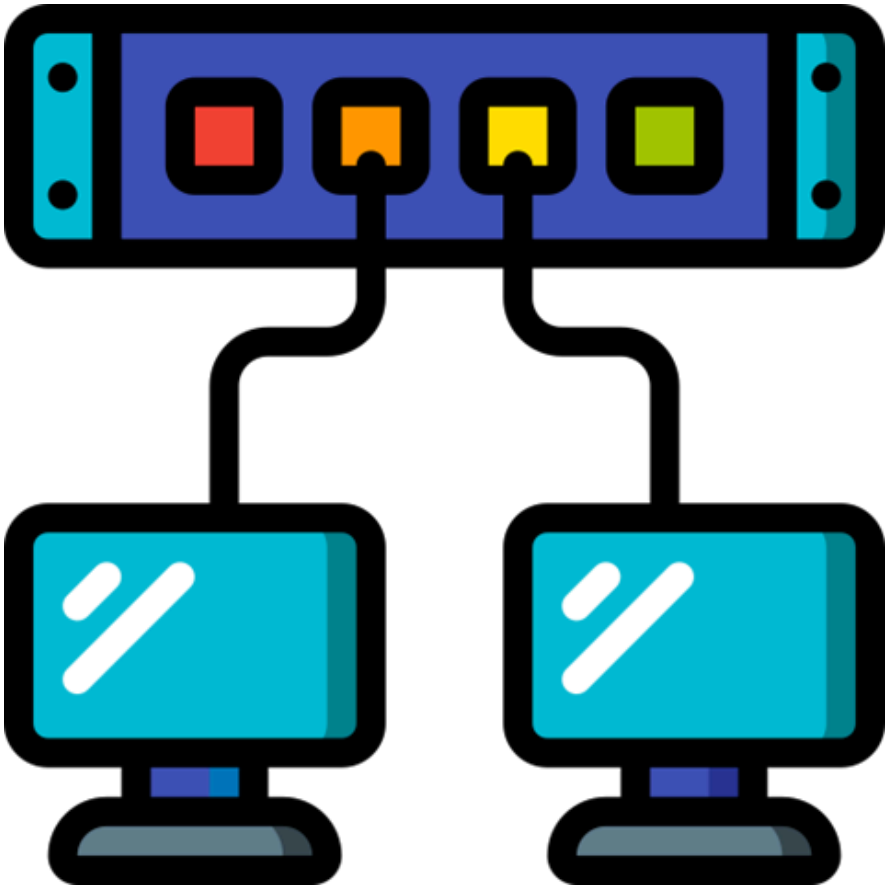
Networking Interview Q&A



By: Osman Alaa

linkedin

1. إيه الفرق بين Switch وRouter ؟

- **السويتش (Switch) :** بيشتغل في **طبقة الـData Link Layer (Layer 2)** ، وظيفته يربط الأجهزة في نفس الشبكة (LAN) وبيشتغل بالـ MAC Address .
- **الراوتر (Router) :** بيشتغل في **طبقة الـNetwork Layer (Layer 3)** ، ووظيفته يربط شبكات مختلفة ببعض (زي توصيل شبكة بيتك بالإنترنت)، وبيشتغل بالـIP Address .

2. إيه هو الـIP Address ؟ وإيه الفرق بين الـ Public و الـPrivate IP ؟

- **الـ IP Address** هو العنوان اللي الجهاز بياخده عشان يتعرف عليه في الشبكة.
- **Public IP :** بيكون عنوان عالمي يقدر أي حد من الإنترنت يوصل له.
- **Private IP :** بيستخدم داخل الشبكات المحلية (زي اللي في البيت أو الشركة) ومش بيظهر على الإنترنت مباشرة.

3. إيه الفرق بين TCP وUDP ؟

- **TCP (Transmission Control Protocol) :** بروتوكول موثوق، بيعمل **تأكيد للبيانات** اللي بتتبعت وبيضمن إنها توصل بترتيب صحيح، لكن بطيء شوية (زي لما تبعت ملف).
- **UDP (User Datagram Protocol) :** أسرع، لكنه مش بيعمل تأكيد استلام، ومفيد في التطبيقات اللي محتاجة سرعة زي الفيديو كول والألعاب الأونلاين.

4. إيه الفرق بين Hub وSwitch ؟

- **الـ Hub** بيبعت الداتا لكل الأجهزة المتوصلة بيه، بغض النظر عن الجهاز المقصود، فبيسبب **ازدحام(Collision) .**
- **الـ Switch** بيبعت الداتا للجهاز المطلوب بس، لأنه بيستخدم الـMAC Address ، فبيكون أسرع وأكفأ.

5. إيه الفرق بين IPv4 وIPv6 ؟

- **IPv4**بيستخدم عناوين من 32 بت (زي 192.168.1.1).
- **IPv6**بيستخدم عناوين من 128 بت، وده بيحل مشكلة نقص عناوين الـ IP فيIPv4 .

6. إيه هو الـDNS ؟

- الـ **DNS (Domain Name System)**هو اللي بيحول **أسماء المواقع زي(google.com)** لعناوين **IP** يقدر الكمبيوتر يتعامل معاها.

7. إيه هو الـDHCP ؟

- الـ **DHCP (Dynamic Host Configuration Protocol)**هو اللي بيوزع الـ IPs بشكل أوتوماتيكي على الأجهزة في الشبكة، بدل ما تعمله **Manual** لكل جهاز.

8. إيه الفرق بين Subnetting وSupernetting ؟

- **Subnetting** : تقسيم شبكة كبيرة لعدة شبكات أصغر.
- **Supernetting** : دمج عدة شبكات صغيرة في شبكة واحدة كبيرة.

9. إيه هو الـVLAN ؟

- **VLAN (Virtual Local Area Network)** بيستخدم في تقسيم شبكة واحدة لكذا شبكة افتراضية بدون ما تحتاج تفصلهم فعليًا بأسلاك، وده بيساعد في الأمان وتقليل الازدحام.

10. إزاي تعرف إذا كان جهازك متصل بشبكة الانترنت؟

- تقدر تستخدم **أمر Ping** في الـCommand Prompt:

ping 8.8.8.8

لو جالك رد، يبقى الإنترنت شغال، لو مفيش رد، يبقى فيه مشكلة في الاتصال.

11 .إيه الفرق بين OSI Model وTCP/IP Model ؟

- **OSI Model** : نموذج مكون من 7 طبقات بيشرح إزاي البيانات بتتنقل في الشبكة.
- **TCP/IP Model** : نموذج عملي مكون من 4 طبقات بيستخدم فعليًا في الشبكات (زي الإنترنت).

