

SOFTİTO YAZILIM-BİLİŞİM AKADEMİSİ

Siber Güvenlik Uzmanlığı – Ağ Trafiği ve Paket Analizi Laboratuvar Raporu

Ödev Konusu:	Senaryo A: Wireshark ile HTTP ve HTTPS Trafiğinin Karşılaştırmalı Analizi	Öğrenci:	Kerem Kaan AVCI
Eğitmen:	Erhan KAYA	Tarih / Dönem:	2026 / 4. Dönem

1. GİRİŞ VE ÇALIŞMANIN AMACI

Bu laboratuvar çalışmasında, web iletişiminin temelini oluşturan **HTTP (Hypertext Transfer Protocol)** ile şifreleme katmanı eklenmiş hali olan **HTTPS (HTTP Secure / TLS)** protokolleri arasındaki çalışma prensibi ve güvenlik farkları incelenmiştir.

Deney kapsamında, VirtualBox üzerinde izole bir yerel ağ oluşturulmuş; kurulan Ubuntu Web Sunucusu üzerinden hem açık metin (HTTP) hem de SSL/TLS ile şifrelenmiş (HTTPS) web istekleri gerçekleştirilmiştir. İstemci tarafında yer alan Kali Linux üzerindeki **Wireshark** aracıyla paketler dinlenmiş, veri paketlerinin şifrelenip şifrelenmediği ve içeriklerin üçüncü taraflarca okunabilirlik durumu adım adım test edilmiştir.

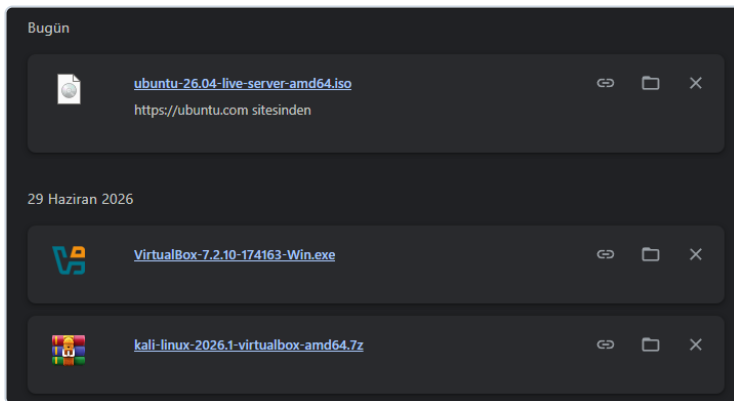
Kullanılan Temel Sistem ve Araçlar:

- Hipervizör:** Oracle VM VirtualBox (v7.2.10)
- Sunucu (Server):** Ubuntu Server 26.04 LTS (Apache2 Web Server & OpenSSL) - IP: 10.10.10.2/24
- İstemci (Client / Sniffer):** Kali Linux 2026.1 - IP: 10.10.10.3/24
- Paket Analiz Aracı:** Wireshark & Mozilla Firefox
- Ağ Mimarisi:** İzole Dahili Ağ (Internal Network / intnet)

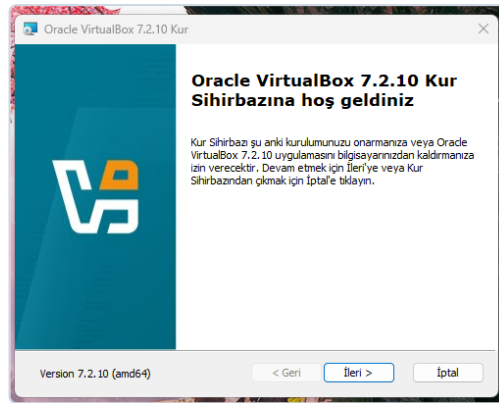
2. LABORATUVAR ORTAMININ KURULUMU VE YAPILANDIRILMASI

2.1. İmajların Hazırlanması ve VirtualBox Kurulumu

İlk olarak laboratuvar ortamında ihtiyaç duyulan VirtualBox kurulum dosyası, Ubuntu Server 26.04 ISO kalıbı ve hazır Kali Linux sanal makine diskisi temin edilmiştir. Ardından VirtualBox 7.2.10 ana makineye kurulmuştur.

