Network Security Course Summary

ملخص كورس أمان الشبكة

إعداد: إسماعيل محمد قطان

Prepared by: Ismail Muhammed Kattan

التاريخ: أكتوبر/ تشرين الأول 2025

Date: October, 2025



تمت كتابة هذا الملخص بناء على كورس Network Security المقدم من CISCO على منصة Coursera

هذا الملخص يجمع ما قد يجهله أو ينساه خريج علوم الحاسوب وقد تم تجاهل بعض الدروس البسيطة والتي قد لا يحتاجها إلا من ليس له أدنى إطلاع على الشبكات.

## البنية التحتية للشبكة وأدوات مراقبة أمان الشبكة

### أساسيات ترجمة عناوين الشبكة NAT Fundamentals

(NAT (Network Address Translation هي تقنية تعمل على الطبقة الثالثة (Layer 3) من نموذج OSI، وظيفتها تحويل العناوين الخاصة (Private IPs) المستخدمة داخل الشبكة المحلية إلى عناوين عامة (Public IPs) يمكنها التواصل عبر الإنترنت.

تُستخدم بشكل أساسي لربط الشبكات الداخلية (RFC 1918) مع الإنترنت، مع توفير الأمان وإخفاء البنية الداخلية وتقليل استهلاك العناوين العامة.

##### الفوائد الرئيسية لـ NAT

* عدم الحاجة لإعادة ترقيم الشبكة عند الاتصال بالإنترنت.
* توفير عناوين IPv4 عبر السماح لعدة أجهزة بمشاركة عنوان عام واحد.
* تحسين الأمان بإخفاء العناوين الداخلية عن الخارج.

##### المصطلحات الأساسية (حسب Cisco)

| المصطلح | الوصف |
| --- | --- |
| Inside Local Address | عنوان الجهاز داخل الشبكة (غالبًا من عناوين RFC 1918 مثل 192.168.x.x). |
| Inside Global Address | العنوان العام الذي يمثّل الجهاز الداخلي أمام الإنترنت. |
| Outside Local Address | عنوان الجهاز الخارجي كما تراه الشبكة الداخلية (قد لا يكون عامًا). |
| Outside Global Address | العنوان العام الحقيقي للجهاز الخارجي على الإنترنت. |

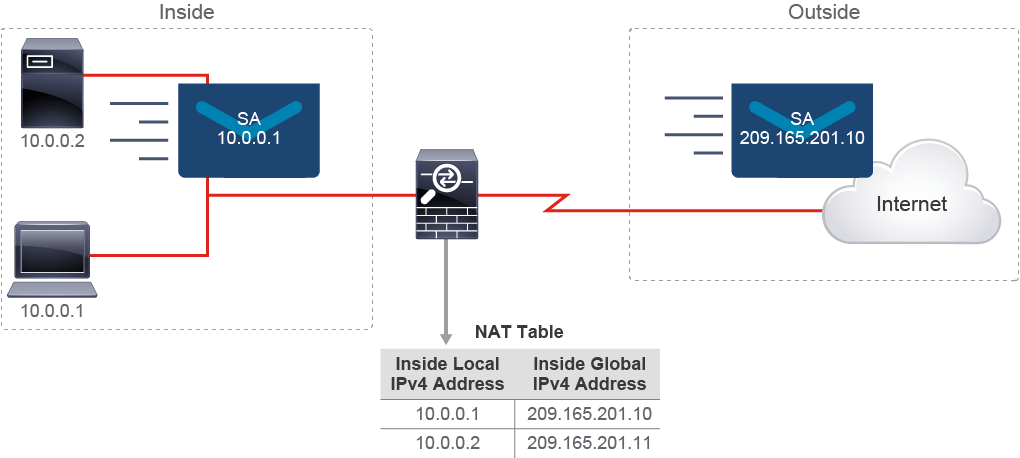
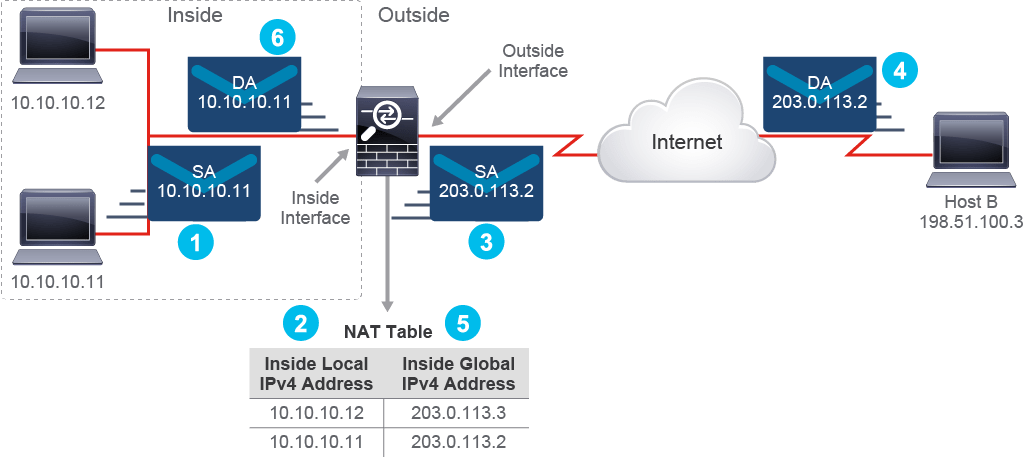
##### طريقة عمل NAT (خطوات الترجمة)

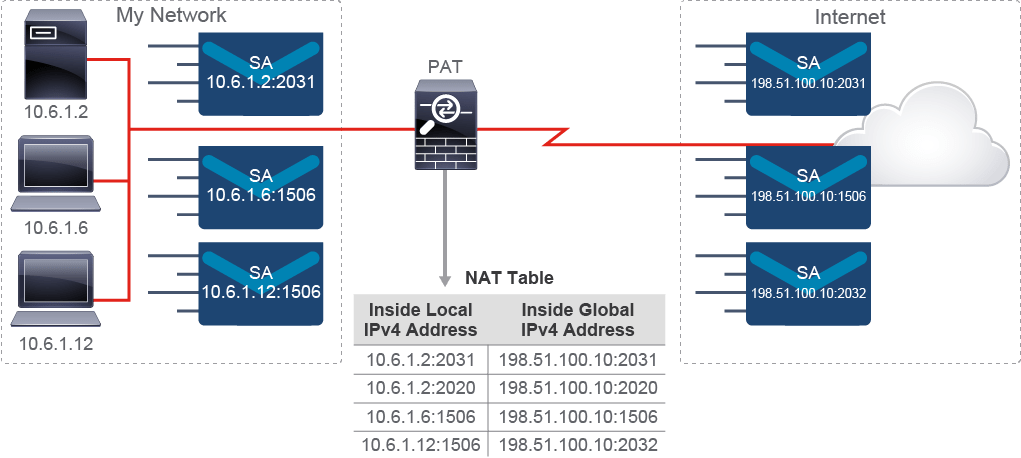
1. جهاز داخلي (مثلاً 10.10.10.11) يرسل طلبًا إلى الإنترنت.
2. الراوتر أو الجدار الناري يتحقق من جدول NAT:
   * إن وُجدت ترجمة مسبقة، يستخدمها.
   * إن لم توجد، يبحث في القواعد (rules) ويُنشئ ترجمة جديدة إذا لزم.
3. يتم استبدال العنوان الداخلي المحلي (10.10.10.11) بـ عنوان داخلي عام (203.0.113.2).
4. عند وصول الرد، يقوم NAT بعكس العملية ويعيد الحزمة إلى الجهاز الداخلي الصحيح.

##### 

##### أنواع NAT الشائعة

| النوع | الاستخدام | الميزة |
| --- | --- | --- |
| Static NAT | ترجمة ثابتة (1:1) بين عنوان خاص وعام. | تُستخدم للأجهزة التي تحتاج وصولًا دائمًا من الإنترنت (مثل خوادم DMZ). |
| Dynamic NAT | ترجمة من عناوين داخلية إلى مجموعة (Pool) من العناوين العامة. | مفيدة للاتصالات الصادرة عند توفر عدد محدود من العناوين العامة. |
| PAT (Port Address Translation) | ترجمة عدة عناوين داخلية إلى عنوان عام واحد باستخدام أرقام المنافذ. | تُعرف بـ NAT Overload، فعّالة جدًا لتوفير العناوين. |
| Static PAT (Port Forwarding) | تحويل منفذ محدد من العنوان العام إلى خدمة داخلية (مثلاً HTTP على المنفذ 80). | تستخدم للسماح بالوصول إلى خدمة داخلية عبر عنوان عام واحد. |
| Policy NAT | ترجمة مشروطة حسب المصدر/الوجهة أو المنفذ. | مرنة، تُستخدم عندما تختلف سياسات الترجمة حسب الوجهة أو الخدمة. |





### تصفية الحزم باستخدام قوائم التحكم بالوصول Packet Filtering with ACLs

**(ACL (Access Control List** هي أداة أمنية أساسية تُستخدم لتصفية حركة المرور (Packet Filtering) عبر الشبكة.  
 تُطبَّق عادة على **الراوترات والمبدّلات (Switches)** أو **الجدران النارية (Firewalls)** لتحديد من يُسمح له بالوصول إلى موارد معينة ومن يُمنع.

بدون ACL، تمر جميع الحزم عبر الراوتر دون قيود.  
 باستخدام ACL، يمكن السماح لمضيف معين بالوصول إلى شبكة محددة ومنع آخر من الوصول إليها.

##### الأهمية والاستخدامات

* تأمين الشبكات الداخلية من التهديدات الخارجية.
* تطبيق سياسات QoS (جودة الخدمة) عبر تصنيف أنواع الحركة (مثل إعطاء أولوية لصوت أو فيديو).
* تحديد البروتوكولات المسموح بها (مثل TCP, UDP, ICMP...).
* التحكم في الوصول بين أجزاء الشبكة (مثل السماح فقط بالوصول من خادم الويب إلى قاعدة البيانات).

##### أنواع ACL

| النوع | الوصف |
| --- | --- |
| Standard ACL | تعتمد فقط على عنوان المصدر (Source IP). |
| Extended ACL | تعتمد على المصدر + الوجهة + البروتوكول + المنفذ. |
| Named ACL | ACL ذات اسم وصفي لتسهيل إدارتها (مثل BLOCK\_HTTP). |

##### كيفية عمل ACL

1. عند مرور الحزمة، تُفحص من الأعلى إلى الأسفل في ترتيب القواعد.
2. إذا تطابقت مع قاعدة permit → تمر.
3. إذا تطابقت مع قاعدة deny → تُرفض.
4. إذا لم تطابق أي قاعدة → يتم رفضها ضمنيًا بسبب قاعدة خفية في النهاية:

deny ip any any

⚠️ هذا يعني أن ترتيب القواعد في غاية الأهمية.

##### مثال على استخدام ACL للأمان

يوجد:

* Web Server في DMZ) Demilitarized Zone: المنطقة المنزوعة السلاح، وهي منطقة بين الشبكة الداخلية والإنترنت لتقليل المخاطر الأمنية)
* Database Server داخل الشبكة الداخلية.

يمكن إعداد ACL للسماح فقط لـ خوادم الويب في DMZ بالاتصال بقاعدة البيانات عبر منفذ محدد (مثل 3306 لـ MySQL).

أي حركة مرور أخرى تُمنع لتقليل نطاق الهجوم (Attack Surface).

##### مثال عملي

access-list 100 permit tcp any 10.10.10.10 eq www

access-list 100 permit tcp any 10.10.10.10 eq 443

access-list 100 permit tcp any 10.10.10.12 eq ftp

access-list 100 permit tcp any 10.10.10.12 eq ftp-data

access-list 100 deny ip any any log

interface gi0/1

ip access-group 100 in

هذا المثال يوضح:

* السماح بالوصول إلى منافذ (**HTTP (80** و (**HTTPS (443** لخوادم الويب.
* السماح بـ **FTP المنفذ (20 و 21)**.
* حظر أي حركة أخرى مع تسجيلها في السجلات (logs).
* منع الوصول المباشر إلى خادم SQL الداخلي، لأن الوصول يجب أن يتم من خلال خادم الويب فقط.

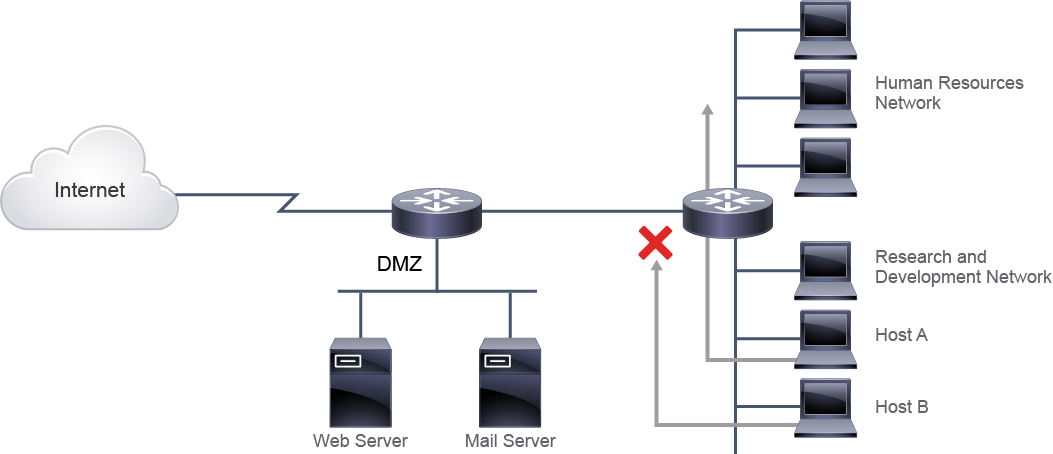
##### أهمية ACL في عمل محلل الأمن (Security Analyst)

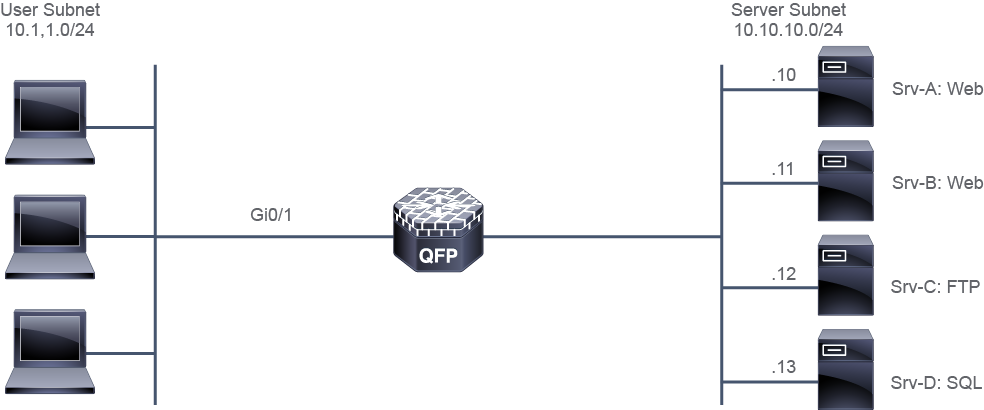
* يستطيع محلل الأمن تحليل **سجلات (ACL (logs** للكشف عن محاولات الوصول غير المصرح بها أو مشاكل الاتصال.

