NAT/DHCP/NMAP

NAT

NAT(Ağ Adresi Çeviricisi)

- IPv4'te her IP adresi kullanılabilir durumda değil. Maks. 3,2 Milyar

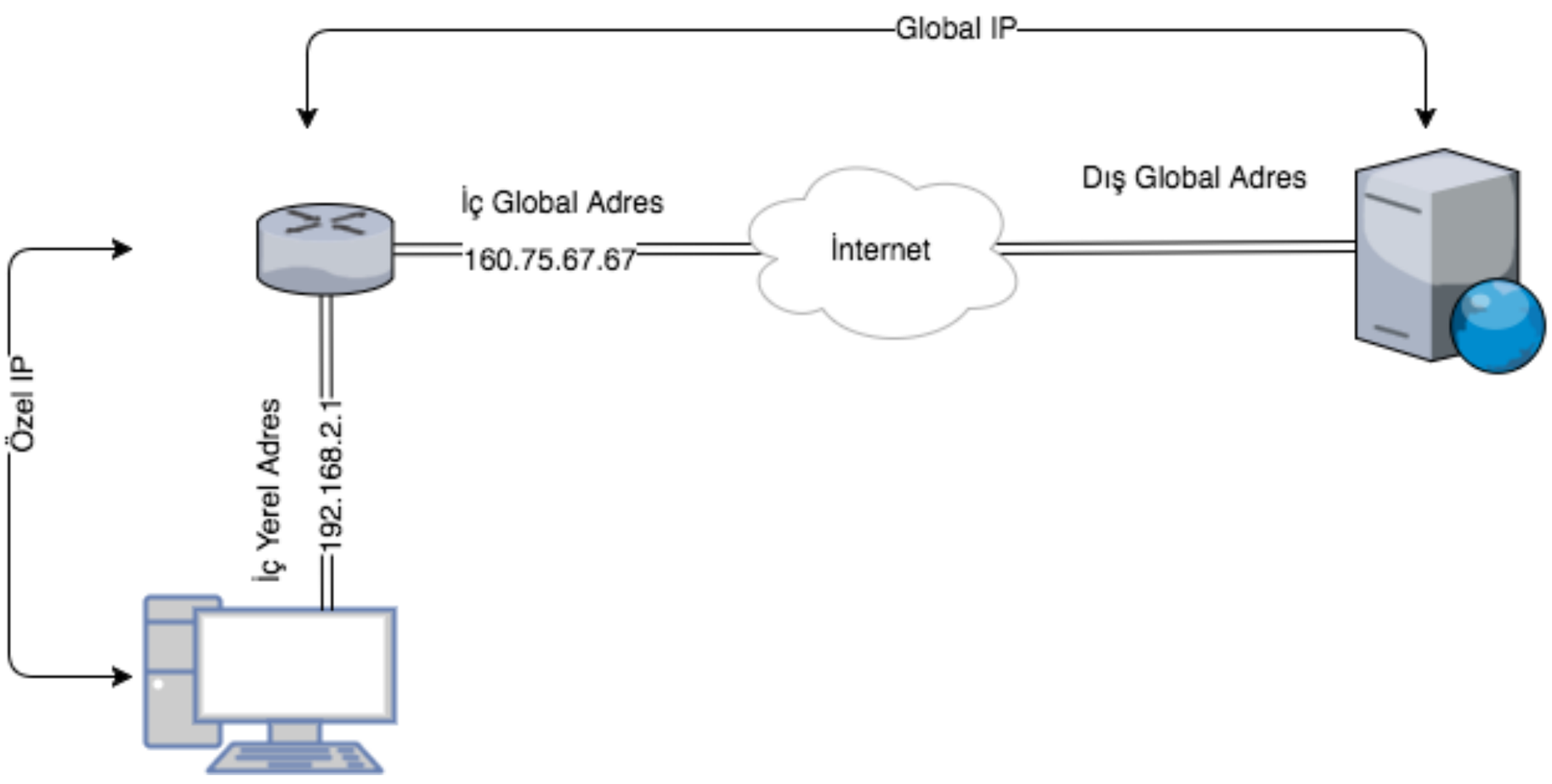
- Bu yetersizlik sebebiyle NAT geliştirilmiştir.

- NAT arkasında yerel ağlarda kullanılmak amacıyla ayrılan özel adresler kullanılmaktadır.

