Public Key Infrastructures (PKIs)

22. a) What is the strongest form of authentication?

Cryptographic authentication is the strongest form of authentication.

b) List the functions of a PKI.

Creating public key–private key pairs.

Distributing digital certificates.

Accepting digital certificates.

Learning a certificate’s revocation status.

Provisioning new users and changing data on existing users.

Having strong initial authentication.

c) Can a firm be its own certificate authority?

Yes.

d) What is the advantage of doing so?

The advantage of being their own CA means that firms have control of trust in their entire PKI.

e) Who creates a computer’s private key/public key pair?

Private/public key pairs are normally created on the client, versus the PKI server.

f) How do CAs distribute public keys?

In digital certificates

g) What is provisioning?

In the context of PKI, provisioning is the accepting of public keys and providing new digital certificates to the users (a very expensive component of the PKI).

h) What is the prime authentication problem?

The prime authentication problem is that unless individuals are carefully vetted before being allowed in a system, imposters can simply enroll through social engineering.

i) What can be done to reduce this risk?

The only thing that can be done to reduce the risk of the prime authentication problem is to have strong procedures for who may submit an account request, who may approve it (always a different party than the applicant), what identification is required, and how to handle exceptions. The procedure must be carefully enforced and audited.

Authorization

The Principle of Least Permissions

23. a) Why are authorizations needed after a person is authenticated?

Simply knowing the identity of the communicating partner is not enough. The specific authorizations of the communicating party also need to be defined. Not everyone who is authenticated may be allowed to do anything he or she wishes in every directory.

b) What is another name for authorizations?

Permissions

c) What is the principle of least permissions?

The principle of least permissions is that each person should only get the permissions that he or she absolutely needs to do his or her job. In practice, this is very difficult to enforce, primarily because there are not enough security personnel to keep track of transient permission requirements.

d) Why is it a good way to assign initial permissions?

Assigning as few permissions as necessary is a good way to assign permissions initially because it reduces potential points of vulnerability, possible unauthorized behaviors, and mitigates the damage an intruder may do.

e) What is bad about assigning all permissions and then taking away the permissions a user does not need?

The bad thing about assigning all permissions and then taking away those that are not needed is that it is easy for security to mistakenly NOT remove a permission that is not required, thus allowing access beyond that which is authorized.

f) What does failing safely mean in a security system?

Failing safely in a security system means that a failure is not likely to lead to security violations. The principal of least permissions ensures that users are not given too many permissions if an error is made.

Auditing

Logging

Log Reading

24. a) What is auditing?

Auditing records and analyzes what the person or program actually did, rather than what was theoretically authorized.

b) Why is it necessary?

Unless authentication and authorization activities are audited frequently, improper behavior can go on for a very long time.

c) Why is log reading important?

Logging records the actions that an account owner takes on a resource. Unless logs are studied/read, they are useless.

d) What are the three types of actions that should be taken on log files?

They should be read regularly by someone who knows what he or she is looking at.

External auditing should be conducted periodically.

Automatic alerts should be established to provide security administrators with real-time feedback.

e) Why are automatic alerts desirable?

Reading log files only tells you about the past. Ideally, logging systems should have active log-reading functions that send the security administrator real-time alerts for certain types of events.

Central Authentication Servers

The Need for Centralized Authentication

25. a) What are the three devices in central authentication using RADIUS servers?

The three devices in central authentication are the supplicant, authenticator, and RADIUS central authentication server.

b) What is the role of the authenticator?

To send the supplicant’s credentials to the authentication server, and then to send a message of authentication back to the supplicant from the authentication server

c) What is the role of the central authentication server?

To test the validity of credentials provided by the user

Kerberos

26. a) In Kerberos, distinguish between the ticket granting ticket and the service ticket.

The ticket granting ticket is the supplicant’s proof that it has already authenticated itself with the Kerberos server. The service ticket is an encrypted session key that only the verifier can decrypt (due to sharing a key with the Kerberos server in a separate communication).

b) What information does the service ticket give the verifier?

The service ticket gives the verifier the symmetric session key to use with the supplicant. The session ticket may also contain permissions that the supplicant should have on the verifier.

c) How does the supplicant get the symmetric session key?

The supplicant gets the symmetric session key from the Kerberos server when the service ticket is sent to the verifier; the session key from the Kerberos server is encrypted to be read only by the server and supplicant.

d) Is the verifier notified explicitly that the supplicant has been authenticated? Explain.

The verifier is not notified explicitly that the supplicant has been authenticated. Authentication is implicit in that if the supplicant has the symmetric session key to communicate with the verifier, it must have been authenticated with the Kerberos server (which generated the session key and would only give it out to an authenticated computer).

Directory Servers

What Are Directory Servers?

Hierarchical Data Organization

27. a) How is information in directory servers organized?

The information in directory servers is organized as a directory server database schema in a hierarchical collection of objects.

b) What are the top two levels of the organization?

Top level is the Organization. This is the name of the organization.

Below the top level are organization units (OU). There can be many OU’s.

c) Do directory servers only hold information about people?

They hold information about many other types of company resources, such as computers.

Lightweight Data Access Protocol (LDAP)

28. What is LDAP’s purpose?

LDAP’s main purpose is to retrieve data from the directory server. However, it can also be used to update information in the directory server.

Use by Authentication Servers

29. a) How do central authentication servers often get their authentication information?

Central authentication servers often get their authentication information from directory servers.

b) What is the advantage of this?

It permits the directory server to be the company’s main repository for information.

Active Directory

30. a) What is Microsoft’s directory server product?

Microsoft’s directory server product is active directory (AD).

b) What is the smallest organizational unit in active directory?

The organizational unit

c) What two things does a domain controller contain?

The domain controller contains an active directory database and a Kerberos authentication server program.

d) Can a domain have multiple domain controllers?

Yes.

e) What is the advantage of having multiple domain controllers?

The advantage is that having multiple domain controllers gives reliability in case one crashes or is successfully attacked.

f) Into what larger structures are domains organized?

Trees

g) Into what larger structure can trees be organized?

Forests

h) Describe replication among domain controllers within a single AD domain.

Within a single AD domain, there is total replication between domain controllers.

i) Describe replication between a domain controller in one domain and the domain controller in the parent domain.

There is partial replication of data to the next-higher-level database.

Trust

31. a) Distinguish between mutual and one-way trust among AD domains.

In mutual trust, each directory server trusts the other.

In one-way trust, one directly server trusts the other, but there is no trust in the opposite direction.

b) Distinguish between transitive and intransitive trust.

An example of transitive trust would be if A trusts B and B trusts C, then A trusts C automatically. An example of intransitive trust would be if A trusts B and B trusts C, but A does not trust C automatically.

c) What principle should companies follow in making trust assignments?

Give only as much trust as necessary.

Toward Full Identity Management

Other Directory Servers and Metadirectories

32. a) Why are metadirectory servers needed?

To coordinate information across different types of directory servers

b) What do metadirectory servers do?

The metadirectory server allows the directory servers to exchange information and to synchronize services in a variety of ways.

Federated Identity Management

33. a) In federated identity management, do firms query one another’s identity management databases?

In federated identify management, firms do not query one another’s identity management databases. Instead, they send assertion statements that may include authenticity, authorization, and attribute information.

b) What do they do instead?

They send assertions to each other.

c) What risk does this method avoid for the firm sending the security assertion?

This method avoids the risk of potential attacks from the other company because the other company never gets direct access to corporate resources.

d) How are risks to Firm B reduced?

The firms first carefully negotiate a contract. The contract specifies penalties if Firm A sends false assertions.

e) What is a security assertion?

An assertion is a statement from Firm A to Firm B that Firm B should accept as true if Firm B trusts Firm A.

f) What three things may it contain?

Authenticity information, such as an employee is actually the employee by that name and has been authenticated by Firm A.

Authorization information, stating that the employee is allowed to access Firm B’s services

Attributes that describe features of the employee (such as spending limit, etc.).

g) What is the main standard for one firm to send security assertion to another firm?

The main standard for sending security assertions today is the Security Assertion Markup Language (SAML).

h) What is the major benefit of using XML?

The major benefit of using XML in SAML is that it is platform-independent. This means that it does not matter what programming language either firm uses as long as they implement XML successfully.

