CHAPTER 15

System Security

(58 Questions)

01: When we can say that the system is secure?

02: What is the difference between ***Threat and Attack***?

03: Which one is easier to protect, ***Accidental or malicious***?

04: What are the ***Security Violation Categories***?

05: What are the ***methods of standard Security Attacks***?

06: Is it possible to have absolute security?

07: What are the ***four levels of security measures*** that are necessary for system protection?

08: What are the common methods by which programs cause security breaches (***Programs Threats***)?

09: What are ***Trojan horse*** properties?

10: What are ***Trap Doo***r properties?

11: What is a ***Logic Bomb***?

12: What are ***Stack and Buffer Overflow*** properties?

13: What are ***Viruses*** properties?

14: What is ***Virus Dropper***?

15: What are the ***types of Viruses***?

16: How ***Keystroke logger*** is work?

17: Why is Windows the target for most attacks?

18: Are ***Network threats*** harder to detect and prevent? Why?

19: What are the ***types of System and Network Threats***?

20: What is a ***Worm***?

21: How ***Internet Worm*** is work?

22: What is ***Port Scanning*** and how is it typically launched?

23: What are ***Port Scanning properties***?

24: What are ***Denial of Service Properties***?

25: Where ***broadcast security tool*** available?

26: Can we trust ***the source and destination*** of messages on network without cryptography?

27: What does ***Cryptography*** mean?

28: What are ***the uses of Encryption***?

29: What are the ***components that an encryption algorithm consist of***?

30: What is the ***difference between Symmetric and Asymmetric encryption***?

31: What is the ***difference between Public and Private Key***?

32: What is ***based on Symmetric and Asymmetric Cryptography***?

33: What is the ***difference between Encryption and Authentication***?

34: What are the ***features of authentication***?

35: How many ***types of Authentication Algorithm***?

36: Why ***Authentication if a subset of encryption***?

37: What is ***Key Distribution***?

38: What are ***Digital Certificates***?

39: What is ***SSL***?

40: What ***SSL used for***?

41: What ***Asymmetric cryptography used to***?

42: What is a ***User authentication***?

43: How ***establishes User identity***?

44: How to ***keep passwords as a secret***?

45: Does encrypting passwords solve the exposure problem?

46: What is ***Passwords***? ***What its features***?

47: What is ***One-time passwords***?

48: What is ***Biometric***?

49: What is ***Multi-factor authentication***?

50: What is ***Defense in Depth***?

51: What is ***Security Policy doing***?

52: What is ***Vulnerability Assessment***?

53: What is ***Intrusion detection endeavors***?

54: What is a ***Network Firewall***?

55: What is ***the difference between Tunneled and spoofed***?

56: What is ***a Personal Firewall***?

57: What is ***an Application Proxy Firewall***?

58: What is ***a System-call Firewall***?

End of Questions.

Chapter 15

System Secure

1: نستطيع أن نقول بأن النظام آمن إذا كانت مصادره مستخدمه ويمكن الوصول إليها كما هو معد تحت جميع الظروف.

2: **الفرق بين Threat and Attack:**

- **التهديد (Threat):** هو انتهاك أمني محتمل (is potential security violation).
- **الهجوم (Attack):** هي محاول للاختراق الأمني (is attempt to breach security). والهجوم بإمكانه أن يكون مصادفة أو مقصود (accidental or malicious).