12 .إيه وظيفة كل طبقة في الـOSI Model ؟

1. **Physical Layer-** إرسال الإشارات عبر الكابلات.
2. **Data Link Layer-** تنظيم نقل البيانات باستخدام MAC Address.
3. **Network Layer-** تحديد مسار البيانات باستخدام IP Address.
4. **Transport Layer-** التأكد من توصيل البيانات(TCP/UDP).
5. **Session Layer-** إدارة الجلسات بين الأجهزة.
6. **Presentation Layer-** تحويل البيانات للصيغة المناسبة (مثلاً تشفير).
7. **Application Layer-** توفير الخدمات للمستخدم (زي HTTP, FTP).

13 .إيه الفرق بين STP وRSTP ؟

- **STP (Spanning Tree Protocol)**: بيمنع الحلقات (Loops) في الشبكة لكنه بطيء شوية.
- **RSTP (Rapid Spanning Tree Protocol)**: نسخة أسرع من STP وبيحسن وقت الاستجابة.

14 .إيه الفرق بين RIP و OSPF وEIGRP ؟

- **RIP (Routing Information Protocol)**: بسيط، بيستخدم عدد الـ Hops لتحديد الطريق، لكنه مش مناسب للشبكات الكبيرة.
- **OSPF (Open Shortest Path First)**: أسرع، بيستخدم الـ Cost بدل الـHops ، وبيناسب الشبكات الكبيرة.
- **EIGRP (Enhanced Interior Gateway Routing Protocol)**: خاص بسيسكو، سريع وذكي جدًا.

15 .إيه الفرق بين Static Routing وDynamic Routing ؟

- **Static Routing**: الراوتر بياخد الطريق يدويًا، مناسب للشبكات الصغيرة.
- **Dynamic Routing**: الراوتر بيكتشف الطرق تلقائيًا باستخدام بروتوكولات زيOSPF و EIGRP.

16 .إزاي تفرق بين Class A و B و C في الـIP ؟

- **Class A**: من 1.0.0.0 إلى 126.255.255.255 (للشبكات الكبيرة).
- **Class B**: من 128.0.0.0 إلى 191.255.255.255 (للشبكات المتوسطة).
- **Class C**: من 192.0.0.0 إلى 223.255.255.255 (للشبكات الصغيرة).

17 .إيه هو الـ NAT وليه بنستخدمه؟

- **NAT (Network Address Translation)** بيستخدم لتحويل **Private IPs** إلى **Public IPs** عشان الأجهزة في الشبكة الداخلية تقدر تتصل بالإنترنت.

✅لو المقابلة فيها عملي، ركز على أوامر CLI زي ping, tracert, show ip route, show running-config.

18 .إيه الفرق بين Half Duplex وFull Duplex ؟

- **Half Duplex**: البيانات بتتنقل في اتجاه واحد في كل مرة (زي Walkie-Talkie).
- **Full Duplex**: البيانات بتتنقل في الاتجاهين في نفس الوقت (زي المكالمات الهاتفية الحديثة).

19 .إيه الفرق بين Access Port و Trunk Port في السويتش؟

- **Access Port**: بيتصل بجهاز واحد وبيمرر بيانات VLAN واحدة بس.
- **Trunk Port**: بيعدي بيانات كذا VLAN باستخدام **Dot1Q** أو **ISL** (في سويتشات Cisco القديمة).

20 .إيه الفرق بين Standard و(Extended Access Control Lists (ACLs ؟

- **Standard ACL:** بيتحكم في الترافيك بناءً على **Source IP فقط**.
- **Extended ACL**: بيتحكم في الترافيك بناءً على **Source & Destination IP + Port + Protocol**.

◆ **مثال على Standard ACL :**

```
access-list 10 permit 192.168.1.0 0.0.0.255
ip access-group 10 in
```

◆ **مثال على Extended ACL :**

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 80
ip access-group 100 in
```

21 .إزاي تفرق بين أنواع الـ Cables في الشبكات؟

- **Straight-through Cable**: بيستخدم لتوصيل **جهاز بجهاز مختلف** (مثلاً PC بـ Switch).
- **Crossover Cable**: بيستخدم لتوصيل **جهازين متشابهين** (مثلاً PC بـ PC).
- **Rollover Cable**: بيستخدم لتوصيل **الجهاز بالـ Console Port في الراوتر أو السويتش**.

22 .إيه الفرق بين VLAN و Inter-VLAN Routing ؟

- **VLAN**: بتقسم الشبكة الواحدة إلى عدة شبكات افتراضية.
- **Inter-VLAN Routing**: بيسمح للأجهزة الموجودة في VLANs مختلفة إنها تتواصل مع بعض، وده بيتم بطريقتين:
  1. **Router-on-a-Stick**: استخدام راوتر بواجهة واحدة تعمل Trunk مع السويتش.
  2. **Layer 3 Switch**: بيقوم بوظيفة الراوتر باستخدام الـ SVI (Switched Virtual Interface).

23 .إيه وظيفة STP وليه بنستخدمه؟

- **STP (Spanning Tree Protocol)** بيمنع مشكلة **Loops** في الشبكات اللي فيها أكتر من طريق للـ Switches.
- أهم أوضاع (States) الـ STP:
  - **Blocking**: مش بيعدي أي ترافيك.
  - **Listening**: بيشوف الترافيك بس مش بيعديه.
  - **Learning**: بيبدأ يتعلم MAC Addresses.
  - **Forwarding**: بيعدي الترافيك فعليًا.

24 .إيه الفرق بين DHCP Relay و DHCP Snooping ؟

- **DHCP Relay**: لما يكون الـ DHCP Server مش في نفس الشبكة، الراوتر أو السويتش بيبعت الطلبات له.
- **DHCP Snooping**: ميزة أمان بتمنع الـ DHCP Spoofing Attacks عن طريق مراقبة الطلبات وتأكيدها.

25 .إيه الفرق بين Static Routing وDynamic Routing ؟

- **Static Routing:**
  - بيتم تحديد المسارات يدويًا عن طريق أمر**ip route.**
  - بيستخدم في الشبكات الصغيرة والبسيطة.
  - مفيش استهلاك لموارد الجهاز (CPU & Bandwidth).
- **Dynamic Routing**
  - المسارات بتتحدث تلقائيًا باستخدام بروتوكولات زي **RIP, OSPF, EIGRP, BGP**.
  - مناسب للشبكات الكبيرة والمتغيرة باستمرار.
  - بيستهلك بعض الموارد لأنه بيحتاج يرسل التحديثات بين الأجهزة.

26 .إيه وظيفة ARP في الشبكة؟

- **ARP (Address Resolution Protocol)** بيربط بين عنوان **IP Address** و **MAC Address** الأجهزة اللي متصلة في نفس الشبكة علشان الأجهزة تتواصل مع بعض .

27 .إزاي تخلي VLANs مختلفة تتواصل مع بعض؟

1. استخدم **Router on a Stick**