على سبيل المثال:

%SEC-6-IPACCESSLOGP: list 185 denied tcp 172.16.1.92(59078) -> 192.168.2.1(80)

* تعني أن اتصالًا من 172.16.1.92 إلى 192.168.2.1 على المنفذ 80 تم رفضه.  
   يمكن للمحلل تحديد ما إذا كان هذا مقصودًا أو بسبب خطأ في الإعداد.





### قوائم التحكم بالوصول ACL باستخدام خيار Established

الـ (**ACL (Access Control List** في أجهزة الراوتر التقليدية هي **stateless**، أي لا تحتفظ بمعلومات عن حالة الاتصال (state).

لكن يمكن استخدام الكلمة المفتاحية **established** في قوائم التحكم الممتدة (Extended ACLs) لتقليد سلوك “شبه حالـي” (**quasi-stateful**) يسمح بتمييز حركة المرور **الراجعة (return traffic)** عن **الحركة الجديدة (initiating traffic)**.

##### طريقة عمل الكلمة المفتاحية established

عند استخدام الأمر:

access-list 102 permit tcp any any established

سيقوم الراوتر **بالسماح فقط للحزم التي تحتوي على أحد البتّين التاليين في ترويسة TCP**:

* **ACK (Acknowledgment)**
* **RST (Reset)**

وهذا يعني أن هذه الحزم **تنتمي إلى جلسة TCP قائمة بالفعل** (أي أن الـ 3-way handshake قد اكتمل).

بالمقابل، الحزم التي تحتوي فقط على **SYN** (أي تحاول إنشاء اتصال جديد من الخارج) سيتم **رفضها** لأنها ليست جزءًا من اتصال سابق.

##### مثال تطبيقي أساسي

access-list 102 permit tcp any any established

interface ethernet0

ip access-group 102 in

* تُطبّق على الواجهة المتصلة بالشبكة غير الموثوقة (untrusted).
* تسمح فقط للحركة الراجعة التي بدأت من الشبكة الداخلية (trusted).
* تمنع الاتصالات التي تُنشأ من الخارج نحو الداخل.

##### ملاحظات أمنية مهمة

* استخدام established لا يجعل الراوتر جهاز Stateful Firewall؛

فهو لا يتتبع حالة الاتصال فعليًا، بل يعتمد فقط على فحص أعلام (TCP (TCP flags في كل حزمة بشكل مستقل.

* لذلك، يمكن للمهاجم إرسال حزم مزيفة فيها بت ACK مفعّل لتجاوز القاعدة — ما يُعرف بـ ACK Scan، وهي طريقة لجمع معلومات عن الأجهزة النشطة دون ICMP.

##### تطبيق عملي: حالة FTP

بروتوكول **FTP** يستخدم قناتين:

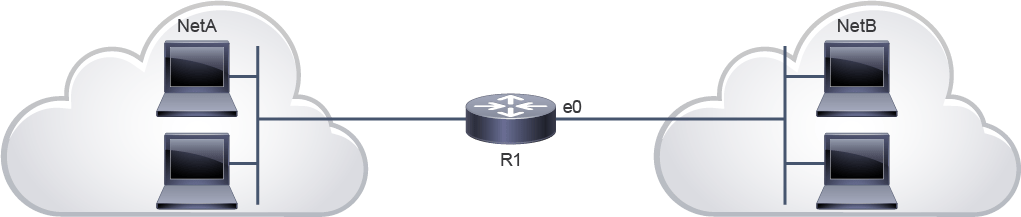
* **Port 21**: قناة التحكم (Control)
* **Port 20**: قناة البيانات (Data)

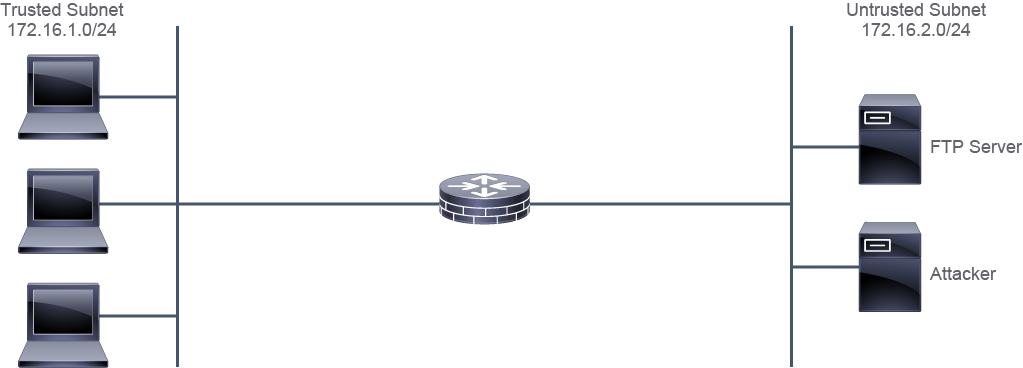
1. في FTP Passive Mode:

* العميل يفتح اتصالًا من الداخل إلى خادم خارجي.
* كل الردود من الخادم تحتوي على **بت ACK** → مسموح بها ✅

2. في FTP Active Mode:

* الخادم هو من يبدأ قناة البيانات نحو العميل (من Port 20).
* أول حزمة من الخادم تحتوي على **SYN فقط** → تُرفض 🚫 لأنها لا تحقق شرط “established”.

🔹 هذا يوضح أن established لا يتعامل مع الاتصالات الديناميكية المعقدة،  
 ولذلك يفضل وجود **Firewall فعلي (stateful)** قادر على تتبّع الجلسات ومعالجة بروتوكولات مثل FTP.



### نماذج التحكم في الوصول Access Control Models

التحكم في الوصول (Access Control) يحدد **من يمكنه الوصول إلى ماذا** داخل النظام أو الشبكة.  
 يُعتبر من الركائز الأساسية في الأمن السيبراني لحماية المعلومات والموارد من الوصول غير المصرّح به.

##### أنواع نماذج التحكم في الوصول

1. (Mandatory Access Control (MAC – التحكم الإلزامي
   * يُستخدم غالبًا في الأنظمة الحكومية والعسكرية.
   * كل **مورد (resource)** و**مستخدم (user)** يحمل **تسمية أمنية (Security Label)** تحتوي:
     + **تصنيف (Classification):** مثل *Top Secret, Secret, Confidential*
     + **فئة (Category):** مثل *قسم، مشروع، إلخ*
   * النظام يقرر السماح أو الرفض بناءً على **مطابقة التصنيف والفئة** بين المستخدم والمورد.
   * ⚠️ **عيبها:** تحتاج إدارة معقدة وتحديثات مستمرة للتصنيفات والفئات.
2. (Discretionary Access Control (DAC – التحكم الاختياري
   * المستخدم (المالك) يقرر من يمكنه الوصول إلى بياناته.
   * يعتمد على **قوائم التحكم بالوصول (ACLs)** التي تحتوي أسماء المستخدمين والمجموعات وصلاحياتهم (قراءة، كتابة، تحكم كامل...).
   * مثال: صلاحيات الملفات والمجلدات في أنظمة التشغيل.
   * ✅ مرن وسهل الإدارة.
   * ⚠️ خطر أكبر بتسريب البيانات لأن المالك قد يمنح صلاحيات خاطئة.
3. (Role-Based Access Control (RBAC – التحكم القائم على الدور
   * الوصول يعتمد على **دور المستخدم داخل المؤسسة** (وظيفته أو مسؤوليته).
   * المسؤول يحدد القواعد والسياسات مركزياً.
   * مثال:
     + "محلل" يمكنه قراءة سجلات الجدار الناري فقط.
     + "مدير النظام" يمكنه تعديل الإعدادات.

🔸 قواعد RBAC الأساسية:

* + **Role Assignment:** يجب أن يُعيّن المستخدم لدور.
  + **Role Authorization:** لا يمكن للمستخدم تولي دور إلا إذا كان مخولًا له.
  + **Transaction Authorization:** يمكن للمستخدم تنفيذ عمليات فقط إن كانت مسموحة لدوره.

1. (Rule-Based Access Control (RuBAC – التحكم القائم على القواعد
   * يعتمد على **قواعد يحددها المسؤول**، مثل:
     + السماح فقط لعناوين IP محددة.
     + حظر الوصول من IP معين.
     + السماح بالدخول فقط عبر منافذ معينة.
   * يُستخدم غالبًا في **أنظمة الجدران النارية (Firewalls)**.
   * يمكن أيضًا تطبيقه بزمن محدد (Time-Based).
2. (Time-Based Access Control (TBAC – التحكم الزمني
   * يحدد الوصول بناءً على **الوقت أو اليوم**.
   * مثال:
     + منع تصفح الإنترنت بين 9:00 و17:00.
   * مفيد لتقليل الهجمات أثناء أوقات غير العمل.
3. (Context-Based Access Control (CBAC – التحكم بالسياق
   * تطور لفكرة الـ ACL في الجدران النارية.
   * يفحص **مستوى التطبيق (Application Layer)** لفهم حالة الاتصال.
   * يسمح بدعم بروتوكولات معقدة مثل **FTP, RPC, SQL\*Net**.
   * يمكنه أيضًا حظر Java أو تصفية HTTP.
   * يشبه **جدار ناري ذكي Stateful Firewall** من حيث تحليل الجلسة.
4. (Attribute-Based Access Control (ABAC – التحكم القائم على السمات
   * **الأحدث والأكثر ذكاءً**.
   * يعتمد على **السمات (Attributes)** مثل:
     + سمات المستخدم (User attributes): المسمى الوظيفي، القسم، الدولة.
     + سمات المورد (Resource attributes): نوع البيانات، الحساسية.
     + سمات البيئة (Environment attributes): الوقت، الموقع، نوع الجهاز.
   * تستخدم سياسات منطقية مثل:
     + “If user.role = Manager → Allow read/write access.”
   * مبنية على معايير مثل **XACML** و**ALFA**.
   * تعرف أحياناً باسم **Policy-Based Access Control (PBAC)**.

##### مبادئ أساسية في التحكم بالوصول

مبدأ أقل صلاحية (Least Privilege)

* يمنح المستخدم أقل مستوى من الصلاحيات اللازمة فقط.
* الصلاحيات تكون مؤقتة حسب الحاجة.
* يقلل من فرص استغلال المستخدمين أو البرامج الضارة للنظام.

مبدأ فصل المهام (Separation of Duties)

* توزيع المهام بين أكثر من شخص لتجنب الأخطاء أو الاحتيال.
* مثال: شخص يُنشئ فاتورة وآخر يُوافق عليها.

### Authentication, Authorization, and Accounting (AAA)

تم شرح هذه المبادئ في ملف مدخل إلى أساسيات الأمن السيبراني, بإمكانك مراجعة هذه المبادئ من [هنا](https://docs.google.com/document/d/1qTDUHvHtsnW-pAoX-BOQvKC3QF2QIZrVHgnZVFBqMB8/edit?usp=sharing) في الصفحة 19

هناك لبس حصل بين الشرحين لهذا الموضوع, الـA الثالثة هي في الواقع Accounting بينما Access Control تشمل المبدأ الأول والثاني Authentication و Authorization.

هاك شرح Accounting ومن ثم أنواع تنفيذ AAA والبروتوكولات المستخدمة في AAA

##### Accounting – المحاسبة

تسجّل ما فعله المستخدم أثناء الجلسة، مثل:

* وقت الدخول والخروج
* الأوامر التي تم تنفيذها
* كمية البيانات المنقولة

الهدف: المراقبة، التدقيق (auditing)، والتحليل الأمني أو المحاسبي لاحقًا.

##### أنواع الوصول

* Administrative Access: دخول موظفي IT لتكوين الأجهزة (مثل راوتر أو سويتش).
* Network Access: دخول المستخدمين العاديين إلى الشبكة (مثل VPN).

في الحالتين، تمر العملية عبر نفس الخطوات الثلاث: Authentication → Authorization → Accounting.

##### أنواع تنفيذ AAA

🔸 Local AAA – محلي

* يُخزن المستخدمين والصلاحيات في الجهاز نفسه.
* بسيط لكنه غير قابل للتوسع.
* يحتاج تحديث يدوي لكل جهاز.
* لا يدعم المحاسبة (Accounting) بشكل جيد بسبب محدودية التخزين.

🔸 Centralized AAA – مركزي

* جميع البيانات والسياسات محفوظة في خادم مركزي واحد.
* كل الأجهزة تتصل به كـ “عملاء (clients)”.
* سهل الإدارة، ويدعم المحاسبة المركزية والتدقيق.
* يمكن دمجه مع Active Directory أو LDAP للمصادقة وإدارة المستخدمين.

##### البروتوكولات المستخدمة في AAA

(RADIUS (Remote Authentication Dial-In User Service

* يستخدم UDP (المنفذ 1812 للمصادقة، و1813 للمحاسبة).
* يجمع بين المصادقة والتفويض في عملية واحدة.
* يُشفّر فقط كلمة المرور، بينما باقي البيانات تكون نصًا واضحًا (غير مشفرة).
* مناسب للوصول عبر الشبكة (VPN، Wi-Fi...).

(TACACS+ (Terminal Access Controller Access-Control System Plus

* يستخدم TCP (المنفذ 49).
* يفصل المصادقة، التفويض، والمحاسبة.
* يُشفّر كامل محتوى الرسالة (ما عدا الرأس).
* أكثر أمانًا ومرونة، وغالبًا يُستخدم لإدارة أجهزة الشبكة (مثل Cisco).

### موازنة الأحمال Load Balancing

هي توزيع حركة المرور (الطلبات) القادمة إلى مجموعة من الخوادم **بشكل متوازن**، لتجنب الضغط على خادم واحد وتحقيق **الاستقرار، الأداء العالي، والتوافر المستمر**.