Identity Management

34. a) What is identity management?

Identify management is the centralized policy-based management of all information required for access to corporate systems by people, machines, programs, or other resources.

b) What are the benefits of identity management?

Reduced costs by reducing the work needed to manage user access, including provisioning, password resets, and so forth

Enforcing consistency by permitting a single change on an identity management server to affect employee access permission on all servers in an organization

Centralized auditing of all an employee’s access permissions across a firm

Possible use of single sign-on, or at least reduced sign on

c) What is SSO?

Single sign-on allows a user to authenticate him or herself to the identity management server once. From that point on, whenever the user asks for access to a specific server, no additional logins are required.

d) Why is full SSO generally impossible?

It is technically impossible.

e) What is reduced sign-on?

It is single sign-on to some resources but not *all* resources, as in full SSO.

f) What is an identity?

An identity is the set of attributes about a person or resource that must be revealed in a particular context.

g) Why is providing minimum identity data an important principle?

You will not accidentally reveal information about yourself that you do not have to reveal and that may be used against you.

35. a) In identity management, what are provisioning, reprovisioning, and deprovisioning?

Provisioning entails granting authorizations and authentications carefully and then changing them whenever roles or other conditions change. Reprovisioning occurs when there are changes. Deprovisioning occurs when the authorizations and authentications are no longer appropriate (e.g., when an employee leaves the company, etc.).

b) Why is decentralized management desirable?

Decentralized management is desirable because identities should be managed by people closest to the situation.

c) Why are self-service functions desirable?

To reduce costs of the identity management staff

d) What changes should be made through self-service functions?

Only non-sensitive information changes should be made through self-service functions.

Trust and Risk

36. a) In what sense is identity management really just another form of risk management?

Identity management allows risk reduction by reducing risk from individuals accessing computer resources to acceptable levels. Risk reduction is the primary risk management technique.

b) How can identity management reduce risk?

Identity management can reduce risk by limiting the amount of potential damage an employee can do based on computer resource privileges, as well as allows detection of malicious activities in real-time (via auditing).

c) How much should companies spend on identity management?

A company must balance these risk reductions with the amount of money that identity management will cost to implement over their entire life cycle.

=======================

Firewalls

Introduction

1. a) What is a pass/deny decision?

When the firewall receives a packet, it must decide whether to pass the packet or drop it.

b) What type of packet does a firewall drop and log?

Firewalls will drop and log a provable attack packet.

c) What does the firewall do about packets that it suspects (but cannot prove) are attack packets?

It will pass the packet because it’s not a provable attack packet.

d) Why does the firewall log information about dropped packets?

To keep a record of it for later analysis

e) Distinguish between border firewalls and internal firewalls.

Border firewalls sit at the boundary between the corporate website and the external Internet. Internal firewalls filter traffic passing between different parts of the website’s internal network.

f) Distinguish between ingress and egress filtering.

In ingress filtering**,** the firewall examines packets *entering the network from the outside*, typically from the Internet. The purpose of ingress filtering is to stop attack packets from entering the firm’s internal network.

In egress filtering**,** by contrast, the firewall filters packets when they are *leaving the network*. This prevents replies to probe packets from leaving the network.

The Danger of Traffic Overload

2. a) What does a firewall do if it cannot keep up with the traffic volume?

It will drop all the packets it cannot process.

b) Why is this action good?

This action is good because the firewall will drop all packets not examined, not allowing unexamined attack packets into the network.

c) Why is this action bad?

This action is bad because valid, non-attack packets will be dropped and effectively create a self-generated DoS attack.

d) Why can a firewall keep up with traffic in general but fail to do so during a major attack?

Firewalls are only able to filter traffic at wire speed, which is the maximum speed of the lines that connect to it.

e) As processing power increases in the future, what will this mean for firewall filtering?

It means that firewalls will be able to do ever more sophisticated processing.

f) What is unified threat management (UTM)?

Unified threat management (UTM) consists of a firewall handling all traditional firewall functions (e.g., SPI, ACLs, etc.) as well as additional security functions such as antivirus filtering, spam filtering, application proxy filtering, etc.

g) What does it mean that a firewall should operate at wire speed?

Firewalls that operate at wire speed are able to filter traffic at the maximum speed of the network lines connected to it.

Firewall Filtering Mechanisms

3. a) Is there only one firewall filtering mechanism?

No.

b) What filtering mechanisms do almost all main border firewalls use?

Stateful packet inspection

c) Do SPI firewalls only do stateful packet inspection?

SPI firewalls can do more than just stateful packet inspection.

Static Packet Filtering

4. a) What are the two limitations of static packet filtering? Explain why each limitation is bad.

(1) By looking at only one packet at a time, static packet inspection does not stop attacks that can only be determined by knowing the packet’s place in a stream of traffic; in other words, no context is applied to the packet. For example, static packet inspection cannot protect against a TCP half-open DoS attack because it only examines individual packets, versus determining the state of a connection and a related (or unrelated) packet.

(2) By only inspecting certain fields of the Internet and Transport headers, static packet inspection cannot stop attacks that utilize other portions of the packet. For example, attacks utilizing the data field of application messages will not be examined.

b) For what two reasons do companies not use static packet filtering as the main filtering mechanism in border firewalls today?

For the two reasons mentioned in the previous question part

c) In what two secondary ways do corporations sometimes use static packet filtering?

One way is that static packet filtering may be used as a secondary filtering mechanism on main border firewalls.

The other way is they may also be implemented in border routers, which lie between the Internet and the firewall.

Stateful Packet Inspection (SPI)

Basic Operation

5. a) What is a state?

A state is a distinct phase in a connection between two applications.

b) Are most packets part of the connection-opening state or the ongoing communication state?

Most packets are part of the ongoing communication state.

c) Why is the answer to Question 5b important for stateful packet inspection’s efficiency?

SPI efficiency is based upon the two categories of states – because most packets belong to ongoing communication, a different (and less expensive) set of filters can be used compared to connection opening states, which require more scrutiny, and thus are more expensive.

d) What is a connection?

A connection is a persistent conversation between different programs on different computers.

e) How is a connection between two programs on different computers represented?

A connection between two programs on different computers is represented by its socket (i.e., IP address: port).

Packets that Do Not Attempt to Open Connections

6. a) Give the simple stateful packet inspection firewall rule for packets that do not attempt to open connections.

When a packet arrives that does not attempt to open a connection, SPI firewall checks to see if it is part of a previously opened connection. If it is, then the packet is passed, usually without filtering. If it is not, the packet is dropped and logged.

b) Is SPI filtering for packets that are part of ongoing communications usually simple and inexpensive? Explain.

Yes, simply because if the packet is part of an existing connection in the connection table, the packet is passed, usually without further filtering. If it is not part of an existing connection in the connection table, it is dropped and logged.

c) UDP is connectionless. How is it possible for an SPI firewall to handle UDP connections? .

SPI firewalls can treat UDP communications as if they were stateful by treating some certain UDP messages as connection opening attempts. If subsequent messages match the connection table for the UDP packet, the incoming UDP packet will be passed.

Packets that Do Attempt to Open a Connection

7. Give the two simple default SPI firewall rules for packets that attempt to open connections.

Permit all attempts to open a connection from an internal host to an external host.

Deny all attempts from external hosts to open a connection with an internal host.

Access Control Lists (ACLs) for Connection-Opening Attempts

8. a) For stateful packet inspection firewalls, what do ingress ACLs permit in general?

Ingress ACLs typically permit a specific type of externally originated connection to network resources.

b) What do egress ACLs disallow in general in SPI firewalls?

SPI firewall egress ACLs disallow communication between internal and external hosts in specific ways. For example, an egress ACL can prevent ICMP Echo Reply messages from internal hosts from exiting the network.

c) What do well-known port numbers designate?

Well-known port numbers designate specific applications running on a server.

d) Is Figure 6-10 an ACL for ingress filtering or egress filtering?

Ingress filtering

e) Why is Rule 2 in Figure 6-10 safer than Rule 1?

Rule 2 is safer than Rule 1 because Rule 2 allows a connection to only a specific SMTP mail server, while Rule 1 allows connections to all internal webservers. More limited access is safer than broader access.

f) Which rule in the ACL in Figure 6-10 represents the default behavior of SPI firewalls for ingress connection-opening attempts?

