# Saldırı Tespiti ve Ağ Tabanlı Saldırılar

# Konular

- Temel Kavramlar ve İlkeler
- Kriptografik Yapı Taşları
- Kullanıcı Kimlik Doğrulaması - Parolalar, Biyometri ve Alternatifler
- Kimlik Doğrulama Protokolleri ve Anahtar Kurulumu
- İşletim Sistemi Güvenliği ve Erişim Denetimi
- Yazılım Güvenliği - İstismarlar ve Ayrıcalık Arttırma
- Kötü Amaçlı Yazılımlar
- Açık Anahtar Sertifika Yönetimi ve Kullanım Durumları
- Web ve Tarayıcı Güvenliği
- Güvenlik Duvarları ve Tüneller
- Saldırı Tespiti ve Ağ Tabanlı Saldırılar

# Giriş

- Ağ güvenliğiyle ilgili iki bölümden bu ikincisi, önceki güvenlik duvarları ve tünellerle ilgili konuları tamamlar.
- Burada, saldırı tespiti ve ağ izleme (paket dinleme) ve güvenlik açığı değerlendirme araçlarını, ardından hizmet reddi ve standart TCP / IP veya Ethernet protokollerini kullanan ağ tabanlı saldırıları tartışıyoruz.
  - DNS tabanlı saldırılar ve Adres Çözümleme Protokolüne (ARP) yapılan saldırılar.
- Bu tür ağ tabanlı saldırılara karşın en iyi savunma iletişim oturumlarının kriptolanmasıdır.

# Terimler

- İzinsiz giriş (veya Saldırı) (Intrusion), bir bilgisayar veya ağda güvenlik politikasını ihlal eden bir olaydır veya bir sistemi yetkisiz bir duruma sokmak için yakın bir tehdittir.
- Saldırı tespiti (Intrusion detection), bu tür izinsiz girişleri tanımlamak ve raporlamak için sistem olaylarını izleme ve analiz etme sürecidir.
- Saldırı tespit sistemi (Intrusion detection system - IDS) süreci otomatikleştirir ve olayları izleme, ilgili verileri kaydetme, analiz ve insan dikkatini gerektiren olayları raporlama araçlarını içerir.

# Tespit Etme / Önleme

- Bir IDS, izinsiz girişleri ve diğer olumsuz olayları, devam etmekte iken veya olaydan sonra tespit eder.
- IDS'nin temeli, bulmayı kolaylaştıran ve adli analizi destekleyen kanıtları toplayan bir izleme sistemidir. Uygulamada, gerçekte ne olduğunu çözmek genellikle insan uzmanlar tarafından analiz gerektirir ve keşif, yeni saldırılar için açık uçlu olabilir; bu tür sistemler tipik kullanıcılar için pragmatik değildir.
- Pasif izlemenin ötesinde bir saldırı önleme sistemi (intrusion prevention system - IPS), örneğin devam eden ihlalleri durdurmak veya ağ yapılandırmalarını değiştirmek gibi aktif yanıtları içerir. Güvenlik duvarını bir adım öteye taşıyan bir IPS, paketleri değiştirebilir, kötü amaçlı yazılımları kaldırabilir veya bağlantıları sonlandırmak için TCP sıfırlamaları gönderebilir; bilgisayar tabanlı IPS, işlemleri sonlandırabilir.

