SiberGuvenlikMufredati.pdf dosyasındaki içerikler, istediğiniz "Senior Mindset" formatında ve detaylarda boğulmadan aşağıda özetlenmiştir:

AŞAMA 1: Seviye 101 - Temeller, Ağ ve Görünürlük (Hafta 1-5)

Odak: Bilgisayar ve ağ mimarisi, paket analizi, işletim sistemleri ve web güvenliği temellerinin uygulamalı olarak anlaşılması 1-5.

HAFTA 1: Siber Güvenlik Temelleri ve CTI

- **Konu Başlıkları:**
- Bilgisayar ve Ağ Mimarisi: OSI vs TCP/IP modelleri 1.
- Saldırı Vektörleri: Phishing, Malware, Ransomware, Zero-Day 6.
- Savunma Teknolojileri: Firewall, IDS/IPS, SSL/TLS, VPN, SOC kavramları 6.
- Siber Tehdit İstihbaratı (CTI) ve Mavi Takım önemi 6.
- **Haftalık Görev (Boss Fight): CTI Vaka Analizi**
- **Senaryo:** Şüpheli bir IP (45.128.232.67) ile oluşan trafiğin analizi 7.
- **Görev:** Pasif bilgi toplama kaynaklarıyla (VirusTotal, AbuseIPDB vb.) IP repütasyon analizi yap ve kriz yönetim planı hazırla 7, 8.
- **Kazanılacak Yetkinlikler:** Temel terminoloji hakimiyeti, trafik görme yetisi ve pasif istihbarat raporlama 8, 9.

HAFTA 2: Wireshark ve Ağ Adli Analizi

- **Konu Başlıkları:**
- Protokol Anatomisi: TCP Handshake (SYN, ACK) ve UDP farkları 10.
- Dosya Analizi: Magic Bytes (Hex Signature) ve MD5 Hash kontrolü 10, 11.
- Saldırı İmzaları: Ağ üzerindeki port tarama paternlerinin tespiti 11.
- **Haftalık Görev (Boss Fight): Packet Detective**
- **Görev:** Evidence pcap dosyalarını analiz ederek gizli mesajları (TCP Stream), transfer edilen dosyaları ve saldırganın tarama türlerini tespit et 12, 13.
- **Kazanılacak Yetkinlikler:** Derin paket inceleme (DPI), file carving ve ağ tabanlı saldırı tespiti 14, 15.

HAFTA 3: İşletim Sistemleri Mimarisi (Linux & Windows)

- **Konu Başlıkları:**
- Linux: "Her şey bir dosyadır" mantığı, SUID izinleri ve Bash scripting 3, 16.
- Windows: Registry (Kayıt Defteri), Process & Threads yapısı ve NTFS izinleri 16.
- Araçlar: Sysinternals (Process Hacker/Explorer) ile sistem analizi 17.
- **Haftalık Görev (Boss Fight): System Engineer Raporu**
- **Görev:** OverTheWire: Bandit (0-10) seviyelerini tamamla; Windows sistem süreçlerini (svchost.exe vb.) analiz ederek virüs-sistem ayrımını raporla 4, 18.
- **Kazanılacak Yetkinlikler:** Çekirdek ve süreç yönetimi bilgisi, terminal hakimiyeti ve sistem içi anomali tespiti 3, 19.

HAFTA 4: Web Recon (Keşif) ve Mantık Hataları

- **Konu Başlıkları:**
- Web Anatomisi: HTTP/HTTPS protokolü, Cookie ve Session yönetimi 20.
- Keşif (Recon): Subdomain, gizli dizin ve endpoint keşfi (Subfinder, Amass, httpx) 20, 21.
- Zafiyetler: IDOR (Insecure Direct Object Reference) ve Broken Access Control 21.
- **Haftalık Görev (Boss Fight): Bug Hunter Başlangıç**
- **Görev:** Belirlenen bir hedef üzerinde saldırı yüzeyi haritalandırması yap ve PortSwigger üzerindeki IDOR lablarını tamamla 5, 22.

- **Kazanılacak Yetkinlikler:** Web mimarisi analizi ve yetki atlatma teknikleri 22, 23.

