DHCP Protokolü Nedir?

DHCP (Dynamic Host Configuration Protocol) protokolü çok büyük bir ağda statik olarak ip adresi veremeyeceğimiz için DHCP protokolünü kullanarak yerel alan ağımıza (LAN) katılan cihazlara dinamik olarak benzersiz ip adresi (LAN içerisinde özel ip adresleri atanıyor), alt ağ adresi, geçit yolu (gateway) adresi ve DNS bilgilerinin verilmesini sağlayan protokoldür. Bu adres atamalarını istemci için 68 UDP portunu, sunucu için ise 67 UDP portunu kullanarak gerçekleştirir.

DHCP Protokolü Nasıl Çalışır?

LAN içerisindeki bir bilgisayara ağ bilgileri atanırken dört adımdan oluşan mesajlaşma yapısı kullanılır. Bu adımlara bakacak olursak;

1)DHCP Discovery(DHCP Keşfi): Herhangi bir bilgiye sahip olmayan bir istemci ağ içerisinde tanınabilir olmak için ilk aşama olan DHCP Keşfi mesajı gönderir. Bu mesajın içeriğinde kendi ip adresi olmadığı için kaynak ip adresi 0.0.0.0 olacaktır. Ağ hakkında bir bilgisi olmadığı için hedef ip adresi ise 255.255.255.255 (alt ağlara bölünmemiş ağlarda broadcast yayın için kullanılan ip adresidir) olarak verilir. Paket ağın içine broadcast yayın ile bütün cihazlara gönderilir. Burada DHCP keşif mesajı bütün cihazlara iletilecektir yalnız DHCP sunucusu dışında diğer cihazlar bu mesajı açmadan drop edeceklerdir. Eğer ağ içerisinde bir dhcp server tanımlı değilse cihazlara geçici olarak APIPA adresleri atanır. Bu durumda cihaz belirli periyotlarda DHCP keşif mesajını ağa göndermeye devam edecektir.

2)DHCP Offer(DHCP Teklifi): Broadcast yayını ile ağa bırakılan DHCP keşif mesajını DHCP sunucusuna ulaştıktan sonra ip adresi havuzundan kullanılmayan bir ip adresini ve geçit yolu , DNS sunucu adresi ve alt ağ adresi gibi bilgileri içeren bir DHCP teklif mesajı gönderir. Bu gönderimi hedef istemcinin henüz bir ip adresi olmadığı için ağa broadcast yayın ile gönderir. DHCP keşif mesajından farklı olarak burada kaynak ip adresi sunucunun ip adresi verilir ve broadcast yayın olduğundan dolayı hedef ip adresine de 255.255.255.255 adresi girilir. (NOT: eğer ağ alt ağlara bölünmemiş ise broadcast yayını 255.255.255.255 adresinden gerçekleştirir. Alt ağlara bölme işlemi hakkındaki yazıma buradan ulaşabilirsiniz.)

3)DHCP Request(DHCP istek):Broadcast yayın olarak gönderilen DHCP teklif paketini alan istemci paket içerisindeki değerleri kabul ettiğini gösteren DHCP istek mesajı gönderecektir. Bu mesajı da henüz kabul ettiğini sunucuya bildirip DHCP kabul mesajı almadığı için kaynak ip adresini 0.0.0.0 , hedef ip adresini de yine broadcast yayın yapacağı için 255.255.255.255 olarak ağa bırakacaktır. Burada istemcinin yayın için ip adresini kullanabilmesi için sunucudan (ack-acknowledgement) kabul mesajını almış olması gerekiyor.

