Laboratuvar Raporu 6

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Şevval Ayça Çerence

152120211128

Dr. Öğr. Üyesi İlker Özçelik

2024-2025

2.GİRİŞ

Wireshark NAT Lab çalışması, ağ trafiğini analiz etme ve NAT (Network Address Translation) mekanizmasının işleyişini detaylı şekilde inceleme fırsatı sunan bir laboratuvar uygulamasıdır. Bu laboratuvar ortamı, özellikle NAT'ın ağ yapılarındaki rolünü ve nasıl çalıştığını anlamak amacıyla tasarlanmıştır.

NAT, özel IP adreslerinin genel IP adreslerine dönüştürülerek internete erişimin sağlanmasına olanak tanıyan bir yönlendirme tekniğidir. Bu yöntem, IP adreslerinin sınırlı olduğu durumlarda, birden fazla cihazın aynı genel IP üzerinden internet bağlantısı kurabilmesine imkân verir. Böylece hem adres tasarrufu sağlanır hem de ağ yönetimi kolaylaşır.

Bu laboratuvar uygulaması kapsamında şu hedeflere ulaşılmıştır:

1. NAT'ın temel işleyişi, yakalanan paketler üzerinden gözlemlenmiş ve iç ağ ile dış ağ arasında gerçekleşen adres dönüşümleri analiz edilmiştir.
2. Port yönlendirme mantığı üzerinden, belirli bir portun NAT cihazı tarafından iç ağdaki belirli bir cihaza nasıl iletildiği incelenmiştir.
3. Yakalanan ağ trafiği detaylı olarak analiz edilerek, veri paketlerinin içerikleri, kullanılan protokoller ve ağ katmanları hakkında çıkarımlar yapılmıştır.

Bu analizler sayesinde hem NAT'ın teorik hem de pratik yönleri kavranmış, aynı zamanda bu bilginin ağ güvenliği, performans izleme ve hata ayıklama gibi alanlardaki önemi pekiştirilmiştir.

3.SORULAR

3.1

Client IP adresi 192.168.1.100 olarak bulunmuştur.

No.	Time	Source	Destination	Protocol	Length Info
7	1.208040	192.168.1.100	74.125.91.113	HTTP	1035 POST /safebrowsing/downloads?client=navclient-auto-

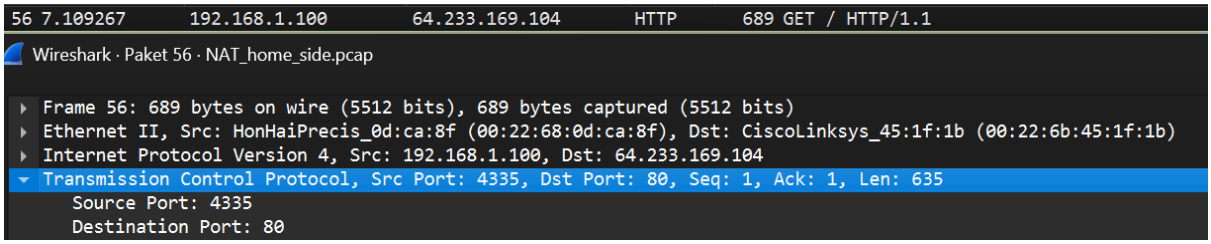
3.2

Filtre uygulandı, 64.233.169.104 adresine ait HTTP paketleri listelendi.

No.	Time	Source	Destination	Protocol	Length Info
56	7.109267	192.168.1.100	64.233.169.104	HTTP	689 GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814 HTTP/1.1 200 OK (text/html)
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226 HTTP/1.1 200 OK (GIF89a)
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809 GET /extern_js/f/CgJlbhICdXMrWAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTgJLCswHTgZLCswJTjJiAEsKzAmOAUsKzAnOAIsKzAqOAEsKzArOAQsKzA8OAAs/Q6MZP2n6D9M.js HTTP…
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648 HTTP/1.1 200 OK (text/javascript)
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695 GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870 HTTP/1.1 200 OK (text/html)
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712 GET /images/nav_logo7.png HTTP/1.1
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806 GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&ei=2502Ssb1G4_CeJvxxaMO&rt=prt.128,xjs.287,ol.437 HTTP/1.1
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359 HTTP/1.1 200 OK (PNG)
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670 GET /favicon.ico HTTP/1.1
124	7.737783	64.233.169.104	192.168.1.100	HTTP	269 HTTP/1.1 204 No Content
127	7.763501	64.233.169.104	192.168.1.100	HTTP	1204 HTTP/1.1 200 OK (image/x-icon)

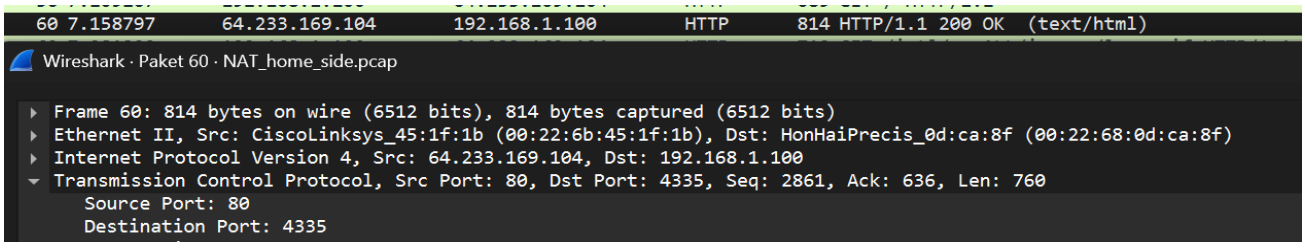
3.3

Kaynak IP adresi 192.168.1.100, hedef IP adresi ise 64.233.169.104 olup, TCP kaynak portu 4335 ve TCP hedef portu ise 80'dir.