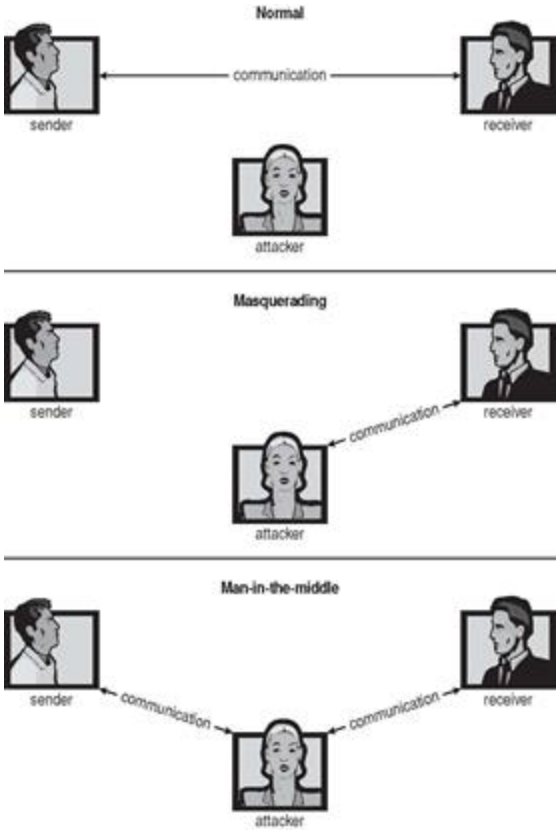
3: **الاختراق الأمني عن طريق المصادفة (accidental)** هو أسهل في الحماية من الاستخدام السيء المقصود (malicious misuse).

4: **الانتهاك الأمني له خمس فئات (Security Violation Categories):**

1) **خرق السرية (Breach of Confidentiality):** وهي قراءة البيانات الغير مصرح بها.
2) **خرق النزاهة (Breach of Integrity):** وهو تعديل البيانات الغير مصرح بها.
3) **خرق الصلاحيات (Breach of Availability):** وهو هدم (destruction) البيانات الغير مصرح بها.
4) **سرقة الخدمة (Theft of Service):** وهو استخدام المصادر الغير مصرح بها.
5) **الحرمان من الخدمة (DOS: Denial of Service):** وهو المنع من الاستخدامات القانونية (Prevention of legitimate use).

5: **الهجمات الأمنية القياسية (Standard Security Attacks) لها ثلاثة طرق:**

a) **العادي (Normal):** وهنا الاتصال يكون بين المرسل والمستقبل.
b) **المتخفي (Masquerading):** وهنا يكون الاتصال بين المهاجم والمستقبل. وهو الأكثر شيوعا.
c) **الشخص المتوسط (Man-In-the-middle):** وهنا يكون الاتصال بين ثلاث أطراف المرسل مع المهاجم والمستقبل أيضا مع المهاجم. انظر للأسفل الرسم التوضيحي لطرق الهجمات الأمنية القياسية:



6: من المستحيل أن يكون الأمن مطلقا؛ ولكن لجعل التكلفة عالية بما يكفي لمرتكبي الاعتداء (perpetrator) ولردع (to deter)
معظم المتسللين (most intruders).

7: **لحماية النظام؛ يجب علينا أخذ مقاييس الأمن على أربع مستويات (Four levels Security Measures):**

1) **الفيزيائي (Physical):**
يجب التأمين فيزيائيا على المواقع التي تحتوي على أنظمة كمبيوتر ضد دخول أي شيء غير مرغب فيه أو غير مصرح له.

2) **البشري (Human):**
يجب اختيار الأشخاص المناسبين واعطاءهم الترخيص للوصول إلى النظام. وتحذير الأشخاص المصرح بهم من إعطاء صلاحياتهم لأي شخص كان. والحذر أيضا من الوقوع في فخ الهندسة الاجتماعية من مواقع مشبوهة أو عن طريق الـ phishing.

3) **نظام التشغيل (Operating System):**
النظام يجب أن يحمي نفسه من الخروقات الأمنية (security breach) سواء كان غير مقصود أو مستهدف (accidental or purposeful). فعملية الفرار قد يشكل هجوم حرمان من الخدمة غير مقصودة. واستفسار خدمة قد يفشي (reveal) كلمة السر. وقائمة الخروقات المحتملة معظمها قد تكون أبدية.