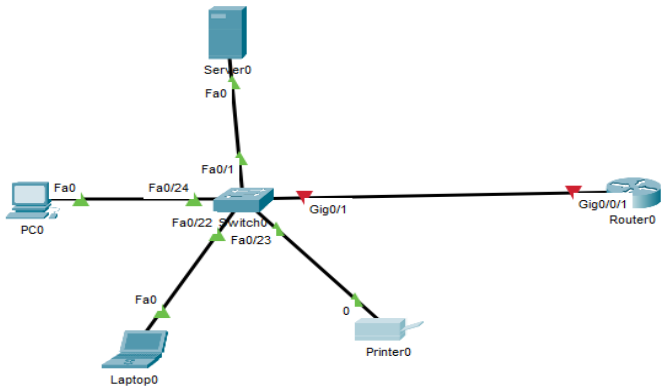
4)DHCP istek mesajını alan sunucu istemciye DHCP kabul mesajını yine broadcast yayın ile iletir. Artık istemci bu adresleri kullanmaya başlayabilir.

NOT : Bu mesajlaşmalarda ip adresini kullanım sürelerini içeren “lease” yani kiralama süresi bulunur. Bu süre dolduğunda istemci yine sunucu ile iletişime geçecektir.

SİMİLASYON UYGULAMASI:

Uygulama için Cisco Packet Tracer uygulamasını kullanacağım. İlk olarak “Network Devices” kısmından birer tane anahtar (switch) ve yönlendiriciyi (router) ekliyoruz. Daha sonda “End Devices” kısmına gelerek buradan bir sunucuyla beraber pc ve laptop cihazlarını ekleyelim. Cihazları ekledikten sonra cihazlar arasındaki bağlantıları aşağıdaki tabloya bakarak bağlayabilirsiniz. Son hali aşağıda gösterilmektedir. (Özetle aynı cihazlar çapraz, farklı cihazlar düz bağlanır.)

ÇAPRAZ			DÜZ	
SWİTCH	SWİTCH		SWİTCH	ROUTER
SWİTCH	HUB		SWİTCH	PC
HUB	HUB		SWİTCH	SUNUCU
ROUTER	ROUTER		HUB	PC
ROUTER	PC		HUB	SUNUCU
PC	PC			



Cihazları bağladıktan sonra ilk olarak yönlendiricinin ağımıza bağlandığı portunu gateway (geçit yolu) olarak yapılandırmalıyız. Bunun için aşağıdaki komutları girelim;

-no (router açıldığında hızlı yapılandırmayı istemediğimizi belirttik)

-en(ayrıcalıklı moda geçiş yaptık)

-configuration terminal(konfigürasyon moduna geçiş yaptık)

- interface gigabitEthernet 0/0/1(yönlendiricinin LAN a bağlı olan portunu seçtik(yapılandırma için))

- ip address 192.168.1.1 255.255.255.0(porta ip adresini atadık)

- no sh(portu aktif ettik)

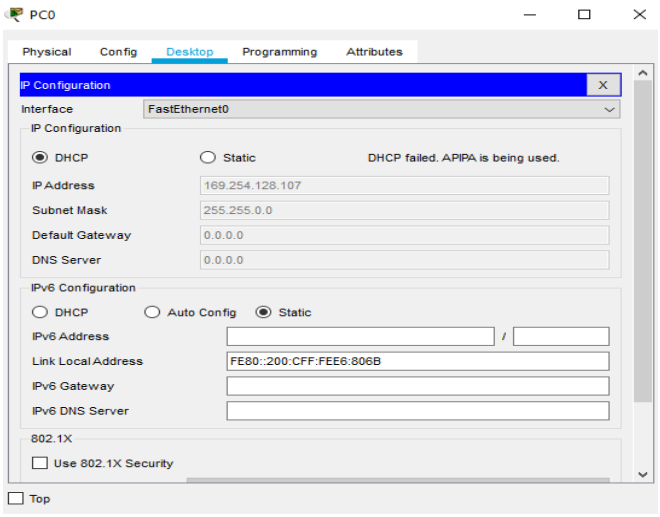
-end(ayrıcalıklı moda geçiş yaptık)

-wr(yapılandırmalarımızı NWRAM a kaydettik(kalıcı olması için))

DHCP sunucusunu yapılandırmaya başlamadan önce uç cihazlarımızın (end devices) ip atamasını statik yerine DHCP protokolü seçildiğinde karşımıza aşağıdaki gibi bir mesaj verecektir. Peki nedir bu APIPA.