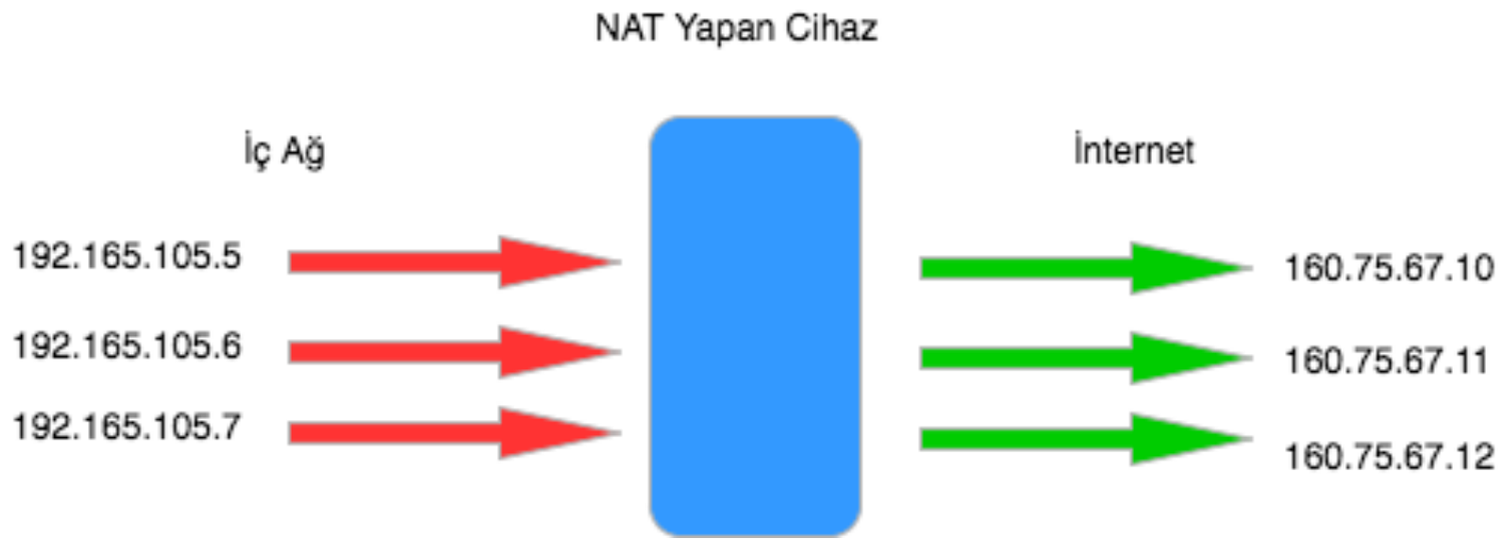
NAT

- Bir NAT yönlendiricisi NAT tablosu adı verilen bir tablo yardımıyla IP çevirme işlemini gerçekleştirir.
- Kullanıcının bilgisayarında özel IP adresleri aralığından bir adres bulunur.
- Buradan yerel ağın içinde olmayan bir adrese gitmek için talep gelince, NAT yönlendiricisi daha önceden kullanıcının ayarladığı NAT tablosuna bakarak özel IP adresini genel bir IP adresine çevirir ve bu şekilde dış ağlara ya da İnternete çıkılmış olur.
- Yönlendiricinin çeviri yaparak değiştirdiği bu IP, kullanıcının internetteki bilinen IP'sidir.
- Aynı şekilde dış ağlardan bu bilinen IP'ye doğru bir istek gelince, yönlendirici tablosuna bakarak bu IP'yi kullanıcının özel IP adresine yönlendirir ve paketi kullanıcının bilgisayarına gönderir.

NAT


Global IP
İç Global Adres
160.75.67.67
İnternet
Dış Global Adres
Özel IP
İç Yerel Adres
192.168.2.1