4) **الشبكة (Network):**
الكثير من بيانات الكمبيوتر في الأنظمة الحديثة تسافر عبر الخطوط المؤجرة الخاصة (Private leased lines)، والخطوط المشتركة مثل الانترنت أو الاتصالات اللاسلكية أو خطوط الـ Dial up. واعتراض مثل هذا البيانات من الممكن أن تكون ضارة كاقتحام جهام الكمبيوتر. وقطع الاتصالات قد يشكل هجوم حرمان خدمة (Denial-of-Service) عن بعد.

8: **هناك عدة أسماء وطرق مختلفة من البرامج التي تسبب في الخروقات الأمنية أو Program Threats:**

1. حصان طروادة (Trojan Horse).
2. الباب المفخخ (Trap Door).
3. Logic Bomb.
4. Stack and Buffer Overflow.
5. الفيروسات (Viruses).
6. قطارة الفايروس (Virus Dropper).

9: **من خصائص حصان طروادة (Trojan horse properties):**

- تقسيم الكود (Code Segment) التي تسيء استخدام بيئتها.
- استغلال الاليات (Exploits mechanisms) من أجل السماح للبرامج المكتوبة من قبل المستخدم ان تكون منفذة من قبل مستخدمين اخرين.
- لها أنواع مختلفة (Spyware, Pop-up browser windows, covert channels).
- أكثر من 80% من الـ spam تصل عن أنظمة Spyware-infected.

10: **من خصائص الباب المفخخ (Trap Door):**

- معرف (Identifier) مستخدم معين أو الرقم السري الذي يبطل (circumvents) الإجراءات الأمنية العادية.
- يمكن ادراجها في المترجم (complier).

11: **Logic Bomb:** هو البرنامج الذي يبدأ بحادث أمني (initiates a security incident) في ظل ظروف معينة (under certain circumstances).

12: **من خصائص Stack and Buffer Overflow:**

- يستغل الـ bug في البرنامج (overflow either the stack or memory buffers).
- الفشل في فحص القيود على المدخلات (bounds on inputs) والحجج (arguments).
- كتابة الحجج (arguments) الماضية على stack في داخل عنوان العائد على stack.
- عندما يعود الروتين من الاستدعاء، يعود إلى العنوان المخترق (hacked address).
  - الإشارة على كود مخزن داخل stack ذلك ينفذ كود برمجي ضار (malicious code).
- المستخدم الغير مصرح به أو Privilege escalation.

13: **من خصائص الفيروسات (Viruses):**

- جزء من كود مرسخ (Code fragment embedded) في برنامج قانوني (legitimate program).
- التكرار الذاتي (Self-replacing)، مصممة لتصيب أجهزة أخرى.
- خاص جدا لبنية CPU، ونظام التشغيل، والتطبيقات.
- عادة تنقل (borne) عبر البريد الالكتروني أو كـ ماكرو (macro).

14: **قطارة الفايروس (Virus Dropper):** قطارة الفايروس يقوم بإدراج الفايروس إلى داخل النظام.

15: **أنواع الفايروسات (Viruses types):**

1) File / Parasitic
2) Boot / memory
3) Macro
4) Source code
5) Polymorphic to avoid a virus signature
6) Encrypted
7) Stealth
8) Tunneling
9) Multipartite
10) Armored

16: **Keystroke logger** يعمل للاستيلاء (to grab) على كلمات السر وأرقام بطاقات الائتمان.

17: **نظام الويندوز هو هدف معظم الهجمات لأنه:**

a) نظام الويندوز هو الأكثر شيوعا.
b) كل واحد هو administrator.
c) Monoculture تعتبر ضارة.

18: **تهديدات الشبكة أصعب للكشف والمنع لأن:**

1) أنظمة الحماية أضعف.
2) صعب جدا لتملك سر مشترك من حيث الوصول إلى القاعدة.
3) لا يوجد حدود فيزيائية بمجرد ارفاق النظام إلى الانترنت أو على الشبكة مع نظام مرفق إلى الانترنت.
4) حتى تحديد مواقع نظام الاتصال صعب لأن IP address هو المعرف فقط.