الفوائد:

* تحسين الأداء وتقليل زمن الاستجابة.
* زيادة الاعتمادية (redundancy).
* إمكانية إضافة أو إزالة خوادم بدون إيقاف الخدمة.

أنواع التنفيذ:

* Software-based (برمجياً).
* Hardware appliance (جهاز مادي).
* As-a-Service (خدمة سحابية).

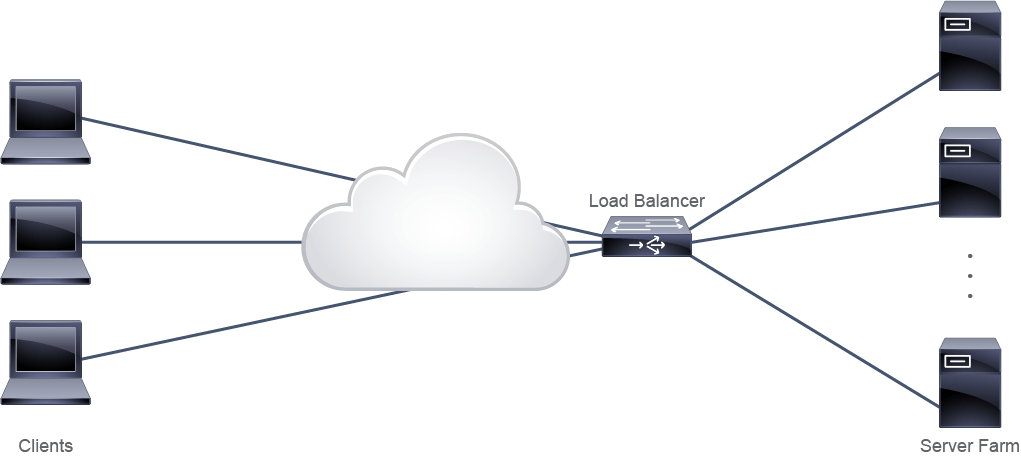
طبقات العمل:

* (Layer 4 (TCP: موازنة على مستوى الاتصال.
* (Layer 7 (HTTP/HTTPS: موازنة على مستوى التطبيق (تحليل الطلبات).

خوارزميات شائعة:

| الخوارزمية | المبدأ |
| --- | --- |
| Round Robin | توزيع الطلبات بالتسلسل بين الخوادم. |
| Least Connections | إرسال الطلب للخادم الأقل اتصالات حالية. |
| Least Time | اختيار الخادم الأسرع استجابة والأقل ازدحاماً. |
| Hash-based | استخدام قيمة تجزئة (مثل IP) لتحديد الخادم. |

آلية العمل:

الـ Load Balancer يستقبل الطلبات عبر **Virtual Server** (عنوان IP واحد يمثل مجموعة الخوادم الحقيقية) ثم يوزعها وفقاً للخوارزمية المناسبة.

##### جدار حماية تطبيقات الويب Web Application Firewall

**الفكرة الأساسية:** هو جدار حماية على مستوى تطبيقات الويب (HTTP/HTTPS) يحمي من الهجمات الشائعة مثل:

* **(Cross-Site Scripting (XSS**
* **SQL Injection**
* **DDoS**
* **Data Leakage**

**آلية العمل:**

* يفحص الطلبات **الواردة** ويمنع المشبوهة.
* يمكنه أيضاً تطبيق سياسات على **الاستجابات الصادرة** لمنع تسريب البيانات الحساسة.

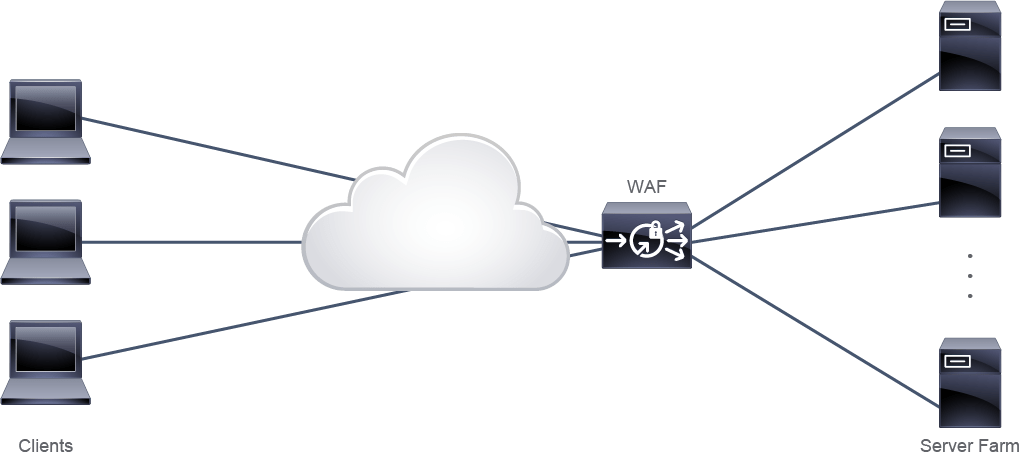
**طرق الكشف:**

1. **Signature-based:** مقارنة مع أنماط معروفة (مثل مضاد الفيروسات).
2. **Signature-less (الحديثة):** تعتمد على السلوك، التعلم الآلي، والذكاء الاصطناعي.
   * تستخدم بيانات ضخمة من تهديدات عالمية لتحديث القواعد بسرعة.

**أشكال التنفيذ:**

* **Software / Hardware / Cloud Service**
* غالباً يُستخدم كـ **Reverse Proxy** أمام الخوادم:
  + يحميها من العملاء الخبثاء.
  + يخفي هوية الخوادم (cloaking).
  + يمنع تسريب بيانات مثل بطاقات الائتمان.

**الفوائد الأساسية:**

* تقليل خطر الهجمات المكلفة على تطبيقات الويب، تسهيل نشر التطبيقات بأمان.
* تبسيط إدارة أمن الويب المستمرة.

### Network-Based Malware Protection

**الحماية من البرمجيات الخبيثة (Malware) على مستوى الشبكة** وليس على مستوى الأجهزة الفردية (Endpoints).

الهدف هو **كشف الملفات الخبيثة أثناء انتقالها عبر الشبكة** قبل أن تصل إلى المستخدمين أو الأنظمة.

##### الفرق بين الحماية التقليدية والحماية على مستوى الشبكة:

| المقارنة | التقليدية (Host-based) | الشبكية (Network-based) |
| --- | --- | --- |
| مكان الفحص | داخل الجهاز (نظام التشغيل) | أثناء عبور البيانات في الشبكة |
| الوسيلة | برنامج مكافحة فيروسات محلي | جهاز أمني (مثل Next-Generation Firewall) |
| نطاق الرؤية | محدود إلى الجهاز فقط | يشمل كل الأجهزة المتصلة بالشبكة |
| نسبة الكشف | منخفضة (~40%) بسبب تطور البرمجيات الخبيثة | أعلى لأن التحليل يتم مركزياً ويستفيد من الذكاء السحابي |

##### كيفية عمل نظام Network-Based Malware Protection:

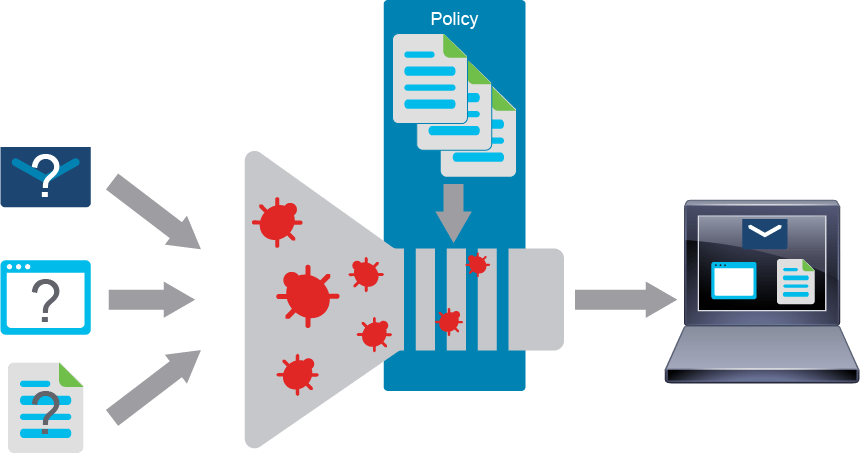
1. **تحليل الملفات أثناء عبورها الشبكة** (من الإنترنت أو البريد الإلكتروني أو FTP...).
2. **تطبيق سياسات التحكم بالملفات والتطبيقات** (Application & File Control Policies) لتحديد ما يُفحص أو يُمنع.
3. **حساب بصمة رقمية (SHA-256)** لكل ملف.
4. **مقارنة البصمة مع قاعدة بيانات محلية أو سحابية:**
   * إذا **موجودة ومعروفة** → النظام يحدد إن كانت نظيفة أو خبيثة.
   * إذا **غير معروفة** → تُرسل إلى السحابة لتحليل ديناميكي (Dynamic Analysis / Sandboxing).

##### الذكاء السحابي (Cloud Intelligence):

* مثال عملي: **Cisco Collective Security Intelligence Cloud (CSI Cloud)**
  + تجمع عينات من ملايين الملفات حول العالم.
  + تُجري عليها تحليلًا تلقائيًا لتحديد حالتها (**Disposition**):
    - ✅ **Clean**: الملف آمن.
    - ❌ **Malware**: الملف خبيث.
    - ❔ **Unknown**: غير معروف → يُرسل إلى Sandbox للتحليل.
  + إذا تغيرت حالة الملف لاحقاً (مثلاً من Unknown إلى Malware)، يتم **تحديث الحدث بأثر رجعي (Retrospective Event)**.

##### 

##### دور الإدارة (Management Console):

* تُظهر نتائج التحليل والسياسات المطبقة.
* تسمح لمسؤول الأمان بتحديد الإجراءات عند اكتشاف البرمجيات الخبيثة:
  + 🔔 إصدار تنبيه فقط.
  + 🚫 حظر نقل الملف تماماً.
  + 🧹 أو عزل الجهاز المصاب (Quarantine).

##### تطبيق عملي مهم (Cisco Firepower Example)

**السيناريو:**

* الملف **tool.exe** مر عبر الشبكة.
* جهاز **Cisco Firepower** فحص الملف وحسب بصمته (SHA-256).
* النظام صنّف الملف كـ **Malware**.
* من خلال التحليل، تبيّن أن الجهازين:
  + 🖥️ 192.168.10.90
  + 🖥️ 192.168.133.50  
     قد أصيبا بالملف.

**النتائج المعروضة في النظام:**

* 🔹 **Threat Name & Score:** اسم ونسبة خطورة التهديد.
* 🔹 **Trajectory Map:**
  + خريطة تُظهر كيف انتقل الملف بين الأجهزة عبر الزمن.
  + الخطوط العمودية تمثل نقل الملفات بين الأجهزة.
  + الخطوط الأفقية تمثل نشاط الجهاز عبر الزمن.
  + تُستخدم لتحديد مصدر العدوى وانتشارها.
* 🔹 **Events Table:**
  + تعرض تفاصيل الأحداث (من أين بدأ الملف، الأجهزة المصابة، وقت الإصابة).
  + تساعد المحلل في **تحديد نطاق الإصابة** و**خطة الاستجابة** لإزالة البرمجية.

### أدوات مراقبة أمان الشبكة Network Security Monitoring Tools

أدوات **NSM** هي برامج تُستخدم لجمع، ومعالجة، وتخزين، وعرض بيانات المراقبة الأمنية للشبكات، وهي الأساس لعمل محللي الأمن في مراكز العمليات الأمنية (**SOC**). بدون هذه الأدوات لا يمكن جمع البيانات التي يعتمد عليها التحليل الأمني.

##### الوظائف الأساسية لأدوات NSM (مثل أدوات إدارة الـ Syslog المركزية):

1. **استقبال السجلات (logs)** من الأجهزة والخوادم عبر الشبكة.
2. **تخزين السجلات** في ملفات نصية أو في قاعدة بيانات علائقية عالية الأداء.
3. **تحليل البيانات الأولية (raw data)** لتحويلها إلى معلومات مفهومة ومرتفعة المستوى.
4. **عرض النتائج** في تقارير تلقائية، لوحات تحكم (dashboards)، واستعلامات لحظية (real-time queries).

بعض الأدوات تنفذ كل هذه الوظائف في نظام واحد، بينما بعضها يعتمد على أكثر من أداة متخصصة لكل وظيفة.

##### أنواع أدوات NSM

1. **Commercial (تجارية)**
   * مميزات: احترافية، واجهات سهلة، دعم فني من الشركة.
   * عيوب: مرتفعة الثمن.
2. **Open Source (مفتوحة المصدر)**
   * مميزات: قوية وقابلة للتعديل بحرية.
   * عيوب: تحتاج موارد للتثبيت والصيانة، والدعم الفني محدود أو مدفوع أحيانًا.
3. **Homegrown (محلية أو مخصصة)**
   * تُطوّر داخل المؤسسات لتلبية احتياجات خاصة.
   * قد تكون بسيطة (مثل سكربتات صغيرة) أو متقدمة جدًا حسب حجم الفريق.
   * امتلاك مهارات **البرمجة وكتابة السكربتات** يُعتبر ميزة مهمة لمحلل الـSOC.

##### خصائص عامة

* لا يوجد **مجموعة أدوات قياسية موحدة** لجميع مراكز SOC.
* كل مركز يختار الأدوات التي تناسب احتياجاته.
* حتى داخل نفس الفريق قد يفضل المحللون أدوات مختلفة.
* أدوات SOC تتطور باستمرار مع مرور الوقت.

## أشهر هجمات TCP/IP

### (Address Resolution Protocol (ARP

ARP هو البروتوكول المسؤول عن ربط عنوان الـ **IP (المنطقي - الطبقة 3)** مع عنوان الـ **MAC (الفيزيائي - الطبقة 2)** داخل الشبكات المحلية (LAN).

بدونه، لا يمكن للأجهزة إرسال البيانات عبر شبكة Ethernet لأن إرسال الإطارات (frames) يتطلب معرفة عنوان MAC للوجهة.

