HAFTA1

- **Sunucu (Server)** - Bilgisayar ağlarında, istemcilerin (kullanıcıların) erişebileceği, kullanımına ve paylaşımına açık kaynakları veya bazı servisleri (FTP, E-Posta, Web Sitesi) çalıştıran bilgisayar birimlerine verilen genel bir addır.

- **Sunucu işletim sistemleri**, ağ üzerindeki istemcilerin ve diğer donanımların birbirleri arasında veri alıp göndermelerini sağlayan ve kaynakların paylaşımını yöneten işletim sistemleridir.
    - Windows Server 2008, diğer Windows Server işletim sistemlerinin tamamen donanımdan bağımsız ilk sürümüdür. her şeyi komut satırından yapılıyor.

- **Hyper-V Sanallaştırması teknolojisi** ile aynı fiziksel sunucu üzerinde birden fazla işletim sistemi çalıştırmaktadır.

- **Network Access Protection (NAP)** - Windows Server 2008 ile birlikte gelen bir ağ güvenliği uygulamasıdır.
    - Sistem ağa bağlanan bilgisayarların durumlarına göre erişim izni verip vermemeye karar verir.
        - Güncel ve aktif bir anti-virüs programı olması
        - Etkin bir güvenlik duvarı bulunması
        - Belirli yazılım güncellemelerini yapmış olması gibi

HAFTA2

- **Sanallaştırma (Virtualization)** - Tek bir fiziksel makineden birden çok sanal makine (VM) yaratma işlemi.
    - SANALLAŞTIRMANIN AVANTAJLARI
        - Sunucu kapasitesini yüksek verimle kullanma olanağı sağlar.
        - Kurulum ve bakım maliyetlerinde ciddi düşmeler görülür.
        - Sanal işletim sistemine kurulmuş olan herhangi bir uygulamayı kaybetmeden alınan yedekleme ile yeni bir PC üzerine rahatlıkla aktarılabilir. Kaldığı yerden devam ederek, zaman ve bilgi kaybını önler.

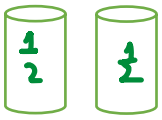
    - SANALLAŞTIRMA TÜRLERİ
        - Sunucu Sanallaştırma
        - Depolama Sanallaştırma
        - Ağ Sanallaştırma
        - Masaüstü ve Dizüstü Sanallaştırma
        - Uygulama Sanallaştırma

- SANALLAŞTIRMA YAZILIMLARI (Sunucu Sanallaştırma Çözümü)
  - Microsoft Hyper-v
  - Vmware
  - VirtualBox …

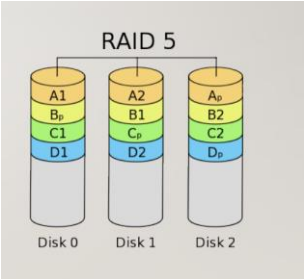
- **RAID (Redundant Array of Independent Disks)** - çeşitli nedenlerle bozulan harddisklerdeki kritik veri kayıplarını önlemek veya en aza indirmek amacıyla geliştirilmiş, diskleri ister performans isterseniz güvenlik gibi konularda konfigüre edebileceğiniz bir yapı sunar.
  - RAID oluşturulmasının amacı:
    - Hata toleransı sağlamak
    - Dizideki diskleri birleştirip yüksek depolama kapasitesi elde etmek
    - Performansı yükseltmektir
  - Yazılımsal RAID
    - Özel bir RAID kontrolörüne ihtiyaç duymadan RAID kurabileceğiniz anlamına gelir
  - Donanımsal RAID
    - RAID denetçi kartları (RAID Controller) ile yapılandırılan RAID teknolojisine verilen addır.

- **Popüler RAID Türleri**
  - RAID 0 - Disk şeritleme
    - En azından 2 diske ihtiyaç vardır, Hata toleransı yoktur!

  - RAID 1 - Disk yansıtma (Mirrorring)
    - Raid kartına aktarılan tüm veriler eş zamanlı olarak disklere yazılır
    - Raid 0'dan farklı olarak hata toleransı sağlar
    - disk kapasitesini 2'ye böldüğüdür.



  - RAID 5 - Eşlikli Disk Şeridi
    - En çok kullanılan RAID türüdür
    - Dosya ve uygulama sunucuları, okuma işlemlerin daha yoğun yapıldığı veritabanı sunucuları, WEB, mail sunucular için tavsiye edilir
    - Veriler disklere dağıtılarak yazılır. Aynı yazım sırasında verinin bir diskin hataya düşmesi durumunda verinin kurtarılması için bir veri bloğu daha, verinin yazılmadığı diğer diske yazılır. Bu veriye parite (eş veri) denir.