Rule 3, denying all connections, represents the default SPI rule for ingress connection opening attempts.

9. Given the ACL in Figure 6-10, what would the firewall do with an incoming ICMP echo message? (This will require some thought. Think about how ICMP messages are encapsulated and what field in the IP header indicates that the packet’s data field contains an ICMP message.)

An incoming ICMP Echo message is a layer 3, connectionless message. The firewall using the ACL in Figure 6-10 would disallow the ICMP message because it does not meet Rule 1 or 2, so it would apply Rule 3 (deny).

10. Redo the ACL in Figure 6-10 to add rules for the following conditions. After Rule 1, create a rule that permits all connections to internal DNS servers. After the original Rule 2, create rules that permit connections to all Trivial File Transfer Protocol (TFTP) servers and that permit access to FTP Server 60.33.17.1. (Hint: Only allow an FTP supervisory connection; the SPI firewall will later open data connections automatically as needed.)

If TCP destination port = 80 or 443, then allow

If TCP destination port = 53, then allow

If TCP destination port = 25 AND destination IP = 60.47.3.35, then allow

If TCP destination port = 21 AND destination IP = 60.33.17.1, then allow

Disallow all connections

11. a) In ingress and egress filtering, does an SPI firewall always consider its ACL rules when a new packet arrives that attempts to open a connection?

SPI firewalls always execute the ACL.

b) In ingress and egress filtering, does an SPI firewall always consider its ACL rules when a new packet arrives that does not attempt to open a connection? (The answer was not specifically in this section.)

No.

12. a) Why are stateful packet inspection firewalls inexpensive?

Stateful packet inspection firewalls are inexpensive because most packets are not connection opening requests. Determining whether to drop or pass a packet requires a simple connection table lookup, which is fast and cheap.

b) In practice, are they fairly safe?

Yes, in practice, they are fairly safe.

c) Are SPI firewalls limited to SPI filtering?

No, they can implement other protections as well.

d) What firewall inspection mechanism do nearly all main border firewalls today use?

Nearly all main border firewalls today use stateful packet inspection.

Network Address Translation (NAT)

Sniffers

NAT Operation

Perspective on NAT

13. a) When NAT is used, why can sniffers not learn anything about the internal IP addresses of internal hosts?

When using NAT firewalls, the IP addresses and port addresses of hosts are translated. Attackers can only see the translated IP addresses and port numbers.

b) Why does NAT stop scanning probes?

Scanning probes are based on IP addresses and port numbers. Sniffers can only read translated IP addresses and port numbers, and these become invalid when connections end. If an attacker acts quickly, it can use translated information, but it is very difficult to act quickly.

c) Why is NAT traversal necessary?

So applications that require true internal IP addresses and port numbers can still work when companies use NAT.

d) Is a NAT traversal method easy to select?

No, selecting them can be complex because there are many NAT traversal methods and all have limitations.

Application Proxy Firewalls and Application Content Filtering

Application Proxy Firewall Operation

14. a) What distinguishes an application proxy firewall from static packet filtering firewalls and SPI firewalls?

Application proxy firewalls examine application messages while static packet filtering does not, nor do SPI firewalls.

b) Distinguish between proxy programs and application proxy firewalls.

An application firewall has an application proxy program for each application it will filter.

c) If you will proxy four different applications, how many proxy programs will you need?

You will need four separate proxy programs.

d) How many application proxy firewalls will you need at a minimum?

One application proxy firewall can support multiple proxy application programs, so you will need at least one application proxy firewall to support the four proxy programs.

e) Can nearly all applications be proxied?

Only a few applications can be proxied. Most application proxies are HTTP or SMTP.

f) Why is application proxy firewall operation processing-intensive?

Application proxy firewall operation is processing-intensive because it must maintain two connections for each client/server pair.

g) Why do firms not use application proxy firewalls as main border firewalls?

They are not used as border firewalls because of the high processing load required to maintain the number of connections required by an application proxy firewall. They simply would not be able to handle the traffic load.

h) What are the two main roles of application proxy server firewalls today?

Protect internal clients from malicious external servers by forcing all client connections through the proxy, which examines the application content of all packets.

Sit between an internal server and external clients to protect the server by examining the application layer content of all incoming client requests for dangerous behavior.

Application Content Filtering in Stateful Packet Inspection Firewalls

15. a) Do stateful packet inspection firewalls automatically do application content filtering? Explain.

No, application content filtering is seen as an extra feature because stateful packet inspection firewalls don’t have to implement relay operation like application firewalls do.

b) Do they have the slow speed of relay operation?

No, they do not do relay operation, so they do not suffer the slow speed of relay operation.

c) What three advantages do application proxy firewalls have in protection that SPI firewalls with content inspection not have?

Application proxy firewalls always examine application layer content, are more capable of application layer content filtering, and use relay operation with two connections per client/server pair.

d) Why are SPI content filtering firewalls faster than application proxy firewalls?

They do not use relay operation.

Application Proxy Firewall Protections

16. a) What filtering actions were listed to protect clients from malicious webservers?

First, the proxy can inspect the URL and compare it with a table of blacklisted URLs that are known phishing sites, pornography sites, or recreational sites.

Second, the proxy can inspect scripts in downloaded webpages, dropping these webpages if the scripts appear to be malicious or if policies prohibit either certain types of scripts or all scripts.

Finally, the proxy can inspect the MIME type in an HTTP response message. Files with certain MIME types might be allowed or dropped by policy.

b) What filtering action was mentioned to prevent internal client misbehavior in HTTP?

The filtering action that prevents internal client misbehavior in HTTP is for the HTTP proxy to examine outgoing packets from the internal client to the external webserver in order to detect client misbehavior. For example, the proxy can inspect the method in the URL header. While the HTTP GET method is generally safe, the POST method can send files out of the firm. Many firms drop any HTTP request message that uses the POST method in order to provide extrusion prevention.

c) What two filtering actions were mentioned for protecting webservers from malicious clients?

First, the proxy can inspect the method in the URL header. The POST method will allow clients to upload files to the webserver. This might be disallowed by policy to prevent clients from uploading malware, pornography, or any other type of unapproved content.

Second, the HTTP proxy can filter out HTTP request messages that appear to contain SQL injection attacks.

d) What three automatic protections do application proxy firewalls provide simply because of the way in which they operate?

The three automatic protections of application proxy firewalls are internal IP address hiding, header destruction, and protocol fidelity.

Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs)

Intrusion Detection Systems (IDSs)

17. a) Distinguish between firewalls and IDSs.

Firewalls only stop and log provable attack packets. IDSs identify suspicious packets that may or may not be part of an attack and alert network administrators of potential threats, but do not drop suspicious packets.

b) Why are IDS alarms often a problem?

IDS alarms are often a problem because they tend to generate far too many false alarms or false positives. IDSs tend to be ignored after exhausted security staff members receive too many false alarms.

c) What is a false positive?

A false positive is when an IDS issues an alarm for legitimate traffic. Another term is false alarm.

d) What two types of filtering do IDSs use?

The two types of filtering IDSs use are Deep Packet Inspection and Packet Stream Analysis.

e) Why is deep packet inspection important?

This is important because it looks at all fields in the packet, including the IP header, the TCP or UDP header, and the application message. Many attacks cannot be stopped if a firewall only looks at application content or only at internet and transport layer headers.

f) Why is deep packet inspection processing-intensive?

Deep packet inspection is processing-intensive because it looks at every field in the packet, which takes more time and processing power.

g) Why is packet stream analysis important?

Packet stream analysis is important because single packets are not enough to determine certain types of attacks. For example, it takes multiple packets to determine if a network is being systematically scanned, or if a TCP half-open DOS attack is occurring.

h) Why does packet stream analysis place a heavy load on IDSs?

Packet stream analysis requires the IDS to reassemble or maintain and compare many packets in order to determine if an attack is taking place; the increased packet total and reassembly places a heavy processing load on IDS.

Intrusion Prevention Systems (IPSs)

18. a) Distinguish between IDSs and IPSs.

Intrusion prevention systems (IPSs) actually stop attacks rather than detecting them and sending out alarms like IDSs do.

b) Why is the attack identification confidence spectrum important in deciding whether to allow IPSs to stop specific attacks?