# Mimari Türler

- Sensörlerin olay akışlarını nereden topladığına bağlı olarak iki tamamlayıcı IDS kategorisi, ağ tabanlı IDS'ler (NIDS'ler) ve host tabanlı IDS'lerdir (HIDS'ler).
- NIDS olayları, stratejik bir gözlem noktasında, örneğin bir ağ geçidinde veya bir LAN (yerel alan ağı) anahtarında elde edilen paketlerden türetilir.
- HIDS olayları,
  - işletim sistemi çekirdek tarafından oluşturulan işlemlerden ve
  - denetim kayıtlarından, uygulama günlüklerinden (kullanıcı kimliğini not ederek),
  - dosya sistemi değişikliklerinden (dosya bütünlüğü kontrolleri, dosya izinleri, dosya erişimleri) ve sistem çağrısı izlemesinden türetilebilir;
  - bilgisayara, ağ erişimlerine, gelen / giden paket içeriklerine ve ağ arayüzlerindeki durum değişikliklerine (açık portlar, çalışan servisler) özeldir.
  - Kaynak kullanım modelleri (CPU süresi, disk alanı) şüpheli işlemleri ortaya çıkarabilir.

# IDS Olay Sonuçları

| | intrusion | no intrusion |
|---|---|---|
| alarm raised | True Positive (TP)<br>intrusion detected | False Positive (FP)<br>false alarm |
| no alarm raised | False Negative (FN)<br>intrusion missed | True Negative (TN)<br>normal operation |

| | |
|---|---|
| False positive rate | $FPR = \frac{FP}{(FP+TN)}$ |
| True negative rate | $TNR = 1 - FPR$ |
| False negative rate | $FNR = 1 - TPR$ |
| True positive rate | $TPR = \frac{TP}{(TP+FN)}$ |
| Alarm precision | $AP = \frac{TP}{(TP+FP)}$ |

Figure 11.1: IDS event outcomes (left) and metrics (right). FP and FN (yellow) are the classification errors. TPR is also called the *detection rate*.

# Baz Oran (Base Rate)

- Bir X hastalığı ve onu tarayan bir test var. 100 hasta olmayan kişi verildiğinde, test ortalama olarak bir kişiyi hastalıklı olarak işaretler - yani yanlış pozitif oranı (FPR) = 1 / (1 + 99) = 0.01 =% 1. TNR = 1 – FPR = % 99.
- Ayrıca 100 hasta verildiğinde, test ortalama olarak 98 deneği hasta bulur - bu nedenle iki yanlış negatif ve FNR = 2 / (98 + 2) = 0,02 =% 2 veya eşdeğer TPR = 98 / (98 + 2) = 0.98 =% 98.

- Bu başarılı bir test midir? Bu testi kullanır mısınız?

# Baz Oran Yanılgısı (Base Rate Fallacy)

- Böyle bir test, "% 98 doğru" veya "% 99 doğru" olarak pazarlanabilir ancak bunu, kullanılan metriği açıklamadan yapmak hem uzman olmayanların hem de uzmanların kafasını karıştırabilir.
- X hastalığının nüfustaki oranı 100.000'de 1 olsun.
- Tarama testi uygulanırsa, 99.999 kişinin % 1'ini yani 1000 yanlış pozitif bulmasını bekleyebiliriz. Muhtemelen, gerçekten hasta olan kişi de pozitif test yapacaktır (% 98 TPR nedeniyle).
- Doktorların sonuç olarak gördüğü şey, "X hastalığı olabilir" olarak işaretlenen 1001 kişidir, bu nedenle 1001 alarmdan 1000'i yanlış alarmdır.
- Alarm hassasiyetini (Alarm precision- AP), doğru şekilde verilen alarmların toplam alarmlara (gerçek pozitiflerin toplam pozitiflere) oranı olarak ifade edersek:
  - AP = TP / (TP + FP) = 1 / (1 + 1000) = 1/1001 ≈ % 0.1.
- Bunu alarm belirsizliği (alarm imprecision) olarak tersten konumlandırırsak:
  - AIP = FP / (TP + FP) = 1000 / (1 + 1000) ≈ 0,999.
- Sonuç: Alarmların % 99,9'u (!) yanlış alarm.
- Bu testi kullanır mısınız?