HAFTA3

- **WEB SUNUCU YAZILIMLARI**

    - Microsoft IIS (Internet Information Services)
        - Web sayfaları yayınlamak, Web uygulamaları çalıştırmak ve Web sunucuları kurup yayınlamak için kullanılan servislerdir.
        - .NET ortamında yazılım geliştirecek ve Web servisleri kullanacak yazılım geliştiriciler de IIS kurulu bir Windows işletim sistemine ihtiyaç duymaktadırlar.

    - Apache
        - Apache Yazılım Vakfı tarafından geliştirilen, açık kaynak kodlu ve ücretsiz bir web sunucu yazılımıdır
        - Hem Windows hem Linux üzerinde çalışır.
        - Yüksek trafiğe sahip web sitelerinde performans problemleri!

    - NGINX
        - Ücretsiz, açık kaynak kodlu, yüksek performanlı web sunucusu yazılımıdır.
        - Eğer yüksek trafiğe sahip bir web sitesi yönetiyorsanız, Nginx harika bir seçimdir
        - c10k problemine çözüm olarak oluşturulmuştur. (Bir web sunucusu eş zamanlı olarak 10,000'in üzerinde bağlantının altından kalkamama durumudur.)

    - XAMPP - Apache-Myqsl-Php-Perl
        - XAMPP en popüler PHP geliştirme ortamıdır.
        - Php kodlarının çalışması için gerekli olan apachi, mysql gibi sistemleri kurup çalıştıran programdır.

HAFTA 4

- **Domain Name System (DNS) -** İnternet uzayını bölümlemeye, bölümleri adlandırmaya ve bölümler arası iletişimi organize etmeye yarayan, bilgisayar, servis, internet veya özel bir ağa bağlı herhangi bir kaynak için hiyerarşik dağıtılmış bir adlandırma sistemidir.

    - Top Level Domain (TLD)
        - com – Commercial businesses.
        - gov – U.S. government agencies.
        - eu – European Union.

- Domain Name Server
  - BIND (Berkeley Internet Name Domain) - İnternet üzerinde kullanılan en yaygın DNS sunucusu yazılımıdır. Çözümleyici isimler ile ilgili sorguları ilgili sunucuya göndererek ve sunucudan yanıt alarak çözümleyen programdır.

  - Windows DNS Server - Microsoft tarafından geliştirilmiş ve Windows işletim sistemlerinde ek özellik olarak aktif edilip ayar yapılabilen yazılımdır.`

- DNS Çözümleme İteratif vs Rekürsif
  - Performans açısından hangisi daha iyidir? (Rekürsif)
  - Hangisi cache i şlemi i şlemi ile birlikte daha iyi çalışır? (Rekürsif)
  - İletişim maliyeti açısından hangisi daha iyidir? (Rekürsif)

- Registery Kavramları
  - Registry
    - Alan adların veritabanı
    - Bu veritabanını düzenleme yetkisi bulunan organizasyon
  - Registrar
    - Registrant için Registry ye de ğişiklik iste ğini ileten elçi
  - Registrant
    - Alan adını kullanan varlık

- Types of Name Servers
  - Authoritative: Veriyi yöneten
    - Master: Verinin düzenlendiği
    - Slave: Verinin kopyasının tutulduğu
  - Caching: Authotitative sunuculardan alınan verinin saklandığı

- A kaydı
  - DNS sunucularda en çok kullanılan kayıt türüdür.
  - Alan adı altında bulunan herhangi bir alt alan adının hangi IP adresi ile eşleştiği bilgisini içerir.

- CNAME kaydı
  - CNAME kayıtları her hangi bir A (Host) kaydına takma ad olarak farklı alt alan adı kayıtları tanımlamak için kullanılır.
  - Başka bir deyişle CNAME kaydı kullanmadaki esas amaç, tek bir host kaydını değiştirerek ona bağlı çalışan alias kayıtlarını bir seferde güncelleyebilmektir.

- NS kaydı
  - NS kayıtları, kullanıldıkları bölge için yetkili olan alan adı sunucularını tanımlamak için kullanılır.
- MX kaydı
  - MX kayıtları, bir alan adı için gelen e-postaların işlendiği veya forward edildiği sunucu bilgisini içerir.
  - Aynı alan adı için birden fazla sunucuya MX kaydı tanımlamak mümkündür.