Because IDSs offer many false positives and alarms, the attack identification confidence spectrum allows the network security administrator to establish packet dropping policies that are based on a high degree of confidence that an attack is taking place.

IPS Actions

19. a) What two actions can IPSs take when they identify an attack?

The two actions taken by IPSs when identifying an attack are to simply drop the packet like a traditional firewall, and to limit suspicious traffic to a certain percentage of the total bandwidth.

b) Which can be the most effective?

Dropping packets

c) Which can do the most damage?

Dropping packets is the most damaging because it can lead to lost packets that are important to a firm’s operations (such as orders, payment processing, etc).

Antivirus Filtering and Unified Threat Management (UTM)

20. a) How do firewalls and antivirus servers work together?

The packet will arrive at the firewall, and the firewall will decide what to do with it. To decide, the firewall will check its policy rules base. If the policy rules base says to pass a certain object to an antivirus server, the firewall will do so. Then the antivirus server will examine the object.

b) Are antivirus servers limited to looking for viruses? Explain.

Antivirus servers can do more than just look for viruses. They can scan for worms, rootkits, phishing, Trojan horses, spam, malicious scripts, and other types of malware.

c) What may the antivirus server do after it performs filtering?

After an antivirus server filters, it can drop the object, send it to the firewall to pass to the destination, or pass the object to the destination directly.

d) What type of firewall does both traditional firewall filtering and antivirus filtering use?

Unified Threat Management (UTM) firewalls provide both traditional and antivirus filtering. However, UTMs rarely offer best of breed services and should be considered for small offices only.

Firewall Architectures

Types of Firewalls

21. a) Why are screening routers used in a firewall architecture?

The screening border router stops simple high-volume attacks and ensures that responses to external scanning probes cannot reach an external attacker. It economically reduces the load on the main border firewall.

b) Why are internal firewalls desirable?

These are desirable because they control traffic flowing between different parts of the firm’s internal network. In contrast to border firewalls, they can stop internally generated attacks.

c) Why is it easier to create appropriate ACL rules for server host firewalls than for border firewalls?

Most servers only have a single application or a few applications. It is easier to develop specific rules for a few applications than to develop rules for all internal hosts.

d) How does the use of border, internal, and host firewalls provide defense in depth?

Their use provides defense in depth because if the main border firewall or an internal firewall has an ACL configuration error, individual hosts will still be protected.

The Demilitarized Zone (DMZ)

22. a) What is a multihomed router?

It is a router that connects to three or more subnets. A tri-homed firewall has one connection to the internal network, one to the DMZ, and one to the border router (leading to the Internet).

b) What is a DMZ?

The DMZ (Demilitarized Zone) is a subnet that contains all of the servers and application proxy firewalls that must be accessible to the outside world.

c) Why do companies use DMZs?

All externally initiated attempts must go to hosts in the DMZ. This permits companies to focus special attention on these hosts, which are under frequent external attack. It also keeps attackers from attacking internal hosts.

d) What three types of hosts are placed in the DMZ?

Public servers, application proxy firewalls, and external DNS servers

e) Why do companies put public servers in the DMZ?

Placing all hosts that must be available to the outside world in a single place, where protection can be concentrated, ensures that no externally initiated connections go to internal hosts.

f) Why do companies put application proxy firewalls in the DMZ?

Because they enforce a policy that all communication with the outside world must pass through the DMZ.

g) What host names does the external DNS server know?

The external DNS server will only know the host name information for computers in the DMZ.

h) Why do all hosts in the DMZ have to be hardened stringently?

DMZ hosts must be hardened stringently because they will be accessible to the outside world and will be frequently attacked.

Firewall Management

Defining Firewall Polices

23. a) Distinguish between firewall policies and ACL rules.

Firewall policies are high-level statements that reflect corporate security policies and guide firewall implementers. ACL rules are the implementations of the firewall policies at the firewall, and are very specific.

b) Why is creating firewall policies desirable compared to just creating a list of ACL rules?

Creating firewall policies is more desirable than just creating a list of ACL rules because policies should be clearly understood in plain English, while allowing for the firewall administrator to implement ACL rules that fit the policies with maximum efficiency and lowest cost. It is always smart to state the requirement first, followed by the technical implementation; this prevents locking a network into antiquated equipment or techniques.

c) Create three firewall policies not listed in the text.

Allow the database server at Company A (that supplies critical parts to the company) to connect to the corporate database for inventories.

Only allow secure FTP connections.

Log all large (1MB>) file transfers.

Stop all inbound and outbound ICMP messages.

Drop inbound connections to TCP port 445 from hosts 192.168.4.0 through 192.168.20.255.

Implementation

24. a) Compare firewall hardening needs for firewall appliances, vendor-provided systems, and firewalls built on general-purpose computers.

For firewall appliances, a firm simply installs the appliance between its Internet access router and its internal network. Operation is largely automatic. Firewall appliances are hardened at the factory.

Firewall vendors often sell firewall computers that have pre-hardened versions of UNIX or Windows. These limit the ability of an organization to make mistakes in hardening the operating system.

Strong actions must be taken to harden the firewalls on general-purpose computers if the firm purchases the computers and installs the firewall software itself.

b) List what centralized firewall management systems do.

Centralized firewall management systems use a firewall policy management server to centrally control many firewalls to ensure consistency and save time and money in firewall administration. It converts policies to ACLs and sends these ACLs to individual servers.

c) What columns does the firewall policy database described in the text contain? Be able to describe each and what options it offers.

Policy number (self explanatory): Each policy has a unique number.

Source and destination: Can be host names, groups of IP addresses, subnets, etc. The firewall administrator must manually define groups.

Service: Describes the service to be filtered (TCP http, UDP dns, ICMP, etc.).

Action: Describes what to do (usually pass, drop, or authenticate).

Track: Describes what the firewall should do after the action (log, nothing, alert, etc.).

Firewalls: Designated which firewall routers should be sent ACLs based upon the policy

d) Why is vulnerability testing necessary?

ACLs are complex, based upon complex firewall policies that are not easy to translate to ACLs. Vulnerability testing is required to ensure errors in ACL creation are detected and fixed.

e) Why should firewall policies govern both configuration and testing?

If firewall policies govern both, then testers can create tests based on policies. If tests fail, then either the configuration or the test violated the policy. The firm must decide which is wrong.

f) What are the steps in firewall change management?

First, only certain people are allowed to request changes. Even fewer people should be allowed to approve changes. The requestor must be different from the approver.

Second, firewall changes should be implemented in the most restrictive manner that will pass the smallest number of additional packets.

Third, the change should be documented carefully and completely.

Fourth, the firewall should be vulnerability tested after each change, to make sure the change works and that all of the previous behavior is intact.

Fifth, the company should audit the change process frequently, to ensure compliance with procedures.

g) Why is reading firewall logs important?

To develop an understanding of the changing threat environment. It will also help to determine what traffic is unusual.

h) What is the most time-consuming part of firewall management?

The most time-consuming part of firewall management is reading firewall logs.

Reading Firewall Logs

25. a) What packets are usually logged in log files?

Dropped packets from firewalls are usually logged in log files.

b) What are the fields in the log file shown in Figure 6-25?

ID number for the packet dropping event.

Time: The time the packet arrived at the firewall.

Rule: The rule that caused the packet to be dropped.

Source and destination IP addresses found in the dropped packet.

Service: The service requested in the dropped packet.

c) In the examples given, by what field was the log file sorted?

In Figure 6-25, the log file is sorted by ID number.

The log file is sorted by the time field at which the packet arrived at the firewall.

d) From the log file, what could we infer about the Echo probe attack?

The log file shows that a majority of the Echo probes are coming from the same IP (14.17.3.139), targeting successive client IP addresses. It appears the attacker is trying to map the internal network based on receiving Echo Request reply messages.

e) Did this attack seem to be serious? Explain.

The attack does not seem to be serious. This appears to be an attacker trying to map a network for IP addresses and host OS. The more serious attacks could be coming after the mapping.

f) From the log file, what could we infer about the FTP attack?