19: **تهديدات النظام والشبكة لها ثلاث أنواع (System and Network Threats):**

1) الديدان (Worms).
2) مسح المنافذ (Port Scanning).
3) الحرمان من الخدمات (Denial of Service).

20: **الدودة (Worm):** هي عملية تستخدم فيها ألية التكاثر (Spawn mechanism) لتكرار نفسه. وآلية التكاثر تقوم بنسخ نفسها باستخدام مصادر النظام وربما يوقف جميع العمليات الأخرى.

21: **دودة الانترنت (Internet Worm) تقوم بـ :**

a) استغلال ميزات شبكة اليونكس (الوصول عن بعد) والـ bugs الموجود في برامج finger and sendmail.
b) استغلال ألية علاقة الثقة المستخدمة بواسطة rsh للوصول إلى الأنظمة الودية بدون استخدام كلمة المرور.
c) برنامج Grappling Hook محمّلة برنامج الدودة الرئيسية.
d) النظام Hooked ثم الكود الرئيسي uploaded، لتحاول الهجوم على الأنظمة المتصلة.
e) أيضا تحاول اقتحام حسابات المستخدمين الاخرين على النظام المحلي عبر تخمين كلمة المرور.

22: **مسح المنافذ (Port Scanning):** هي عملية إرسال مجموعة من الحزم (range of packets) إلى منفذ معين من أجل معرفة إذا كان مفتوح أو لا ومعرفة ما هي الخدمات التي يقدمها هذا المضيف وبالتالي استغلال ذلك المنفذ عبر جمع معلومات وثغرات النظام (system's vulnerabilities) لأجل الهجوم.
ومسح المنافذ عادة تكون اوتوماتيكية، فهي تشمل أداة تحاول انشاء اتصال TCP/IP إلى منفذ معين أو مجموعة من المنافذ.

23: **من خصائص مسح المنافذ (Port Scanning Properties):**
1) هجومه أتوماتيكي للاتصال مع مجموعة من المنافذ (range of ports) على عنوان أو مجموعة من عناوين IP.
2) الكشف عن بروتوكول خدمة الرد (answering service protocol).
3) الكشف عن نظام تشغيل ونسخة تعمل على النظام.
4) nmap يقوم بمسح جميع المنافذ في مجموعة IP معطاه للرد.
5) nessus له قاعدة بيانات من البروتوكولات و bugs لتوظيفها ضد النظام.
6) يطلق باستمرار من أنظمة zombie، للتقليل من قدرة تقفي الأثر.

24: **من خصائص الحرمان من الخدمة (Denial of Service properties):**
1) الحمولة الزائدة من الكمبيوتر المستهدف تمنعه من العمل بأي شيء مفيد.
2) الحرمان من الخدمة الموزعة (DDOS: Distributed denial of service) يأتي من مواقع متعددة في وقت واحد.

25: تتوفر أداة **Broadcast Security** داخليا في كمبيوتر معين، ويكون مصدر وغاية (source and destination) الرسائل
معروفة ومحمية. ويقوم نظام التشغيل بإنشاء وإدارة وحماية عملية Ids واتصال المنافذ.

26: مصدر وغاية (Source and Destination) الرسائل على الشبكة لا يمكن الوثوق بها بدون تشفير (cryptography).

27: **الشفرة (Cryptography):** لتقييد المرسلين المحتملين (to constrain potential senders) "sources" أو مستقبلي
"destinations" الرسائل. بناءا على السرية Keys. والتي تمكن:
1) تأكيد المصدر.
2) الاستقبال فقط عن طريق destination معين.
3) علاقة الثقة بين المرسل والمستقبل.