##### آلية عمل ARP

* عندما يعرف الجهاز عنوان الـIP المطلوب لكنه لا يعرف الـMAC المقابل، يرسل طلب ARP (ARP Request) إلى الشبكة بصيغة بث (broadcast).
  + مثال الرسالة: “من صاحب الـIP 172.16.3.2؟ أريد عنوانك الفيزيائي.”
* الجهاز الذي يحمل هذا الـIP يرد مباشرة بـ ARP Reply يحتوي على عنوانه الفيزيائي (MAC Address).
* الجهاز المرسل يحفظ هذا الربط في جدول ARP (ARP Table أو Cache) لتسريع العمليات المستقبلية.
* جدول ARP يتم تحديثه تلقائيًا، حيث تُحذف العناوين القديمة بعد فترة (عملية تسمى aging) لتفادي بقاء بيانات لأجهزة لم تعد متصلة.

##### الأوامر العملية

#### الأمر المهم:

arp -a

* يُستخدم على Windows و Linux لعرض جدول الـARP الحالي.
* يُظهر كل IP مع الـMAC المقابل ونوع الربط (ديناميكي أو ثابت).
* بعض العناوين الخاصة مثل 224.x.x.x و 239.x.x.x تشير إلى multicast وهي طبيعية في الجدول.

##### طبقة العمل في نموذج OSI

* يعمل ARP بين **الطبقة الثانية (Data Link)** و **الطبقة الثالثة (Network)**.
* يُحدد نوع الإطار عبر **EtherType = 0x0806**.
  + 0x0800 → IPv4
  + 0x86DD → IPv6

##### الجانب الأمني المهم – ARP Poisoning

من أبرز ثغرات ARP أنه **لا يتحقق من صحة الردود**، مما يسمح للمهاجم بإرسال **ردود مزيفة (Fake ARP Replies)**:

* في هذه الحالة، يخدع المهاجم الضحية ليعتقد أن **عنوان MAC الخاص بالمهاجم يخص IP آخر**.
* النتيجة: تتحول الضحية لإرسال البيانات إلى المهاجم بدل الوجهة الحقيقية.
* هذا الهجوم يعرف باسم **(Man-in-the-Middle (MITM** ويمكن من خلاله **اعتراض أو تعديل البيانات**.

🎯 لذلك فهم آلية ARP أمر ضروري لمحلل الأمن السيبراني، خاصة في الكشف عن الهجمات على الطبقة الثانية.

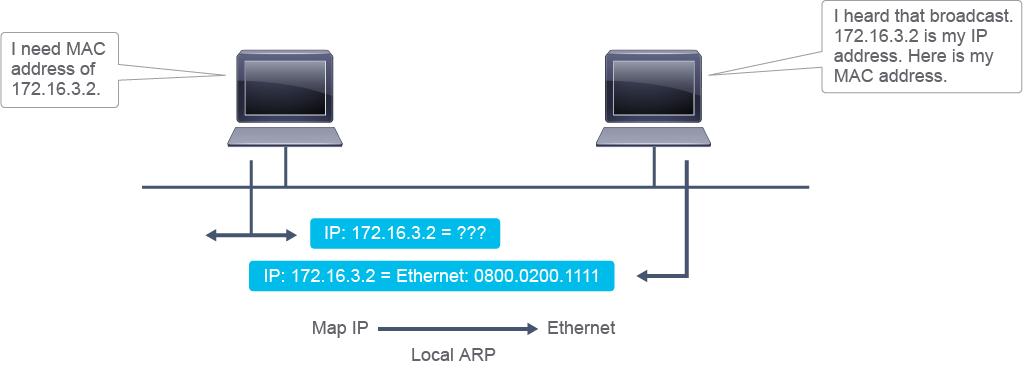
##### تطبيق عملي مهم

🔍 تجربة ARP في بيئة حقيقية:

1. على جهازك، افتح الطرفية (Terminal أو CMD).
2. 2. اكتب:

arp -a

1. لاحظ:
   * عناوين IP المقترنة بـ MAC.
   * نوع الربط (dynamic/static).
   * عناوين multicast أو broadcast.
2. يمكنك مسح الكاش لتحديث الجدول:

arp -d \* 

### Legacy TCP/IP Vulnerabilities

تم تصميم بروتوكولات **TCP/IP** في الأصل (وفق RFC 793) لتوفير نقل موثوق وسريع للبيانات في بيئة **موثوقة** — أي أن الأمن لم يكن ضمن أولويات التصميم. لذلك تحتوي هذه البروتوكولات على **نقاط ضعف موروثة (Legacy Vulnerabilities)** من الصعب التخلص منها لأنها جزء من بنيتها الأساسية.

🔹 **أسباب الضعف:**

* البروتوكولات القديمة مثل **rlogin, rcp, rsh** كانت تسمح بالوصول بين أجهزة UNIX **بدون كلمات مرور**، وهو ما جعلها عرضة لهجمات مثل **Password Sniffing** و**(Denial of Service (DoS**.
* بعض البروتوكولات العليا مثل **HTTP, Telnet, SMTP** تعتمد على TCP، وبالتالي **ترث نقاط ضعفه** (مثل إمكانية اعتراض أو اختطاف الجلسة).

🔹 **هجمات شهيرة مرتبطة بالتصميم القديم:**

* **(Morris Worm (1988:** أول دودة انتشرت عبر الإنترنت، استغلت ثغرات في أدوات مثل **sendmail** و finger. كانت نيتها قياس حجم الشبكة (ARPANET)، لكنها تسببت في بطء الأجهزة وتعطلها عند تكرار العدوى.  
   ➤ هذا الحدث كان نقطة التحول التي جعلت **أمن الشبكات موضوعًا علميًا جادًا**.
* بعد ذلك ظهرت هجمات مشابهة مثل:
  + **(Melissa (1999**
  + **(Code Red (2001**
  + **(SQL Slammer (2003** وكلها أكدت أن **الشبكات ستبقى عرضة لهجمات جديدة رغم التحديثات**.

🔹 **تحسينات وتطورات لاحقة:**

* تم **تعطيل** استخدام أدوات مثل **rsh** في الشبكات غير الموثوقة.
* تم **تصحيح ثغرات sendmail وfinger**.
* تم تعزيز الأمان عبر **جدران الحماية (firewalls)** و**الوعي الأمني** وكلمات المرور القوية.
* ومع ذلك، فإن أي **ثغرة في أحد بروتوكولات TCP/IP الأربعة الرئيسية** (IP, TCP, UDP, ICMP) يمكن أن تؤثر على كل ما يعتمد عليها في الطبقات الأعلى.

🔹 **ما يجب على محلل الأمن السيبراني فهمه:**

* معرفة **هيكل البروتوكولات** الأربعة الرئيسة وعلاقاتها ببعض.
* القدرة على **تحليل الحزم (packet analysis)** وفهم **نقاط الضعف المحتملة** في الطبقات السفلى.

### نقاط ضعف بروتوكول الإنترنت (IP Vulnerabilities)

بروتوكول الإنترنت (IP) يعمل في **الطبقة الثالثة (Network Layer)** من نموذج OSI، وهو أساس توجيه البيانات بين الأجهزة.

لكن بسبب بساطة تصميمه وغياب مفاهيم الأمان في نسخته الأصلية (IPv4)، فهو عرضة لعدة أنواع من الهجمات.

#### أهم أنواع الهجمات على بروتوكول IP

##### 1. Man-in-the-Middle (MITM) Attack

* المهاجم يضع نفسه بين جهازي الاتصال (A وB) دون علمهما.
* يستطيع **اعتراض البيانات، تعديلها، أو سرقة المفاتيح** أثناء تبادلها.
* مثال: تغيير رقم الحساب في عملية مالية أثناء النقل.
* **سبب الثغرة:** لا يوجد تحقق أصيل من هوية المرسل أو المستقبل في بروتوكول IP.

🔸 **أنواع فرعية مرتبطة:**

* **Session Hijacking:** المهاجم يخطف جلسة نشطة لتقمص هوية المستخدم.
* **Sidejacking:** سرقة ملفات تعريف الارتباط (Cookies) للحصول على جلسة المستخدم.
* **Evil Twin:** نقطة Wi-Fi مزيفة تُستخدم لاعتراض بيانات المستخدمين.
* **Packet Sniffing:** التقاط وتحليل الحزم المنقولة عبر الشبكة.

##### 2. IP Address Spoofing

* المهاجم يزوّر عنوان IP ليبدو وكأنه جهاز آخر (غالباً البوابة Gateway أو مستخدم موثوق).
* يمكن أن يحدث عبر **ARP Spoofing**، حيث يعلن المهاجم أنه البوابة الافتراضية.
* النتيجة: تمر كل حركة المرور من خلال المهاجم، مما يمكّنه من **التنصت أو التلاعب بالبيانات**.

##### 3. Denial of Service (DoS) Attack

* المهاجم يغمر الخادم بطلبات اتصال مزيفة (عادة SYN packets) ليستهلك موارده.
* يستخدم **عنوان IP مزيف (spoofed)**، مما يجعل من الصعب تعقبه.
* يؤدي إلى **استنزاف موارد الخادم (Resource Exhaustion)** وعدم قدرته على خدمة المستخدمين الحقيقيين.

##### 4. (Distributed Denial of Service (DDoS

* نفس مبدأ DoS لكن من **عدة أجهزة حول العالم (Botnet)**.
* يصعب التصدي له لأنه يأتي من مصادر متعددة عبر الإنترنت.
* غالبًا ما يتم التحكم بالأجهزة المشاركة عبر **قنوات (Command & Control (C2**.

##### 5. Smurf Attack

* نوع خاص من DDoS يعتمد على **بث (broadcast) رسائل (ICMP Echo Request (ping** مع عنوان مصدر مزيف.
* تُرسل الرسائل إلى شبكة كاملة بعنوان بث مثل 10.1.1.255، ويُزيف المهاجم عنوان المصدر ليكون عنوان الضحية.
* كل الأجهزة ترد على الضحية، مما يؤدي إلى **شلّ النظام المستهدف**.

##### 6. Resource Exhaustion

* نتيجة مشتركة لكل الهجمات السابقة.
* يتم **استنزاف المعالج والذاكرة ومنافذ الشبكة** بسبب كمّ هائل من الطلبات أو الردود المزيفة.

ملاحظات مهمة للدراسة

* كل هذه الهجمات تعتمد على غياب **التحقق الأصلي (Authentication)** في الطبقة الثالثة.
* تُعالج هذه الثغرات في الشبكات الحديثة عبر:
  + **ARP Inspection** و **Port Security** في المحولات.
  + **Firewalls** و **IDS/IPS Systems**.
  + استخدام **VPNs** و**TLS Encryption** لتأمين الاتصالات.

### ثغرات بروتوكول ICMP Vulnerability - ICMP

##### مقدمة عن ICMP

* بروتوكول (**ICMP** (Internet Control Message Protocol يعمل في طبقة الشبكة (Network Layer).
* لا يستخدم المنافذ مثل TCP أو UDP، بل يُستخدم لإرسال **رسائل تشخيصية** (diagnostic messages) أو **تنبيهات عن أخطاء الشبكة**.
* أمثلة استخدام:
  + **ping**: اختبار الوصول (echo request/reply).
  + **traceroute**: تحديد المسار باستخدام رسائل TTL Expired.
* تولده أجهزة الشبكة (موجهات، جدران نارية، نقاط النهاية) لتحديد مشاكل الاتصال.
* رغم فائدته في التشخيص، يمكن أن يكون أداة لجمع المعلومات واستغلال الشبكات، ولهذا بعض المسؤولين يعطلونه كليًا.

##### ثغرات واستغلالات ICMP المهمة

1. **Reconnaissance & Scanning (الاستطلاع والمسح)**
   * المهاجمون يستخدمون ICMP لاكتشاف الأجهزة النشطة (ICMP sweep) أو المسارات (traceroute) لجمع معلومات عن البنية التحتية.
   * ICMP يساعدهم في **رسم خريطة للشبكة** قبل بدء الهجوم.
2. **ICMP Unreachables**
   * رسائل مثل *Port Unreachable* أو *Protocol Unreachable* تُخبر المهاجم بأن خدمة أو بروتوكول معين غير مستخدم،  
      مما يساعده في **تحليل ما هو نشط** على الجهاز.
3. **ICMP Mask Reply**
   * تُستخدم لتحديد **قناع الشبكة (Subnet Mask)**، مما يمكن المهاجم من **رسم مخطط دقيق للشبكة الداخلية**.
4. **ICMP Redirect Attack (إعادة التوجيه الخبيث)**
   * المهاجم يرسل رسالة "Redirect" مزيفة لإجبار الضحية على تمرير بياناتها عبر جهاز المهاجم (MITM).
   * نتيجة: **هجوم رجل في المنتصف** أو تعطيل الاتصال.
5. **(ICMP Router Discovery (IRDP**
   * يُستخدم لتحديد الموجهات (Gateways) في الشبكة، لكنه **يفتقر للمصادقة**.
   * المهاجم يمكنه **تزييف الرسائل** لخداع الأجهزة وتمرير البيانات إلى عناوين مزيفة (MITM أو DoS).
6. **Firewalking**
   * تقنية استطلاع متقدمة تشبه traceroute، تُستخدم لاكتشاف **القواعد في جدران الحماية (ACLs)** وتحديد ما إذا كانت المنافذ مسموحة أو محجوبة.
7. **ICMP Tunneling (نفق ICMP)**
   * تقنية لإخفاء البيانات داخل حزم ICMP (مثل echo request/reply).
   * تُستخدم لإنشاء قناة اتصال سرية **تتجاوز جدران الحماية**.
   * أداة مشهورة: **LOKI** التي تخفي الاتصالات داخل ICMP.
8. **ICMP-based OS Fingerprinting (تحديد نظام التشغيل)**
   * يمكن تحليل **TTL أو IP ID أو نوع الرد** لتخمين نظام التشغيل:
     + TTL = 128 → غالبًا Windows
     + TTL = 64 → غالبًا Linux
9. **Denial of Service (DoS) Attacks باستخدام ICMP**
   * **ICMP Flood:** إغراق الهدف بطلبات ping هائلة تؤدي إلى **استنزاف الموارد**.
   * **Smurf Attack:**
     + المهاجم يُرسل طلبات ICMP إلى عنوان بث (Broadcast) مستخدمًا IP الضحية كمصدر.
     + جميع الأجهزة ترد على الضحية → **شلل في الشبكة**.

##### الخلاصة الأمنية

* ICMP مفيد جدًا في إدارة الشبكات، لكنه **أداة قوية بيد المهاجمين** أيضًا.
* على محلل الأمن أن يراقب:
  + النشاط الزائد في ICMP.
  + الاتصالات غير المعتادة (خصوصًا ICMP echo أو redirect).
  + استخدام ICMP كنفق (Tunneling).
* يُنصح بتقييد ICMP أو مراقبته بدلاً من منعه كليًا، لأن بعض خدمات الشبكة تعتمد عليه.