# IDS Metodolojileri

| IDS approach | Alarm when... | Pros, cons, notes |
|---|---|---|
| *signature-based* (expert defines malicious patterns) | events match known-bad patterns | signatures built from known attacks; fast, accurate (fewer false positives); detects only already-known attacks |
| *specification-based* (expert defines allowed actions) | events deviate from per-application specifications of legitimate actions | manually developed spec of allowed; can detect new attacks; no alarm on newly seen allowed event; specs are protocol or program-specific |
| *anomaly-based* (learning-based profile of normal) | events deviate from profiles of normal | need training period to build profiles; can detect new attacks; false alarms (abnormal may be benign); accuracy depends on features profiled |

Table 11.1: IDS methodologies. Signature-based approaches use expert-built patterns (manual blacklists). Specification approaches use expert-built specs (manual whitelists). Anomaly approaches define "normal" behavior from training data (empirical whitelists).

# IDS Yaklaşımlarının Karşılaştırması

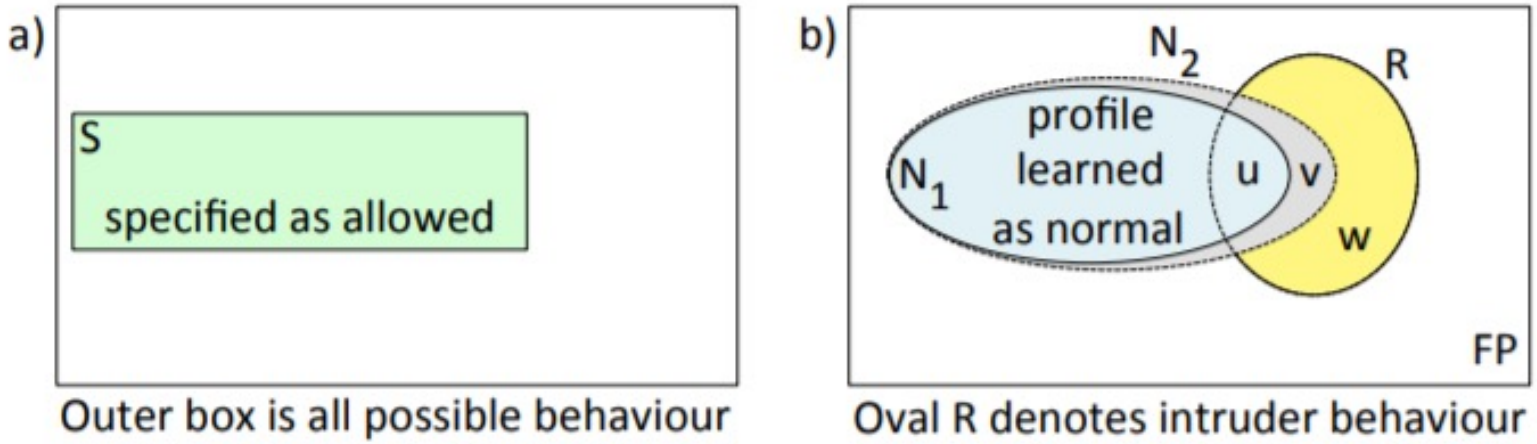


Figure 11.2: Visual model of IDS approaches. a) Specification-based; activity outside the shaded region raises an alarm. b) Anomaly-based and signature-based. Anomaly-based methods alert on detecting activity outside $N_1$; this may be a true positive if in $v$ or $w$, but a false positive if in FP. To reduce false positives, parameters or thresholds may be tuned to recognize a larger area ($N_2$) as normal, but this increases false negatives, as intruder activity in $v$ will no longer trigger an alarm. For signature-based approaches, attack signatures, from a subset of $w$, are created from known attacks.

# Anomali Tabanlı Yaklaşımlar

Avantaj:

- Daha önce görülmemiş saldırılar tespit edilebilir.

Dezavantajlar:

- Özniteliklerin seçimi zordur.
- Saldırıların eğitim esnasında olmadığı varsayımı gerçekçi olmayabilir.
- Normal profiller normal davranışları zaman içinde öğreniyor ise saldırganlar kendi davranışlarını normal profillere yerleştirebilirler.