```
interface gigabitEthernet 0/1
no shutdown
interface gigabitEthernet 0/1.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0
```

2. أو استخدم **Layer 3 Switch**وعمل **SVI (Switched Virtual Interface)**

```
interface vlan 10
ip address 192.168.10.1 255.255.255.0
no shutdown
```

28 .إيه الفرق بين Port Security وDHCP Snooping ؟

- **Port Security**: بيمنع الأجهزة غير المصرح ليها من الاتصال بالسويتش.
- **DHCP Snooping**: بيمنع الهجمات اللي بتستخدم DHCP Server مزيف.

29 .إيه الفرق بين SNMP وSyslog ؟

- **SNMP (Simple Network Management Protocol)**: بيستخدم في **مراقبة الشبكة** وجمع بيانات عن الأجهزة.
- **Syslog**: بيستخدم في **تسجيل الأحداث** واللوجات المهمة اللي بتحصل في الشبكة.

30 .إيه الفرق بين Collision Domain وBroadcast Domain ؟

- **Collision Domain:**
  - أي مجموعة أجهزة ممكن يحصل بينها تصادم في البيانات.
  - كل بورت في السويتش بيكون Collision Domain مستقل.
  - في الهب(Hub) ، كل الأجهزة في نفس الـ Collision Domain.
- **Broadcast Domain:**
  - أي مجموعة أجهزة بتستقبل نفس رسالة الـBroadcast.
  - الراوتر بيكسر الـBroadcast Domain ، لكن السويتش مش بيكسره إلا باستخدام VLANs.

31 .إزاي تمنع الـ Broadcast Storm في الشبكة؟

1. **استخدام STP (Spanning Tree Protocol)** لمنع حلقات (Loops).
2. تقسيم الشبكة باستخدام VLANs.
3. تفعيل الـ Storm Control في السويتش.

32 .إيه الفرق بين Link Aggregation وEtherChannel ؟

- **Link Aggregation (LACP)**: بيجمع أكثر من بورت عشان يشتغلوا كأنهم واحد لزيادة السرعة والتكرار(Redundancy)).
- **EtherChannel**: هو اسم تقنية Link Aggregation في Cisco.

33 .إزاي تمنع أي حد إنه يعمل Telnet على الراوتر؟

- استخدام