- PTR kaydı
  - Ters DNS kayıtları için reverse zone dosyalarında tanımlanan kayıtlardır
  - IP adresine karşılık host ismine çözümleme yapmak için kullanılır.

- AAAA Kayıtları
  - A kaydı ile aynı işi yapan fakat IPv6 ile kullanılmak üzere tasarlanan kayıtlardır.

- TXT Kayıtları
  - Gerektiğinde kullanılmak üzere metin tabanlı bilgi tutan kayıtlardır. Genelde e-posta sunucularında doğrulama için kullanılan SPF kayıtlarını tutmak üzere tercih edilmektedirler.

HAFTA 5

- **DHCP (Dynamic Host Configuration Protocol) server** - IP adreslerini dağıtan bir servistir. DHCP, PC static IP adresi tahsisi yapıyor

  - DHCP sunucu, kendisine ulaşan isteklere karşılık, kendi IP havuzundan bir IP adresini istemciye gönderir. stemci kapandığında aldığı IP adresini bırakmış olur. Bu işleme "Kiralama (lease)" denir.

  - DHCP ILE ATANABİLEN ADRESLER
    - Ip adresi
    - Default gateway adresi
    - Subnet mask adresi
    - Dns adresleri DHCP ile otomatik olarak atanabilir

  - DHCP'NİN AVANTAJLARI
    - IP adresleri merkezi yoldan dağıtılır.
    - Cihazlar arası IP çakışmaları engellenir.
    - Cihazları tek tek dolaşıp elle Ip vermektense otomatik olarak dağıtır bu sayede sistem yöneticisinin i ş yükünü hafifletir.

- DHCP'NİN BİLEŞENLERİ

  - Scope (kapsam): Network ortamındaki istemcilere verilecek Ip adresi aralığı ve kiralama süresi gibi bilgileri içerir.

  - SuperScope (üst kapsam): SuperScope aynı fiziksel networkte bulunan birden çok mantıksal IP Networkünü desteklerken kullanılabilecek kapsamların yönetimsel gruplandırmasıdır

  - Exclusion Range (dışlama aralığı): Kapsamdaki IP aralığı içinden başka bir IP aralığını dışlamak için kullanılır.Dışlama aralığındaki IP adresleri networkteki hiç bir bilgisayara atanmaz.

  - Address Range (adres aralığı): Dhcp kapsamında otomatik olarak Ip atanabilecek Ip adresleri havuzudur.

  - Lease (kiralama): Dhcp sunucusu tarafından belirlenen ve istemci bilgisayarın kendisi için atanan Ip adreslerini kullanabileceği süredir. Default gelen süre : 8 gün'dür

  - Reservation (rezervasyon): Dhcp sunucusu tarafından kalıcı bir Ip adresi atanmak istendiği zaman rezervasyon işlemi kullanılır. Rezervasyon cihaz'ın her zaman aynı Ip adresi almasını sağlar.

  - Scope Options: Ip adresi ve SubnetMask değerinin dışındaki TCP/IP yapılandırma bilgisidir.Network'teki Router veya Dns server'ın bilgileri gibi

  - Dhcp relay agent: Kendi segmentinde Dhcp sunucusu bulunmayan istemcilerin Ip almasını sağlar.

- DHCP Client Haberleşme Protokolü

  - DHCP Discover (DHCP keşfi): Client pc Broadcast yaparak ortamda DHCP server var mı bakar. Broadcast herkese gönderilen paketlerdir. Burada paketi alan ki şi bu hizmete cevap verebilecek kişidir. (DHCP Server)

  - DHCP Offer (Ip kiralama teklifi): Bu bir bilgi paketidir. DHCP hizmetini veren makine kendisinin verebileceğini burada belirtiyor. DHCP Server Broadcast yaparak IP teklif eder.

  - DHCP Request (Kiralanacak Ip isteği): Client pc Broadcast yaparak teklif edilen ipyi kabul ettiğini söyler.