# Paket Dinleme

- İyi Kullanım:
  - IPS için gerçek zamanlı analiz (IDS için de hızlı işlem önemlidir).
  - Ağ izleme (ağdaki faaliyetler, trafik düzenleri ve kullanım hakkında öngörü sağlar).
  - Ağ adli analizi.

- Kötü kullanım:
  - Saldırı amacıyla (iyi bir önlem: şifreleme)

# Hub ve Switch

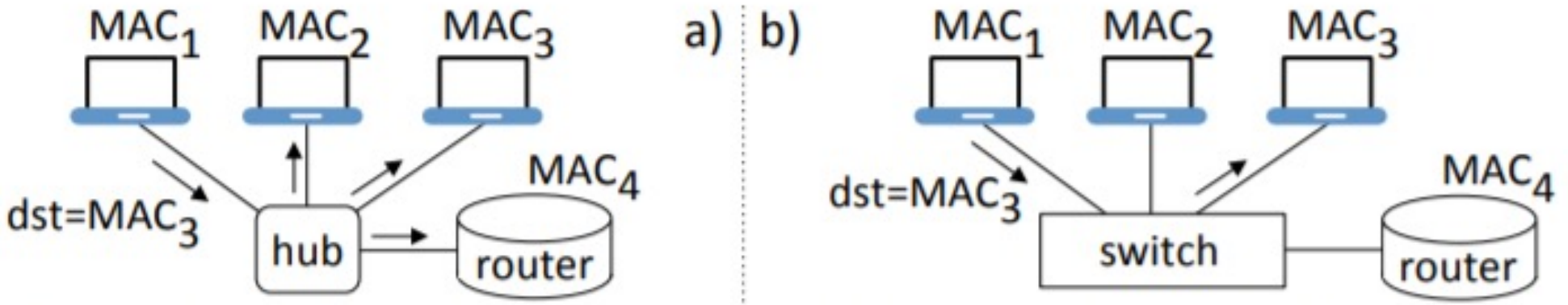


Figure 11.3: LAN hub vs. LAN switch. A hub broadcasts. A switch isolates.

# Zafiyet Değerlendirme Araçları

- Zafiyet değerlendirme araçları, izinsiz giriş tespit araçlarının bir alt kümesi olarak görülebilir - ancak artık savunmak yerine, büyük ölçüde üç kategoride kendi ana bilgisayarlarınızda zayıflıklar ararsınız:
- Sonuçlar, yazılım güncellemelerini, yapılandırma değişikliklerini ve varsayılan parolaların değiştirilmesini gerektirebilir.
- Hem bilgisayar tabanlı araçlar hem de ağ tabanlı araçlar kullanılır, ağ tabanlı araçlar üç kategoriye ayrılır:
    1. keşif araçları (reconnaissance tools) (örnek: Nmap)
        a. Port tarayıcıları
        b. İşletim sistemi parmakizi çıkarma
    2. zafiyet tarayıcıları (örnek: Nessus)
    3. sızma testi araçları (yetkilendirilmiş) / sömürü araç takımları (siyah şapkalar) (örnek: Metasploit).

# Sorumlu Açıklama (Responsible Disclosure) Ne Demektir?

# DoS Saldırı Sınıfları

1. gizli uygulama kusurlarından (zafiyetler) yararlanır.
2. kaynakları (bant genişliği, CPU, ana bellek, disk) tüketir.
   - sabit kaynakları tüketerek (örnek: SYN Flooding),
   - yoğun kaynak gerektiren işlemlerin talep edilmesi (örneğin, asimetrik anahtar çiftlerinin oluşturulması).