```
line vty 0 4
transport input ssh
```

34 .إيه الفرق بين Trunk و Access Mode في السويتش؟

- Access Mode: بيربط الجهاز بـVLAN واحدة فقط.
- Trunk Mode: بيمرر بيانات أكتر من VLAN باستخدام Q802.1.

35 .إيه الفرق بين CDP و LLDP؟

- CDP: بيعرف معلومات عن الأجهزة المتصلة يعتبرCisco Proprietary.
- LLDP: نفس الفكرة لكنه معيار مفتوح Standard.

36 .إيه الفرق بين Unicast و Multicast وBroadcast ؟

- **Unicast**: إرسال البيانات لجهاز واحد بس.
- **Multicast**: إرسال البيانات لمجموعة أجهزة معينة (زي فيديو بث مباشر).
- **Broadcast**: إرسال البيانات لكل الأجهزة في الشبكة (زي DHCP Discover).

37 .إيه الفرق بين Public IP وPrivate IP ؟

- **Public IP**: عنوان عالمي يمكن الوصول إليه من الإنترنت، زي **8.8.8.8.**
- **Private IP**: يستخدم داخل الشبكة الداخلية، زي **192.168.1.1.**

38 .إيه الفرق بين LAN و WAN وMAN ؟

- **LAN (Local Area Network)**: شبكة محلية داخل شركة أو بيت.
- **WAN (Wide Area Network)**: شبكة تربط بين المدن أو الدول (زي الإنترنت).
- **MAN (Metropolitan Area Network)**: شبكة متوسطة تربط بين عدة مواقع في مدينة واحدة.

39 .إيه الفرق بين Subnet Mask وDefault Gateway ؟

- **Subnet Mask**: بيحدد عدد الأجهزة في الشبكة (زي 255.255.255.0).
- **Default Gateway**: هو الـ Router اللي بيوصل الشبكة بالإنترنت أو الشبكات الأخرى.

40 .إيه الفرق بين VLAN وSubnet ؟

- **VLAN**: تقسيم الشبكة على مستوى Layer 2 (السويتشات) بدون راوتر.
- **Subnet**: تقسيم الشبكة على مستوى Layer 3 (الراوترات) باستخدام IPs.

41 .إيه الفرق بين Half Duplex وFull Duplex ؟

- **Half Duplex**: الجهاز يرسل أو يستقبل، لكن مش في نفس الوقت.
- **Full Duplex**: الجهاز يرسل ويستقبل في نفس الوقت، زي الموبايلات الحديثة.

42 .إيه فائدة الـNAT ؟

- يسمح للأجهزة داخل الشبكة المحلية باستخدام عنوان IP واحد للدخول إلى الإنترنت و يحسن مستوى الأمان عن طريق إخفاء عناوين الأجهزة الداخلية ويقلل استهلاك عناوين **Public IP.**

43 .إيه الفرق بين STP وRSTP ؟

- **STP (Spanning Tree Protocol)**: يمنع حدوث Loops في الشبكة لكنه بطيء.
- **RSTP (Rapid STP)**: إصدار أسرع من STP وبيتعامل مع الفشل أسرع.

44 .إيه الفرق بين Packet وFrame ؟

- **Packet**: تعمل في Layer 3 وبتحمل عنوان IP.
- **Frame**: تعمل في Layer 2 وبتحمل عنوان MAC.

45 .إيه أهمية الـQoS ؟

- بتحسن جودة الخدمات زي الفيديو والمكالمات بتحدد الأولوية لحركة المرور المهمة بتقلل التأخير (Latency) في التطبيقات الحساسة.

46 .إزاي تكتشف إن فيه Loop في الشبكة؟

- ارتفاع استهلاك الـ **CPU** في السويتش تأخير كبير في استجابة الشبكة تكرار إرسال نفس البيانات في الشبكة بشكل غير طبيعي.

47 .إيه الفرق بين الـ Firewall و IDS وIPS ؟

- **Firewall**: يمنع الاتصالات غير المرغوبة بين الشبكات.
- **IDS (Intrusion Detection System)**: يراقب حركة المرور ويبلغ عن التهديدات.
- **IPS (Intrusion Prevention System)**: زي الـ IDS لكنه يمنع الهجمات بدلاً من مجرد الإبلاغ عنها.

48 .إيه الفرق بين الـ VPN وVLAN ؟

- **VPN (Virtual Private Network)**: بيعمل اتصال آمن بين شبكتين عبر الإنترنت.
- **VLAN (Virtual LAN)**: بيقسم الشبكة الداخلية إلى أجزاء مختلفة لتحسين الأمان والأداء.

48 .إيه الفرق بين الـ PoE والـ Ethernet العادي؟

- **PoE (Power over Ethernet)**: بينقل البيانات والكهرباء معًا في نفس الكابل.
- **Ethernetالعادي:** بينقل بيانات فقط، ولازم توصل الجهاز بالكهرباء بشكل منفصل.

49 .إيه وظيفة الـMAC Address ؟

- هو عنوان فريد لكل كارت شبكة بيحدد هوية الجهاز داخل الشبكة المحلية بيستخدمه السويتش عشان يوجّه البيانات للجهاز الصحيح.

50 .ليه نحتاج Subnetting في الشبكة؟

- لتقليل الزحام داخل الشبكة لتحسين الأمان والفصل بين الأقسام المختلفة لاستخدام عناوين IP بشكل أكثر كفاءة.

51 .إزاي الأجهزة بتتواصل في Layer 2 وLayer 3 ؟

- **Layer 2 (Data Link Layer)**: بتستخدم MAC Address عشان تنقل البيانات داخل الشبكة المحلية.
- **Layer 3 (Network Layer)**: بتستخدم IP Address عشان تنقل البيانات بين الشبكات المختلفة.

52 .إيه الفرق بين Collision Domain وBroadcast Domain ؟

- **Collision Domain**: المنطقة اللي ممكن يحصل فيها تصادم بيانات (في الـ Hubs والـ Switches القديمة).
- **Broadcast Domain**: المنطقة اللي بتستقبل فيها كل الأجهزة نفس الـ Broadcast Message.

53 .إيه الفرق بين TCP 3-Way Handshake وUDP ؟

- **TCP 3-Way Handshake:**

1. الجهاز الأول يرسل.SYN
2. الجهاز الثاني يرد بـ.SYN-ACK
3. الجهاز الأول يرسلACK ، ويتم الاتصال.

- **UDP**: بيبعت البيانات مباشرة بدون خطوات تأكيد.

54 .ليه بنستخدم الـMTU ؟

- **MTU (Maximum Transmission Unit)** بيحدد أكبر حجم للبيانات اللي ممكن تمر في الشبكة بدون تقسيم.
- لو الـ MTU كبير جدًا، ممكن يحصل **Fragmentation** وتبطأ الشبكة لو الـ MTU صغير، ممكن يزيد عدد الحزم وتقل الكفاءة.

55 .إيه هي مشكلة الـIP Conflict ؟

- بتحصل لما جهازين يكون عندهم نفس عنوان الـ IP في نفس الشبكة و بتسبب توقف الأجهزة عن العمل.

56 .إيه الفرق بين الـ Load Balancer والـFailover ؟

- **Load Balancer**: بيقسم الحمل بين سيرفرات متعددة لتحسين الأداء.
- **Failover:** بينقل الخدمة لسيرفر احتياطي لو الأساسي فشل.

57 .إيه الفرق بين الـ Hub و الـ Switch من حيث الأداء؟

- **Hub:**
  - كل الأجهزة في الشبكة بتسمع كل البيانات المرسلة و أبطأ بسبب التداخل والمشاركة بين الأجهزة.
- **Switch:**