28: **التشفير (Encryption):** يقوم بحل مجموعة واسعة من المشاكل الأمنية للاتصالات، ويستخدم بشكل متكرر في العديد من
جوانب (aspects) الحوسبة الحديثة. ويستخدم في ارسال الرسائل بشكل آمن عبر الشبكة كما يحمي بيانات الـ database
والملفات. وخوارزمية التشفير تمكن المرسل من التأكد بأن الكمبيوتر فقط من يمتلك (possessing) مفتاح معين لقراءة
الرسالة أو التأكد بأن كاتب البيانات هو فقط من يستطيع أن يقرأ تلك البيانات.

29: **خوارزمية التشفير (encryption algorithm) تتألف من خمس مكونات:**
1) مجموعة K من المفاتيح.
2) مجموعة M من الرسائل.
3) مجموعة C من النصوص المشفرة (ciphertexts).
4) وظيفة التشفير E. $E: K \rightarrow (M \rightarrow C)$
5) وظيفة فك التشفير D. $D: K \rightarrow (C \rightarrow M)$

30. **الفرق بين Symmetric and Asymmetric encryption:**

- **التشفير المتماثل (Symmetric Encryption):**

يعرف أيضا بتشفير المفتاح الخاص (Private Key Encryption) حيث يستخدم فيه نفس المفتاح لتشفير الرسالة وفك التشفير ويجب أن يتفق المرسل والمستقبل على مفتاح التشفير. فهو سريع وسهل الاستخدام ولكن مشكلته أنه لا يوجد أمان عند تبادل مفتاح التشفير وأيضا سهولة فك تشفيرها إذا تم سرقة مفتاح التشفير من قبل شخص آخر.

- **التشفير الغير متماثل (Asymmetric Encryption):**

يعرف أيضا بتشفير المفتاح العام (Public Key Encryption) حيث يستخدم فيها زوج من المفاتيح أحدهما لتشفير الرسالة بالمفتاح العام (public key) لأنه يكون معروف للمستخدمين في بيئة معينة والأخر لفك التشفير بالمفتاح الخاص (Private key) وهو لمستخدم واحد فقط وهو مالك الرسالة ويستخدم لفك الرسائل المشفرة بالمفتاح العام المقابل له. وتعتبر هذه الطريقة آمنة ولكنها بطيئة في التنفيذ وتستخدم مفاتيح كثيرة في التشفير وأيضا في فك التشفير.

31. **الفرق بين Public and Private Key:**

- مفتاح التشفير العام (Public Key):

وهو أن يكون المفتاح معروف للمستخدمين في بيئة معينة ويستخدم لتشفير الرسائل.

- مفتاح التشفير الخاص (Private Key):

وهو أن يكون المفتاح معروف لمستخدم واحد فقط وهو مالك الرسالة. ويستخدم لفك الرسائل المشفرة.

32. **Symmetric Cryptography** مبني على التحولات (based on transformations).
Asymmetric Cryptography مبنى على الوظائف الحسابية (based on mathematical functions).
- الغير متماثلة حسابها مكثف أكثر بكثير (much more compute intensive).
- عادة لا تستخدم في تشفير البيانات الكبيرة (bulk data encryption).

33. **الفرق بين Encryption and Authentication:**

- **التشفير (Encryption):**

تقييد (Constraining) مجموعة من مستقبلي الرسائل الممكنة (possible).

- **المصادقة (Authentication):**

تقييد (Constraining) مجموعة من مرسلي الرسائل المحتملة (Potential).

- مع العلم بأن التشفير والمصادقة يمكن استعمالهما معا ويمكن استعمالهما بشكل منفصل.

34. **من ميزات المصادقة (Features of Authentication):**

1) قد تكون مكملة (complementary) وبعض المرات تكون زائدة عن الحاجة (redundant) في التشفير.
2) أيضا تستطيع تثبيت (prove) الرسائل الغير معدلة (unmodified).