# Dağıtık DOS (DDOS)

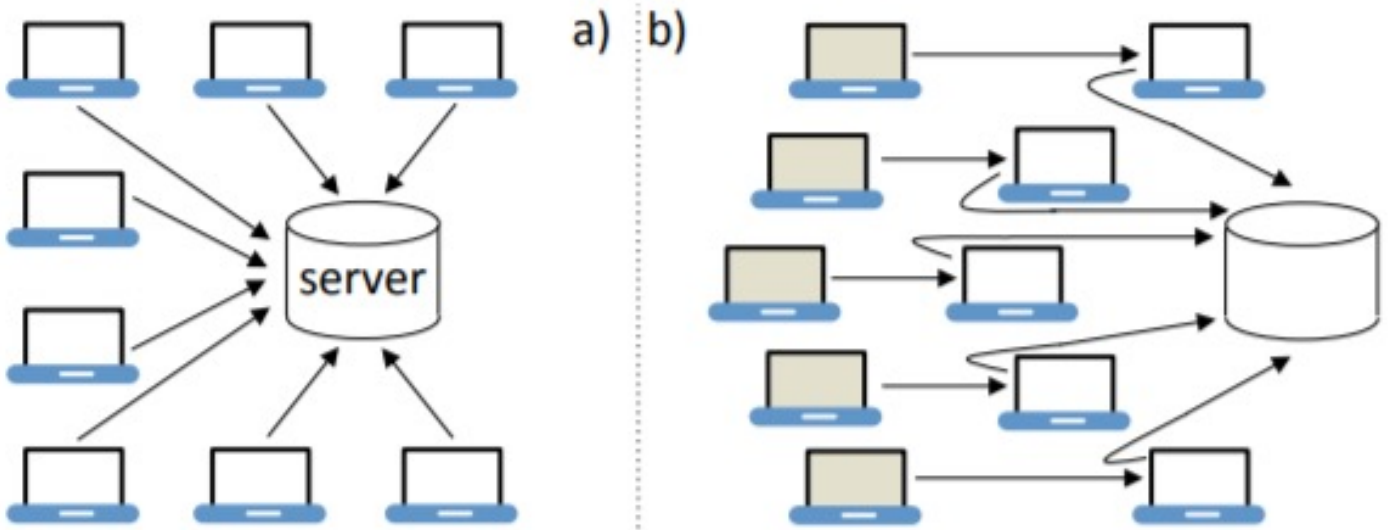


Figure 11.4: DDoS. a) The individual hosts (zombies) flooding the server are controlled by a botnet master directly, or by a large number of "handler" devices, which themselves take directions from the master. b) The shaded hosts (zombies) send packets spoofing the source address of a common (end) victim, such that the responses flood that victim.