  - DHCP ACK (Ip kiralama onayı): DHCP Server Broadcast yaparak Ipyi kullanması için izin verir

HAFTA 6

- **VPN** - herkese açık bir iletişim altyapısı üzerinden, iki veya daha fazla doğrulanmış/onaylanmış taraflar arasında güvenli veri iletişimi sağlamak üzere oluşturulmuş sanal ağlardır.
    - VPN AMACI
        - Güvenli olmayan bağlantı üzerinden güvenli iletişim
        - Özel adres ve protokölleri public adresler üzerinde işleme
    - VPN sanaldır:
        - VPN kullanıcısı bağlı olduğu esnada bağlantı yaptığı networkü sahiplenmez, bu network aynı anda birçok VPN kullanıcısı tarafından paylaşılır.
    - VPN özeldir:
        - VPN trafiğinin Internet üzerinden güvenli geçişini sağlamak için özel network önlemlerine ihtiyaç vardır
    - VPN bir Networktür
        - VPN, iki uç arasında güvenilir tünel bağlantısı sağlayan bir networktür.

- Bir İstemci VPN yoluyla bir ağa bağlanacaksa o ağa ait bir IP adresi alarak ilgili ağa katılır. O ağın üyesi olarak çalışır.

- VPN bağlantıları **PPTP, L2TP, SSTP** isimli protokoller kullanılarak sağlanır. Bu protokollere **TÜNEL protokolleri** denir.

    - Bu protokollerin temelinde PPP (Point to point Protokol) protokolü vardır. PPP protokolü çevirmeli bağlantı ve noktadan noktaya veri aktarımı için geliştirilmişlerdir

        - PPTP tünel yönetimi TCP bağlantısını (1723. port) ve tünel oluşturan veri için ise GRE kullanır
        - L2TP Cisco tarafından geliştirilen L2F ve PPTP protokollerinin birleşiminden oluşur. Ayrıca IPSec desteği mevcuttur.
        - SSTP(Secure Soket Tunel Protokolu) 443.TCP portu üzerinden HTTPS protokolünü kullanır.

- VPN ağları kullanım alanlarına göre **Access VPN**, **İntranet** Tabanlı VPN ve **Extranet** (İnternet) Tabanlı VPN olmak üzere üç çeşittir.

    - ***Access VPN*** gerçek kişiler tarafından bireysel kullanım amacıyla tercih edilir
        - Uzaktan erişimli VPN ile mobil kullanıcılar, küçük/ev uzak ofis (SOHO) merkeze dial-up olarak güvenli bir şekilde bağlanabilirler.
    - ***İntranet ve Extranet*** Tabanlı VPN ağlar tüzel kişiler (şirketler, üniversiteler gibi kurum ve kuruluşlar) tarafından tercih edilmektedir.
        - Siteden Siteye VPN bağlantısı özel bir ağın iki bölümünü birbirine bağlar. Karşılıklı doğrulama sağlanır.
        - İş ortakları, iştirakler, ortak çalışılan şirketler ile yapılan güvenli bağlantılardır. *Extranet VPN* network kaynaklarına kontrollü erişim sağlar

- ***Extranet VPN'in sağladığı avantajlar***
  - VPN 'siz extranet bağlantılara göre maliyeti çok düşüktür.
  - birçok servis sağlayıcı seçeneği vardır.
  - İnternet üzerinden bağlantı ISP tarafından sağlandığı için ilave bir iş gücü gerektirmez dolayısı ile operasyon maliyeti de çok düşüktür

- Temelde iki tip VPN teknolojisi vardır

  - Remote Access VPN (Uzaktan erişim VPN)
    - Remote Access VPN'nin en önemli özelliği kimlik sorgulaması ile uzak ve gezgin kullanıcıların kimliklerini doğrulamasıdır. Kullanıcılar uygun erişim ve teknolojiye sahipse ISP ile bağlanabilir.
    - VPN tüneli'nin kurulması ve yönetimi istemcidedir ***voluntary tunnel*** - ***gönüllü tünel*** " olarak adlandırılır.

  - Site-to-site VPN (Siteden siteye VPN)
    - Bu VPN bağlantısı WAN (Wide Area Network) bağlantısı gibi çalışır. Ağlar, İnternet üzerinden verileri bir yönlendirici ile başka bir yönlendiriciye iletir.
    - Uzak erişim VPN istemcisinin aksine erişim kısmı (hiçbir şifreleme, hiçbir özel IP) özel değildir.
    - VPN istemcisi kendisi kontrolü altında olmadığından , Bu VPN moduna ***compulsory tunnel –zorunlu tunel*** " denir.