##### تطبيق عملي

**كشف الأجهزة النشطة:**

nmap -sn 192.168.1.0/24

1. → يقوم بمسح الشبكة باستخدام ICMP لمعرفة الأجهزة المتصلة.

**تتبع المسار**

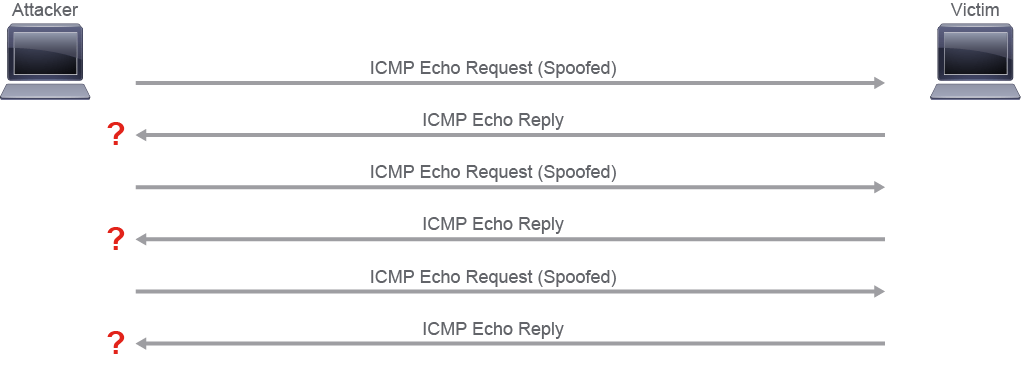
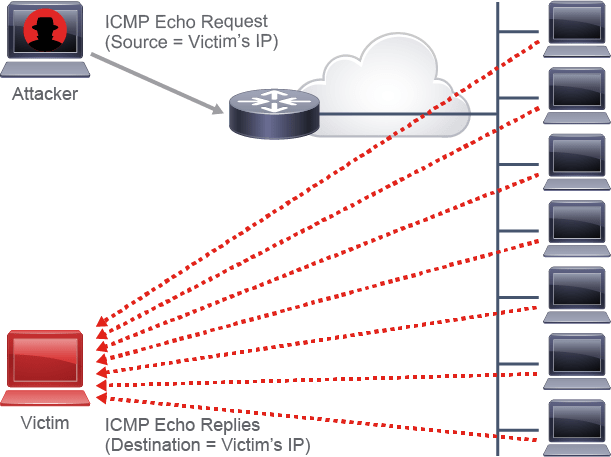
traceroute 8.8.8.8

1. → يوضح مسار الحزم بينك وبين الهدف ويُظهر الموجهات في الطريق.

**محاكاة ICMP Flood (في بيئة اختبارية فقط):**

ping -f -s 65500 target\_ip

1. → يولد ضغطًا كبيرًا على الهدف لتوضيح فكرة الـ **Flood attack** (تجريبي فقط في مختبر مغلق).

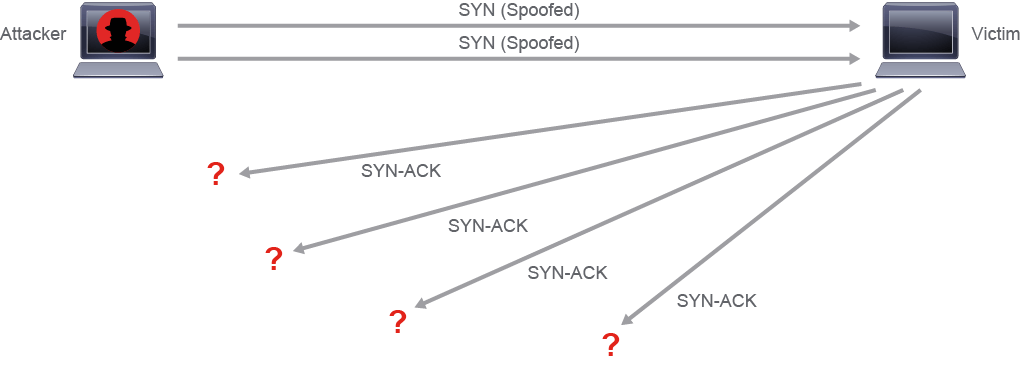


### تغرات TCP Vulnerabilites - TCP

* **(TCP (Transmission Control Protocol** هو بروتوكول اتصال موثوق يعتمد على الاتصال (connection-oriented).
* يضمن نقل البيانات من خلال آليات مثل **Acknowledgment**, **Sequence Numbers**, و**Flow Control**.
* يبدأ الاتصال بـ **(Three-Way Handshake (SYN → SYN-ACK → ACK** وينتهي بـ **(Four-Way Handshake (FIN و ACK**.

#### أهم الثغرات والهجمات في TCP

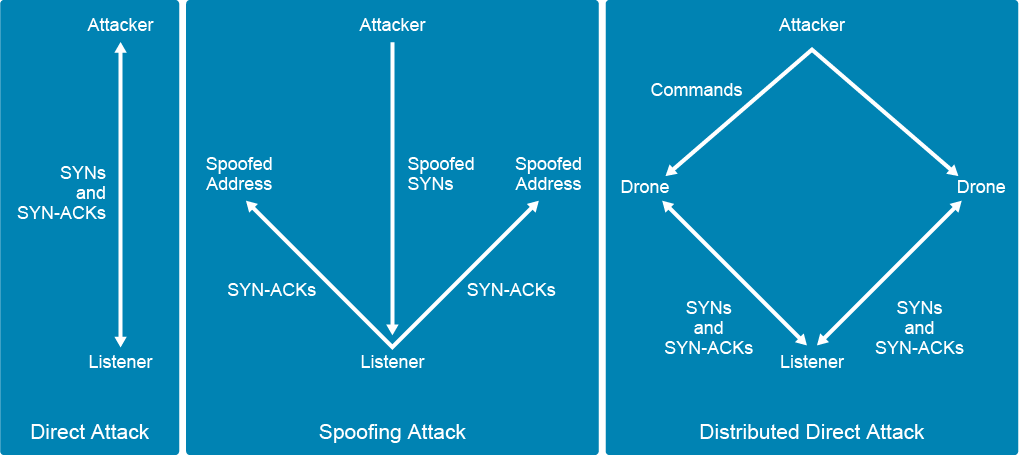
##### 1. TCP SYN Flooding (هجوم حجب الخدمة - DoS)

**الفكرة:** استغلال آلية المصافحة الثلاثية في TCP بإرسال عدد ضخم من طلبات الاتصال (SYN) دون إكمال المصافحة، مما يترك الاتصالات في حالة **نصف مفتوحة (Half-Open)** ويستهلك موارد الخادم.

**النتيجة:** الخادم لا يستطيع استقبال طلبات حقيقية من المستخدمين الشرعيين.

**أنواع الهجوم:**

* **Direct Attack:** المهاجم يستخدم عنوانه الحقيقي ويمنع استجابة SYN-ACK من الوصول إليه (بجدار ناري مثلاً).
* **Spoofing-Based Attack:** المهاجم يرسل SYN باستخدام عناوين IP مزيفة (غالبًا غير موجودة)، مما يجعل رد الخادم يضيع.
* **(Distributed Attack (DDoS:** المهاجم يستخدم شبكة ضخمة من الأجهزة المخترقة (Botnet) لإطلاق هجوم منسق، مما يجعل من الصعب جدًا منعه.

**وسائل التخفيف:**

* وضع حد زمني للاتصالات نصف المفتوحة.
* استخدام Firewalls أو IDS/IPS لاكتشاف ومنع هذه الاتصالات.

##### 

##### 2. TCP Session Hijacking (اختطاف الجلسة)

**الفكرة:** السيطرة على جلسة TCP نشطة بين مضيفين بعد أن يتم توثيق الاتصال بينهم.

**كيف يعمل:**

* يعتمد على التنبؤ بـ **رقم التسلسل (Sequence Number)** المستخدم بين الطرفين.
* إذا نجح المهاجم في تخمين أو رؤية الرقم الصحيح، يمكنه إرسال حزم بيانات وكأنه أحد الأطراف الشرعيين.

**أنواع الهجوم:**

* **Non-Blind Spoofing:** المهاجم يرى حركة المرور (Traffic) بين الطرفين، مثلاً عند وجوده في نفس الشبكة.
* **Blind Spoofing:** المهاجم لا يرى الحركة ويعتمد على تخمين رقم التسلسل — أصعب نوع لأنه يتطلب دقة عالية جدًا.

**أدوات شهيرة للهجوم:** Juggernaut، Hunt، TTY Watcher، T-Sight (توجد في توزيعات مثل Kali Linux).

**الهدف:** استغلال الجلسة الحالية (التي تم توثيقها مسبقًا) للوصول إلى النظام أو سرقة البيانات.

##### 3. TCP Reset Attack

**الفكرة:** إرسال حزمة TCP مزيفة تحتوي على **علم (RST (Reset** لقطع الاتصال بين طرفين بشكل مفاجئ.

**كيف يتم:**

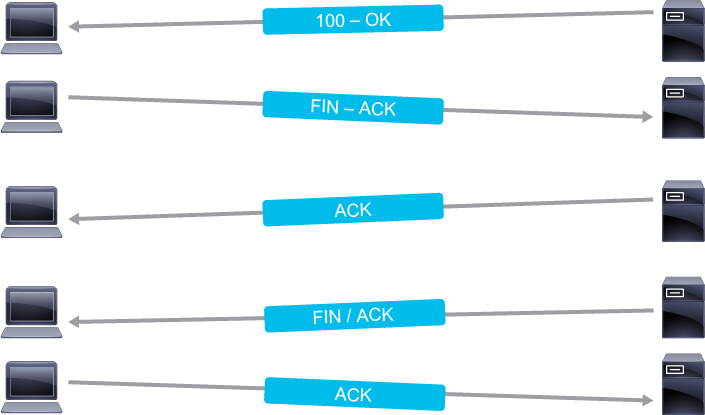
* المهاجم يراقب الاتصال، ثم يرسل حزمة RST مزيّفة توحي بأنها من أحد الطرفين.
* عند استلامها، يقوم الطرف الآخر بإغلاق الاتصال فورًا.

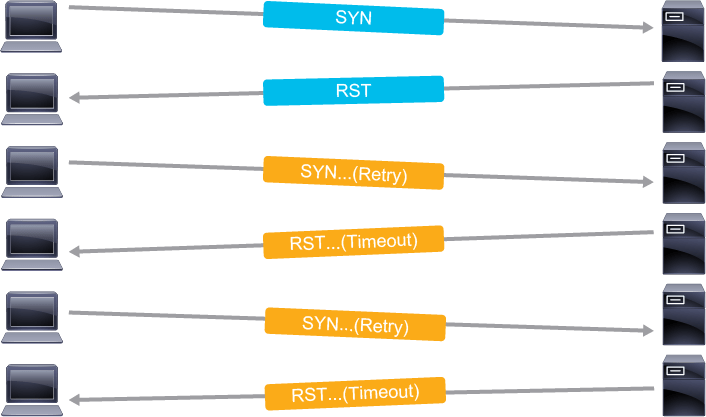
**الاستخدام الشرعي:**

* أنظمة **(IPS (Intrusion Prevention Systems** تستخدم هذه التقنية لقطع الاتصالات الضارة.

**الاستخدام الخبيث:**

* تعطيل الاتصالات الشرعية (DoS على مستوى الجلسة).
* منع المستخدمين من الاتصال بخدمات معينة.





##### تطبيق عملي (يمكن تجربته في مختبر تعليمي أو بيئة آمنة فقط)

**الهدف:** فهم آلية SYN Flooding على مستوى عملي.

الخطوات النظرية:

1. استخدم أداة مثل hping3 أو nping لإرسال حزم SYN متكررة إلى خادم وهمي (test server).

sudo hping3 -S -p 80 --flood <target\_ip>

1. راقب على الخادم الاتصالات نصف المفتوحة باستخدام:

netstat -ant | grep SYN\_RECV

1. لاحظ كيف ترتفع الاتصالات غير المكتملة وتستهلك الموارد.

**ملاحظة:** يُمنع تنفيذ هذا النوع من الاختبار على خوادم حقيقية دون إذن رسمي، وإلا يُعتبر هجومًا.

### ثغرات UDP Vunlnerabilities - UDP

* **(UDP (User Datagram Protocol** هو بروتوكول **بلا اتصال (Connectionless)** في طبقة النقل.
* لا يحتوي على آليات **موثوقية أو تحكم بالتدفق أو استعادة الأخطاء** مثل TCP.
* لهذا السبب، رأس UDP بسيط جدًا وصغير الحجم — مما يقلل الحمل على الشبكة (Low Overhead).
* يستخدمه عدد من البروتوكولات والتطبيقات مثل:
  + **DNS** (نظام أسماء النطاقات)
  + **SNMP** (إدارة الشبكات)
  + **NFS**, **TFTP**
  + تطبيقات الزمن الحقيقي مثل **VoIP**, **الألعاب أونلاين**, **البث المباشر**.

##### نقاط الضعف الأساسية في UDP

1. 🧩 سهولة التلاعب بالبيانات (Data Manipulation)

* **حقل التحقق (Checksum)** في UDP **اختياري** وليس إلزاميًا.
* يمكن للمهاجم **تعديل البيانات داخل الحزمة** ثم **إعادة حساب checksum** الجديد بسهولة.
* لا يوجد في UDP أي نوع من **التحقق من المصدر (Source Verification)**.
* هذا يعني أن المهاجم يمكنه:
  + **التنصت (Eavesdropping)** على البيانات لأنها غير مشفرة.
  + **انتحال الهوية (Spoofing)** عبر إرسال حزم UDP مزيفة من عنوان IP مختلف.
* أمثلة متأثرة:
  + **SNMPv1** و**DNS** (كلاهما يستخدم UDP دون تشفير افتراضيًا).

2. 🧨 هجمات استنزاف الموارد (UDP Flooding – DoS Attack)

* **الهدف:** إنهاك الخادم أو الشبكة عبر إرسال سيل ضخم من حزم UDP إلى منافذ عشوائية.

عندما **لا يوجد تطبيق يستمع على هذه المنافذ**، يرد الخادم برسائل:

ICMP Destination Unreachable (Port Unreachable)

* النتيجة:  
  + الخادم يرسل عددًا هائلًا من رسائل ICMP. **تُستهلك موارد النظام** (CPU، الذاكرة، أو النطاق الترددي). الشبكة تصبح بطيئة أو غير متاحة للمستخدمين الشرعيين.