APIPA (otomatik özel ip adresleme), Bir ağda DHCP sunucusu yapılandırılmadığında bir bilgisayarın kendisine otomatik olarak ip adresi atamasını sağlayan bir özelliğidir. (Not APIPA atanan bilgisayarlar için LAN içerisinde bilgisayarlar MAC adreslerini kullanarak iletişim kurdukları için APIPA adresleriyle sorun yaşamadan bilgisayarlar aralarında iletişim kurabilirler sadece ağ dışına çıkamazlar.) APIPA adresler atana bilgisayarlar belirli zaman aralıklarında yine DHCP keşif mesajları göndermeye devam

ederler. Sunucu ayağa kaldırıldığında cihazlara ip adreslerini ve diğer bilgilerini yukarıda açıkladığımız adımları izleyerek alırlar.



Bu durumu da açıkladıktan sonra artık istemci-sunucu arasındaki iletişimi gözlemlemek için DHCP sunucusunu yapılandırmaya başlayabiliriz. İlk olarak yönlendiricide bir ip adresi havuzu tanımlamamız gerekiyor. Bu havuzda DHCP protokolünün teklifte bulunacağı ip adresi aralığını belirliyoruz. Statik ip adresini ise havuzun ip aralığı dışında kalan ip adreslerini kurumdaki sunucular, yazıcılar gibi ip adresinin sabit olmasını istediğimiz cihazlara veriyoruz. Yapılandırmayı iki şekilde gerçekleştirebiliriz. İlk olarak yönlendiriciyi sunucu olarak yapılandırarak gerçekleştireceğiz. Bu kullanımı önerilmez çünkü yönlendiricilere iş yükü bindirmiş oluyoruz. Ardından tercih edilen uygulamamalarından biri olan sunucu üzerindeki yapılandırmasını gerçekleştireceğiz.

1-Yönlendiricide Yapılandırma-

-en

-conf ter

- ip dhcp excluded-address 192.168.1.1 192.168.1.15 (havuz dışında kalacak ip adreslerinin araığını belirledik 1-15 arasında)

- ip dhcp pool dynamicip (ardından bir havuz tanımladık)

- network 192.168.1.0 255.255.255.0 (ip adresi verilecek network adresini tanımladık)

- default-router 192.168.1.1 (istemcilere verilecek geçit yolu (gateway) adresini tanımladık)

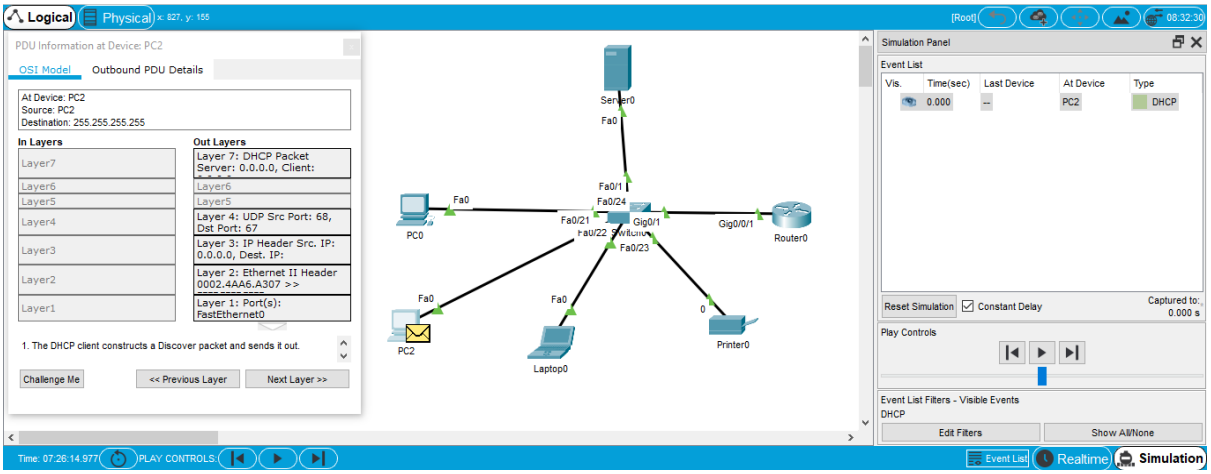
- dns-server 8.8.8.8 (istemcilere verilecek dns sunucu adresini belirledik)

