# Chapter 7: Denial of Service

- Delving into the world of Denial of Service (DoS) attacks.
- Exploring the impact of DoS attacks.
- Examining prevention and mitigation strategies.
- Analyzing real-world examples and case studies.

88

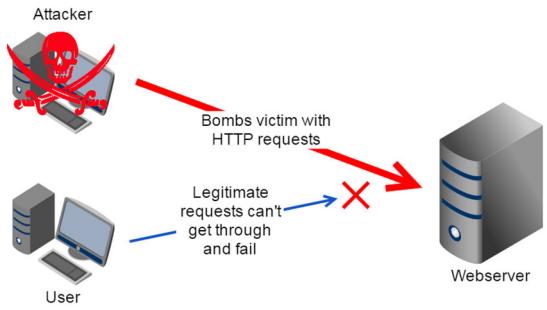
88

## نظرةعامة على هجمات DoS

- تعريفهجوم رفض الخدمة (DoS).
- الهدفمن هجوم DoS: جعل جهاز أو موردشبكة غير متاح.
- الطريقة:إغراق الهدف بطلبات مفرطة.

# Overview of DoS Attacks

- Definition of a Denial of Service (DoS) attack.
- The goal of a DoS attack: making a machine or network resource unavailable.
- The method: overwhelming the target with excessive requests.




89

89

# أنواعهجمات DoS:

- مقدمةلأشكال مختلفة من هجمات DoS.

1. **الهجمات على أساس الحجم**: تشبع النطاق الترددي لشبكة الضحية.
2. **هجمات البروتوكول**: استهلاك موارد الخادم أو موارد معدات الشبكة الوسيطة.
3. **هجمات طبقة التطبيق**: استهداف نقاط ضعف محددة في التطبيقات.

## Types of DoS Attacks:

- Introduction to various forms of DoS attacks.
  1. **Volume Based Attacks**: saturating the victim's network bandwidth.
  2. **Protocol Attacks**: consuming server resources or those of intermediate network equipment.
  3. **Application Layer Attacks**: targeting specific vulnerabilities in applications.

90

90

# تأثيرهجمات DoS:

- التأثيرالكبير لهجمات DoS.
  - **العواقبالمحتملة للشركات**: تعطل ، خسارةالإيرادات ، الإضرار بالسمعة.
  - **العواقبالمحتملة على الأفراد**: فقدان الوصول إلىالخدمات عبر الإنترنت ، وفقدان البيانات الشخصية.
  - **الأثرالمالي**: كلفت بعض الهجمات الشركاتملايين الدولارات.

## Impact of DoS Attacks:

- The significant impact of DoS attacks.
  - **Potential consequences for businesses**: downtime, revenue loss, reputational damage.
  - **Potential consequences for individuals**: loss of access to online services, loss of personal data.
  - **Financial impact**: some attacks have cost companies millions of dollars.


91

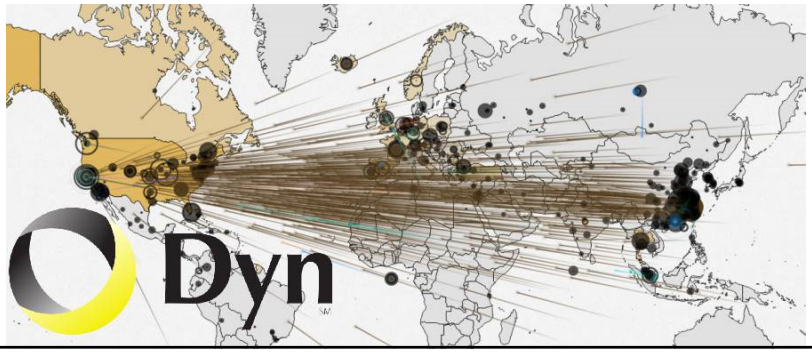
91

## أمثلةمن العالم الحقيقي:

- هجومDoS الملحوظ في عام 2016 ضد Dyn.
- مشاركةعشرات الملايين من عناوين IP.
- تسببالاضطراب الكبير في منصات وخدمات الإنترنت في أوروبا وأمريكا الشمالية.

## Real-world Examples:

- The notable DoS attack in 2016 against Dyn.
  - The involvement of tens of millions of IP addresses.
  - The major disruption caused to Internet platforms and services in Europe and North America.




92

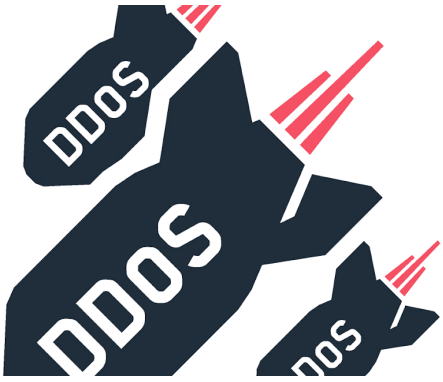
92

## هجماتDDoS:

- مقدمةلهجمات رفض الخدمة الموزعة (DDoS).
- استخدام**عديد**أجهزة الكمبيوتر المخترقة لمهاجمة نظامواحد.
- ال**ضحايا**: كل من النظام المستهدف النهائي وجميعالأنظمة المستخدمة بشكل ضار في الهجوم الموزع.

## DDoS Attacks:

- Introduction to Distributed Denial of Service (DDoS) attacks.
  - The use of **multiple** compromised computers to attack a single system.
  - The **victims**: both the end targeted system and all systems maliciously used in the distributed attack.




93

93

# Mitigation Strategies:

- Strategies to prevent and mitigate DoS and DDoS attacks.
  - Implementing **rate limiting**.
  - Using **content distribution networks** (CDNs) to distribute traffic.
  - Deploying **anti-DDoS** hardware and software solutions.

## استراتيجيات التخفيف:

- استراتيجيات لمنع وتخفيف هجمات DoS وDDoS.
  - تنفيذ **تحديد المعدل**.
  - استخدام **شبكات توزيع المحتوى** لتوزيع حركة المرور (CDNs)
  - النشر **مكافحة DDoS** حلول الأجهزة والبرامج.

94



# Case Study:

## دراسة الحالة:

- تحليل هجوم DDoS لعام 2016 على Dyn.
  - استخدام الروبوتات مع الأجهزة المصابة بامتداد **البرمجيات الخبيثة Mirai**.
  - الاضطراب الكبير في خدمات مثل Twitter و Amazon و Tumblr و Reddit و Spotify و Netflix.
  - إجراءات التخفيف التي نفذها مهندسو Dyn: **تحديد المعدل** و **تصفية IP**.

- Analysis of the 2016 DDoS attack on Dyn.
  - The use of a botnet with devices infected with the **Mirai malware**.
  - The significant disruption to services like Twitter, Amazon, Tumblr, Reddit, Spotify, and Netflix.
  - The mitigation measures implemented by Dyn's engineers: **rate limiting** and **IP filtering**.


95

## خاتمة:

- أهميةفهم هجمات DoS وكيفية منعها والتخفيف من حدتها.
- الحاجةإلى تدابير أمنية قوية والبقاء على اطلاع بأحدث التهديدات.
- حمايةالشركات والأفراد من الهجمات الضارة.

## Conclusion:

- The importance of understanding DoS attacks and how to prevent and mitigate them.
- The need for robust security measures and staying informed about the latest threats.
- The protection of businesses and individuals from damaging attacks.

96

96