Static NAT

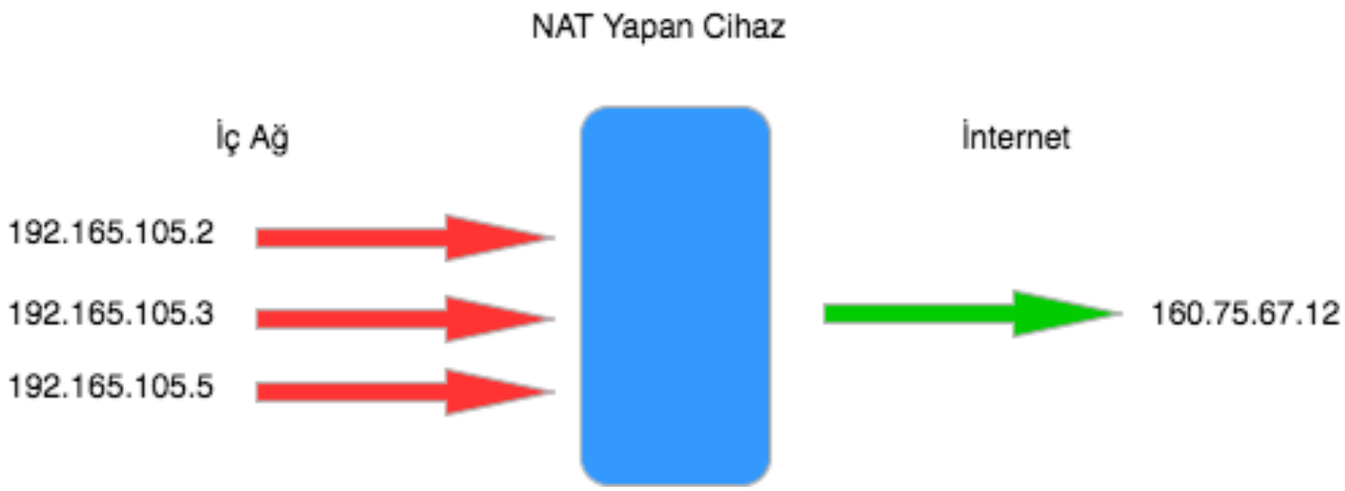


- Yerel ağda kullanılmakta olan özel IP’yi dışarıda kullanılacak olan genel IP'ye birebir çevirmedir.
- NAT tablosu doğrudan ağ yöneticisi tarafından doldurulur.
- Bu şekilde belirlenmiş adresler dışında hiç bir IP adresi dış ağlara bağlanamaz.

Dinamic NAT

- Sahip olunan genel IP adresi bloğu dinamik olarak özel IP adresleriyle eşleştirilir.
- Ağ yöneticisi bir IP adres havuzu belirler ve NAT yönlendiricisi otomatik olarak IP adreslerini eşleyerek dış ağlara bağlantıyı sağlar.
- Hangi IP ilk önce eşleşirse ilk önce İnternete o çıkar, eğer yeterli sayıda genel IP adresi varsa özel IP'lerin hepsi eşleştirilerek İnternete bağlanabilirler.
- Bağlantı kesildikten sonra ise NAT tablosundaki kayıtlar bir dahaki bağlantı kurulana kadar silinir.

Overloading NAT



- Bu NAT türüne aynı zamanda PAT (Port Address Translation – Port Adres Çevirimi) da denir.Ağ yöneticisi bir IP adres havuzu belirler ve NAT yönlendiricisi otomatik olarak IP adreslerini eşleyerek dış ağlara bağlantıyı sağlar.

- PAT'ta genel IP adresi olarak bir tane IP bulunur.

- Dinamik NAT'ta olduğu gibi yönlendirici NAT tablosunu kendisi oluşturur. Yerel ağda bulunan bir kullanıcıdan dışarıdaki ağlara bağlanmak için bir istek geldiğinde, yönlendirici bu kullanıcının özel IP adresini ve ona verdiği port numarasını NAT tablosuna kaydeder.

- Sahip olunan genel IP adresini yerel ağda bulunan kullanıcının özel IP adresi ve ona verdiği port numarası ile eşleştirerek internete erişmesini sağlar. Örn: 192.168.105.2:13511 | 160.75.67.12:13511

- Ağ yöneticisi isterse IP adreslerini kendi belirlediği port numaralarına kalıcı olarak atayabilir.

Pros vs Cons

- Az sayıda genel IP kullanılarak çok sayıda kullanıcı internete bağlanabildiği için IPv4'te bulunan IP yetersizliği sorunu azaltılmış olur. Birçok kullanıcı ve şirket İntranet adı verilen özel IP adreslerinden oluşmuş yerel ağlarını kullanarak, mümkün olduğunca az sayıda genel IP adresi üzerinden dış ağlara bağlanmaktadır.

- Yerel ağdaki kullanıcıların dış ağlara yönlendirici tarafından çevrilmiş IP'lerle bağlanması sonucunda etkili bir güvenlik sistemi sağlanmış olur. Özel IP kullanarak yerel ağda bulunan IP adresleri ve ağın topolojisi dış ağlara karşı gizlenmiş olur.