***NOT Packet tracer uygulaması lease(kiralama) özelliğini desteklemediği için burada kullanamadık .

-end

-wr

Yönlendiriciyi DHCP sunucusu olarak yapılandırıldı. Artık yönlendiriciye bağlı cihazların ip adreslerine bakarsak ip adreslerinin atandığını görmüş olacağız. DHCP protokolünün çalışma adımlarını simüle etmek için uygulamamızı “Simulation” moduna getirdikten sonra anahtarımıza yeni bir cihaz bağlayarak ip konfigürasyonunu “DHCP” olarak seçiyoruz. Bu adımdan sonra artık gösterilen işaretleri kullanarak her adımda gönderilen ve alınan paket içeriklerini inceleyebilirsiniz.



Yönlendiricide yapılandırma sonrası atanan adresleri gözlemlemek için ise “en” komutuyla ayrıcalıklı moda geçerek “sh ip dhcp binding” komutunu kullanarak hangi ip adresinin hangi cihazlara atandığını gözlemleyebiliriz. Yapılandırma bilgilerini görebilmek için “sh ip dhcp pool dynamicip” komutu kullanabiliriz. Çakışan adresler olabilir. Bu çakışmaları görebilmek için “sh ip dhcp conflict” komutunu kullanıyoruz.

```
Router#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.1.16     0000.0CE6.806B            --                    Automatic
192.168.1.17     0060.3E1B.4B3E            --                    Automatic
192.168.1.18     00D0.BA57.58A9            --                    Automatic
192.168.1.19     000C.CF0E.0244            --                    Automatic
192.168.1.20     0002.4AA6.A307            --                    Automatic
```

NOT Burada yönlendiricinin farklı portlara bağlanmış farklı ağlar için de DHCP sunucusu gerçekleştirerek kullanmak mümküdür. Bunun için aynı yönlendiricide kullanılan örnek bir yapılandırma:

-en

-conf ter

- ip dhcp excluded-address 192.168.2.1 192.168.2.11

- ip dhcp pool dinamikip2

- network 192.168.2.0 255.255.255.0

- default-router 192.168.2.1

- dns-server 8.8.8.8

-end

-wr

Ardından yönlendiricinin “192.168.2.0” ağına bağlanan portuna ip adresi atayarak ayağa kaldırmak için:

-conf ter

- interface gigabitEthernet 0/0/0

- ip address 192.168.2.1 255.255.255.0

-no sh

Sonuç olarak “192.168.2.0” ağına bağlanan bilgisayara atanan bilgiler aşağıda gösterilmektedir.

2-Sunucuda Yapılandırma – İlk olarak yönlendiricide yapılandırmada oluşturduğumuz ağ topolojisini burada da oluşturmakla başlıyoruz. Cihazlar arasındaki bağlantıyı gerçekleştirdikten sonra yönlendiricinin portlarına geçit yolu görevi görebilmesi için ip adresi atayarak portlarını aktif hale getirdik. Kullanılan komutlar aşağıdaki gibidir;