It appears that the primary target of the FTP attack is the .56 server. The source IP addresses are never the same, but it does include the 14.17.3.139 host that is trying to map the network. It is possible that the attacker is trying to access the FTP server using several zombie machines.

g) Did this attack seem to be serious? Explain.

This attack is more serious than the Echo mapping attack because it is targeting a specific host with multiple different computers. The attacker knows there is a server at that IP address and is trying to gain access via multiple captured hosts.

h) Why was the dropping of a single packet because of lack of firewall capacity a cause for concern?

Dropping any packets in such a short capture because of lack of capacity indicates that there is insufficient firewall capacity that must be addressed immediately.

i) What cannot be determined if log files cover too short a period of time?

If the log files cover too short a period of time, you lose the ability to examine attacks that take place over a considerable period of time.

j) Why is it difficult for a log file to cover a long period of time?

It is difficult for a log file to cover a long period of time because long log files require a great deal of disk capacity.

k) What is the advantage of logging *all* packets passing through a firewall?

A firm can see packets from an attacker that were not dropped by the firewall because it could not identify them as provable attack packets.

l) Why is logging all packets problematic?

Logging all packets makes for very large log files, which means the period of logging is shorter for the same amount of log storage capacity than if only provable attack packets are logged.

Difficult Problems for Firewall Filtering

The Death of the Perimeter

26. a) How can attackers avoid the border firewall?

Attackers can avoid the border firewall by becoming an internal attacker, attacking internal hosts not protected by the border firewall, or entering or attacking though a wireless access point.

b) How has the perimeter extended outside the site?

It has extended outside the site by remote employees giving access.

Consultants, outsources, customers, suppliers, and other subsidiaries must be given access.

Essentially, all of these tend to use VPNs to make external parties “internal” to your site.

c) How can firms react to this decline in the effectiveness of border firewall filtering?

Firms will have to increasingly rely upon hardening internal hosts against attacks as the effectiveness of the border firewall declines.

Attack Signatures versus Anomaly Detection

27. a) Distinguish between signature detection and anomaly detection.

Signature detection relies upon a unique pattern in the network traffic to identify the threat (like an attack fingerprint). Anomaly detection looks at traffic patterns for deviations from set norms in order to identify possible attacks.

b) What is a zero-day attack?

A zero-day attack is one that is made before attack signatures for the threat are defined for firewalls and antivirus programs to use.

c) Why are zero-day attacks impossible to stop with attack signatures?

Zero-day attacks do not yet have attack signatures, therefore firewalls and antivirus programs will not be able to detect the attack.

d) What is the promise of anomaly detection?

The promise of anomaly detection is that they could stop attacks without known attack signatures, such as zero-day attacks.

e) Why is anomaly detection becoming critical for firewalls?

Given the speed with which vulnerability exploits, worms, and viruses are beginning to spread, depending solely on attack signatures is not reliable, so anomaly detection is essential in firewalls today.

Host Hardening

Introduction

1. a) What is our definition of a host?

Any device with an IP address is a host.

b) Why is host hardening necessary?

This is necessary to protect the host against attacks.

c) What major categories of hosts did this section mention?

Servers, clients, routers, firewalls, and even many mobile phones

d) List the elements of host hardening.

Back up the host regularly. Without this, nothing else matters.

Restrict physical access to the host.

Install the operating system with secure configuration options. In particular, be sure that all default passwords are replaced by strong passwords. Adversaries know every default password. If you fail to change even one, they can use it to get into your system immediately.

Minimize the applications and operating system services that run on the host to reduce the ability of hackers to take over the host by compromising an application or service. Minimizing the number of running programs reduces the “attack surface” of hosts.

Harden all remaining applications on the host.

Download and install patches for known operating system vulnerabilities.

Manage users, including account profiles, passwords, and other matters.

Manage access permissions for users and groups securely.

Encrypt data if appropriate.

Add a host firewall

Read operating system logs regularly to look for suspicious activities

e) Why is it important to replace default passwords during configuration?

Anyone who knows anything about the subject will know the default password. The default password is usually the first thing an attacker will check.

f) What is a security baseline, and why is it important?

Security baselines are sets of specific actions to be taken to harden all hosts of a particular type and of particular versions within each type. This is important because it is another rule to follow to harden hosts and prevent attacks.

g) Why is the downloading of disk images of the operating system desirable compared to configuring each host individually?

This method will save labor time and cost on each subsequent installation. It also ensures that each server is properly configured according to the firm’s security baselines and general policies.

h) What is virtualization?

Virtualization is the process whereby multiple operating systems, with their associated applications and data, run independently on a single physical machine.

i) What are some of the advantages of using virtual machines?

The benefits of virtualization include a single baseline for each host, rapid deployment, reduced system misconfiguration, reduced labor costs, reduced utility expenses, and greater fault tolerance and availability.

j) What does a systems administrator manage?

Systems administrators manage individual hosts or groups of hosts.

k) Does a systems administrator generally manage the network?

System administrators generally do *not* administer the network.

2. a) What is cloud computing?

Cloud computing utilizes processing power, applications, data storage, and other services over the Internet.

b) How do cloud computing and mainframe architectures differ?

Mainframe architectures consist of several thin clients connected to a single powerful computer called a mainframe. Thin clients are essentially a screen, keyboard, and a connection to the mainframe. Commands are sent to the mainframe where all application processing occurs, and data is stored. Computing is done locally, not over the Internet.

c) How do cloud computing and client–server architectures differ?

Stand-alone clients do not have to be connected to a mainframe. Clients can run applications and store data locally. They can also communicate with servers over the Internet and access data, applications, and additional processing power. Client-server architectures can share some of the processing too. Servers are much less expensive than mainframes and can support users at many locations as long as they have an Internet connection.

d) What are the advantages of cloud computing?

Advantages of cloud computing include reduced costs, increased reliability, quicker disaster recovery, reduced data loss, better scalability, greater agility, and better accessibility.

e) Which security concerns are specific to cloud computing? Why?

Security concerns specific to cloud computing center on the cloud service provider. Can users, or corporations, trust their cloud provider to securely store their data? Can cloud providers be trusted with critical systems? Will there be any conflicts of interest with other clients and the cloud provider? Will the cloud provider act in the company's best interests?

f) How could attackers use cloud computing?

Attackers could use cloud computing to launch attacks, store illegal digital media, crack stolen passwords, or even host phishing scams.

Important Server Operating Systems

Windows Server Operating Systems

3. a) What is the name of Microsoft’s server operating system?

Windows Server

b) What security protections do recent versions of this operating system offer?

They intelligently minimize the number of running applications and utilities by asking the installer questions about how the server will be used. They also make the installation of vulnerability patches very simple and usually automatic. They include server software firewalls, the ability to encrypt data, and many other security enhancements.

c) Why is Microsoft Windows Server easy to learn?

Windows Server is easy to learn because the interface looks like the interfaces in client versions of Windows.

d) What are MMCs? (Do not just spell out the acronym.)

Microsoft Management Consoles (MMCs) are Microsoft Server’s administrative tools that use a consistent GUI.

e) On what object does an icon bar icon operate?

When a user selects an object in one of the two lower panes, the icons specify actions that the administrator can take on the selected object. One of the most important choices is Action, which is specific to the selected object.

f) What is in the tree pane?

It is a tree of administrative applications. The tree pane is located in the lower-left pane of GUI.

g) To what things do items in the sub object pane refer?

These things refer to objects on which actions can be taken.

h) What is a snap-in?

A snap-in is an individual application on the tree pane of an MMC that can be added or dropped from the tree list easily.

i) Why are they called “snap-ins”?

They are called this because they can be added or dropped from the tree list easily.

j) Why is the standardized layout of MMCs beneficial?

Standardized layouts that provide a consistent user interface make learning how to use MMCs and snap-ins relatively easy.

k) How does the systems administrator get to most administrative tool MMCs?

By following the sequence of “start,” then “programs,” and finally “administration tools”

l) What does selecting *Action* do?

It shows the actions that the administrator can take on the selected object.

UNIX (Including LINUX) Servers

4. a) Why is UNIX systems security difficult to describe generally?

UNIX consists of a family of OSs that are similar in that they are compatible at the kernel level, but differ in other aspects of implementing the OS, such as implementing system security. Thus, there is no standard UNIX system security setting; each OS has its own baseline.

b) Distinguish between UNIX and Linux.