HAFTA 5: Web Exploitation ve Profesyonel VDP

- **Konu Başlıkları:**
- Enjeksiyon Zafiyetleri: XSS (Cross Site Scripting), SQL Injection ve File Upload 24.
- Raporlama: VDP süreçleri ve CVSS skorlama mantığı 24.
- **Haftalık Görev (Boss Fight): Final Projesi - The Bug Bounty Hunter**
- **Görev:** Kritik bir web zafiyetini (SQLi, XSS veya RCE) sömür ve profesyonel bir sızma testi raporu hazırla 25, 26.
- **Kazanılacak Yetkinlikler:** Zafiyet doğrulama, sömürme (exploitation) ve iş odaklı raporlama 27, 28.

AŞAMA 2: Seviye 201 - Sistem, Analiz ve Simülasyon (Hafta 6-9)

Odak: İleri seviye yetki yükseltme, kurumsal ağ saldırıları, malware analizi ve saldırgan stratejilerinin simülasyonu 26, 29-31.

HAFTA 6: Windows Privilege Escalation

- **Konu Başlıkları:**
- Yetki Seviyeleri: User, Admin ve SYSTEM (God Mode) farkları 32.
- Teknikler: Unquoted Service Path, Kernel Exploits ve LOLBAS (Living Off The Land) 32, 33.
- Otomasyon: WinPEAS ile zafiyet taraması 33, 34.
- **Haftalık Görev (Boss Fight): PrivEsc Specialist**
- **Görev:** Standart kullanıcıdan SYSTEM yetkisine yüksel ve bu işlemin EDR (Wazuh) üzerindeki izlerini raporla 29, 35.
- **Kazanılacak Yetkinlikler:** Sistem yapılandırma hatalarını sömürme ve savunma atlatma mantığı 34, 36.

HAFTA 7: Active Directory ve Kerberos Saldırıları

- **Konu Başlıkları:**
- AD Mimarisi: Domain Controller, Kerberos bilet mantığı (TGT, TGS) 37.
- Saldırı Türleri: Pass the Ticket, Kerberoasting, AS-REP Roasting, Golden Ticket 37, 38.
- **Haftalık Görev (Boss Fight): Domain Dominance**
- **Görev:** "Attacktive Directory" makinesini çöz; kullanıcı keşfi, hash kırma ve Domain Admin yetkisine ulaşma sürecini raporla 39, 40.
- **Kazanılacak Yetkinlikler:** Kurumsal ağ güvenliği ve kimlik tabanlı saldırı yönetimi 41.

HAFTA 8: Zararlı Yazılım Analizi ve Tersine Mühendislik

- **Konu Başlıkları:**
- Analiz Türleri: Statik (Hash, Strings) vs Dinamik (Sandbox, Behavioural) analiz 30, 42.
- Tersine Mühendislik: Assembly dili temelleri ve kalıcılık (Persistence) mekanizmaları 42, 43.
- **Haftalık Görev (Boss Fight): Malware Hunter**
- **Görev:** Şüpheli bir zararlıyı analiz et; IP bağlantılarını, kayıt defteri değişikliklerini tespit et ve YARA kuralı mantığını açıkla 44, 45.
- **Kazanılacak Yetkinlikler:** Güvenli analiz ortamı yönetimi ve zararlı yazılım davranış tespiti 43, 46.

HAFTA 9: Red Team Operasyonları (Initial Access)

- **Konu Başlıkları:**
- Metodoloji: Cyber Kill Chain ve MITRE ATT&CK kullanımı 47.
- İlk Erişim: Phishing, Payload hazırlama ve Listener yönetimi 47.
- Erişim Sonrası: "Living off the Land" prensibi ve kalıcılık 47, 48.
- **Haftalık Görev (Boss Fight): Adversary Simulation**
- **Görev:** AI kullanmadan, bir saldırı senaryosu için strateji raporu hazırla; bayrak odaklı değil, "mantık" odaklı ilerle 49.
- **Kazanılacak Yetkinlikler:** Saldırgan zihniyeti (Adversary Mindset) ve uçtan uca saldırı zinciri analizi 50, 51.

