi portami, które są skanowane na początku ze względów wydajnościowych). Takie zachowanie jest normalnie pożądane, jednak można je wyłączyć za pomocą opcji -r, wymuszającej sekwencyjną kolejność skanowania.

Przykład wykonania skanu portów:
Przykładowe adresy IP i nazwy domen powinny zostać zastąpione adresami/nazwami ze skanowanej sieci po wcześniejszym uzgodnieniu z Zamawiającym i otrzymaniu zgody na przeprowadzenie skanu portów.
Do celu testów, otrzymano do skanowania hosta scanme.nmap.org. Zgoda pozwala jedynie na skanowanie za pomocą Nmapa, nie zaś na testowanie exploitów czy przeprowadzanie ataków typu Denial of Service. Dla oszczędności pasma, nie uruchamiamy więcej niż tuzina skanowań tego hosta dziennie. W przypadku nadużyć, host zostanie wyłączony, a Nmap będzie zwracał komunikat Failed to resolve given hostname/IP: scanme.nmap.org. pozwolenie dotyczy także adresów scanme2.nmap.org, scanme3.nmap.org i następnych, choć hosty te jeszcze nie istnieją.
nmap -v scanme.nmap.org
Pozwoli na przeskanowanie wszystkich portów TCP adresu scanme.nmap.org. Opcja -v podwyższy poziom szczegółowości zwracanych informacji.
nmap -sS -O scanme.nmap.org/24
Uruchamia skanowanie SYN wszystkich 255 hostów znajdujących się w tej samej klasie „C”, co host scanme.nmap.org. Dodatkowo wykonywana jest próba detekcji systemu operacyjnego dla każdego hosta, który jest aktywny. Wymaga to uprawnień użytkownika root, z powodu wykorzystania skanowania SYN i wykrywania systemu operacyjnego.
nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127
Uruchamia enumerację hostów i skanowanie TCP pierwszej połowy każej z 255 możliwych 8-mio bitowych podsieci klasy B 198.116. Wykrywane jest działanie usług sshd, DNS, pop3d, imapd i portu 4564. Dla każdego z tych portów, który został wykryty jako otwarty przeprowadzane jest wykrywanie wersji działającej aplikacji.
nmap -v -iR 100000 -P0 -p 80

Poleca Nmapowi na wybranie 100,000 losowych hostów i przeskanowanie ich w poszukiwaniu serwerów WWW (port 80). Enumeracja hostów jest wyłączona za pomocą opcji -P0, ponieważ wysyłanie najpierw pakietów w celu określenia czy host jest aktywny nie ma sensu, jako że i tak jest wykonywany test tylko na jednym porcie per host.
nmap -P0 -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20
Skanuje 4096 adresów IP w poszukiwaniu serwerów WWW (bez pingowania ich) i zapisuje wyniki w plikach XML i grepowalnym.
Etap 2. Wykonanie wizualizacji topologii zbudowanej infrastruktury

Magda Moczkodan
2022-08-24