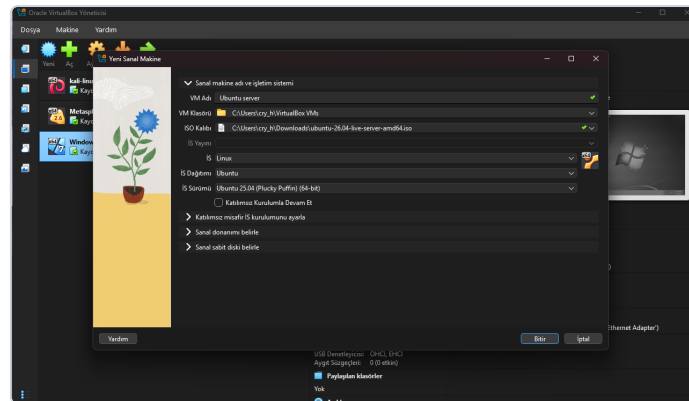


Görsel 1: Temin edilen Ubuntu Server ISO, VirtualBox ve Kali Linux kurulum dosyaları

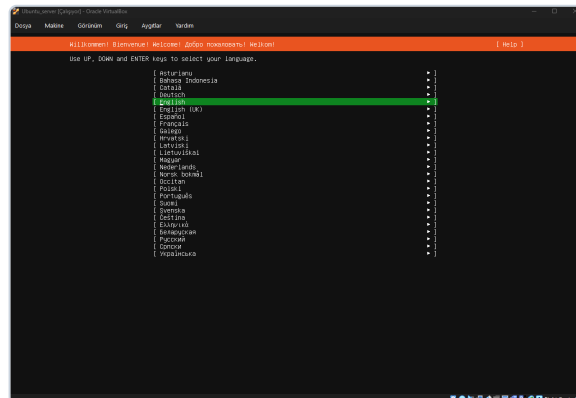


2.2. Ubuntu Sunucusunun Oluşturulması ve İlk Kurulum

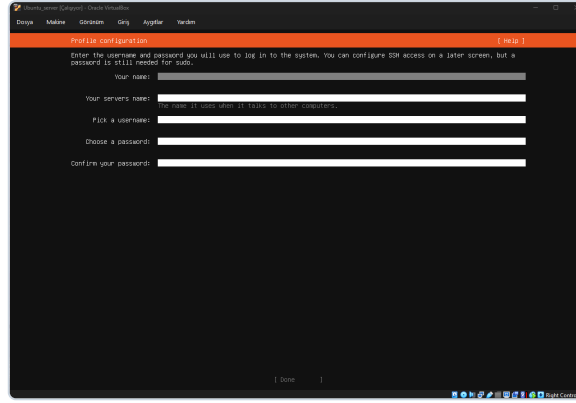
VirtualBox üzerinde "Yeni Sanal Makine" seçeneği ile Ubuntu Server için kaynaklar ayrılmış, indirilen ISO kalıbı bağlanarak sistem kurulumu (dil seçimi, kullanıcı ve şifre tanımlamaları) tamamlanmıştır.