35. **خوارزمية المصادقة (Authentication algorithm) لها نوعان رئيسيان هما:**

1) **النوع الأول:** يستخدم التشفير المتماثل في كود رسائل المصادقة MAC وهي توفر وسيلة مصادقة للقيم الصغيرة بشكل آمن.
2) **النوع الثاني:** خوارزمية التوقيع الرقمي (Digital-signature algorithm) وهي مفيدة جدا لأنها تمكن أي شخص للتحقق من صحة الرسالة (to verify the authenticity of the message).

36: **عادة نستخدم المصادقة (authentication) عند المجموعات الفرعية من التشفير:**

a) الحسابيات أقل (Fewer computations) ما عدا التواقيع الرقمية للـ RSA.
b) عادة المصادق (authenticator) يكون أقصر من الرسالة.
c) بعض المرات تريد المصادقة وليس السرية.
d) يمكن أن تكون أساسا لعدم الرفض (non-repudiation).

37: **توزيع المفاتيح (Key Distribution):**

- لتوصيل المفاتيح المتماثلة وتعتبر تحدي كبير، وبعض الأحيان يتم خارج النطاق (done out of-band).
- المفاتيح الغير متماثلة قد تتكاثر (proliferate) وتخزن على key ring، وحتى توزيع المفاتيح الغير متماثلة تحتاج إلى اهتمام man-in-the-middle attack.

38: **الشهادات الرقمية (Digital Certificates):**

a) دليل (Proof) لمن يملك أو ماذا يملك المفتاح العام.
b) المفتاح العام رقميا موقع كطرف موثوق فيه (a trusted party).
c) الطرف الموثوق فيه يستقبل دليل المطابقة من الـ entity ويصادق (certifies) بأن المفتاح العام ينتمي إلى entity.
d) Certificate authority هو طرف موثوق فيه – مفاتيحهم العامة مشمولة مع توزيعات متصفح الويب.

39: **طبقة المقابس الآمنة (SSL: Secure Socket Layer):** هو بروتوكول تشفير (Cryptographic protocol) الذي يحد كمبيوترين من تبادل الرسائل مع بعضهما البعض. وهي معقدة للغاية مع وجود اختلافات كثيرة.

40: **طبقة المقابس الآمنة (SSL)** يستخدم بين خوادم الويب والمتصفحات (browsers) لأجل الاتصال الآمن مثل أرقام بطاقات التأمين. والخادم (server) يقوم بالتحقق من شهادة ضمان العميل (certificate assuring client) وأنه يتحدث إلى الخادم الصحيح.

41: **الشفرة الغير متماثلة (Asymmetric cryptography)** تستخدم لتوظيف مفتاح جلسة أمنة (secure session key) وهو يعتبر تشفير متماثل للجزء الاكبر (bulk) من الاتصالات خلال الجلسة (during session). والاتصالات تحدث بين كل كمبيوتر وبعد ذلك يستخدم تشفير المفتاح المتماثل (symmetric key cryptographic).

42: **مصادقة المستخدم (User Authentication):** هو حاسم (Crucial) لتعريف المستخدم بشكل صحيح كما أن أنظمة الحماية تعتمد على User ID.

43: غالبا ما تنشأ هوية المستخدم من خلال كلمات المرور (passwords) ، ويمكن اعتباره حالة خاصة إما للمفاتيح أو الامكانيات.

44: **للاحتفاظ بكلمات المرور سرا علينا بالآتي:**

- تغيير كلمات المرور بشكل مستمر.
- التاريخ لتجنب التكرار (History to avoid repeats).
- استخدام كلمات مرور لا يمكن تخمينها (non-guessable).
- تسجيل كافة المحاولات الغير صالحة (ولكن ليست كلمات المرور نفسها).
- النقل الغير مصرح به.