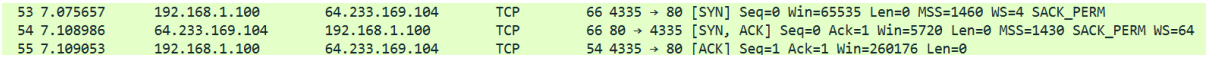
3.4

Zaman 7.158797 olarak kaydedilen veride, kaynak IP adresi 64.233.169.104, hedef IP adresi ise 192.168.1.100'dür. TCP kaynak portu 80, TCP hedef portu ise 4335'tir.



3.5

SYN paketi, 7.075657 zamanında kaydedildi; kaynak IP adresi 192.168.1.100, hedef IP adresi ise 64.233.169.104'tür. Kaynak portu 4335, hedef portu ise 80'dir. SYN-ACK paketi ise 7.108986 zamanında kaydedildi ve kaynak IP adresi 64.233.169.104, hedef IP adresi ise 192.168.1.100'dür. Son olarak, 7.109053 zamanında gönderilen ACK paketi, istemciye başarıyla ulaşmıştır.



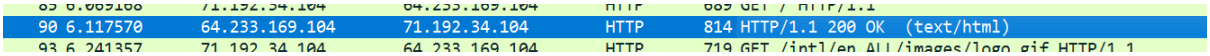
3.6

Zaman 6.09168 olarak kaydedilen veride, kaynak IP adresi 71.192.34.104 (NAT) ve hedef IP adresi 64.233.169.104'tür. 3. soru ile 6. soru arasındaki fark, kaynak IP adreslerinin farklı olmasıdır; 3. soruda kaynak adresi 192.168.1.100 iken, 6. soruda kaynak adresi 71.192.34.104 olarak gözlemlenmiştir.

3.7

Checksum değişmiş çünkü NAT sonrası IP adresi değişti, bu da header checksum'un yeniden hesaplanmasını gerektirdi.Onun dışındaki alanlarda herhangi bir değişiklik olmamıştır.

3.8



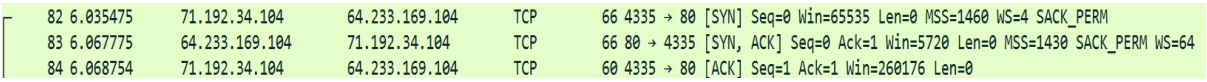
Wireshark üzerinde yapılan incelemede, zaman damgası 6.117570, kaynak IP adresi 64.233.169.104 ve hedef IP adresi 71.192.34.104 olarak gözlemlenmiştir. Bu bilgiler, ilgili trace dosyası üzerinden elde edilmiştir. Bu veriler, 4. ve 8. sorular karşılaştırıldığında ortaya çıkan farkı da açıklamaktadır. 4. soruda hedef IP adresi 192.168.1.100 iken, 8. soruda bu adres 71.192.34.104 olarak değişmiştir. Bu durum, NAT cihazının IP adres çevirme işlevini açıkça göstermektedir.

3.9

Wireshark analizine göre, 82. segment bir TCP SYN paketidir ve zaman damgası 6.035475 olarak kaydedilmiştir. Bu pakette kaynak IP adresi 71.192.34.104, hedef IP adresi ise 64.233.169.104'tür. 83. segment ise bu SYN paketine yanıt olarak gönderilen

TCP ACK paketidir. Bu paketin zaman damgası 6.067775 olup, kaynak IP adresi 64.233.169.104, hedef IP adresi ise 71.192.34.104 olarak belirlenmiştir.

Bu iki segment karşılaştırıldığında, TCP SYN paketinde kaynak IP adresinin önceki bağlantıdan farklı olduğu, ACK paketinde ise hedef IP adresinin değiştiği gözlemlenmiştir. Ancak her iki pakette kullanılan port numaralarının aynı kaldığı dikkat çekmektedir. Bu durum, NAT işlemi sonucu gerçekleşen adres dönüşümünü açıkça göstermektedir.



3.10

NAT TRANSITION TABLE	
WAN	LAN
71.192.34.104 - 4335	192.168.1.100 - 4335

3.11

1.572315 Zamanındaki GET İsteği:

Bu GET isteği, istemcinin Google sunucusuyla ilk temaslarından biridir ve yeni bir oturum başlatmak amacıyla gönderilmiştir. İstemci, belirli bir kaynağa erişmek için sunucuya bu isteği iletir. Genellikle bu tür isteklerde, hedef URL, protokol bilgisi ve başlıklar yer alır. Sunucu bu bilgileri aldıktan sonra uygun yanıtı göndererek iletişimi başlatır. Bu mesaj, istemci ve sunucu arasındaki veri alışverişinin temelini oluşturur.

7.573305 Zamanındaki GET İsteği:

Bu ikinci GET isteği, ilk bağlantı kurulduktan sonra gerçekleşmiştir ve genellikle web sayfasının tam görüntülenebilmesi için gerekli ek dosyaları (örneğin resimler, CSS ya da JavaScript dosyaları) almak için kullanılır. Ayrıca, kullanıcının oturumuna özgü dinamik içeriklerin alınması da bu istekle mümkün olabilir. Bu durum, modern web uygulamalarının çoklu kaynak iletişimi kurduğunu gösterir.

4-KAYNAKÇA

Wireshark Lab: NAT v8.0 Supplement to Computer Networking: A Top-Down Approach, 8th ed., J.F. Kurose and K.W. Ross