# SYN Selleme (SYN Flooding)

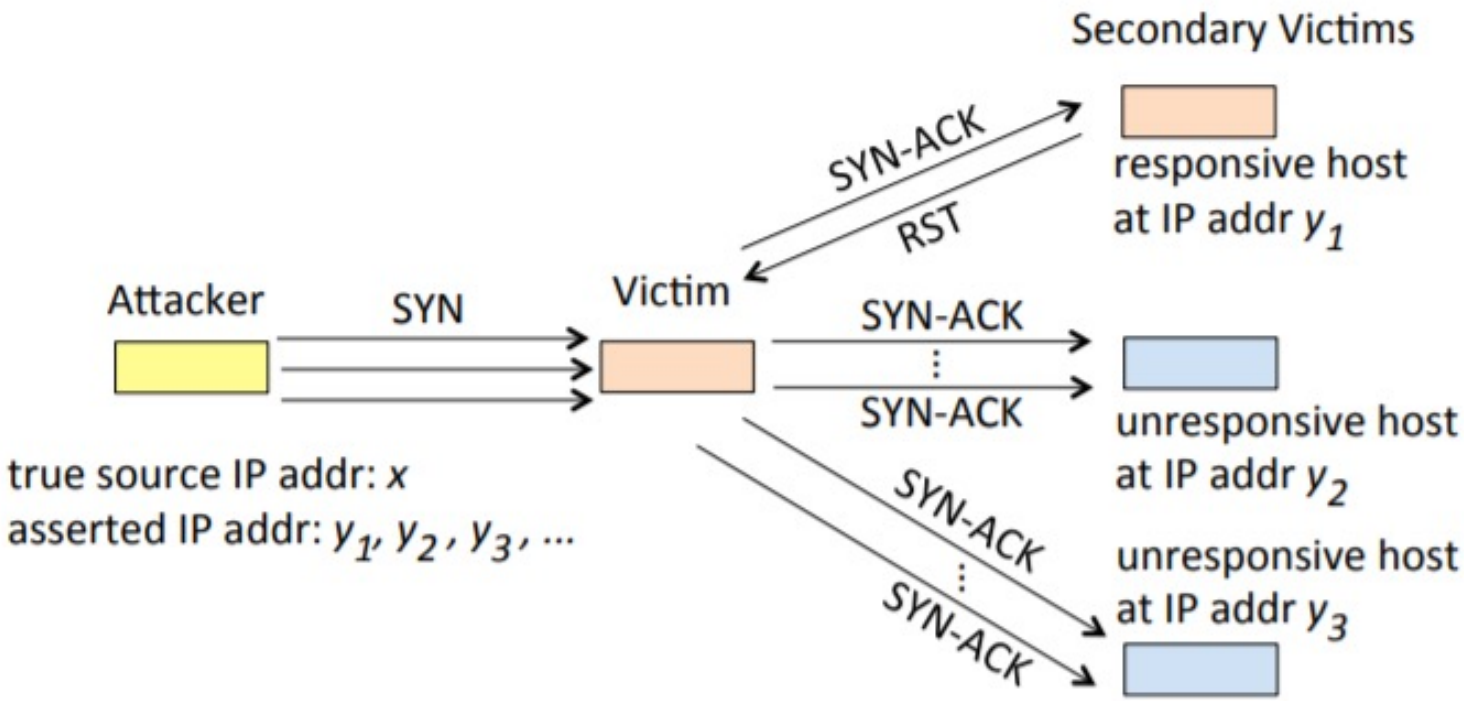


Figure 11.5: SYN flooding with spoofed IP address.

# Smurf Saldırısı

- Ping paketleri ve yanlış IP adresleri kullanan ICMP flood: bir yükseltme (amplification) faktörü elde etmek için yayın adreslerini (broadcast address) kullanır.
- Bir yerel ağ yayın adresine gönderilen paket, o ağdaki tüm ana bilgisayarlara gider.