- <u>VPN Çalışma Yapısı</u>
  - Özel ağ bağlantısını taklit etmek için, gönderilen veriler gizlilik amacıyla şifrelenir. Paylaşılan veya ortak ağda ele geçirilen paketlerin şifreleri, şifreleme anahtarları olmadan çözülemez. Özel ağ verilerinin kapsüllendiği ve şifrelendiği bağlantı VPN bağlantısı olarak bilinir.

- **VPN 4 kritik Fonksiyonu yerine getirir**
  - Authentication
    - Veriyi gönderen, alanın doğru kişi olduğunu bilir.
  - Access control
    - Yetkisiz kişiler VPN'i kullanamaz.
  - Confidentiality
    - Veri gizliği garanti edilir.
  - Data Integrity
    - Veri bütünlüğü garanti edilir.

- **VPN ile 3 farklı güvenlik tekniği sağlanır.**

  - *Kapsülleme (VPN Tünelleme işlemi)*
    - Public ağlar üzerinden, Kiralık hatlar (Lease-line), Frame Relay, ISDN gibi iki nokta arasında daha sağlam, kesintisiz bir bağlantı hizmeti verir.

  - *Kimlik sorgulaması (Authentication)*

        - sadece yetkili kullanıcıların VPN hizmetini alabilmesi sağlanır

    - *Kriptolama (encryption)*
        - yapılacak haberleşmenin şifrelenerek başka kullanıcıların haberleşmeyi dinlemesi, veri bütünlüğü (data integrity) ile de kötü niyetli kullanıcıların yolladığınız paketlerin içeriğini değiştirebilmeleri engellenir.

- Tünelleme (Enkapsülasyon) - Bu teknik organizasyonlara Internet üzerinden kendi sanal networklerini oluşturma imkanı sağlar. Intranet dışından hiç bir yetkisiz kullanıcı intranete erişim yetkisine sahip değildir.

- Tünelleme protokolleri, tünelin en ucundaki kullanıcı için, oturum yönetimi olarak bilinen işlemleri gerçekleştirmek üzere, tünelleri kurar ve yönetir.

- **Tünel tekniğini 2 fazda anlatılabilir**

    - Faz1: İstemci VPN isteğini gönderir ve HA (Home Agent) sistemi bu istemcinin kimlik sorgulamasını yapar.
    - Faz2: Tünel içinden veri transferi başlatılır.

- **TÜNELLEME PROTOKOLLERİ**
    - Taşıyıcı protokoller
        - Tünellenmiş paketlerin Internet üzerinden iletimini sağlamak için bu paketleri yönlendirir.
        - Tünellenmiş paketler bu protokolün paketleri içine enkapsüle edilir.

    - Enkapsüle protokolleri
        - Pay-load paketin enkapsüle edilmesini sağlar. Bu protokol ile tünel kurulur ve sonlandırılır
        - Günümüzde en yaygın olan enkapsüle protokolleri PPTP, L2TP, ve IPSEC'dir

    - İletim protokolleri
        - Tünel içinden iletilmesi amacıyla enkapsüle edilmesi gereken orijinal veriler için bu protokol devreye girer
        - En yaygın olan iletim protokolleri PPP ve SLIP protokolleridir

FTP

- TCP/IP protokolünü kullanır.

FTP ÇÖZDÜĞÜ SORUNLAR

- İki sistem farklı dosya adı kuralları kullanabilir.
- İki sistemin metin ve verileri temsil etmek için farklı yolları olabilir.
- ki sistem farklı dizin yapılarına sahip olabilir.

- Kontrol bağlantısı için Port 21 kullanılır,
- 20 numaralı bağlantı noktası veri bağlantısı için kullanılır.

BAĞLANTI KONTROLÜ

- Sunucu, 21 numaralı bağlantı noktasında pasif açık (passive open) verir ve bir istemci bekler.
- İstemci, geçici bir bağlantı noktası kullanır ve etkin açık (active open) verir.

- birden fazla dosya aktarılırsa veri bağlantısı birden çok kezaçılıp kapatılabilir

- FTP, kontrol bağlantısı üzerinden iletişim kurmak için SMTP ile aynı yaklaşımı kullanır.

- Heterojenlik sorunu, dosyayı veri bağlantısı üzerinden göndermeden önce üç iletişim özniteliği tanımlanarak çözülür:

- dosya tipi
- veri yapısı
- iletim modu

- FTP, veri bağlantısı üzerinden aşağıdaki dosya türlerinden birini aktarabilir:

• ASCII dosyası.
• EBCDIC dosyası
• Resim dosyası

- FTP, aşağıdaki üç iletim modundan birini kullanarak veri bağlantısı üzerinden bir dosya aktarabilir:

• Akış (stream) modu
• Blok (block) modu.
• Sıkıştırılmış (compressed) mod

SMTP

- Sadece e-posta yollamak için kullanılan protokol.
- 25 numaralı portlar SMTP sunucusu için ayrılmıştır.