وكلمات المرور يمكن ايضا ان تكون إما مشفرة او يسمح باستخدامها مرة واحدة.

45: 1- قد يحل sniffing.
2- يعتبر shoulder surfing.
3- يعتبر حصان طروادة Keystroke logger.

46: كلمات المرور (passwords) تستخدم عادة لحماية objects في نظام الكمبيوتر، وفي حالة غياب برامج الحماية الكاملة. أو التشفير لتجنب الاضطرار لحفظ السرية. ومن مزاته:

1- الحفاظ على السرية في أي حال.
2- يستخدم الخوارزمية السهلة للحوسبة ولكنه صعب عند العكس (but difficult to invert).
3- فقط كلمة المرور المشفرة تكون مخزنة ولا تكون ابدا مفتوحة الشفرة.
4- إضافة salt لتجنب تشفير نفس كلمة المرور مع نفس القيمة.

47: **كلمات المرور لمرة واحدة (One-time passwords):**

- استخدام وظيفة على أساس بذور (seed) لحوسبة كلمة المرور معا المستخدم والكمبيوتر.
- تستخدم في أجهزة الهاردوير وآلات الحاسبة ومفتاح fob لتوليد كلمة المرور.

48: **القياسات الحيوية (Biometric)** هو نوع من أنواع استخدامات كلمات المرور للمصادقة مثل: بصمة الاصبع وماسح اليد.

49: **المصادقة متعددة العوامل (Multi-factor authentication):** فهي تحتاج إلى عاملين أو أكثر من عوامل المصادقة مثل: USB, biometric, and password.

50: **الدفاع في العمق (Defense in depth)** هو نظرية الأمن الأكثر شيوعا وهو ذو طبقات متعددة من الآمن.

51: **سياسة الأمن (Security Policy)** تقوم بوصف ما يجري تأمينها.

52: **تقدير نقاط الضعف (Vulnerability assessment)** يقارن الحالة الحقيقة للنظام والشبكة بالمقارنة مع السياسة الأمنية.

53: **محاولات الكشف عن التطفل (Intrusion detection endeavors)** للكشف عن محاولات الاقتحام أو التطفلات الناجح (detect attempted or successful intrusions). فمثلا:

- كاشف قاعدة التوقيع يكتشف (spots) الأنماط السيئة المعروفة.
- كاشف الحالات الشاذة (Anomaly detection) يكتشف (spots) الاختلافات من السلوكيات العادية. فبإمكانه اكتشاف هجمات الـ Zero-day.
- الإيجابيات الخاطئة والسلبيات الخاطئة تعتبر مشكلة.

54: **جدار حماية الشبكة (a network firewall)** يتم وضعه بين المضيفين (hosts) الموثوق فيهم والغير موثوق فيهم. فجدار الحماية يضع حد لوصول الشبكة بين هذين المجالين الأمنيين (security domains) الموثوق والغير موثوق فيه. وجدار الحماية بإمكانه أن يصبح tunneled أو spoofed.

55: **الفرق بين tunneled and spoofed:**

1. Tunneling تسمح بترحال البروتوكولات الغير مسموح لها إلى داخل البروتوكولات المسموح لها.
2. قوانين جدار الحماية عادة مبنية على أساس اسم المضيف أو عنوان IP حيث بإمكانها أن تكون spoofed.

56: **جدار الحماية الشخصي (A personal firewall)** هو برنامج طبقي إما أن تكون مشمولة مع نظام التشغيل أو مضافة كتطبيق.

57: **جدار حماية بروكسي التطبيق (Application proxy firewall)** يقوم بفهم بروتوكول التطبيق وبإمكانه السيطرة عليهم.

58: **جدار حماية استدعاء النظام (System-call firewall)** يقوم بمراقبة (monitors) جميع استدعاءات النظام المهمة وتوظف القوانين إليها. وهذا البرنامج بإمكانه تنفيذ استدعاء النظام.

END of Chapter 15