UNIX is a family of OSs that share interoperability at the kernel level. Linux is a specific operating system kernel used in many PCs because of its price (free).

c) What is the LINUX kernel?

The Linux kernel is the core part of the operating system, upon which LINUX vendors provide additional software for sale or as free downloads.

d) What is a LINUX distribution?

Linux distribution consists of the Linux kernel packaged by vendors with additional programs for added functionality. Often these additional packages are created by the GNU project for free, but are packed and sold for a profit by enterprising capitalists.

e) Comment on the cost of Linux.

The purchase price of a Linux distribution is free or almost free. However, Total Cost of Ownership (TCO) for Linux can be considerable, especially if there are multiple varieties of Linux in use on a network that requires product-specific knowledge to operate and secure.

f) Does a particular version of UNIX have a single user interface?

No. Even within a specific version of UNIX, the operating system software may come with several alternative user interfaces. Some of these interfaces will be graphical user interfaces (GUIs) similar to the interface of Microsoft Windows. On Linux, there are two popular GUIs: Gnome and KDE.

g) What are UNIX CLIs called?

UNIX’s command line interfaces are called shells.

h) How are CLIs beneficial?

CLI shells use fewer resources than GUIs, so they place lower processing burdens on the computer than GUIs.

i) Why are CLIs difficult to use?

They are difficult to use because the CLIs in UNIX are picky with syntax and spacing.

Vulnerabilities and Patches

Vulnerabilities and Exploits

5. a) What is a vulnerability?

Vulnerabilities are security weaknesses that open a program to attack.

b) What is an exploit?

An exploit is a program that takes advantage of a vulnerability to allow the attacker to take over the computer or at least an individual account.

c) What is a zero-day attack?

Attacks that come before fixes are released are called zero-day attacks.

d) Why is the quick application of critical fixes important?

Because attackers usually exploit the vulnerability soon *after* a fix is released by a vendor

Fixes

6. a) List the four types of fixes for vulnerabilities.

The four types of fixes for vulnerabilities are work-arounds, patches, service packs, and version upgrades.

b) Distinguish between work-arounds and patches.

Work-arounds are labor-intensive processes of manual steps that system administrators must take to address a vulnerability. Patches are small programs that fix a particular vulnerability. Patches fix the problem by adjusting system configuration (as with work-arounds).

c) What is a service pack in Microsoft Windows?

These are vulnerability fixes and sometimes functionality improvements together in a single, large update.

d) Why is upgrading to a new version of an operating system usually good for security?

Security problems are corrected in newer versions and, in general, each newer version of an operating system has improved security. In addition, if a version is too old, the vendor will stop creating fixes for it.

The Mechanics of Patch Installation

7. a) In Windows Server 2003 and 2008, how automatic can patching be?

Windows Server 2003 has updating on the main start menu.

Windows Server 2008 can do updating automatically.

b) What patch downloading method is commonly used in Linux?

Many Linux vendors follow the rpm method created by Red Hat for downloading patches.

Problems with Patching

8. a) Why do firms have a difficult time applying patches?

Firms have a difficult time because firms use many application programs and vendors release many patches per product. In contrast, they only use a few operating system versions.

b) Why do many firms prioritize patches?

Firms prioritize patches by criticality. Some patches may not apply if risk analysis does not justify it.

c) How do patch management servers help?

Patch management servers help by learning what software a firm is using on its network, actively assessing which programs on specific hosts need to be patched, and then pushing the patches to the hosts. Patch management servers can greatly reduce patching costs.

d) What two risks does patching raise?

The two risks of patching are: (1) the loss of functionality due to implementing a patch, and (2) the negative impact of some patches on host system performance.

Managing Users and Groups

The Importance of Groups in Security Management

9. Give two reasons why assigning security measures to groups is better than assigning security measures to individuals within groups.

Applying security measures to groups takes less time than assigning them individually (and thus is cheaper).

Applying security measures in groups reduces errors in assigning security settings because group permissions are fairly obvious compared to individual permissions.

Creating and Managing Users and Groups in Windows

10. a) What Windows snap-in is used to manage users and groups?

It is the Local Users and Group snap-in.

b) On which MMC is this snap-in available?

This snap-in is available in the computer management snap-in.

c) In this snap-in, if the administrator clicks on an account, what may he or she do?

The administrator will be able to rename the account, delete it, change its security properties, or take other actions.

d) How does the administrator create a new account?

Administrators create new accounts by using the Action command, and entering a name, password, and other information about the account.

e) How does an administrator add an account to a group?

The administrator can select the group section instead of the user section and, from there, the administrator will be able to add an account to the group.

f) How does the administrator create a new group?

In the group sections

11. a) What privileges does the super user account have?

The super user has full access to anything on the computer. The owner of the super user account can see or do anything on the computer.

b) What is the super user account in Windows?

The super user account in Windows is called “Administrator.”

c) What is the super user account in UNIX?

It is called “root.”

d) What is hacking root, and why is it desirable to hackers?

Hacking root is taking over that super user account. This is desirable because the attacker can do whatever he or she wants with this type of account.

e) When should a Windows systems administrators use the Administrator account?

Administrator accounts should be used sparingly, and only for circumstances that merit full privileges to accomplish a task.

f) How does the administrator get to the super user account in Windows? In UNIX?

In Windows, run the RunAs command to switch to and from the super user account. In UNIX, the administrator accesses the super user account via a CLI, using the su command.

Managing Permissions

Permissions

Assigning Permissions in Windows

12. a) How are permissions applied to a directory in Windows?

Permission are applied to a directory in Windows by right clicking on File or Directory in My Computer or Windows Explorer. Then select Properties, then the Security tab. Then select User or Group and click on or off the 6 standard permissions (permit or deny).

b) List each standard Windows privilege and explain it briefly.

They are full control, modify, read & execute, list folder contents, read, and write.

c) To how many accounts and groups can different permissions be applied in Windows?

There is no limit to the number of accounts and groups that can have different permissions applied.

d) How can inheritance reduce labor costs in assigning permissions?

Inheritance reduces labor costs in assigning permissions by receiving permissions from the parent directory. This eliminates a process of permissions being assigned by inheritance individually.

e) How can inheritance be modified?

Inheritance can be modified from the Allow permissions and the Deny permissions selections in the Security tab.

f) How are a user’s effective permissions calculated for a directory?

User’s effective permissions are all those inherited from its parent directory *plus* any specifically allowed permission, minus those removed.

g) How would you set up a top-level directory for a firm’s public policy documents, which should be readable by all logged-in users?

At the top-level directory (i.e., public programs), assign the group called “all logged in users” read permissions.

Assigning Groups and Permissions in UNIX

13. a) What are the three UNIX permissions?

The three UNIX permissions are read, write, and execute.

b) Briefly characterize each.

Read gives the permission to read only.

Write gives permission to make changes.

Execute permits the execution of programs.

c) Compare the number of UNIX directory and file permissions with that of Windows.

UNIX allows only three directory permissions, while Windows allows six primary directory permissions and 13 specialized permissions.

d) To which three individual accounts or groups can permissions be assigned for a particular directory in UNIX?

They are the account owner, a single group, and all other accounts.

e) How does the number of accounts or groups to which permissions can be assigned in UNIX compare with that of Windows?

UNIX allows permissions to be assigned to three groups/accounts. Windows can give permissions to an unlimited number of individual accounts and groups.

14. a) What is brute-force password guessing?

Brute-force password guessing is an approach that tries all possible passwords on all (or selected) accounts. This approach tries all possible single-character passwords, then all possible two-character passwords, and so forth.

b) Why is it important to not simply use all lowercase letters in passwords?

It is important to not simply use all lowercase letters in passwords because that limits the possible characters in a password to only 26 (the alphabet). Thus, the possible combinations are 26^N (N = password length), much less than if all characters on a keyboard are used (75^N combinations).

c) What are complex passwords?

Complex passwords are passwords that use several types of keyboard characters—upper and lowercase letters, digits, and special characters.

d) Why is password length important?

Longer passwords take much more time to crack than shorter passwords.

e) What is a dictionary attack?

A dictionary attack is an attack that compares passwords to lists of common words.

f) Why are dictionary attacks faster than brute-force guessing?