  - يرسل البيانات للجهاز المقصود فقط عن طريقMAC Address و أسرع وأكثر كفاءة في نقل البيانات.

58 .إيه هي طريقة عمل الـNAT ؟

- **NAT (Network Address Translation):**
  - هو تقنية بتسمح لأجهزة الشبكة الداخلية باستخدام عنوان IP واحد للتواصل مع الإنترنت.
  - يقوم بترجمة العناوين الداخلية إلى عنوان Public عند الاتصال بالإنترنت بيحسن من الأمان عن طريق إخفاء العناوين الحقيقية للأجهزة.

59 .إيه هي تقنية الـ VLAN وكيفية عملها؟

- **VLAN (Virtual Local Area Network)**
  - بتقسم الشبكة الكبيرة إلى شبكات أصغر (مناطق منفصلة) بتحسن الأمان والأداء داخل الشبكة.
  - يمكن تخصيص الـ VLANs لأغراض مختلفة مثل فصل الموظفين عن الزوار أو فصل الأنظمة حسب النوع.

60 .إيه هو الـ Spanning Tree Protocol (STP) و ليه مهم؟

- **STP (Spanning Tree Protocol)**
  - هو بروتوكول بيحمي الشبكة من مشاكل الـ Loop الناتجة عن وجود أكثر من مسار بين الأجهزة.
  - بيمنع وقوف الشبكه أو تعطل الشبكة وتجنب التكرار في نقل البيانات. بسبب الـLoop .

61 .إيه هي مشكلة الـARP Spoofing ؟

- **ARP Spoofing:**
  - هو هجوم يستخدمه الهكر ليخدع الأجهزة في الشبكة عن طريق تغيير الـ ARP Table الخاص بها.
  - ممكن الهكر يعمل إعادة توجيه حركة الداتا أو سرقة البيانات عن طريق التلاعب بـMAC Address .
  - من الممكن الدفاع ضدها باستخدام **Static ARP Entries** أو **Dynamic ARP Inspection.**

62 .إيه الفرق بين الـ Access Control List (ACL) والـFirewall ؟

- **ACL (Access Control List):**
  - بتستخدم للتحكم في الوصول للبيانات داخل الشبكة عن طريق تحديد من يقدر يرسل أو يستقبل البيانات ممكن تحديدها على السويتشات أو الراوترات.
- **Firewall:**
  - جهاز يقوم بفحص وتصفية البيانات التي تدخل أو تخرج من الشبكة لحمايتها من التهديدات.

63 .إيه هو الـ VPN و إزاي بيشتغل؟

- **VPN (Virtual Private Network)**
  - هو شبكة خاصة تُستخدم لتوصيل أجهزة عبر الإنترنت بشكل آمن بيوفر تشفير البيانات وحمايتها من المتسللين على الإنترنت.
  - بيخفي عنوان الـ IP الحقيقي للمستخدم ويجعله يظهر وكأنه متصل من مكان مختلف.

64 .إيه هي أنواع الـVPN ؟

- **PPTP (Point-to-Point Tunneling Protocol):** أقدم أنواع الـ VPN وأبسطها، لكنه أقل أمانًا.
- **L2TP (Layer 2 Tunneling Protocol):** أكثر أمانًا منPPTP ، ولكن يحتاج إلى IPSec للتشفير.
- **IPSec (Internet Protocol Security):** يُستخدم لتوفير تشفير قوي في الشبكات الخاصة.
- **SSL (Secure Sockets Layer):** يُستخدم لتأمين الاتصال عبر الإنترنت، مثل فتح المواقع الآمنة (HTTPS).
- **OpenVPN:** أكثر أنواع الـ VPN أمانًا ومرونة، ويعمل على العديد من البروتوكولات.

65 .إيه هو الـ NAT و إزاي بيشتغل؟

- **NAT (Network Address Translation)**
  - هو عملية تحويل عنوان الـ IP الداخلي إلى عنوان خارجي (Public IP) بيحسن من الأمان عن طريق إخفاء العناوين الداخلية.
  - غالبًا بيتم استخدامه في الشبكات الخاصة، حيث تستخدم الأجهزة داخليًا عناوين IP خاصة، لكن عند الوصول إلى الإنترنت، بيتم ترجمة العنوان إلى Public IP.

67 .إيه هو الفرق بين الـ Static NAT و الـDynamic NAT ؟

- **Static NAT:** فيه ترجمة ثابتة بين عنوان IP داخلي وعنوان IP خارجي العنوان الداخلي يبقى دائمًا مرتبط بنفس العنوان الخارجي
- **Dynamic NAT:** يتم ترجمة العنوان الداخلي إلى عنوان خارجي من مجموعة عناوين مخصصة، العنوان يتغير بناءً على الطلب مش لازم كل جهاز يحصل على نفس العنوان الخارجي في كل مرة

68 .إيه هو الـ PAT و إزاي بيختلف عن الـNAT ؟

- **PAT (Port Address Translation)**
  - هو نوع خاص من الـ NAT بيترجم عناوين الـ IP مع إضافة رقم الـ Port لكل اتصال.
  - بيخلي أكتر من جهاز داخل الشبكة الخاصة يستخدم نفس الـPublic IP ، لكن باستخدام أرقام Ports مختلفة لتحديد كل اتصال ده بيحسن من استخدام العناوين العامة ويسمح بوجود عدد أكبر من الأجهزة المتصلة بالشبكة باستخدام نفس العنوان.

69 .إيه الفرق بين الـ VPN و الـNAT ؟

- **NAT** بيستخدم لترجمة عناوين الـ IP بين الشبكة الخاصة والعامة، وبالتالي يسمح لأجهزة داخل شبكة خاصة بالتواصل مع الإنترنت باستخدام عنوان IP واحد.
- **VPN** بيشفر البيانات ويؤمن الاتصال بين الشبكات عبر الإنترنت، مما يتيح للمستخدمين الاتصال بشبكة بعيدًا عن طريق الإنترنت بشكل آمن.
- **الفرق الأساسي** NAT **:**بيغير العناوين فقط، أما VPN بيشفر البيانات ويؤمن الاتصال بين الشبكات.

70 .إيه هو الـNAT Table ؟

- **NAT Table:** هو جدول يحتوي على عناوين الـ IP وترجمتها من داخلي إلى خارجي، بيتم تخزينه في جهاز التوجيه (Router) أو جدار الحماية (Firewall)اللي بيقوم بتنفيذ عملية الـNAT .

71 .إيه هي المشاكل اللي ممكن تحصل لو استخدمنا NAT في الشبكة؟

- **مشاكل مع التطبيقات التي تعتمد على الـIP** : بعض التطبيقات زي الألعاب أو VoIP ممكن تواجه مشاكل في NAT لأن البروتوكولات دي بتعتمد على معرفة (IP و Port).
- **مشكلة في تحديد الهوية:** لو أكتر من جهاز في الشبكة الداخلية استخدم نفس الـ Public IP مع PAT، ممكن يحصل تعارض في تحديد الهوية

72 .إيه هو مفهوم الـVPN Tunneling ؟

- **VPN Tunneling:**
  - هو إنشاء قناة مشفرة بين العميل والخادم أو بين شبكتين عبر الإنترنت بيتم إرسال البيانات عبر هذه القناة كـ "نفق" محمي، بحيث تكون البيانات محمية من المهاجمين خلال انتقالها عبر الإنترنت بيتم استخدام بروتوكولات زي PPTP، L2TP، أو IPSec لإنشاء الـ Tunneling.

73 .إيه الفرق بين NAT وPAT ؟

- **NAT:** هو تحويل عناوين الـ IP من داخل الشبكة إلى عناوين عامة عندما يتم إرسال البيانات إلى الإنترنت، وتتم الترجمة بين عنوان داخلي وعنوان خارجي ثابت.