- NAT genel ağa olan bağlantıların esneklik derecesini artırır. Çoklu IP havuzları, yedek IP havuzları ve yük dengeleme havuzları güvenilir bir ağ bağlantısı sağlamak için uygulanabilirler.

- NAT yapılmamış ve özel IP adresleri kullanılmamış bir ağda, genel IP adreslerini değiştirmek için, mevcut ağ içerisindeki kullanıcılara yeniden bir adresleme yapmak gerekir. Bütün kullanıcıların IP adreslerini değiştirmek maliyet açısından da karlı bir durum değildir. NAT yapıldığında ağ yöneticisi yerel ağdaki kullanıcılar arasında kolaylıkla değişiklik yapılabilir, yeni kullanıcılar ekleyebilir ya da var olanları çıkarılabilir. NAT tablosu ayarları değiştirilerek, esnek bir şekilde hareket edilebilir.

- IP adresi ve port numaraları değiştirildiği için FTP ve bazı oyun protokolleri çalışmaz. Bazı İnternet protokolleri ve uygulamaları, çalışabilmesi için kaynak ve hedef IP adreslerine ihtiyaç duyar. Örneğin sayısal imza gibi bazı uygulamalar NAT tarafından kaynak IP adresi değiştirildiği için, NAT kullanılan yerel ağlarda çalışmazlar. Bazen bu sorun sabit (static) NAT kullanılarak ortadan kaldırılabilir.

- Belirli bir genel IP ile birçok kullanıcının İnternete bağlanmasından dolayı o IP'nin takip edilmesi mümkün değildir. NAT tarafından IP adreslerinin değiştirilmesi sonucunda IP paketlerinin izlenmesi ve kaynak IP adresinin bulunması zorlaşır.

- Fazladan bir yönlendirici daha kullanıldığı için paketlerde gecikme artabilir. Çünkü fazladan eklenen bir yönlendirici IP paket başlıklarının çevrilmesi ve etiketlenmesi sırasında oluşabilecek gecikmeleri artırır.

- NAT kullanmak IPsec gibi tünel protokollerinin kullanımını karmaşıklaştırır.

- Bir ağı NAT kullanımına uygun hale getirmek için topolojide değişiklik yapmak gerekir.

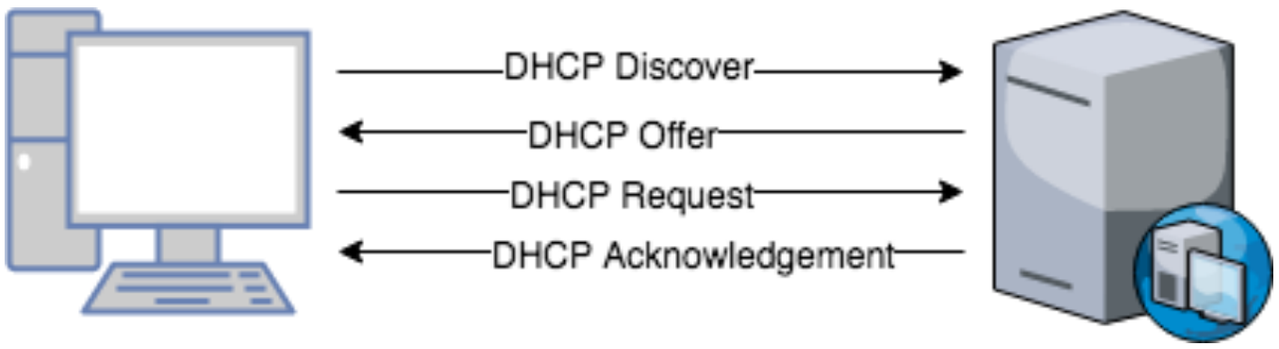
DHCP

DHCP

- Bir TCP/IP ağı üzerindeki her bir makineye dinamik olarak IP dağıtmak ve diğer yapılandırma ayarlarının yönetimini kolaylaştırmak için kullanılan bir IP standartıdır.

- TCP/IP protokolü ile çalışan bir ağ üzerindeki her bilgisayarın kendine özgü bir IP adresi olmalıdır. IP adresi ve alt ağ maskesi, ana makineyi ve bağlı olunan alt ağı belirlediği için; bir bilgisayar farklı bir alt ağa taşındığında IP adresinin de değişmesi gerekir.