AŞAMA 3: Seviye 301 - Hakimiyet, Web ve Raporlama (Hafta 10-14)

Odak: EDR atlatma, SOC operasyonları, adli bilişim (DFIR), bulut güvenliği ve yönetici seviyesinde raporlama 52-56.

HAFTA 10: EDR Atlatma ve Atomic Red Team

- **Konu Başlıkları:**
- Savunma Atlatma: Obfuscation (Karartma), Encoding ve AV/EDR farkları 52, 57.
- Atomic Red Team: Güvenlik testlerinin otomatize edilmesi ve TTP simülasyonu 57.
- **Haftalık Görev (Boss Fight): Purple Team Lab**
- **Görev:** Kendi lab ortamında Defender'ı atlatarak Reverse Shell al ve Atomic testlerin Wazuh üzerindeki alarmlarını analiz et 58, 59.
- **Kazanılacak Yetkinlikler:** Evasion teknikleri ve savunma mekanizmalarının doğrulanması 60, 61.

HAFTA 11: SOC ve Sürekli İzleme

- **Konu Başlıkları:**
- SOC Mimarisi: SIEM (Splunk, Wazuh) ve SOAR farkları 53, 62.
- Log Analizi: Windows Event IDs (4624, 4625 vb.) ve Sysmon kullanımı 62.
- Anomali Tespiti: Süreç analizi ve ağ bağlantısı takibi 63.
- **Haftalık Görev (Boss Fight): Junior SOC Analyst Günlüğü**
- **Görev:** Splunk üzerinden bir Brute Force saldırısını tespit et ve Sysmon loglarını kullanarak şüpheli bir işlemi raporla 64, 65.
- **Kazanılacak Yetkinlikler:** Log korelasyonu ve operasyonel olay müdahale yetisi 66.

HAFTA 12: Dijital Olay Yeri (DFIR) ve Kriz Yönetimi

- **Konu Başlıkları:**
- Adli Bilişim: RAM analizi (Volatility) ve Disk analizi (Autopsy) 54, 67.
- Incident Response (IR): NIST aşamaları ve kriz anında karar verme 67.
- Kriz Senaryoları: Ransomware ve APT belirtilerinin yönetimi 67, 68.
- **Haftalık Görev (Boss Fight): DFIR Specialist**
- **Görev:** Bellek imajı üzerinden zararlı süreçleri ve IP bağlantılarını tespit et; bir fidye yazılımı senaryosu için IR planı hazırla 69, 70.
- **Kazanılacak Yetkinlikler:** Uç nokta adli analizi ve kriz yönetimi stratejileri 71.

HAFTA 13: İleri Seviye Sızma ve Profesyonel Raporlama

- **Konu Başlıkları:**
- İleri Teknikler: RSA şifreleme mantığı ve Web Logic Flaws (Mantık Hataları) 55, 72.
- Senior Raporlama: Yönetici Özeti (Executive Summary) ve teknik bulgu dili 72, 73.
- **Haftalık Görev (Boss Fight): Senior Pentester Simülasyonu**
- **Görev:** Zorlu bir makineyi (Hammer vb.) çöz ve ADEO şablonuna uygun profesyonel bir sızma testi raporu sun 74, 75.

- **Kazanılacak Yetkinlikler:** Karmaşık problem çözme ve üst düzey iş iletişimi 76.

HAFTA 14: Bulut ve Konteyner Güvenliği (Cloud & Docker)

- **Konu Başlıkları:**
- Cloud: Shared Responsibility Model, IAM (Kimlik) hataları ve S3 güvenliği 56, 77.
- Konteyner: Docker izolasyonu ve Container Breakout (Dışarı sızma) teknikleri 77, 78.
- **Haftalık Görev (Boss Fight): Modern Infrastructure Assessment**
- **Görev:** Docker konteyner analizi yap ve zafiyetli bir S3 bucket senaryosu için iyileştirme raporu hazırla 79, 80.
- **Kazanılacak Yetkinlikler:** Modern altyapı güvenliği ve bulut tabanlı risk analizi 81, 82.