They only have to try a few thousand passwords, instead of millions or billions.

g) What are hybrid dictionary attacks?

Hybrid dictionary attacks try simple modifications of common words (such as Password!).

h) How are mangling rules applied to list of dictionary words?

Mangling rules are applied to each word in sequence. Each mangling rule modifies the dictionary word in order to make a possible password match. Mangling rules are created, and based on, common password patterns.

15. a) What are rainbow tables?

A rainbow table is a list of pre-computed password hashes that are indexed in an attempt to reduce the amount of time it takes to crack a password.

b) How would rainbow tables reduce the time needed to crack a password?

Indexed lists of password hashes are created from large dictionary files, or all possible combinations of characters. This results in a time–memory trade-off where more memory is used to store the pre-computed password hashes, but the time it takes to crack a password is greatly reduced.

c) Would it be possible to create rainbow tables for all possible passwords with 1–20 characters? Would it be practical?

It would be technically possible to create the table. However, the number of possible combinations of known characters for a password consisting of 20 characters would be so large that the table would be practically impossible to create.

16. a) Can you create a truly random password? Will it be used?

Yes, you can create very long, truly random passwords. The downside of completely random passwords is that users find them hard to remember. Users tend not to use passwords that are hard to remember.

b) Should passwords be tested by systems administrators? Why?

Internal corporate passwords should be tested by systems administrators to ensure that each user is using a sufficiently strong password. Users with weak passwords should be directed to change their password to a stronger password.

17. a) What do Trojan horse password capture programs do?

They capture passwords when the user types them.

b) Can antivirus software detect keystroke capture software?

Yes, some antivirus software can detect certain keyloggers, but not all keyloggers. The keystroke software must be included in the list of virus signatures for it to be identified by the antivirus software.

c) How would you detect a physical keylogger?

In order to detect a physical keylogger, you would have to physically inspect your computer.

d) What is shoulder surfing?

Watching someone while they type passwords in order to learn the password.

e) Does the shoulder surfer have to read the entire password to be successful? Explain.

Shoulder surfers do not have to read the entire password to be successful. Just finding out some of the characteristics of the password, such as first/last letters, total number of characters, and whether special characters are used, makes cracking the password significantly easier as it narrows the possible range of password characteristics to be checked in a brute-force attack.

Testing for Vulnerabilities

168. a) Why is vulnerability testing desirable?

Vulnerability testing is desirable because it allows network administrators to identify problems before attackers can exploit them.

b) What two things does vulnerability testing software do?

Vulnerability software runs a battery of attacks and generates reports detailing the vulnerabilities found.

c) Why is it important to get approval in writing before conducting a vulnerability test?

It is important to get approval in writing before conducting a vulnerability test because testing does occasionally cause system crashes and other damage, and the tester should be covered against repercussions.

d) What two things should this written approval specifically mention?

The written approval should specifically mention a detailed description of what will be done, along with a mention that the tester will not be held liable for system degradation from the testing.

e) Why is it important never to diverge from the test plan when running the tests?

One should never diverge from the test plan while running tests because once you diverge, all protections provided by the test plan are negated and you can be held liable for the consequences.

Windows Client PC Security

Client PC Security Baselines

19. What different baselines does a company need for its client PCs?

A company needs security baselines for Windows XP, Vista, and Windows 7. A firm also needs security baselines for its Macintosh and UNIX desktop computers. In addition, for each client operating system, a firm may have multiple baselines, such as for desktop versus laptop computers, for in-site versus external computers, and for regular clients versus computers with especially high security needs.

The Windows Security Center

20. a) How can you quickly assess the security posture of your Windows PC?

The Windows Security Center allows a user to quickly assess the security posture of a Windows PC.

b) What provides a quick summary of security components needed to harden a client PC?

The Windows Action Center provides a quick summary of all the security components needed to harden a client PC.

c) Why are multiple types of protection necessary?

Multiple types of protection work together to provide defense in depth and protection from a variety of threats.

Windows Firewall

21. a) What SPI firewall has come with client version of Windows since Windows XP SP2?

It is called Windows Firewall. This SPI firewall has been included in all subsequent client versions of Windows.

b) What improvements come with Windows Firewall with Advanced Security?

Windows Firewall with Advanced Security comes with additional functionality such as custom ingress/egress rules, separate network profiles, more detailed rules, and the ability to be managed via group policy.

Automatic Updates

22. Why should updating be done completely automatically on client PCs?

Due to the shortening time between patch release and widespread use of exploits for unpatched vulnerabilities, client PCs should be configured for automatic updates.

Antivirus and Spyware Protection

23. What can go wrong with antivirus protection?

Common problems with antivirus protections include users turning off the AV program, automatic updates of virus signatures that can be inadvertently turned off, and the virus program contract that may expire with no new updates coming.

Implementing Security Policy

24. a) Why is it important to implement security policy?

It is important to implement security policies because they protect computing resources. They also help minimize corporate liability and legal compliance.

b) What are the advantages of implementing password policies?

Implementing these password policies increases the effectiveness of passwords as an access control mechanism.

c) What are the advantages of implementing account policies?

Properly implemented account policies can stop certain attacks. For example, an account policy could prevent attackers from endlessly trying to guess a user’s password if the account were locked after a given number of attempts.

d) What are the advantages of implementing audit policies?

Audit policies provide systems administrators with detailed information about who caused events to occur, what they may have changed, and when the event occurred.

Protecting Notebook Computers

25. a) What are the three dangers created by notebook computer loss or theft?

The three dangers of notebook computer loss are (1) loss of capital investment, (2) loss of all data that was not backed up, and (3) loss of sensitive data.

b) When should backup be done for mobile computers?

Mobile computers should be backed up before being taken offsite and then regularly while offsite.

c) What four policies are necessary to protect sensitive information?

Limit what sensitive data can be stored on mobile PCs.

Encryption is required on all mobile PCs regardless of data content.

All mobile PCs should be protected with strong passwords, biometrics, or both.

Audit the first three policies.

d) To what should these policies be applied?

The above policies should be applied to all mobile data on notebook hard drives, USB RAM drives, MP3 players, and mobile phones that store company data.

e) What training should be provided?

The type of training that should be provided is to teach users loss and theft protection techniques.

f) What does computer recovery software do?

This software will contact the recovery company the next time the computer connects to the Internet so the recovery company can contact the local police to recover the software.

Centralized PC Security Management

26. a) Why is central PC security management desirable?

Central PC security management is desirable because ordinary users lack the knowledge to manage security on their PCs, they sometimes knowingly violate security policies, and it can often reduce cost through automation.

b) Why are standard configurations attractive?

Standard configurations are attractive because they reduce PC troubleshooting and general maintenance while affording the best control over system security configuration.

c) What does NAC do when a computer attempts to connect to the network?

NAC queries the PC for information present in the Windows Security Center to determine if all updates are current, AV is loaded, and other items.

d) If a PC fails its initial health assessment, what are a NAC system’s two options?

NAC’s two options are to forbid access or provide access to a remediation server in order to fix the security issues.

e) Does NAC control usually stop after access is granted?

After access is granted, the NAC will perform ongoing traffic monitoring. If the traffic after admissions indicates malware on the client, the NAC will drop or remediate.

f) What things can Windows GPOs restrict?

Windows GPOs can restrict PCs from changing standard configurations and other important policies.

g) Why are Windows GPOs powerful tools for managing security on individual Windows PCs?

GPOs are powerful tools because they can maintain a high security standard on client PCs.

Application Security

General Application Security Issues

Executing Commands with the Privileges of a Compromised Application

1. a) What can hackers gain by taking over application programs?

They get the privileges of the application program they take over.

b) What is the most popular way for hackers to take over hosts?

By taking over an application with root privileges

Buffer Overflow Attacks

2. a) What is a buffer?

A temporary storage area in memory

b) What is a buffer overflow attack?

An attack that writes data longer than the space allocated for it in the buffer.

c) What impacts can buffer overflows have?

The impact of a buffer overflow can range from nothing to the crashing of the server, or the ability to execute any command on the server.

d) In a stack overflow, what is overwritten by the overflow?

The return address in a stack is overwritten in a stack overflow.

e) To where does the overwritten return address point?