- **PAT (Port Address Translation):** هو نوع من NAT، لكن بيضيف عنصر جديد وهو رقم الـ Port. بيتيح لكل الأجهزة استخدام نفس العنوان العام مع تخصيص رقم Port مختلف لكل اتصال، وبالتالي يمكن لأكثر من جهاز في الشبكة الداخلية أن يتشاركوا نفس الـ IP العام.

74 .إيه هو مفهوم أمن الشبكات؟

- **أمن الشبكات** هو حماية الشبكات والبنية التحتية للشبكة من الوصول غير المصرح به، التهديدات الإلكترونية، والهجمات. يشمل تأمين البيانات، والأجهزة، والخوادم، وأي نقطة وصول في الشبكة من المهاجمين الهدف الأساسي هو الحفاظ على سرية البيانات، الداتا تكون زي ما هي ومحدش لعب فيها، متاحه ع مدار الـ24 ساعه.

75 .إيه هي أنواع التهديدات الأمنية في الشبكات؟

- **التهديدات الداخلية(Internal Threats) :** تهديدات تأتي من داخل الشبكة نفسها، زي الموظفين أو المستخدمين الذين لديهم صلاحيات للوصول إلى الأنظمة
- **التهديدات الخارجية(External Threats) :** تهديدات تأتي من المهاجمين من خارج الشبكة، مثل القراصنة (Hackers) أو الهجمات الإلكترونية من جهات أخرى
- **البرمجيات الخبيثة(Malware) :** برامج خبيثة زي الفيروسات، الديدان، التروجان، التي تهدف إلى تدمير أو تسريب البيانات أو اختراق الأنظمة
- **الهجمات الموزعة(DDoS) :** هجمات حجب الخدمة الموزعة التي تهدف إلى تعطيل الشبكة أو الخوادم عن طريق إرسال كميات ضخمة من البيانات

76 .إيه هو الـ IDS و الـIPS ؟

- **IDS (Intrusion Detection System):** هو نظام للكشف عن التسللات أو الهجمات داخل الشبكة. بيقوم بتحليل حركة البيانات ويقوم بتحذير المسؤولين عند اكتشاف أنماط مشبوهة أو محاولات اختراق
- **IPS (Intrusion Prevention System):** هو نظام يشبه الـ IDS ولكن بالإضافة إلى الكشف، يقوم بإيقاف الهجوم أو التسلل قبل أن يحدث ضرر

77 .إيه هي تقنيات التشفير المستخدمة في أمن الشبكات؟

- **التشفير(Encryption) :** هو عملية تحويل البيانات إلى شكل غير قابل للقراءة إلا إذا تم فك تشفيرها باستخدام مفتاح صحيح
- **تقنيات التشفير الشائعة:**
  - **AES (Advanced Encryption Standard):** من أقوى تقنيات التشفير التي تستخدم في الشبكات لضمان سرية البيانات
    - **RSA (Rivest-Shamir-Adleman):** يستخدم في تأمين المفاتيح عبر الإنترنت (مثل SSL/TLS).
  - **TLS/SSL (Transport Layer Security / Secure Sockets Layer):** بيستخدم لتأمين نقل البيانات عبر الإنترنت بين العميل والخادم

78 .إيه هي أنواع الـ VPN من حيث الأمان؟

- **Site-to-Site VPN:** يتم استخدامه للاتصال بين شبكتين مختلفتين على الإنترنت بشكل آمن
- **Remote Access VPN:** يُستخدم من قبل الأفراد للوصول إلى الشبكة من أماكن مختلفة باستخدام اتصال آمن عبر الإنترنت

79 .إيه هي أهمية الـ Access Control في الشبكات؟

- **(Access Control) :** هو عملية تحديد من يمكنه الوصول إلى الشبكة أو موارد معينة وكيفية الوصول إليها
  - بيشمل تحديد السياسات مثل:
    - **التحقق من الهوية(Authentication) :** التأكد من هوية المستخدم.
    - **(Authorization):** تحديد الصلاحيات الممنوحة للمستخدم.
    - **(Accounting) :** تتبع الأنشطة والإجراءات التي تمت على الشبكة.

80 .إيه هو مفهوم الـZero Trust Security ؟

- **Zero Trust Security:** هو نموذج أمني يعتمد على مبدأ أن لا أحد داخل الشبكة موثوق به بشكل كامل ويجب على كل المستخدمين والأجهزة التحقق من هويتهم وصلاحياتهم، حتى لو كانوا داخل الشبكة

81 .إيه هي الـ VPN وازاي بتساهم في حماية الشبكة؟

- **VPN (Virtual Private Network):** بيعمل على تشفير الاتصال بين العميل والخادم، مما يحمي البيانات من المهاجمين على الإنترنت بيسمح للمستخدمين بالاتصال بشبكة العمل من أي مكان بشكل آمن

82 .إيه هو الـ Social Engineering في أمن الشبكات؟

- **Social Engineering:** هو نوع من الهجمات اللي بتعتمد على خداع الأفراد للحصول على معلومات سرية مثل كلمات المرور أو بيانات الحسابات تقنيات مثل **Phishing**أو **Vishing**(الهجمات عبر الهاتف) هي أمثلة شائعة على الهجمات باستخدام الـ Social Engineering.

83 .إيه هي الـ Network Segmentation وليه مهمة في الأمان؟

- **Network Segmentation:** هو تقسيم الشبكة إلى أجزاء أصغر لتقليل المساحة التي يمكن أن يتحرك فيها الهكر ده بيزيد من الأمان لأنه بيقلل الوصول غير المصرح به ويسمح بإجراءات أمان أكثر مرونة على كل جزء من الشبكة

84 .إيه هو الـ SIEM وازاي بيساعد في أمن الشبكات؟

- **SIEM (Security Information and Event Management):** هو نظام بيجمع ويحلل البيانات الخاصة بالأمن من مختلف مصادر الشبكة بيساعد في كشف الهجمات الأمنية في الوقت الحقيقي عن طريق تحليل الأنماط الغير طبيعية في الأنشطة على الشبكة.

85 .إيه هو مفهوم الـ Honeypot في أمن الشبكات؟

- **Honeypot:** هو نظام أمني مصمم لجذب المهاجمين من خلال محاكاة شبكة أو خدمة ضعيفة الهدف هو مراقبة وتحليل أساليب الهجوم الخاصة بهم، وبالتالي تحسين دفاعات الشبكة

86 .إيه هي أهمية الـ Encryption في حماية الشبكات؟

- **التشفير(Encryption) :** مهم جدًا لحماية البيانات أثناء انتقالها عبر الشبكة. بيحول البيانات من شكل قابل للقراءة إلى شكل غير قابل للقراءة إلا إذا تم فك تشفيرها باستخدام مفتاح التشفير المناسب حماية البيانات دي بتكون ضرورية خاصةً في الشبكات العامة زي الإنترنت أو الشبكات اللاسلكية

87 .إيه هو الـ DNS Spoofing أوDNS Poisoning ؟

- **DNS Spoofing / DNS Poisoning:** هو هجوم بيقوم بتغيير أو تزوير سجلات الـ DNS في جهاز كمبيوتر أو سيرفر بحيث يتم توجيه المستخدم إلى موقع مزيف بدلاً من الموقع الصحيح الهدف منه غالبًا هو سرقة البيانات أو نشر البرمجيات الخبيثة