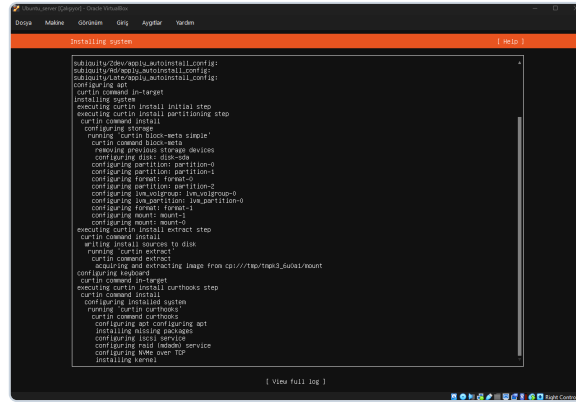
Görsel 3: Ubuntu Server sanal makinesinin VirtualBox üzerinde oluşturulması



Görsel 4: Ubuntu Server kurulum ekranında dil seçimi



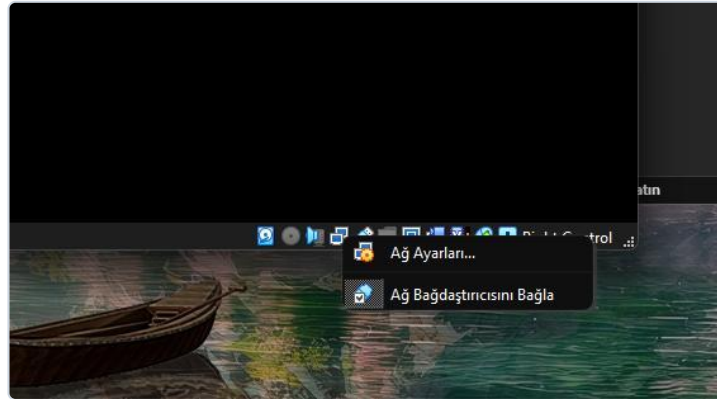
Görsel 5: Sunucu kullanıcı adı, parola ve makine adı yapılandırması



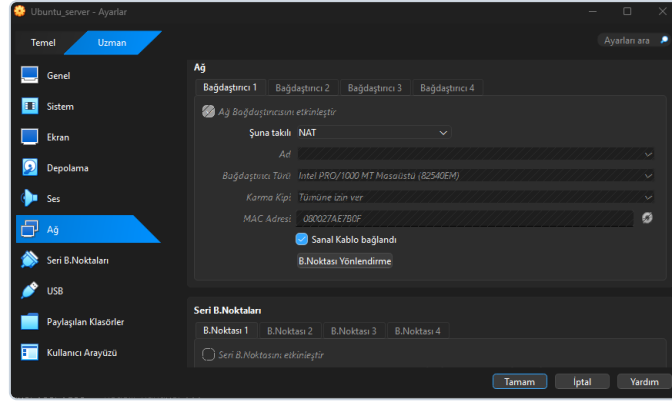
Görsel 6: Sistem dosyalarının ve çekirdek paketlerinin yüklenmesi

2.3. Sunucu Paketlerinin Yüklenmesi ve Web Servisinin Hazırlanması

Ubuntu Server kurulumu tamamlandıktan sonra, gerekli web sunucusu yazılımlarını indirebilmek için sanal makinenin ağ kartı geçici olarak **NAT** moduna ayarlanmıştır.



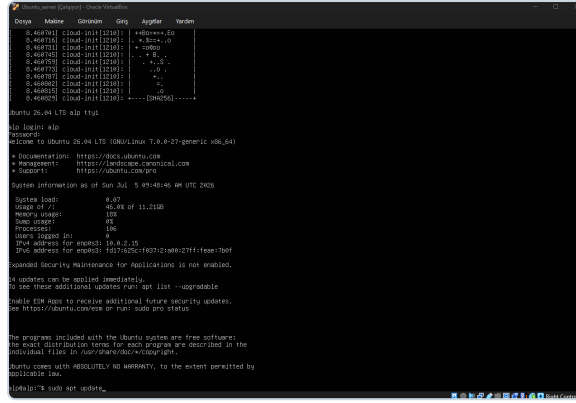
Görsel 7: VirtualBox arayüzünden ağ ayarlarına giriş