SMTP İLETİŞİM İŞLEMİ

1. SMTP İstemcisi, hedef alan adını arar.
2. Oturum Başlatma
3. İstemci Başlatma
4. Posta İşlem(ler)i
5. Sonlandırma

Yanıt kodları

3 basamaktan oluşur: xyz
x – Yanıtın iyi, kötü veya eksik olup olmadığını belirtir
y – Hatanın türünü belirtir
z – Belirtilen hata türünün neden oluştuğuna ilişkin belirli birneden sağlar

SMTP MAIL NESNELERİ

- Mektup
- İçerik

- 587 SMTP sunucusu tarafından desteklenir ve şifresiz veya TLS bağlantılar için kullanılır

IMAP

IMAP4 olarak de bilinen IMAP, yerel kullanıcıların uzaktaki bir e-posta sunucusuna erişmesini sağlayan bir uygulama katmanı protokolüdür.

POP3

POP3, yalnızca e-postayı almak için ve son kullanıcılar tarafından kullanılır.

SMTP İLE İLETİŞİM KURMAK İÇİN GEREKLİ BİLGİLER

*Kullanıcı adı
*Şifre
*Giden sunucu adresi
*Gelen sunucu adresi

EN YAYGIN E-POSTA SUNUCULARI

Windows platformu üzerinde : MS Exchange Server, MailEnable, hMailServer

Unix/Linux üzerinde: Sendmail **Postfix** Qmail Exim

DOCKER

- Docker Linux tabanlı uygulama sanallaştırma teknolojisidir ve Linux konteynerlerin içinde uygulama çalıştıran açık kaynak bir araçtır.
- Oluşturacağınız bir Docker konteynırı, herhangi farklı bir sistemde, her zaman beklenilen şekilde çalışır.

Kıyas türü	VM	Docker
OS	Tam işletim sistemi	Küçültülmüş işletim sistemi imajı
Izolasyon	Yüksek	Daha düşük
Çalışır hale gelmesi	Dakikalar	Saniyeler
Versiyonlama	Yok	Yüksek
Kolay paylaşılabilirlik	Düşük	Yüksek

Docker sistemi 5 ayrı parçadan oluşmaktadır.Bunlar aşağıda sıralanmıştır ;

l Docker Servisi
l Docker İstemcisi
l Docker İmajı
l Docker Kaynağı
l Docker Konteynırı

- Docker istemci ve daemon RESTful API soketi aracılığı ile iletişime geçer

Bir container ; işletim sistemi , kullanıcı tarafından eklenendosyalar ve metadatalardan meydana gelmektedir. Her birkonteynır bir imajdan meydana gelmektedir.

- 2 arayüz vardır. Bunlar ; **Shipyard** ve **DockerUI** dir.

SUNUCU GÜVENLİĞİ

ALINACAK TEDBİRLER

- Güvenlik duvarları sağlamak
- Güvenli iletişim protokolleri sağlamak
- Saldırı tespiti kurmak
- Zarar verici kodlara karşı yazılımlar kullanmak
- Güncel işletim sistemi kullanmak
- Network ayarlarından sadece IPv4 aktif olsun

GÜVENLİK TARAMA UYGULAMALARI

NESSUS :

- Uzaktan tarama aracı olarak kullanılır.
- Nessus, bilinen kurallara bağlı olmadan tarama yapabilmektedir

NMAP :

- Güvenlik denetlemelerinde ve ağ araştırmasında kullanılabilmektedir.
- IP paketleri yollayarak ağ üzerinde canlı bilgisayarı göstermektedir.

ETHEREAL :

- Windows ve UNIX için ağ analizcisidir
- ağ incelemesini gerçekleştirebilmektedir.
- TCP oturumu birleştirerek analiz imkanı tanıması özellikleri arasındadır

WINDOWS SUNUCU KONTROL LİSTESİ

- Destek verilen güncel Windows işletim sistemleri kullanının.
- BIOS ayarları alanını parola ile koruyun.
- Otomatik Güncellemeleri aktif etmeli, SSCM kullanılmalı(mümkünse).
- Sunucular Active Directory üzerine aktarılmalı.