88 .إيه هو الـMan-in-the-Middle Attack (MITM) ؟

- **MITM Attack:** هو هجوم بيقوم فيه الهكر بالاستماع أو التلاعب بالبيانات بين طرفين في اتصال آمن، بدون ما يعرفوا أن البيانات بتتسرب ممكن يستغل الهكر ضعف في التشفير أو الـ Authentication ليقدر يعترض البيانات

89 .إزاي نقدر نمنع هجماتMan-in-the-Middle ؟

- **استخدام التشفير القوي:** زي **SSL/TLS**، بيشفر البيانات بين العميل والخادم بحيث لو تم اعتراض البيانات، تكون غير قابلة للقراءة
- **التوثيق الثنائي(Two-Factor Authentication) :** بيضيف طبقة أمان إضافية عن طريق التحقق من هوية المستخدم باستخدام وسيلتين مختلفتين (مثل كلمة مرور وكود إرسال عبر الهاتف)
- **تحقق من الشهادات:** تأكد من صحة الشهادات في الاتصال، خاصة في حالات HTTPS أوVPN .

90 .إيه هو الـARP Spoofing ؟

- **ARP Spoofingأو (ARP Poisoning):** هو هجوم بيقوم فيه الهكر بتزوير بيانات (ARP (Address Resolution Protocol في الشبكة، بيخليه يوجه بيانات الشبكة إلى جهازه بدلاً من الجهاز الصحيح ده بيتيح للمهاجم تنفيذ هجمات **MITM** أو سرقة البيانات.

91 .إيه هو الـRansomware ؟

- **Ransomware:** هو نوع من البرمجيات الخبيثة (Malware) بيقوم بتشفير ملفات جهاز الكمبيوتر أو الشبكة، وبيطلب من الضحية دفع فدية لفك تشفير الملفات

92 .إيه هو الـSecurity Auditing ؟

- **Security Auditing:** هو عملية فحص وتقييم الأنظمة والشبكات للتأكد من أن السياسات الأمنية مفعلة بشكل صحيح وأن الشبكة محمية من الهجمات يشمل مراجعة سجلات الدخول، وفحص إعدادات الأمان، وتقييم فعالية أدوات الأمان.

93 .إيه هو الـSecurity Patch ؟

- **Security Patch:** هو تحديث بيتم إصدارها من قبل الشركة المنتجة للبرنامج أو النظام لمعالجة ثغرات أمنية أو أخطاء اكتُشِفت في الإصدار السابق
- **أهمية تطبيق الـ Patches بشكل مستمر:** لضمان أن الأنظمة والخوادم محمية ضد الهجمات التي قد تستغل الثغرات القديمة

بخصوص **الاختراقات اللي بتحصل على كل Layer في نموذج OSI** ده هيكون مفيد علشان تعرف أنواع الهجمات اللي ممكن تحصل على كل طبقة من طبقات الشبكة.

1. **Physical Layer (الطبقة الفيزيائية):** الطبقة دي مسؤولة عن إرسال البيانات عبر الوسائط المادية (كابلات، إشارات راديوية، إلخ).

الهجمات المحتملة:

- **Interception (التقاط الإشارة):** مهاجم يقدر يلتقط الإشارات المرسلة عبر الشبكة مثل الأسلاك أو الشبكات اللاسلكية ويقوم بتحليلها أو سرقتها
- **Physical Tapping(التنصت على الأسلاك):** هجوم بيتم من خلال توصيل جهاز خاص لالتقاط البيانات بين الأجهزة على الأسلاك، زي ما بيحصل في الشبكات السلكية
- **Jamming(التشويش):** في الشبكات اللاسلكية، بيحاول المهاجمين إرسال إشارات تداخل أو تشويش على ترددات الشبكة عشان يعطلوا الاتصال

2. **Data Link Layer:** الطبقة دي مسؤولة عن تأمين الاتصال بين الأجهزة عبر الوسائط المادية، وتشمل MAC addresses.

الهجمات المحتملة:

- **MAC Spoofing:** الهكر بيغير عنوان الـ MAC الخاص بالجهاز عشان يظهر كأنه جهاز آخر موثوق فيه
- **ARP Spoofing/Poisoning:** الهجوم ده بيقوم الهكر فيه بتزوير رسائل ARP عشان يربط عنوان IP بعنوان MAC خاطئ، وبالتالي بيقدر يوجه بيانات غير مصرح بها إلى جهازه (يمكن أن يؤدي إلى هجمات Man-in-the-Middle).
- **Frame Injection:** الهكر بيدخل "إطارات" بيانات غير صحيحة أو مزورة داخل الشبكة لتسبب مشاكل مثل تعطيل الاتصال.

3. **Network Layer:** الطبقة دي مسؤولة عن (routing) وتوجيه البيانات بين الأجهزة عبر الشبكة باستخدام بروتوكولات زيIP .

الهجمات المحتملة:

- **IP Spoofing:** الهكر بيغير عنوان الـ IP الخاص به عشان يظهر كأن البيانات جاية من مصدر موثوق فيه
- **Routing Table Poisoning:** الهجوم ده بيشمل تزوير بيانات الروتنج على أجهزة (Routers)، مما يؤدي إلى توجيه البيانات إلى جهاز الهكر
- **Ping of Death:** الهجوم ده بيستخدم رسائل "Ping" كبيرة جدًا أو غير صالحة عشان يؤدي إلى تعطيل الأجهزة المستهدفة أو تعطل الشبكة
- **Denial of Service (DoS):** الهجوم ده بيحاول يمنع الوصول إلى الشبكة أو الجهاز عن طريق إرسال عدد كبير جدًا من البيانات التي تثقل النظام

4. **Transport Layer:** الطبقة دي مسؤولة عن ضمان نقل البيانات بشكل موثوق بين الأجهزة باستخدام بروتوكولات زي TCP وUDP.

الهجمات المحتملة:

- **TCP SYN Flood:** الهجوم ده بيحاول إغراق السيرفر بعدد هائل من طلبات الاتصال(SYN packets) ، مما يجعل السيرفر غير قادر على التعامل مع أي طلبات أخرى
- **Session Hijacking:** الهكر بيستولي على جلسة (session) نشطة بين جهازين بعد أن تم المصادقة عليها، وبالتالي يستطيع التحكم في الجلسة
- **Port Scanning:** الهكر بيقوم بمسح لجميع المنافذ المفتوحة على الجهاز أو الشبكة للكشف عن الخدمات المستضيفة في كل منفذ، ومن ثم يستغل الثغرات

5. **Session Layer:** الطبقة دي مسؤولة عن إدارة الجلسات بين التطبيقات.

الهجمات المحتملة:

- **Session Fixation:** في الهجوم ده، الهكر يثبت أو يحدد معرف الجلسة (Session ID) لمستخدم آخر، وبعدها يقوم بالتحكم في الجلسة أثناء التفاعل مع التطبيق
- **Session Hijacking:** الهكر يستغل الجلسة المفتوحة بين مستخدم والتطبيق ويسحب بيانات حساسة أو يقوم بالتحكم في الجلسة

6. **Presentation Layer:** الطبقة دي مسؤولة عن تنسيق البيانات، مثل التشفير أو ضغط البيانات.

الهجمات المحتملة:

- **Data Interception(اعتراض البيانات):** المهاجمين ممكن يلتقطوا البيانات اللي بتنتقل بين الطبقات، خاصةً لو كانت البيانات غير مشفرة
- **Cryptanalysis:** المهاجمين بيقوموا بتحليل تقنيات التشفير بهدف اكتشاف مفتاح التشفير أو فك التشفير.