DHCP



IP adresinin kullanım süresi bittiği zaman son iki paket yine sunucu ile istemci arasında haberleşmeyi sağlar. Tek bir fark vardır. Bu da bu iki mesaj bu sefer broadcast olarak yayınlanmaz. İstemci ve sunucu makine birbirlerinin IP adreslerini bildiğinden bu mesajları doğrudan birbirlerine yollarlar.

DHCP Discover

- DHCP istemci bilgisayar tarafından ağa gönderilen ilk pakettir. Bu paket genel yayım (broadcast) olarak tüm ağa gönderilir. Bu paketin kaynak IP adresi kısmında istemci henüz bir IP adresine sahip olmadığı için 0.0.0.0 adresi bulunur. Hedef IP adresinde ise 255.255.255.255 bulunur. Bu pakette istemci makinenin MAC adresi, kaynak MAC adresi kısmında bulunur. İstemci makine bu mesaja gerekli cevabı alamadığı zaman periyodik olarak bu mesajı yayınlamaya devam eder.

- Bu mesaj 342 veya 590 byte uzunluğunda olabilir. İlk 14 bayt Ethernet başlık bölümünü içerir. Daha sonraki 20 bayt'ta ise kaynak ve hedef IP adresleri bulunur. Sonraki 8 bayt ise UDP başlık kısmıdır. Burada UDP kaynak ve hedef port adresleri bulunur. Daha sonra ise "**Dhcpdiscover**" mesajının parametreleri gelir. Bu mesajda MAC adresi bulunduğundan eğer istemci makine için bir IP adresi tahsis edilmiş ise bu MAC adresini tanıyarak önceden tanımlı bu adresi gönderir.

DHCP Offer

- DHCP sunucu "discover" mesajını alınca adres alanında kullanılmamış bir IP adresi seçerek bunu bu mesaj ile istemci makineye gönderir. Bu pakette henüz istemci makinenin IP adresi bulunmadığından broadcast olarak yayınlanır. Bu mesajda ayrıca alt ağ maskesi, varsayılan ağ geçidi gibi parametreler de bulunur. Bu mesajın hedef MAC adresi kısmında istemci makinenin MAC adresi bulunur.

- Bu mesaj 342 bayt uzunluğundadır. İlk 14 bayt ethernet başlık kısmıdır. Daha sonraki 20 bayt IP başlık kısmıdır. Bu mesaj da broadcast olarak yayınlandığından hedef IP adresi 255.255.255.255'dir. Burada dikkat edilecek husus kaynak makine IP adresi kısmında DHCP sunucusunun IP adresinin bulunmasıdır. Daha sonra ise 8 baytlık UDP başlık kısmı gelir. Geri kalan 300 baytlık kısımda ise "Dhcpoffer" paketinin parametreleri gelir.

DHCP Request

- İstemci makine "Dhcpoffer" mesajını alınca gerekli parametreleri kabul ettiğini gösteren bu mesajı broadcast olarak yayınlar. DHCP, istemci makine "Dhcpoffer" mesajını alamazsa 2., 4., 8. ve 16. saniyelerde birer "Dhcpdiscover" mesajı daha gönderir. Yine cevap alamazsa her 5 dakikada periyodik olarak birer tane daha gönderir.

- Bu mesajda "Dhcpdiscover" mesajı gibi 342 veya 590 bayt uzunluğundadır. Bu mesaj istemci makinenin sunucu makine IP'sini bilmesine rağmen yine broadcast olarak yayınlanır. Bu pakette yine kaynak makinenin IP adresi kısmında 0.0.0.0 bulunur; çünkü istemci makine gönderilen IP adresini kabul ettiğini söyler; fakat bu IP adresini kullanabilmesi için DHCP sunucusundan "Dhcpnack" paketini alması gerekir.

DHCP Nack

- IP adres önerisini kabul eden istemci makineye DHCP sunucusu tarafından gönderilir. İstemci bu mesajı alamadan makine TCP/IP protokolünü kullanamaz.
- Bu mesaj 342 bayt uzunluğundadır. Bu mesaj da broadcast olarak yayınlanır. Hedef IP adresi kısmında 255.255.255.255 bulunur. Kaynak adresi olarak da DHCP sunucunun IP adresi bulunur. UDP başlık kısmından sonra ise bu mesajın parametreleri gelir. IP adresinin ne kadar süre ile bu istemci tarafından kullanılacağı gibi bilgiler bu mesaj içerisinde bulunur.