**أدوات تُستخدم للهجوم:**

* **UDP Unicorn**
* (**Low Orbit Ion Cannon (LOIC**

**آلية شائعة للهجوم:**

* المهاجم يُزيف (Spoofs) عنوان المصدر لتجنب تتبعه.
* يتم إرسال عدد ضخم من الحزم خلال وقت قصير جدًا.

3. هجوم SQL Slammer (مثال تطبيقي تاريخي)

**الحدث:**

* سنة 2003، انتشر **SQL Slammer Worm** مستغلًا ثغرات في **Microsoft SQL Server 2000** عبر **المنفذ UDP 1434**.

**الآلية:**

* الثغرات كانت من نوع **Buffer Overflow** في خدمة **SQL Server Resolution Service**.
* المهاجم يرسل حزمة UDP صغيرة جدًا لكنها معدّلة خصيصًا لتجاوز الذاكرة.
* إذا نجح الهجوم، يمكن تنفيذ **كود ضار عن بُعد (Remote Code Execution)**.
* إذا فشل، يؤدي إلى **تعطيل الخدمة (Crash)**.
* بعد الإصابة، يقوم الخادم المصاب بإرسال نفس الهجوم لخوادم أخرى — مما سبب **انتشارًا واسعًا (Worm Propagation)** وازدحامًا في الشبكة.

**نتيجة:**

* توقف آلاف الخوادم عن العمل خلال دقائق.
* كشف مدى خطورة الثغرات المرتبطة بـ UDP.

4. ثغرة Keepalive Storm

* تعتمد **SQL Server instances** على آلية "Keepalive" في UDP المنفذ 1434.
* عندما تُرسل حزمة Keepalive تحتوي على القيمة 0x0A، يرد الخادم بنفس القيمة.
* إذا تم **تزوير (Spoofing)** الحزمة لتبدو قادمة من خادم SQL آخر،  
   → يبدأ الخادمان بإرسال الردود لبعضهما بلا توقف ⚠️  
   → مما يولّد **عاصفة حزم (Packet Storm)** → وينتهي بتوقف أحد الخادمين أو تعطله.

##### تطبيق عملي (مختبر تعليمي فقط)

تجربة UDP Flood (في بيئة اختبار):

تشغيل أداة Flood على منفذ وهمي لخادم اختبار:

sudo hping3 --udp -p 53 --flood <target\_ip>

على الخادم المستهدف، راقب الحزم:

netstat -s | grep UDP

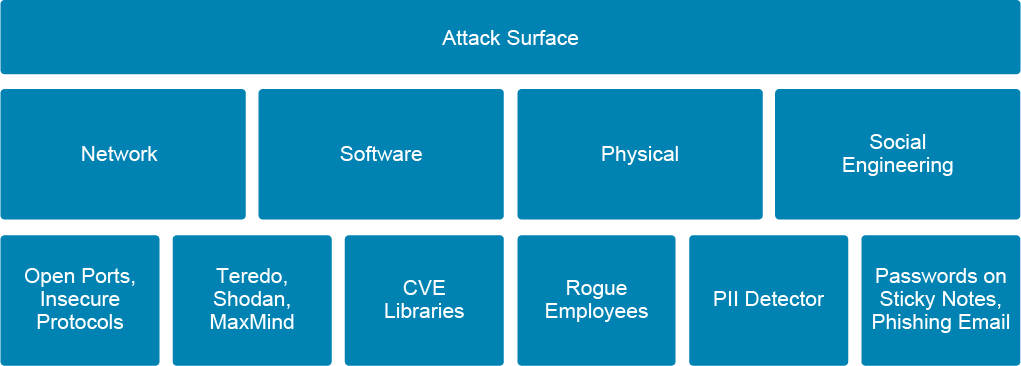
لاحظ ارتفاع عدد رسائل “Port Unreachable” وتباطؤ النظام.

⚠️ ملاحظة: لا يُسمح بتجربة هذا عمليًا على خوادم حقيقية — فقط ضمن بيئة مختبرية أو محاكاة (Virtual Lab).

### واجهات وسبل/مسارات الهجمات Attack Surface and Attack Vectors

* **Attack Surface** (سطح الهجوم): هو مجموع جميع النقاط أو الثغرات التي يمكن أن يستغلها المهاجم للوصول إلى نظام أو شبكة.  
   كلما كان السطح أكبر، زادت احتمالية الاختراق.
* **Attack Vectors** (وسائل/مسارات الهجوم): هي الطرق أو القنوات التي يستخدمها المهاجم لاختراق النظام واستغلال الثغرات.

##### تصنيفات سطح الهجوم (Attack Surface):

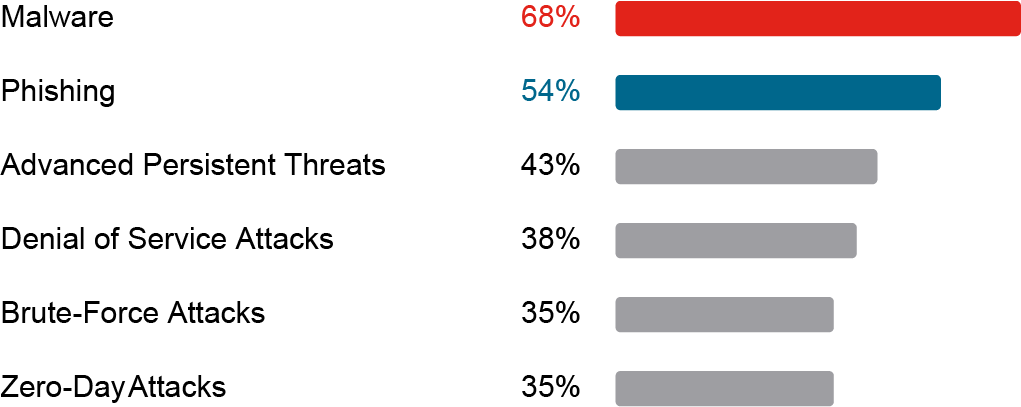
* 🛰 **Network Attack Surface**:  
   يشمل جميع المنافذ المفتوحة والبروتوكولات والخدمات والأجهزة المتصلة.  
   أمثلة: Telnet, FTP, HTTP, SMTP — لأنها ترسل البيانات بدون تشفير.  
   أيضًا الطابعات والشبكات اللاسلكية تمثل نقاط ضعف إذا لم تُؤمّن جيدًا.
* **Software Attack Surface**:  
   يشمل أي كود أو تطبيق متاح للوصول من طرف مستخدم غير مصدّق.  
   الثغرات تظهر في البرامج غير المُحدّثة أو السيئة البرمجة.  
   من المهم متابعة قواعد البيانات مثل **CVE** لتتبع الثغرات المعروفة وتحديث الأنظمة.
* **Physical Attack Surface**:  
   الثغرات الناتجة عن الوصول المادي للأجهزة (مثل منافذ USB، الأجهزة المفقودة أو المسروقة، أو الموظفين المخترقين داخليًا).
* **Social Engineering Attack Surface**:  
   يعتمد على استغلال **العامل البشري** مثل الخداع أو الهندسة الاجتماعية.  
   أمثلة:
  + انتحال هوية موظف للحصول على كلمة مرور.
  + إسقاط فلاش USB خبيث في موقف سيارات.
  + رسائل تصيّد (Phishing / Spear Phishing).

##### مثلة على Attack Vectors (مسارات الهجوم):

* **Malware**: مثل الفيروسات وTrojan والـ Worms التي تُثبت نفسها في النظام.
* **Phishing / Spear Phishing**: رسائل بريدية مزيفة لجمع بيانات الدخول.
* **SQL Injection**: استغلال مدخلات المستخدم غير المؤمنة لاختراق قاعدة البيانات.
* **Known Vulnerabilities**: استغلال الثغرات المعروفة في البرامج (من CVE).
* **(Advanced Persistent Threats (APT**: هجمات طويلة المدى تهدف للتجسس وسرقة البيانات دون التسبب بانقطاع النظام.
* **Weak Authentication**: كلمات مرور ضعيفة أو آليات مصادقة غير آمنة.
* **Reconnaissance**: جمع المعلومات عن الهدف قبل الهجوم مثل نوع النظام والمنافذ المفتوحة.

##### طرق تقليل سطح الهجوم ومواجهة المسارات:

* إغلاق المنافذ غير الضرورية وتعطيل البروتوكولات غير الآمنة.
* تحديث الأنظمة والبرامج بشكل دوري.
* تطبيق التشفير في كل الاتصالات الحساسة.
* مراقبة الشبكة لحظيًا عبر SIEM أو IDS/IPS.
* تدريب الموظفين على التوعية الأمنية.
* عزل الأنظمة باستخدام VLANs وLoad Balancers.
* استخدام Honeypots لجذب المهاجمين وتحليل سلوكهم.

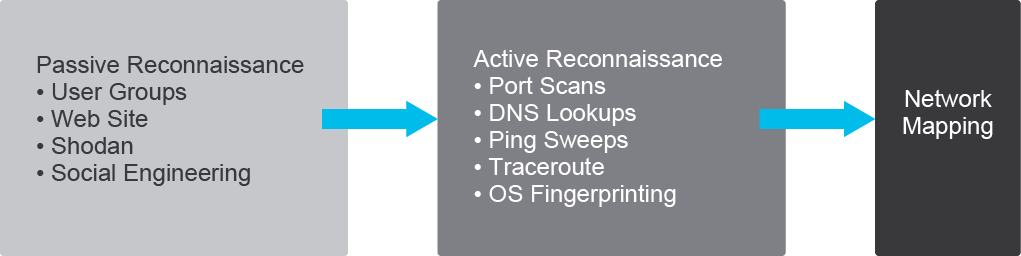


### هجمات الاستطلاع (Reconnaissance Attacks)

هجمات **Reconnaissance** هي المرحلة الأولى في أي هجوم سيبراني، وهدفها **جمع معلومات عن الهدف** (نظام، شبكة، أو مستخدم) قبل تنفيذ هجوم فعلي مثل الاختراق أو الـDoS.  
 التركيز يكون على:

* معرفة **عناوين IP** و**الأجهزة والخوادم** المرتبطة بالشبكة.
* تحديد **المنافذ المفتوحة (open ports)** والخدمات المرتبطة بها.
* تحديد **نظام التشغيل** المستخدم لتخطيط هجوم مخصص له.

##### أنواع هجمات الاستطلاع

1. **Passive Reconnaissance (استطلاع سلبي)**
   * لا يتفاعل المهاجم مباشرة مع النظام المستهدف.
   * يعتمد على جمع معلومات من مصادر علنية أو مراقبة غير مباشرة.
   * **أمثلة:**
     + أدوات مثل whois, dig, nslookup لجمع معلومات DNS.
     + البحث في محرك **Shodan** لتحديد الأجهزة المتصلة بالإنترنت وإصداراتها.
     + تحليل ملف **robots.txt** في المواقع لمعرفة الملفات أو المجلدات المخفية.
     + استخدام **packet sniffers** مثل Wireshark أو NetworkMiner لالتقاط البيانات المارة على الشبكة.
     + أدوات تسجيل المفاتيح (Keyloggers) لجمع كلمات المرور.
2. **Active Reconnaissance (استطلاع نشط)**
   * المهاجم يتفاعل مباشرة مع الهدف لإرسال واستقبال البيانات وجمع ردود فعل النظام.
   * **أمثلة:**
     + **Ping Sweeps:** معرفة الأجهزة النشطة عبر إرسال ICMP Echo Requests.
     + **Port Scanning:** تحديد المنافذ المفتوحة والخدمات باستخدام أدوات مثل **Nmap**.
     + **Traceroute:** تحديد مسار الاتصال والعُقد بين المهاجم والهدف لتحديد الجدران النارية أو الموجهات (Routers).
     + **OS Fingerprinting:** تخمين نظام التشغيل بناءً على ردود المنافذ.

##### أدوات الاستطلاع الشائعة

| **الأداة** | **الاستخدام** |
| --- | --- |
| **Nmap** | فحص المنافذ وتحديد الخدمات ونظام التشغيل (الأداة الأكثر استخدامًا في recon). |
| **Wireshark** | تحليل حركة المرور (Traffic Analysis) والتقاط الحزم. |
| **Nessus / OpenVAS** | أدوات فحص الثغرات الأمنية لتحديد نقاط الضعف (تُستخدم من قِبل المهاجمين والمختبرين الأخلاقيين). |
| **Whois / nslookup / dig** | جمع معلومات DNS والمُسجّلين. |
| **Shodan** | محرك بحث للأجهزة المتصلة بالإنترنت لتحديد الأنظمة الضعيفة. |
| **fping** | أداة لإجراء Ping Sweep لتحديد الأجهزة النشطة. |

##### التطبيق العملي المهم – Nmap Example

في بيئة اختبار مثل Kali Linux:

nmap -v -sN 192.168.80.131

* يقوم Nmap بفحص المضيف (host) لاكتشاف المنافذ المفتوحة مثل:
  + **21 (FTP)** – نقل ملفات بدون تشفير
  + **23 (Telnet)** – إدارة عن بعد بدون تشفير
  + **80 (HTTP)** – خدمة الويب
  + **25 (SMTP)** – البريد الإلكتروني
* يمكنه أيضًا تخمين نظام التشغيل (OS Fingerprinting) لتخصيص الهجوم لاحقًا.

##### طرق الحماية من Reconnaissance Attacks

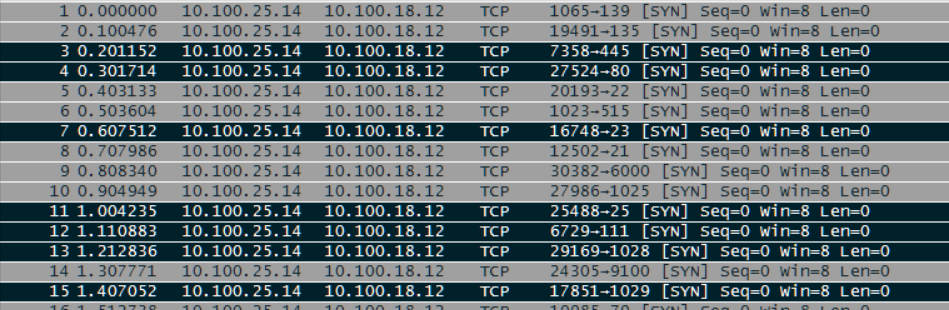
1. إغلاق **المنافذ غير الضرورية** وتعطيل البروتوكولات القديمة (مثل Telnet وFTP).
2. استخدام **SSH** بدل البروتوكولات غير الآمنة لإدارة الأجهزة.
3. **تشفير** الاتصالات لتقليل إمكانية التقاط الحزم (Sniffing).
4. **تغيير أسماء الأجهزة** إلى أسماء غير واضحة (Avoid “Server01”, “CoreSwitch”).
5. تفعيل **IDS/IPS** لاكتشاف عمليات المسح (Scanning).
6. استخدام **NAT** أو **PAT** لإخفاء البنية الداخلية للشبكة.
7. عزل المستخدمين في **Private VLANs** لمنع مسح داخلي بين الأجهزة.
8. تثقيف المستخدمين لتجنب تسريب كلمات المرور أو نشرها في أماكن عامة.