7. Application Layer: الطبقة دي هي اللي بيتعامل معها المستخدم بشكل مباشر وتشمل البروتوكولات زيHTTP ، FTP، SMTP، DNS، وغيرها.

الهجمات المحتملة:

- **Cross-Site Scripting (XSS):** في الهجوم ده، الهكر بيحقن جافا سكربت ضار في صفحات الويب عشان يستولي على بيانات المستخدم أو ينفذ عمليات ضارة
- **SQL Injection:** الهجوم ده بيقوم الهكر بإدخال استعلامات SQL ضارة في حقول الإدخال عشان يحصل على معلومات من قاعدة البيانات أو يعدل فيها
- **Phishing:** الهكر بيخدع المستخدمين ليقدموا معلوماتهم الشخصية أو تفاصيل حساباتهم عبر مواقع مزيفة أو رسائل بريد إلكتروني
- **Buffer Overflow:** الهجوم ده بيقوم بإدخال بيانات أكثر من سعة الذاكرة المخصصة(Buffer) ، مما يتيح للمهاجم التلاعب في البيانات وتشغيل كود ضار
- **DNS Spoofing:** الهجوم ده بيقوم بتزوير استجابة DNS ويقوم بتوجيه المستخدمين إلى مواقع ضارة أو مزيفة

طرق الحماية من الهجمات اللي ذكرناها في كل طبقة من طبقات **نموذج OSI** دي بعض الطرق اللي تقدر تحمي بيها الشبكة من الاختراقات:

1. Physical Layer

الهجمات:
Interception (التقاط الإشارة)
Physical Tapping (التنصت على الأسلاك)
Jamming (التشويش)
طرق الحماية:

- **تأمين الأجهزة الفيزيائية:** تأكد من أن الأجهزة (زي الراوترات والسويتشات) في مكان آمن، بعيد عن الوصول غير المصرح به
- **استخدام الكابلات المزدوجة(Shielded Cables) :** لتقليل التداخل والتشويش، استخدم كابلات محمية (مثل الكابلات المحورية)
- **التحقق من الأجهزة الموصلة بالشبكة:** تأكد من الأجهزة المتصلة بالشبكة باستخدام أدوات للمراقبة
- **استخدام تقنيات تشويش مقاومة:** في الشبكات اللاسلكية، استخدم تقنيات مقاومة للتشويش مثل استخدام ترددات غير مشهورة

2. Data Link Layer

الهجمات:
MAC Spoofing
ARP Spoofing/Poisoning
Frame Injection
طرق الحماية:

- **Static MAC Addresses:** تعيين عناوين MAC ثابتة على الأجهزة لحماية الشبكة من محاولات التلاعب
- **استخدام بروتوكولات الأمان:** مثل **802.1X**للتحقق من الهوية قبل السماح للـ MAC بالاتصال بالشبكة
- **استخدام أدوات للكشف عنARP Spoofing : مثل XArp أو ARPWatch للكشف عن محاولات ARP Spoofing.**
- **استخدام جدران حماية خاصة بالشبكة(Firewalls) :** لتعقب الإطارات الغير صالحة ومنع دخول البيانات المزورة

3. Network Layer

الهجمات:
IP Spoofing
Routing Table Poisoning
Ping of Death
Denial of Service (DoS)
طرق الحماية:

- **استخدام جدران الحماية(Firewalls) :** تأكد من أن الجدار الناري قادر على تصفية الـ IPs المشبوهة ومنع الدخول غير المصرح به

- **استخدام(VPN (Virtual Private Network :** تفعيل الـ VPN لتأمين الاتصال بين الشبكات أو بين المستخدمين والأجهزة
- **تطبيق إجراءات الـ(ACLs (Access Control Lists :** تحديد قواعد الوصول إلى الشبكة مثل تحديد من يمكنه إرسال واستقبال الحزم
- **مراقبة الشبكة:** استخدام أنظمة (Intrusion Detection/Prevention Systems) **IDS/IPS**لمراقبة الهجمات في الوقت الفعلي

4. Transport Layer

الهجمات:
TCP SYN Flood, Session Hijacking, Port Scanning
طرق الحماية:

- **استخدام تقنيات التحكم في التدفق(Flow Control) :** تأكد من أن البروتوكولات مثل TCP تُستخدم بشكل آمن عبر تقنيات مثل SYN Cookies.
- **استخدام الجدران النارية المتقدمة(Advanced Firewalls) :** لتصفية الحزم المُرسلة عبر الشبكة ومنع الهجمات مثل Port Scanning.
- **تشغيل التوثيق الثنائي(Two-Factor Authentication - 2FA) :** استخدام التوثيق الثنائي لحماية الجلسات ومنع سرقتها
- **استخدام بروتوكولات آمنة مثلTLS/SSL :** لتأمين الجلسات من الـ hijacking ومنع المهاجمين من اختراق الاتصال

5. Session Layer

الهجمات:
Session Fixation, Session Hijacking
طرق الحماية:

- **استخدام مفاتيح جلسات غير ثابتة(Dynamic Session Keys) :** تأكد من أن كل جلسة تستخدم مفتاح خاص بها لضمان عدم تثبيت الجلسات
- **تفعيل التوثيق الثنائي(2FA) :** زيادة الأمان على مستوى الجلسات عن طريق إضافة طبقة حماية إضافية
- **إغلاق الجلسات القديمة:** تأكد من أن الجلسات القديمة تُغلق تلقائيًا بعد فترة من عدم النشاط.

6. Presentation Layer

الهجمات:
Data Interception (اعتراض البيانات), Cryptanalysis
طرق الحماية:

- **استخدام تشفير قوي(Strong Encryption) :** استخدام بروتوكولات تشفير مثل **AES**و **RSA**لتأمين البيانات المتنقلة عبر الشبكة
- **إدارة المفاتيح بشكل آمن:** تأكد من استخدام أنظمة لإدارة المفاتيح وضمان أن المفاتيح مش مشهورة أو معرضة للسرقة
- **تطبيقSSL/TLS :** تأكد من أن جميع البيانات الحساسة مثل كلمات المرور والمعاملات المالية مشفرة باستخدام SSL/TLS.

7. Application Layer

الهجمات:
Cross-Site Scripting (XSS), SQL Injection, Phishing, Buffer Overflow, DNS Spoofing
طرق الحماية:

- **تحقق من المدخلات(Input Validation) :** تأكد من فحص جميع المدخلات القادمة من المستخدمين لمنع SQL Injection أو XSS.
- **استخدامPrepared Statements :** استخدم استعلامات Prepared Statements في قواعد البيانات لتجنب SQL Injection.
- **استخدام فلاتر البريد الإلكتروني:** لمنع **Phishing**، استخدم فلاتر قوية للبريد الإلكتروني للكشف عن الرسائل المشبوهة
- **مراقبة الأخطاء:** تأكد من أن التطبيق لا يعرض تفاصيل الأخطاء لمهاجمين محتملين، حيث يمكن أن يستفيدوا منها
- **تقنيات الحماية من الـBuffer Overflow :** استخدم تقنيات مثل Canaries و Stack Cookies لوقف Buffer Overflow.
- **استخدامDNSSEC :** لتأمين استعلامات DNS ومنع DNS Spoofing.

لا تنسونا من صالح دعائكم