# Giriş ve Çıkış Filtreleme

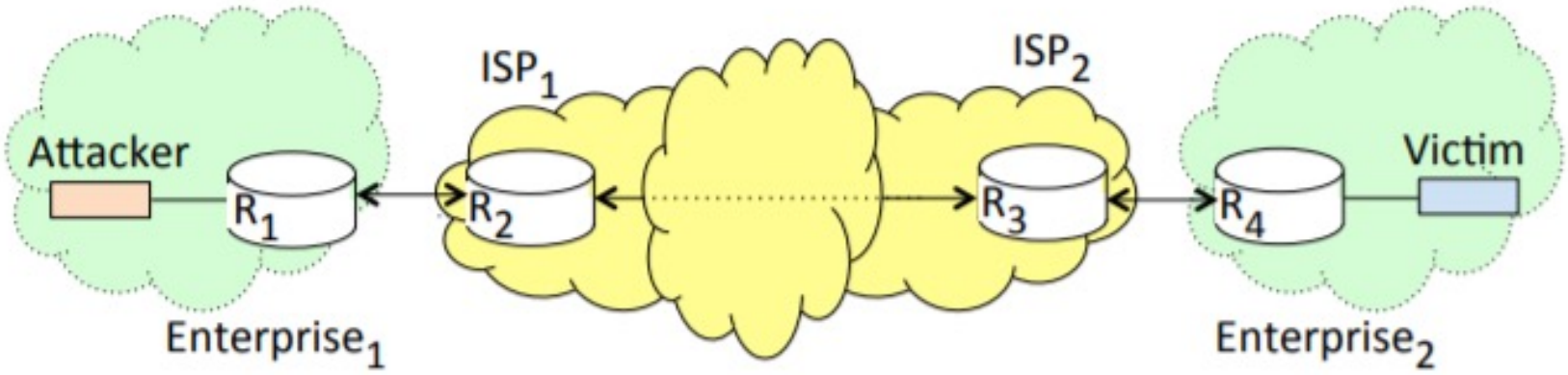


Figure 11.6: Ingress and egress filtering. An attacker may use a spoofed source IP address in traffic sent to a victim. $ISP_1$ does ingress filtering at $R_2$ for traffic entering from $Enterprise_1$. $Enterprise_1$ does egress filtering at $R_1$ for traffic leaving to $ISP_1$. For firewall rules to implement ingress and egress filtering, see Table 10.1 in Section 10.1.

# DNS Çözümleme

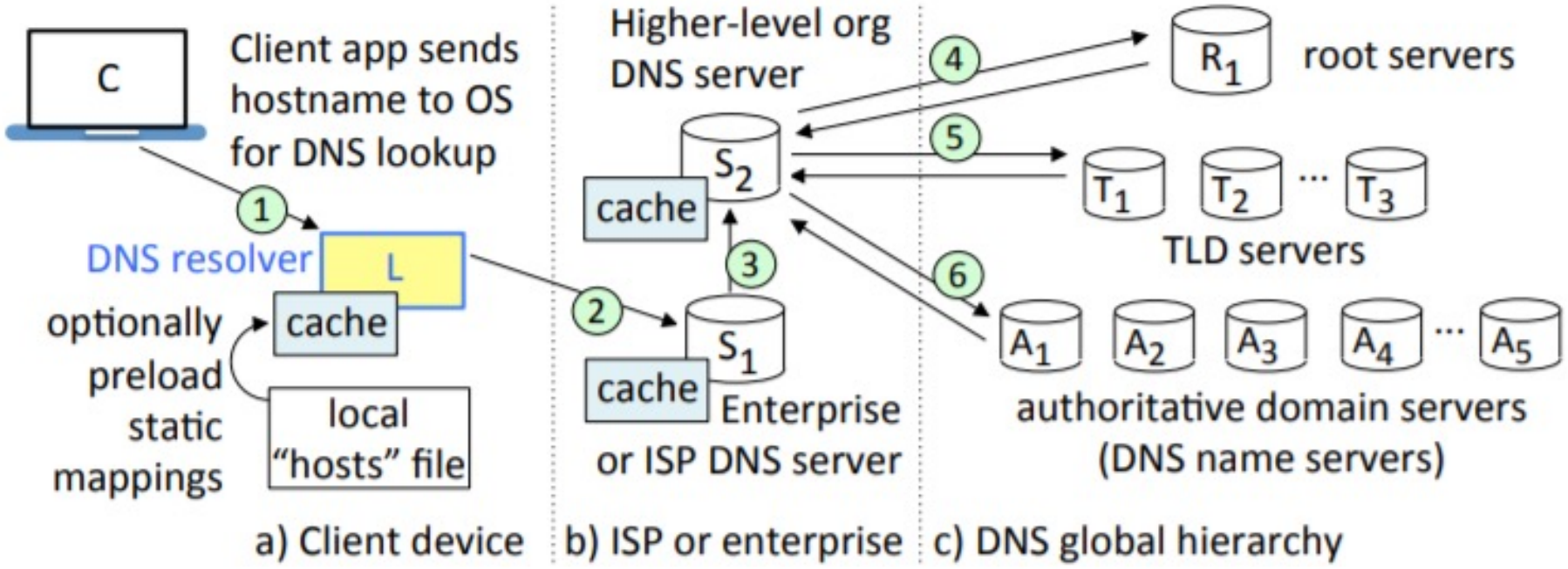


Figure 11.7: DNS name resolution and query hierarchy (simplified).