##### ملاحظات إضافية

* هجمات الاستطلاع **لا تُسبب ضررًا مباشرًا** لكنها تمهّد لهجمات أخطر.
* تستخدم أيضًا في **اختبارات الاختراق الأخلاقية** (Ethical Hacking) لجمع معلومات قبل تقييم الثغرات.
* **Nmap** هو الأداة الأساسية لكل من المختبرين الأخلاقيين والمهاجمين الحقيقيين.

| Shodan Search Engine: | Robots.txt File: |
| --- | --- |
|  |  |

Nmap Port Scan



### هجمات الوصول Access Attacks

هجمات الوصول (Access Attacks) تهدف إلى **الدخول غير المصرّح به** إلى حسابات المستخدمين أو أجهزة الشبكة أو الأنظمة بهدف **السيطرة عليها أو تعديل إعداداتها أو سرقة البيانات**.  
 تحدث عادة بسبب:

* **كلمات مرور ضعيفة** أو مكررة.
* **سوء ضبط إعدادات الأمان** من قبل المدراء.
* **خدمات أو أجهزة لا تتطلب مصادقة مناسبة.**

##### أنواع هجمات الوصول الأساسية

1. Password Attacks (هجمات كلمات المرور)
   * الهدف: كسر أو تخمين كلمات المرور للوصول إلى حسابات المستخدمين.
   * أدوات شائعة:
     + John the Ripper
     + Aircrack-ng (لشبكات الواي فاي)
     + Medusa, Hydra, RainbowCrack, Crunch
   * الأساليب:
     + *Brute Force* (تجربة جميع الاحتمالات).
     + *Dictionary Attack* (استخدام قوائم كلمات مرور شائعة).
     + *Password Recovery Exploits* (استغلال ضعف أنظمة استعادة كلمات المرور).
2. Spoofing / Masquerading (انتحال الهوية)
   * المهاجم يتظاهر بأنه مستخدم أو جهاز موثوق عبر تزييف عنوان IP أو البيانات التعريفية.
   * بعد الدخول، يمكنه:
     + تغيير إعدادات السيرفر أو الشبكة.
     + تحويل أو حذف البيانات.
   * مثال: المهاجم يرسل رزم IP بعنوان مصدر داخلي (Trusted IP) لخداع الجدار الناري.
3. Session Hijacking (اختطاف الجلسة)
   * المهاجم يراقب جلسة فعالة بين مستخدم وخادم، ثم يسيطر عليها ويتصرف كأنه المستخدم الشرعي.
   * يتم عادة عبر:
     + Eavesdropping (التنصت على الحزم).
     + Man-in-the-Middle Attack (MITM) حيث يعترض المهاجم الاتصال بين الطرفين.
4. Malware-Based Access (الوصول عبر البرمجيات الخبيثة)
   * استخدام برامج خبيثة (Trojan, Rootkit, Spyware) للحصول على صلاحيات أو مراقبة المستخدمين.
   * غالباً ما تُزرع في الشبكة وتبقى خاملة لبعض الوقت قبل تنفيذ نشاطها (مثل الـ Logic Bomb).

##### تطبيق عملي مهم – كسر كلمة المرور باستخدام John the Ripper

1. استخراج ملف كلمات المرور (hashed passwords).
2. تشغيل الأمر التالي:

john <password\_file>

1. الأداة تقوم بكسر التجزئة (hash) واسترجاع الكلمة الحقيقية (مثل password123).
2. النتيجة: حساب المستخدم تم اختراقه في ثوانٍ إن كانت الكلمة ضعيفة.

##### إجراءات الحماية من هجمات الوصول

1. **(استخدام ACLs (Access Control Lists** لحظر عناوين IP المزوّرة (مثلاً منع دخول IP داخلي من الإنترنت).
2. **تفعيل المصادقة متعددة العوامل (MFA)** مثل:
   * رمز مؤقت يُرسل عبر SMS.
   * مفتاح أمني (Key Fob) يولد كلمة مرور لمرة واحدة.
3. **استخدام بروتوكولات آمنة:**
   * WPA2 بدل WEP في الشبكات اللاسلكية.
   * SSH بدل Telnet.
4. **تفعيل أنظمة الكشف عن الاختراق (IDS/IPS)** لاكتشاف الهجمات أثناء تنفيذها.
5. **توليد كلمات مرور قوية** باستخدام مولدات كلمات مرور موثوقة.
6. **(تطبيق أنظمة AAA (Authentication, Authorization, Accounting** مثل **Cisco ISE** لتتبع وإدارة هويات المستخدمين وضمان أنهم يستخدمون برامج حماية محدثة.

* هجمات الوصول قد تكون **خارجية** (من الإنترنت) أو **داخلية** (من موظف أو جهاز داخل المؤسسة).
* بعض الهجمات لا تهدف إلى التدمير مباشرة، بل **إنشاء باب خلفي (Backdoor)** للبقاء داخل النظام لفترة طويلة.
* أدوات مثل **John the Ripper** و**Aircrack-ng** تُستخدم أيضًا في **اختبارات الاختراق الأخلاقية** (Pen Testing).

### هجمات الرجل الوسيط Man-In-The-Middle

هو نوع من الهجمات يتم فيه **التسلل بين طرفين يتواصلان** (مثل مستخدم وسيرفر) دون أن يعلم أيٌّ منهما أن هناك طرف ثالث يتجسس على الاتصال أو حتى يغيّر البيانات.

##### آلية عمل الهجوم (How it works)

1. **التجسس (Eavesdropping):** المهاجم يراقب الاتصال ويقرأ البيانات.
2. **التحكم (Manipulation):** المهاجم يمكنه تعديل الرسائل أو إدخال بيانات مزيفة.
3. **إعادة الإرسال (Replay):** أحياناً يعيد إرسال حزم قديمة لاستغلال جلسة معينة.

##### أنواع هجمات MITM حسب طبقات الـ OSI

| الطبقة | طريقة الهجوم | التوضيح |
| --- | --- | --- |
| Physical Layer | التنصت على الكابل مباشرة | مثل تركيب Tap على السلك لنسخ حركة المرور. |
| Data Link Layer | ARP Poisoning | المهاجم يخدع الأجهزة لتظن أن عنوان الـ MAC الخاص به هو عنوان الجهاز الآخر. |
| Network Layer | ICMP Redirect | يرسل رسائل مزيفة لتغيير مسار التوجيه وجعل البيانات تمر عبره. |
| Session Layer | SSL/TLS Hijacking | يفك تشفير الاتصال المشفر ويعيد تشفيره بشهادته الخاصة ليقرأ المحتوى. |
| Application Layer | Man-in-the-Browser | برمجية خبيثة داخل المتصفح تغيّر الصفحات أو تسجل كلمات المرور. |

##### أمثلة على أشكال الهجوم

1. ARP Poisoning

* المهاجم يرسل رسائل ARP مزيفة للأجهزة داخل الشبكة.
* يجعل الأجهزة ترسل بياناتها إليه بدلًا من الوجهة الحقيقية.
* يستخدم هذا النوع كثيرًا في الشبكات المحلية (LANs).

2. DNS Spoofing

* المهاجم يرسل ردود DNS مزيفة لجعل المستخدم يزور موقعًا مزورًا بدل الموقع الحقيقي (مثل بنك مزيف).

3. ICMP Redirect

* يخدع الراوتر ليحوّل مسار البيانات إليه.

4. DHCP Spoofing

* المهاجم يقلد سيرفر DHCP ويوزع عناوين IP مزيفة بحيث تمر كل البيانات عبره.

5. Man-in-the-Browser

* برمجية خبيثة (مثل Zeus) تصيب المتصفح وتغيّر صفحة البنك لتسرق بيانات الدخول.

##### أنواع MITM من حيث النشاط

| **النوع** | **الوصف** |
| --- | --- |
| **Passive (سلبي)** | المهاجم فقط يتنصت دون تعديل البيانات (للتجسس). |
| **Active (نشط)** | المهاجم يغيّر أو يضيف بيانات في الاتصال (مثل تزوير صفحة بنك). |

##### أدوات شائعة تُستخدم في الهجوم

* Bettercap
* dsniff
* Ettercap (كلها أدوات يمكنها التقاط أو تعديل الحزم وتستخدم في الاختبارات الأمنية أو الاختراق).

##### ضحايا محتملين

* المؤسسات المالية والبنوك.
* الأنظمة القديمة ذات البرامج الضعيفة.
* الشبكات العامة (Wi-Fi المفتوح).
* أجهزة إنترنت الأشياء (IoT) غير المؤمنة.

##### 

##### طرق الحماية من MITM

| **الإجراء** | **الهدف** |
| --- | --- |
| 🔒 استخدم HTTPS بدلاً من HTTP | تشفير الاتصال باستخدام SSL/TLS. |
| 🔑 استخدم VPN | تشفير كل حركة المرور بين الجهاز والسيرفر. |
| 🧾 استخدم شهادات رقمية (Digital Certificates) | لتأكيد هوية السيرفر. |
| 🧠 تفعيل DAI و DHCP Snooping و IP Spoofing Detection | حماية الشبكة من التزييف داخل الـ LAN. |
| 🔐 استخدم كلمات مرور قوية ومصادقة متعددة العوامل (MFA) | لتقليل فرصة سرقة الجلسة. |

### Denial of Service (DoS) و Distributed Denial of Service (DDoS)

هجمات DoS و DDoS تهدف إلى **استنزاف موارد النظام أو الشبكة** (مثل المعالج، الذاكرة، أو النطاق الترددي) حتى تصبح **الخدمات غير متاحة للمستخدمين الشرعيين**.

##### أنواع هجمات DoS الشائعة

1. **TCP SYN Flood**
   * يستغل ضعف تصميم الـTCP handshake (SYN, SYN-ACK, ACK).
   * المهاجم يرسل عددًا كبيرًا من طلبات SYN **بعناوين IP مزيفة**، مما يجبر الخادم على الانتظار لردّ لن يأتي، فيمتلئ جدول الاتصالات ويتوقف عن قبول اتصالات جديدة.
2. **Ping of Death (قديمة جدًا، لم تعد فعّالة اليوم)**
   * يقوم المهاجم بإرسال حزم ICMP مجزأة **بحجم يتجاوز 65,536 بايت** (أكبر من الحد المسموح).
   * الأنظمة القديمة كانت تنهار عند محاولة إعادة تجميعها.  
      ⚠️ *تمت حماية الأنظمة الحديثة ضد هذا النوع من الهجوم.*
3. **ICMP Flood و UDP Flood**
   * المهاجم يغرق الهدف بعدد كبير من **حزم ICMP أو UDP**.
   * النتيجة: استهلاك كبير للنطاق الترددي وموارد النظام، مما يؤدي إلى بطء أو توقف الشبكة.

##### DDoS (الهجمات الموزعة)

* نفس فكرة DoS، لكن من **عدة مصادر** (عادةً آلاف الأجهزة المصابة - botnet).
* يتم التحكم بهذه الأجهزة عن بعد عبر **(Command and Control (C2/CnC**.
* يصعب جدًا إيقافها لأنها تأتي من مصادر متعددة ومتفرقة.

##### آلية عمل الـ Botnet

1. **إصابة الأجهزة** ببرمجية خبيثة (bot) قادرة على الاتصال بالسيرفر المركزي (C2).
2. **يتصل كل جهاز مصاب** بالسيرفر وينتظر الأوامر.
3. عندما يطلق المهاجم الأمر، **تبدأ جميع الأجهزة بإرسال الهجوم في وقت واحد** نحو الهدف.
4. غالبًا يتم التحكم عبر **بروتوكولات مثل IRC، P2P، DNS، HTTP، أو HTTPS** (والأخير يخفي الاتصال بالتشفير TLS/SSL).

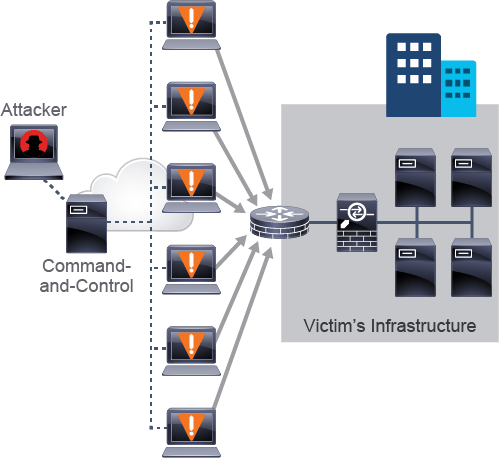
##### أمثلة واقعية على هجمات DDoS

* **Operation Ababil (2012):** هجوم DDoS ضد مؤسسات مالية أمريكية بدوافع سياسية.
* **DarkSeoul (2013):** هجوم على مؤسسات مالية وإعلامية في كوريا الجنوبية. استخدم **“wiper malware”** لتدمير البيانات وربما لإخفاء عمليات سرقة مالية.
* **Spamhaus Attack:** رداً على حظر “CyberBunker”، شنّ المهاجمون هجوم DDoS ضخم عطّل الإنترنت جزئياً حول العالم.
* **Imperva Attack (2019):** أحد أكبر الهجمات في التاريخ، استهدف خدمة بث عبر الإنترنت بـ 292,000 طلب في الثانية من أكثر من 400,000 عنوان IP.

##### اتجاهات حديثة

* المهاجمون يستغلون **خدمات الحوسبة السحابية (مثل Amazon)** لإطلاق هجمات ضخمة.
* بعض الهجمات تستخدم **DDoS كستار** لعمليات اختراق أو سرقة مالية.
* **الدمج بين DDoS وRansomware** أصبح أكثر شيوعاً: المهاجم يشلّ الخدمة ثم يطلب فدية.