-en

-conf ter

-interface gigabitEthernet 0/0/0

-ip address 192.168.1.1 255.255.255.0

-no sh

-end

-wr

-conf ter

-interface gigabitEthernet 0/0/1

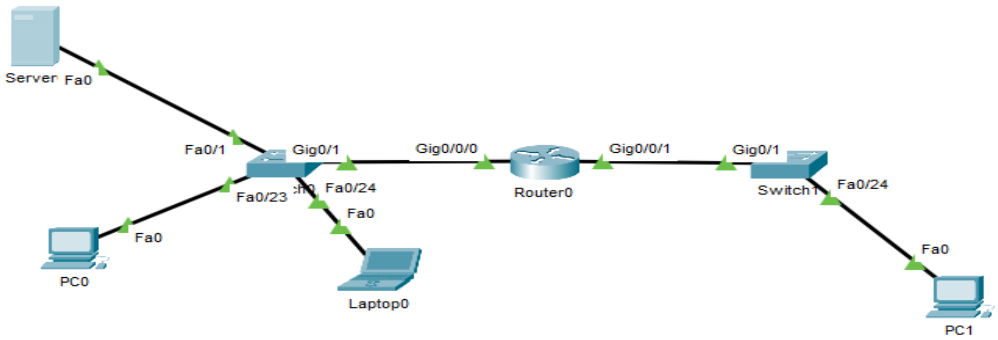
-ip address 192.168.2.1 255.255.255.0

-no sh

-end

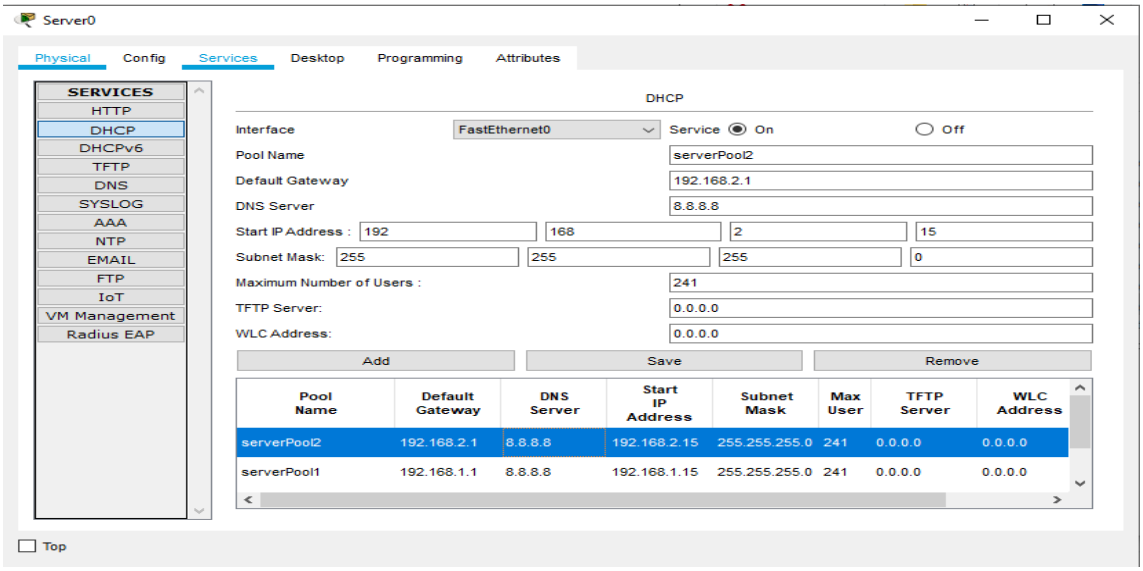
-wr

Yönlendirici portlarını da yapılandırdıktan sonra yapının son hali aşağıdaki gibi görünecektir.



Artık sunucuyu yapılandırmaya başlayabiliriz. Öncelikle sunucuya statik olarak ip adresi (dahil olduğu ağ içerisindeki DHCP havuzuna katılmamış ip adreslerinden kullanıyoruz) , DNS adresi, geçit yolu ve alt ağ bilgilerini veriyoruz. Daha sonra sunucuyu aktif hale getirebilmek için sırasıyla services->dhcp butonlarını seçiyoruz.