# DNS Çözümleme Saldırıları

- Pharming Saldırısı: Alan adı - IP adres dönüşümlerinde değişiklik yapmak.

- Bilinen bazı saldırı vektörleri:

1. Yerel dosyalar.
2. Ara DNS sunucuları.
3. Ağ üzerinden cevap değişiklikleri.
4. Sahte DNS sunucuları.
5. DNS Zehirleme (DNS Poissoning)

# ARP Sahtekarlığı (Spoofing)

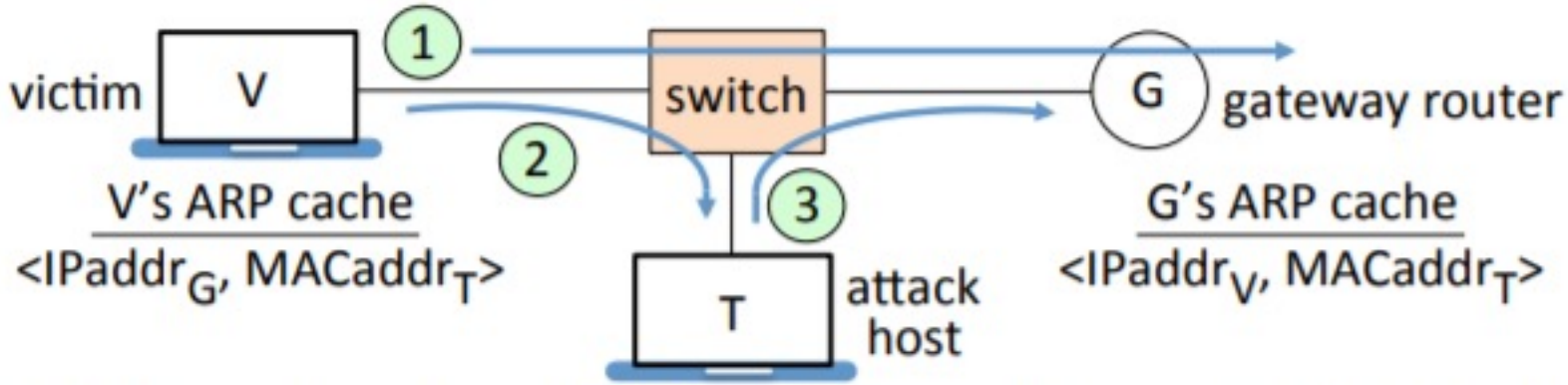


Figure 11.8: ARP spoofing. Intended flow (1), actual flows (2), (3). $T$ poisons $V$'s ARP cache. As a result, traffic sent via $G$ over the LAN, intended (1) for a destination beyond $G$, is instead sent (2) by $V$ to the physical interface of $T$. By also poisoning $G$'s ARP cache, $T$ can arrange that incoming traffic to $V$ via $G$ is sent by $G$ to $T$. Thus $T$ has a LAN middle-person attack between $V$ and $G$. Note: the switch itself is not poisoned.

# Koruma Yöntemleri

- ARP sahtekarlığı, IP adresini MAC adresiyle eşleyen statik, salt okunur cihaz ARP tabloları tarafından durdurulabilir.
  - manuel olarak ayarlamak ve güncellemek ekstra çaba gerektirir.
- Çeşitli araçlar ARP sahtekarlığını algılayabilir ve önleyebilir.
  - örneğin ARP yanıtlarını çapraz kontrol ederek.
- Tercih edilen uzun vadeli bir çözüm, güncellenmiş bir Adres Çözümleme Protokolünde güvenilir bir kimlik doğrulama yöntemi kullanmaktır.