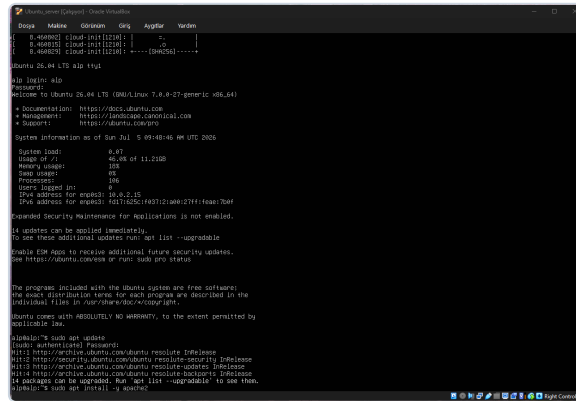
Görsel 8: Paket indirmeleri için ağ bağdaştırıcısının NAT olarak ayarlanması

İnternet bağlantısı sağlandıktan sonra sunucu paket listesi güncellenmiş ve **Apache2** web sunucusu sisteme kurulmuştur:

```
sudo apt update
sudo apt install -y apache2
```



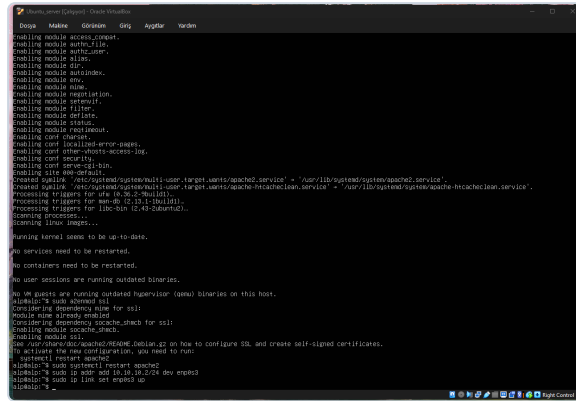
Görsel 9: Paket listelerinin güncellenmesi ('sudo apt update')



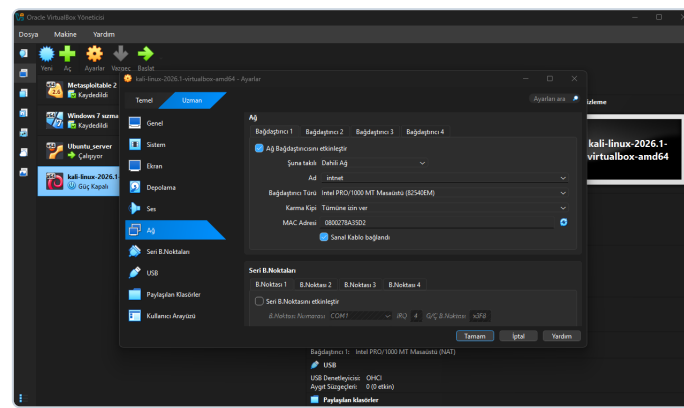
Görsel 10: Apache2 web sunucusunun kurulması ('sudo apt install -y apache2')

HTTPS testini yapabilmemiz için Apache sunucusunda SSL modülünün aktif olması gerekmektedir. `sudo a2enmod ssl` komutu ile SSL modülü etkinleştirilmiş ve servis yeniden başlatılmıştır:

```
sudo a2enmod ssl
sudo systemctl restart apache2
```

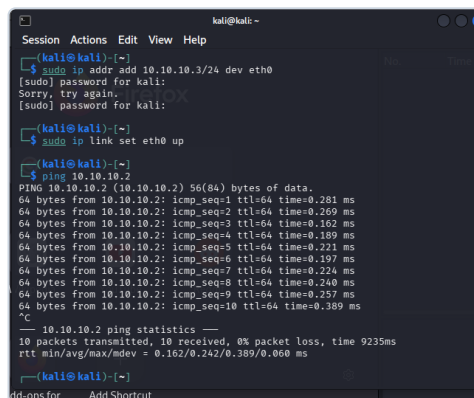



Aynı şekilde istemci rolündeki Kali Linux makinesi de aynı dahili ağa (intnet) dahil edilmiş ve eth0 arayüzüne 10.10.10.3/24 IP adresi atanmıştır:



Kali terminalinde IP adresi atandıktan sonra iki sistemin birbiriyle haberleşip haberleşmediğini doğrulamak için sunucuya 10 adet ICMP (Ping) paketi gönderilmiştir:

```
sudo ip addr add 10.10.10.3/24 dev eth0
sudo ip link set eth0 up
ping 10.10.10.2
```

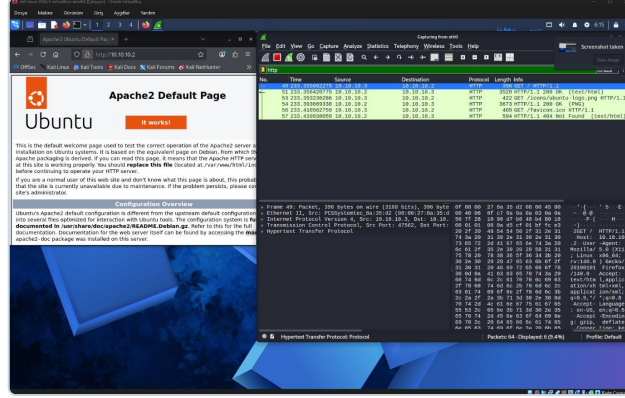


Ping çıktısında görüldüğü üzere 10 paket iletilmiş, 10 paket alınmış ve **%0 paket kaybı** ile L3 seviyesinde tam erişilebilirlik sağlanmıştır.

4. TRAFİK ANALİZİ VE PROTOKOL İNCELEMESİ (WIRESHARK)

4.1. Senaryo 1: HTTP Trafiğinin İncelenmesi (Port 80 - Açık Metin)

Kali Linux üzerinde Wireshark başlatılmış ve filtre alanına http yazılarak yalnızca HTTP paketleri filtrelenmiştir. Ardından Firefox tarayıcısı üzerinden http://10.10.10.2 adresine gidilerek Apache varsayılan sayfasına erişilmiştir.



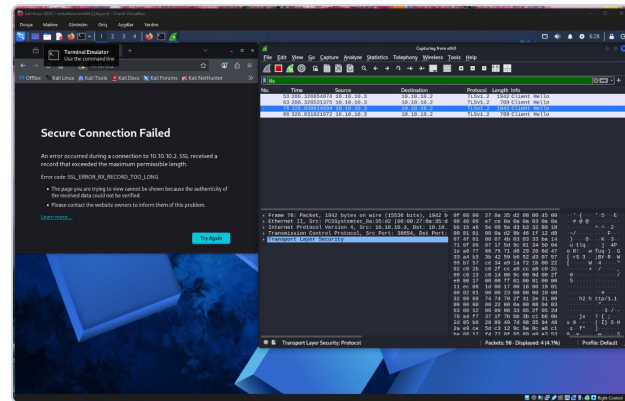
Görsel 17: HTTP GET isteğinin Wireshark üzerinde açık metin olarak incelenmesi

HTTP Analizi Bulguları:

- Yakalanan 49 numaralı pakette görüldüğü üzere istemci tarafından gönderilen GET / HTTP/1.1 isteği tamamen düz metin (cleartext) halindedir.
- Paket detaylarında; istemcinin işletim sistemi (Linux x86_64), tarayıcı sürümü (Firefox/140.0), kabul edilen içerik tipleri ve dil bilgileri (Accept-Language: en-US,en;q=0.5) şifresiz bir şekilde okunabilmektedir.
- Aynı hatta bulunan kötü niyetli bir dinleyici (sniffer), bu trafiği izleyerek istemcinin girdiği sayfaları, gönderdiği form verilerini veya oturum çerezlerini hiçbir ek işlem yapmadan doğrudan ele geçirebilir.