##### نقاط مهمة للحماية والفهم

* لا يمكن **منع جميع هجمات DDoS** تماماً، لكن يمكن **التخفيف منها** عبر:
  + أنظمة كشف التطفل IDS/IPS
  + موازنات التحميل (Load Balancers)
  + جدران حماية ذكية (Next-Gen Firewalls)
  + مزودي حماية متخصصة (مثل Cloudflare, Akamai)

### Reflection and Amplification Attacks

هجمات **الانعكاس (Reflection)** و**التضخيم (Amplification)** هي نوع من **هجمات حجب الخدمة (DoS/DDoS)** التي تستغل بروتوكولات الشبكة لتوجيه كم هائل من البيانات إلى الضحية دون أن يتواصل المهاجم مباشرة معها.

##### Reflection Attack – هجوم الانعكاس

* المهاجم يرسل طلبات (packets) إلى **عدد كبير من الأجهزة (reflectors)**، مع **تزييف عنوان المصدر** ليكون عنوان الضحية.
* الأجهزة المستقبِلة ترد على الطلب — لكنها **ترسل الرد إلى الضحية** بدلاً من المهاجم.
* النتيجة: الضحية تُغرق بالردود من أجهزة متعددة.
* من الصعب جدًا **تتبع المهاجم الحقيقي** لأن العنوان الظاهر هو عنوان الضحية.

##### Amplification Attack – هجوم التضخيم

* يُستخدم عندما **يؤدي طلب صغير إلى رد كبير جدًا** من السيرفر.
* المهاجم يستغل هذه الخاصية ليُضاعف حجم الهجوم باستخدام موارد صغيرة جدًا.
* مثال: **DNS Amplification**
  + المهاجم يرسل **استعلام DNS صغير** إلى خادم DNS مفتوح (Open Resolver) بعنوان مصدر مزيف (الضحية).
  + الخادم يرد **برد كبير جدًا** إلى الضحية.
  + باستخدام آلاف الخوادم، يُمكن توليد **مئات الجيجابت من حركة البيانات** نحو الهدف.

##### Smurf Attack (قديم جدًا لكن مفيد للفهم)

* يعتمد على **ICMP Echo Request (ping)**.
* المهاجم يرسل طلب ping إلى **عنوان البث الموجّه (Directed Broadcast)** لشبكة، ويضع **عنوان الضحية كمصدر**.
* جميع الأجهزة في تلك الشبكة ترد على الضحية في الوقت نفسه.

تم القضاء على هذا النوع من الهجمات بعد أن أصبحت أجهزة Cisco (منذ الإصدار 12.0) تستخدم بشكل افتراضي الأمر:

no ip directed-broadcast

* الذي يمنع تمرير حزم البث الموجّه.

##### أمثلة حديثة على الهجمات

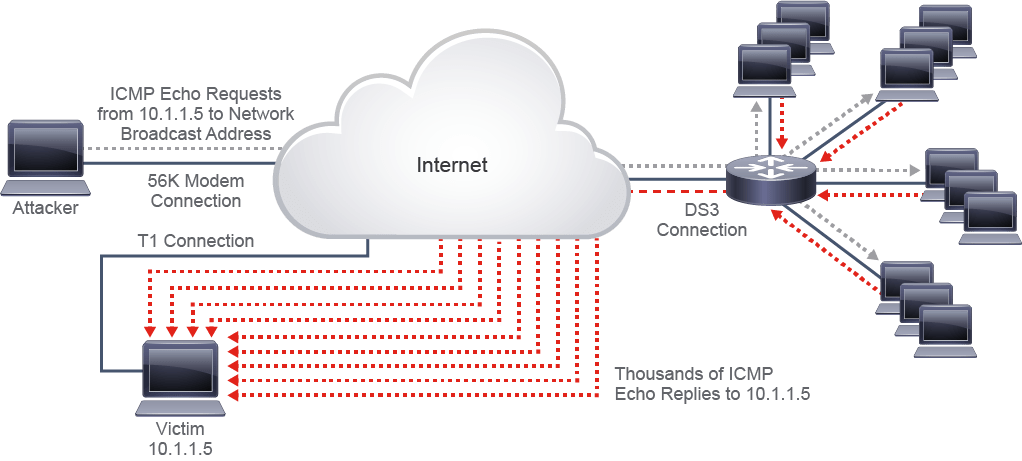
1. **DNS Amplification (2013):**
   * استخدم مهاجمون خوادم DNS مفتوحة لتوليد **300 Gbps** من حركة المرور الخبيثة، مما عطّل مواقع وأبطأ الإنترنت عالميًا.
   * تم تحديد أكثر من **28 مليون DNS Open Resolver** يمكن استغلالها في مثل هذه الهجمات.
2. **NTP Amplification (2014):**
   * استخدم المهاجمون أمر **monlist** في خوادم NTP، الذي يعيد قائمة بآخر 600 جهاز تفاعل معه الخادم.
   * النتيجة: **400 Gbps** من حركة البيانات نحو الضحية.

##### 

##### أسباب صعوبة تتبع الهجوم

* **تزييف عناوين IP** يخفي المهاجم الحقيقي.
* **توزع مصادر الردود** يجعل التتبع شبه مستحيل.

##### طرق الحماية

* إغلاق أو تقييد **الخوادم المفتوحة (Open Resolvers / NTP servers)**.
* تفعيل **rate limiting** للردود على الاستفسارات الكبيرة.
* حظر **directed broadcast** على أجهزة التوجيه.
* استخدام **firewalls وIDS/IPS** لتصفية الحزم المزيفة.

### هجمات الانتحال Spoofing Attacks

هجمات **الـSpoofing** هي محاولات **لانتحال هوية نظام أو مستخدم آخر** بهدف خداع الأنظمة أو المستخدمين الآخرين.  
 ببساطة: المهاجم يرسل **بيانات تبدو وكأنها قادمة من جهاز موثوق**، بينما هي فعليًا قادمة من مصدر آخر (المهاجم نفسه).

الـSpoofing ليست هجومًا بحد ذاتها، لكنها **أسلوب يُستخدم في أنواع مختلفة من الهجمات** (مثل DoS أو Man-in-the-Middle).

##### أنواع هجمات الـSpoofing

1. **IP Address Spoofing**
   * المهاجم يغيّر عنوان الـIP المصدر في الحزمة ليبدو كأنه من جهاز آخر.
   * الهدف عادة:
     + تجاوز فلاتر الحماية.
     + إخفاء هوية المهاجم.
     + استخدامه ضمن **هجمات DoS أو DDoS** (مثلاً بإرسال طلبات تبدو من الضحية نفسها).

**الحماية:**

* + استخدام **ACLs** (Access Control Lists) على مداخل الشبكة لمنع الحزم الواردة من عناوين IP داخلية أو محجوزة (RFC 1918).
  + فحص الحزم القادمة لضمان أن عناوينها منطقية بالنسبة لموقعها في الشبكة (**anti-spoofing filters**).

1. **MAC Address Spoofing**
   * المهاجم يبدّل عنوان MAC الخاص ببطاقة الشبكة الخاصة به ليصبح مثل جهاز آخر.
   * يُستغل هذا النوع غالبًا على **الشبكات المحلية (LAN)** لاستهداف **طبقة الربط (Layer 2)**.
   * الهدف: اعتراض البيانات، أو تجاوز أنظمة التحكم بالوصول المعتمدة على MAC.

**الحماية:**

* + استخدام **Port Security** على السويتشات.
  + تفعيل **Dynamic ARP Inspection (DAI)** للكشف عن العناوين المزيفة.

1. **ARP Spoofing / ARP Poisoning**
   * المهاجم يرسل ردود ARP مزيفة للأجهزة ليقنعها أن عنوان MAC الخاص به هو البوابة الافتراضية (gateway).
   * النتيجة: المهاجم يصبح **Man-in-the-Middle**، يستطيع اعتراض وتعديل الترافيك.

**أدوات المراقبة:**

* + Snort، ARPwatch، أو أي IDS/IPS.
  + **منع الهجوم:** باستخدام DAI أو تثبيت جداول ARP يدويًا للأجهزة الحساسة.

1. **DNS Spoofing**
   * يتم **تغيير سجلّات DNS** بحيث يتم توجيه المستخدمين إلى موقع مزيف بدل الموقع الحقيقي.
   * النتيجة: المستخدم يعتقد أنه على موقع موثوق، بينما هو على موقع المهاجم.

**الحماية:**

* + استخدام **DNSSEC** لتوقيع الردود رقمياً وضمان موثوقيتها.
  + مراقبة سجلات DNS الداخلية ومنع تعديلها غير المصرح به.

1. **DHCP Spoofing**
   * المهاجم ينشئ **خادم DHCP مزيف** يرد على الطلبات قبل الخادم الحقيقي.
   * النتيجة: المستخدم يحصل على إعدادات شبكة من المهاجم (gateway أو DNS مزيفين).
   * يمكن أيضًا أن يرسل المهاجم طلبات وهمية لخادم DHCP ليستهلك العناوين المتوفرة (**DHCP starvation**).

**الحماية:**

* + تفعيل **DHCP Snooping** على السويتشات.
  + تقييد المنافذ المسموح لها بالرد كـDHCP Server.

1. **Email Spoofing**
   * المهاجم يرسل بريدًا إلكترونيًا بعنوان "من" مزيف ليبدو وكأنه من شخص أو جهة موثوقة.
   * شائع جدًا في **هجمات التصيّد (Phishing)**.

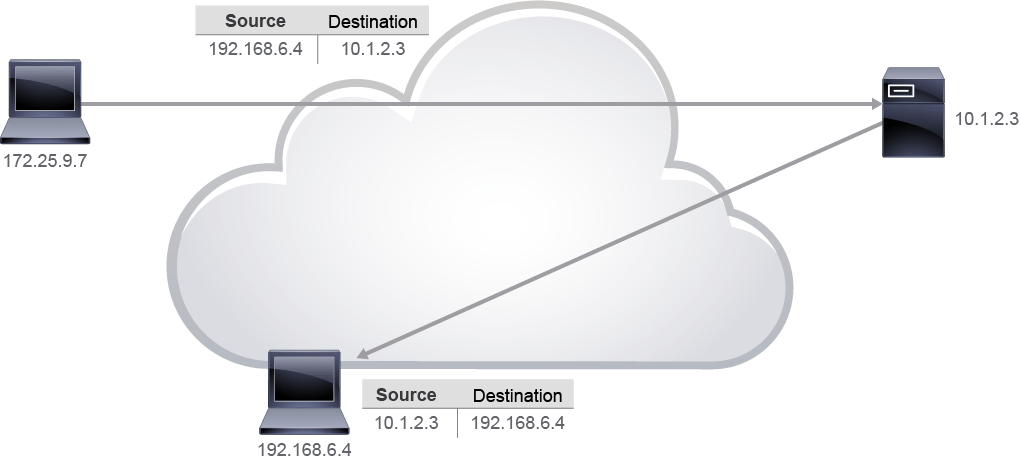
**الحماية:**

* + التحقق من رؤوس البريد (Email headers).
  + استخدام تقنيات **SPF**, **DKIM**, و **DMARC**.
  + عدم فتح الروابط أو المرفقات المجهولة.

1. **Land Attack (قديم وغير مستخدم حالياً)**
   * المهاجم يرسل حزمة TCP SYN تحتوي على **نفس عنوان IP والمنفذ كمصدر ووجهة**.
   * يؤدي إلى أن يستجيب النظام لنفسه مما قد يسبب تجمّده أو انهياره.
   * **تم تجاوزه بالكامل في الأنظمة الحديثة.**

##### أدوات واستخدامات عملية مهمة

* Snort و Cisco Firepower → للكشف عن الهجمات أثناء حدوثها.
* Dynamic ARP Inspection (DAI) → لمنع ARP spoofing.
* ACLs وBogon filtering → لمنع IP spoofing.
* DNSSEC وSPF/DKIM/DMARC → لحماية DNS والبريد الإلكتروني.



### هجمات DHCP

##### 1. DHCP Starvation Attack (هجوم استنزاف DHCP)

**الفكرة:** المهاجم يرسل عددًا ضخمًا من طلبات DHCP مزيفة باستخدام **عناوين MAC مختلفة** في كل طلب، مما يؤدي إلى استهلاك جميع العناوين في خادم DHCP.

* النتيجة: لا يتبقى أي عناوين للأجهزة الحقيقية، فتفشل في الحصول على IP.
* يمكن بعد ذلك أن ينشئ المهاجم **خادم DHCP مزيف (Rogue DHCP Server)** للتحكم في إعدادات الأجهزة.

**الهدف:** حرمان المستخدمين من الخدمة (DoS) وتهيئة البيئة لهجمات أخرى.

##### 2. DHCP Spoofing Attack (هجوم انتحال DHCP)

**الفكرة:** المهاجم يقوم بتشغيل **خادم DHCP مزيف** على الشبكة ويرد على طلبات الأجهزة أسرع من الخادم الحقيقي.

* النتيجة: يحصل الضحية على إعدادات IP من المهاجم بدلًا من الخادم الشرعي.
* يقوم المهاجم بتعيين نفسه كـ **gateway أو DNS**، مما يسمح له بالتجسس على حركة المرور (Man-in-the-Middle Attack).

##### طرق الحماية من هجمات DHCP

1. **DHCP Snooping**
   * ميزة في أجهزة Cisco تُفعّل على مستوى VLAN.
   * نحدد المنافذ الموثوقة (Trusted Ports) التي يُسمح بمرور رسائل DHCP منها فقط.
   * أي رد DHCP من منفذ غير موثوق يتم **حظره تلقائيًا**.
2. **Rate Limiting**
   * لتحديد عدد الطلبات المسموح بها من منفذ معين ومنع الاستنزاف (Starvation).
3. **IP Source Guard**
   * تعمل مع DHCP Snooping للتحقق من تطابق عنوان MAC مع عنوان IP المخصص من الخادم الشرعي.

##### 

##### التطبيق العملي المهم (من الدرس نفسه)

**تفعيل DHCP Snooping على Cisco Switch:**

Switch(config)# ip dhcp snooping

Switch(config)# ip dhcp snooping vlan 10

Switch(config)# interface GigabitEthernet0/1

Switch(config-if)# ip dhcp snooping trust

Switch(config-if)# exit

Switch(config)# interface range GigabitEthernet0/2 - 24

Switch(config-if-range)# ip dhcp snooping limit rate 10

* المنافذ الموثوقة (مثل المنفذ المتصل بالخادم) تُحدّد يدويًا.
* باقي المنافذ تعتبر **غير موثوقة (untrusted)** وتُمنع من تمرير ردود DHCP.