Burada öncelikle “services” kısmını “on” seçerek başlıyoruz. Havuz adını (pool name) belirledikten sonra geçityolu, DNS server adresini, atanmaya başlanacak ip adresinin başlangıç adresini ve alt ağ maskesini verdikten sonra “add” butonuna tıklayarak DHCP sunucusunu tanımlamış oluyoruz. Aynı işlemi DHCP protokolünün uygulanmasını istediğimiz “192.168.2.0” ağı için de tanımlayarak sunucu yapılandırmasını tamamlıyoruz ve “save” butonuyla kaydediyoruz. Sunucunun son durumu aşağıdaki gibidir.



Sunucunun yapılandırılması sonrasında bilindiği gibi DHCP protokolü broadcast yayın yaparak iletişim gerçekleştiriyordu ancak yönlendiriciler broadcast yayını geçirmiyorlar. Bu durumu düzeltmek için farklı ağın bağlı olan portun (Gig 0/0/1) yapılandırmasında sunucunun ip adresini kullanarak DHCP iletilerini geçirmesini sağlayacağız. Açıklamasına buradan https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/15-sy/dhcp-15-sy-book/dhcp-relay-agent.html ulaşabilirsiniz. Uygulamamızda kullandığım komutlar aşağıdaki gibidir;

-en

-conf ter

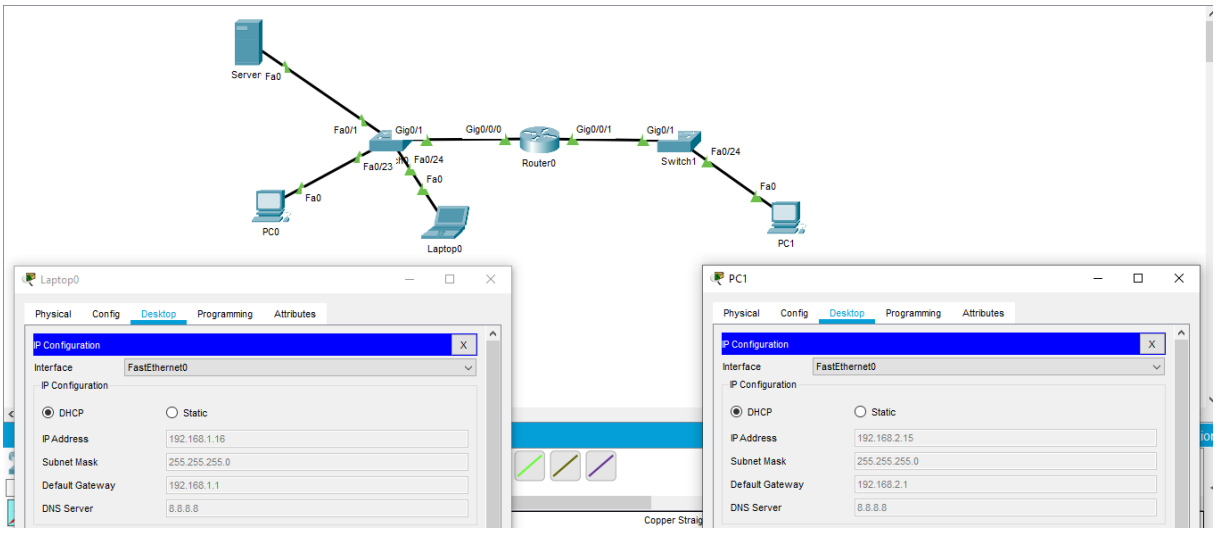
- interface gigabitEthernet 0/0/1

- ip helper-address 192.168.1.2

-end

-wr

Artık yapılandırmamızı tamamladık. Sonucu görmek için Ağa bağlanan cihazların ip atamalarını görebiliriz. Bu olayların akışını adım adım görmek için Packet Tracer uygulamasını “Simulation” modunda çalıştırarak görebilirsiniz. Yapılandırma sonrası durum aşağıdaki gibidir;