Nmap

Nmap

- Nmap, bilgisayar ağları uzmanı Gordon Lyon (Fyodor) tarafından C/C++ ve Python programlama dilleri kullanılarak geliştirilmiş bir güvenlik tarayıcısıdır.

- Taranan ağın haritasını çıkarabilir ve ağ makinalarında çalışan servislerin durumlarını, işletim sistemlerini, portların durumlarını gözlemleyebilir.

- Nmap kullanarak ağa bağlı herhangi bir bilgisayarın işletim sistemi, çalışan fiziksel aygıt tipleri, çalışma süresi, yazılımların hangi servisleri kullandığı, yazılımların sürüm numaraları, bilgisayarın firewall'a sahip olup olmadığı, ağ kartının üreticisinin adı gibi bilgiler öğrenilebilmektedir.

- GPL lisanslı özgür bir yazılımdır.

Nmap Tarama Süreci

1. Taranılacak olan hedef makinanın ismi girilirse, Nmap öncellikle DNS lookup işlemi yapar. Bu aslında bir Nmap fonksiyonu değil, ancak DNS sorguları network trafiğinde gözüktüğünden beri, her durum loglanır. Bu yüzden isim ile tarama yapmadan önce bunun bilinmesinde fayda vardır. Eğer isim yerine IP girilirse, DNS lookup işlemi yapılmayacaktır. DNS lookup işleminin iptal edilmesinin bir yolu bulunmuyor, sadece Nmapin üzerinde bulunduğu makinanın host veya lmhost dosyalarının içinde IP – DNS eşleşmesi varsa DNS lookup yapılmaz.

2. Nmap hedef makinayı “ping”ler. Ancak bu bilinen ICMP ping işlemi değildir. Nmap farklı bir ping işlemi kullanır. Bu işlem hakkında bilgi ilerleyen bölümlerde verilecektir. Eğer ping işlemini iptal edilmek isteniyorsa –P0 seçeneği kullanılmalıdır.

3. Eğer hedef makinanın IP adresi belirtildiyse, Nmap reverse DNS lookup yaparak IP – Hostname eşleşmesi yapar. Bu 1. Adımda gerçekleştirilen olayın tersidir.

4. Nmap taramayı gerçekleştirir. Tarama bittikten sonra, bu dört adımlık süreç sona erer.

TCP SYN Scan

- Hedefe TCP SYN gönderir.
- Portların kapalı olduğu durumlarda hedef makina cevap olarak RST + ACK döner.
- Portların açık olduğu durumlarda ise hedef makina SYN + ACK bayraklı segment döner.
- Son olarak RST bayraklı segment göndererek bağlantıyı koparır ve böylelikle TCP üçlü el sıkışma (TCP three-way handshaking) tamamlanmaz. Ve iz bırakmaz.
- nmap -sS -v [scannedIp]

TCP Connect Scan

- Kaynak makinanın gerçekleştireceği TCP Connect Scan
- Kapalı portlara yapıldığı zaman RST + ACK döner
- Açık portlara yapıldığında SYN + ACK gönderir, kaynak makina ACK bayraklı segment göndererek cevaplar ve üçlü el sıkışmayı tamamlar.İz bırakır.
- nmap -sT -v [scannedIp]

UDP Scan

- UDP portlarını taramak için kullanılır , ICMP Port Unreachable cevabı döndürülüyorsa port kapalı cevap yoksa open|filtered kabul edilecektir.
- UDP paketi dönerse port açık kabul edilir.
- nmap -sU -v [scannedIP]

IP Protocol Scan

- Bu tarama türü standart NMAP tarama türlerinden biraz farklıdır.
- Bu tarama türünde hedef makinaların üzerlerinde çalışan IP tabanlı protokoller tespit edilmektedir.
- Bu yüzden bu tarama türüne tam anlamıyla bir port taraması demek mümkün değildir. Hedef makina üzerinde, taramasını yaptığımız IP protokolü aktif haldeyse hedef makinadan bu taramaya herhangi bir cevap gelmeyecektir. Hedef makina üzerinde, taramasını yaptığımız IP protokolü aktif halde değilse hedef makinadan bu taramaya, tarama yapılan protokolün türüne göre değişebilen RST bayraklı (RST bayrağı "1" yapılmış) bir segment cevap olarak gelecektir.
- nmap -sO -v [scannedIp]

Nmap Script Kullanımı

- nmap -sV --script=rdp-vuln-ms12-020 -p 3389 [scannedIp]

Kaynaklar

- Exploit-db / Ahmet Gürel
- İTÜ BİDB