4.2. Senaryo 2: HTTPS / TLS Trafiğinin İncelenmesi (Port 443 - Şifreli İletişim)

Wireshark filtresi tls olarak güncellenmiş ve Firefox üzerinden https://10.10.10.2 adresine istek atılmıştır.



Görsel 18: HTTPS (TLS) trafiğinin ve şifrelenmiş paket verisinin Wireshark analizi

HTTPS Analizi Bulguları:

- Yakalanan TLS paketleri (örneğin 76 numaralı Client Hello ve veri aktarım paketleri) incelendiğinde, uygulama katmanı yükünün (payload) tamamen şifrelendiği görülmektedir.
- Sağ alt alandaki Hex / ASCII dökümünde anlamlı hiçbir metin, kullanıcı bilgisi veya sayfa içeriği görünmemekte; veriler karmaşık bayt dizilerinden oluşmaktadır.

- Taşıma Katmanı Güvenliği (TLS) sayesinde ağ üzerindeki üçüncü taraflar sadece istemci ve sunucunun IP/port bilgilerini görebilmekte, transfer edilen asıl veriye kesinlikle erişememektedir.

5. PROTOKOL KARŞILAŞTIRMASI VE GÜVENLİK ANALİZİ

Özellik / Kriter	HTTP (Hypertext Transfer Protocol)	HTTPS (HTTP Secure / TLS-SSL)
Varsayılan Port	80 / TCP	443 / TCP
Veri İletim Şekli	Açık Metin (Düz / Cleartext)	Kriptografik Olarak Şifrelenmiş (Ciphertext)
Gizlilik (Confidentiality)	Yok. Paket içeriği doğrudan okunabilir.	Tam koruma. Simetrik/Asimetrik anahtarlarla korunur.
Bütünlük (Integrity)	Yok. Araya giren kişi veriyi değiştirebilir.	Mesaj Doğrulama Kodları (MAC/HMAC) ile korunur.
Kimlik Doğrulama	Yok. Sunucunun gerçekliği doğrulanamaz.	Dijital Sertifikalar (X.509) ile doğrulanır.
Maruz Kaldığı Saldırıları	Sniffing, Man-in-the-Middle (MITM), Session Hijacking	Uçtan uca şifreleme sayesinde dinleme ve tahrifata kapalıdır.

6. SONUÇ VE TAVSİYELER

Gerçekleştirilen laboratuvar çalışmasında, HTTP ve HTTPS protokolleri kontrollü ve izole bir sanal ağ ortamında test edilmiş; Wireshark analizleriyle iki protokolün güvenlik farkları uygulamalı olarak kanıtlanmıştır.

Elde Edilen Temel Çıkarımlar ve Öneriler:

- Kullanıcı Açısından:** Günlük internet kullanımında, özellikle kullanıcı adı, parola veya kart bilgisi girilen tüm sayfalarda bağlantının mutlaka HTTPS olduğundan emin olunmalıdır. Tarayıcılarda "Yalnızca HTTPS" modu aktif edilerek açık HTTP sitelere güvenli olmayan bağlantı yapılması engellenmelidir.
- Sunucu / Sistem Yöneticisi Açısından:**
 - Web sunucularında geçerli ve güvenilir bir Sertifika Otoritesinden (CA) alınmış SSL/TLS sertifikası bulundurulmalıdır.
 - HTTP (80) portuna gelen tüm istekler sunucu tarafında 301 yönlendirmesi ile otomatik olarak HTTPS (443) portuna yönlendirilmelidir.
 - Kullanıcıların araya girilerek HTTP'ye düşürülmesini (SSL Stripping) engellemek amacıyla **HSTS (HTTP Strict Transport Security)** başlığı aktif edilmelidir.
 - Eskiye ve güvenlik açığı barındıran protokoller (SSLv2, SSLv3, TLS 1.0, TLS 1.1) devre dışı bırakılmalı, modern şifreleme algoritmalarıyla en az **TLS 1.2** veya **TLS 1.3** standardı kullanılmalıdır.