Giriş Karışık (Intro Mix)

Bknz: OSI Katmanları

Hizmet Engelleme Neden Yapılır?

Finansal kazanç, siyasal manifestolar, Spam e-posta bildirimi (botnet), Gövde gösterisi, diğer saldırıları gizleme (log kirlenmesi), ihtiyaç oluşturma (anti-ddos)

DoS, tek kaynaktan hedefe (exploitable -> makineye gönderilir ve crash olur. | Kolay engellenebilir. | Kolay hasar verilebilir.)
DDoS, farklı kaynaklardan tek hedefe (korunumu zor, anonimlik için daha iyi)

Botnet (zombi pc)

1. Zararlı yazılımlar (virüs,rat,trojan)

Film oyun siteleri, uygulama edinme portalları, yazılım ve uygulama güncelleme servisi, web portalları

1. Silahlı exploitler (wanna cry)
2. Ev ağı ve IoT cihazları (mirai botnet)

Bknz: HomeGateway vs Modem

Mirai (bütün ipleri tarayalım, default panellere, default giriş bilgisi)

Botnet mining

WireX Android Botnet (1 günde bütün public ip değişiyor durdurulması zor)

pDoS
Arp, broadcast storm
ICMP Fragmentation

Layerlar boyunca DDoS'lar

Layer 7
Get Flood
Post Flood
Yük Saldırıları (AB Tool)
Güvenlik Zafiyetleri ve Exploitler
Slow HTTP
DNS Genişletme (DNS Amplification)

Siber Ölüm Zinciri

1- Keşif(Reconnaissance)

Aktif - Pasif Bilgi Toplama

2- Silahlanma(Weaponization)

Silahın keşif doğrultusunda geliştirildiği aşama.

3- İletme(Delivery)

APT kodunun kurbanı sömürmek için hedef bilgisayara geçmesidir. Phishing ile zararlı yazılım bulaştırılır.
Genelde en zayıf halka seçilerek spear phishing gerçekleştirilir. Genelde word ve pdf gibi ek içermektedir.
Ek ile apt kurum içi ağa erişir.

4- Sömürme(Exploitation)

Hedef sistemde zafiyet varsa bu işlemde zafiyet sömürülür ancak çoğu apt saldırısı phishing ile gerçekleştiğinde içeride çalışması yeterlidir.

5- Installing

Varlığa kötü amaçlı yazılım yüklemek.

6- Komuta ve Kontrol(Command and Control)

İletişim APT kodlarını hedef ağa yerleştirir. APT kodunu tamamen ve daha derin bir şekilde yönetmesine, veri göndermesine ve logları silmesine olanak sağlar.

7- Hedeflenen Eylem(Action on Objectives)

Veri çalma, değiştirme, silme, başka sisteme sıçrama…

Zafiyet Analizi Testleri ve Türleri

Web
WAN
LAN
WiFi

DoS / DDoS
Sosyal Mühendislik

Yazılım Analizi
Mobil Uygulama Analizi
Fiziksel Testler
Red Teaming

CIA

Gizlilik (Confidentiality)
Bütünlük (Integrity)
Erişilebilirlik (Availability)

nc -lvp 6666
Sql
Directory path traversal
lfi