DHCP Sunucu Kullanmanın Faydaları:

-1- İp adreslerinin kolay yönetilebilir kılmasıdır. Ağdaki her cihaz için ip adresi bilgilerini benzersiz ve manuel olarak atanması gerekir. Bu işlem büyük dikkat ve uğraş gerektirir. DHCP protokolü bu durumda cihazlara atanacak cihazlara adresleri en az sorunla atayacaktır.

-2-Atanan adreslerin bilgileri burada tutulacağı için cihazlara atanan bütün adreslerin de kolaylıkla tek bir merkezde görüntülenmesini sağlayacaktır.

-3-Binlerce cihazın bulunduran büyük ağlarda aynı anda birden çok cihazın isteklerini karşılayarak adres atamalarını gerçekleştirebilir.

-4-Ağa bağlanan birden fazla cihazın giriş-çıkış yapmalarında veya mobil cihazlar, laptoplar gibi taşınabilir cihazların her ağ değişimlerinde manuel olarak atanması gereken bilgileri DHCP sunucusuyla ayrıca işlem yapmadan gerçekleştirmemizi sağlıyor.

-5-Sunucu ile atana ip adreslerinde iki cihaza aynı ip adresi atanma ihtimali çok düşüktür. Kısaca ip adreslerinin çakışma ihtimali çok düşüktür ki genelde statik olarak atanan ip adreslerinde karşılaşılan bir durumdur.

-6-Oluşturulan ip havuzunda kullanılacak ip adresi aralığını belirleyerek aralık dışında kalan adreslerle uzaktan erişim sağlayacağımız cihazlar için statik adresler atayabilmemizi sağlıyor.

DHCP Sunucunun Zayıflıkları:

DHCP protokolü de ikinci katman protokollerinden olduğu için arp protokolü gibi gelen paketlerde kimlik doğrulama yapılmıyor. Bu nedenle DHCP POİSONİNG , DHCP STARVATİON ,DNS POİSONİNG , DOS ve MITM gibi saldırılara maruz kalabiliyor. Bu saldırılar hakkında daha fazla bilgi almak ve uygulamalarının nasıl gerçekleştirildiğini görmek istiyorsanız yazılarını paylaştığımda saldırı adlarının üzerlerine tıklayarak öğrenebilirsiniz.

DHCP Protokolüne yönelik saldırılar:

1-DHCP Starvation

DHCP sunucusu yapılandırmasında da gösterildiği gibi sunucu istemcilere sunacağı IP adreslerini oluşturduğumuz bir IP havuzundan seçerek veriyordu. DHCP starvation saldırısı ise sunucunun havuzundaki bütün IP adreslerini kiralayarak sunucunun hizmet dışı kalmasını sağlar. Bu aynı zamanda bir DoS saldırısıdır. Saldırgan bu durumda ortadaki adam saldırıları (MITM) düzenleyebilir veya sahte bir DHCP sunucusu oluşturarak IP adresi almak isteyen cihazlar için geçit yolu adresini kendi bilgisayarının adresi olarak belirleyebilir. Bu durum cihazlara gelen trafiğin saldırgan bilgisayarında izlenebilmesini sağlar.

Bu saldırının uygulamasına ve alınabilecek önlemlere buradan ulaşabilirsiniz.

KAYNAK

https://www.bgasecurity.com/2015/08/dhcp-starvation-ve-sahte-dhcp-sunucusu/

https://www.greycampus.com/opencampus/ethical-hacking/dhcp-poisoning

https://www.cozumpark.com/dhcp-snooping-ve-yapilandirma-adimlari/

NOT: Özel ip adresler

10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255