The overwritten address will point to data in the buffer, which will actually be program/attack code that will be executed instead of legitimate code.

f) In the IIS IPP buffer overflow attack, what buffer is overflowed?

The host to which the request should go is overflowed. The host name is replaced with a 420-character string that causes a buffer overflow.

Few Operating Systems, Many Applications

3. Why is patching applications more time consuming than patching operating systems?

There are many more applications compared to only one OS, and finding information about application vulnerabilities takes a lot of time.

Hardening Applications

4. a) Why must you know a server’s role to know how to protect it?

Knowing what a server is meant to do allows you to determine what services must be kept on, and all others can be disallowed.

b) Why is it important to minimize both main applications and subsidiary applications?

The few applications you have, the fewer security risks there will be.

c) Why are security baselines needed for installing applications?

A complex series of actions is needed for any major application. This requires the checklist of a security baseline.

d) Why is it important to minimize permissions for application programs?

Application permissions must be minimized because if a hacker takes over an application, he or she can take over the entire host if the permissions are too great.

e) Why is application-level authentication superior to operating system authentication?

Application-level authentication is superior because it requires the hacker to not only have an exploit, but also authenticated access to a server (versus just an exploit).

f) Why should cryptographic protections be used?

To prevent eavesdropping by unauthorized people

5. a) How does a SQL injection attack work?

A SQL injection attack works by manipulating the way database parameters are processed. Malformed parameters are passed via a web interface to be processed by a database. The malformed parameters allow an attacker to extract data, shut down a database, or perform a variety of database functions.

b) What is SQL?

SQL is a query language used to extract, insert, or delete data from a database.

c) What is error-based inference?

Error-based inference is used by attackers to manipulate a database based on the errors returned when commands are submitted.

d) What is the difference between in-band and out-of-band SQL injection?

In-band SQL injection extracts data directly from the database and displays it in a web browser. Out-of-band SQL injection uses malformed statements to extract data through a different application, such as e-mail.

e) What is blind SQL injection?

Blind SQL injection uses a series of SQL statements that produce different responses based on true/false questions, or timed responses.

f) How can SQL injection be prevented?

Threats from SQL injection can be mitigated by “parameterizing” queries and sanitizing inputs.

Securing Custom Applications

6. a) What is a login screen bypass attack?

In a login screen bypass attack, the attacker bypasses the login page by typing a URL for a page beyond the login screen.

b) What is a cross-site scripting (XSS) attack?

An XSS attack is one in which some input is echoed back in the form of information on a webpage. If a script can be put into the original input, this script will be executed when it is sent back to the user.

c) What is an SQL injection attack?

SQL injection attacks occur when an attacker enters a string that includes the user’s info and another SQL query. When the program enters the input string in the SQL query, it may execute both the user’s and attacker’s query, providing info the attacker should not have (such as bank account routing info).

d) What attitude should programmers have about user input?

Programmers should never trust user input. Input should be checked to make sure it does not contain anything a valid user would not enter.

e) What training should programmers who do custom programming have?

Programmers need to be trained in secure programming both in general and for their particular language and application.

WWW and E-Commerce Security

The Importance of WWW and E-Commerce Security

7. What risks do webservice and e-commerce service create for corporations?

Attacks can disrupt service, harm a company’s reputation, and expose private information with heavy repercussions to the firm. They can also enable customer fraud against the firm to succeed more effectively.

WWW Service versus E-Commerce Service

8. a) Distinguish between WWW service and e-commerce service.

E-commerce adds functionality to webservice.

b) What kinds of external access are needed for e-commerce?

An e-commerce server needs to have network access to a number of systems external to itself, including servers within firms (for order entry, accounting, shipping, and so forth) and servers outside the firm in merchant banks and companies that check credit card numbers for validity. The webmaster or e-commerce master often has no control over the security of other systems.

c) Does the webmaster or e-commerce administrator have control over the security of other servers?

Neither the webmaster nor e-commerce administrator have control over the security of other systems outside their purview.

d) Why are custom programs especially vulnerable?

Custom programs offer security through obscurity, but because they are often not programmed securely, hackers have automated tools that can find common exploits (such as buffer overflows) to allow them to attack the application.

Some Webserver Attacks

9. a) What is website defacement?

Changing the contents of a webpage

b) Why is it damaging?

It may be embarrassing to the company.

c) In directory access commands and URLs, what does “..” represent?

It means move to the parent of the current directory.

d) What are directory traversal attacks?

Attacks in which a user reaches a directory outside of the WWW root directory and its subdirectories

e) Create a URL to retrieve the file aurigemma.htm under the rainbow directory on the host www.pukanui.com. The WWW root is three levels below the system’s true root directory and the rainbow directory, which is under the projects directory, which is directly under the root directory. (Hint: Draw a picture.)

http://www.pukanui.com/../../projects/rainbow/aurigemma.htm

f) In what two ways have attackers circumvented filtering designed to stop directory traversal attacks?

Hackers have used hexadecimal and Unicode character sets to enter the value for the “..” characters to be executed.

Patching the Webserver and E-Commerce Software and Its Components

Other Website Protections

10. a) What software must be patched on an e-commerce server?

The webserver, the e-commerce server, and subsidiary programs must all be up-to-date on their patches.

b) What three other webserver protections were mentioned in the text?

The three other webserver protections mentioned in the text were (1) website vulnerability assessment tools, like Whisker, (2) reading website error logs, and (3) using a webserver proxy in front of the webserver.

c) Where is an application proxy firewall placed relative to the webserver?

Application proxy firewalls would be placed in front of the webserver, between the webserver and the border router.

Controlling Deployment

11. a) In staged development, what three servers do companies use?

A development server, a testing server, and a production server

b) What permissions does the developer have on the development server?

Developers get extensive permissions on the development server.

c) On the testing server?

Developers get no permissions on the testing server.

d) On the production server?

Developers get no permissions on the production server.

e) On what servers does the tester have access permissions?

The tester should only have access to the test servers.

Browser Attacks

12. a) Why do hackers attack browsers?

Attackers might want to have data stored on the client, and attackers can use a compromised client to attack other systems for which the client has access credentials.

b) What is mobile code?

Mobile code consists of commands written into a webpage that are downloaded when the page is visited.

c) Why is it called mobile code?

It is called mobile code because the code travels from the webpage to the client to execute.

d) What is a client-side script?

A client-side script is code that is written to execute on the client PC, allowing the attacker access to the PC.

e) What is a Java applet?

A Java applet is a small program written in the Java language. The Java applet is downloaded into a webpage.

f) Why is Active-X dangerous?

Active-X is dangerous because it has significant permissions on the machine. If a hacker writes in Active-X, it could compromise the PC easily.

g) How do scripting languages compare to full programming languages?

They are simpler and more limited.

h) Is JavaScript a scripted form of Java?

No

13. a) Why is it bad to go to a malicious website?

Malicious websites can have attack scripts that automatically load an executable on a PC, which is bad.

b) How can social engineering be used to trick a victim to go to a malicious website?

Hackers can send messages saying something bad (or good) has happened and directs you to a malicious website.

c) Why do attackers want to get domain names such as micosoft.com?

Common misspellings of legitimate websites will naturally draw users. Once at the site, the malicious websites can download mobile code to attack the PC.

d) Why may malware that allows an attacker to execute a single command on a user’s computer not really be limited to executing a single command?

Malware that allows an attacker to execute a single command may be used to initiate another program that provides much greater PC access (such as a command shell).

e) What may happen on a compromised computer if a user mistypes the host name in a URL?

Mistyping a URL may send a user to a malicious website, where hostile mobile code is waiting to attack your PC.

f) What dangers do cookies create?

Cookies can be used to track a user’s activity, which could violate privacy. Cookies can also hold PII.

Enhancing Browser Security

14. a) What can users do to enhance browser security?

Ensure patches are installed and upgrade the software when updates are available.

b) Under Internet Options in IE, what can the user do on the Security tab?

The user can select the general security settings for general, intranet, trusted, and restricted websites.

c) What are your computer’s settings for the four zones?

Answers will vary.

d) In which tab are cookies controlled?

Cookies are controlled under the Privacy tab.

E-Mail Security

E-Mail Content Filtering

15. a) Why are HTML bodies in e-mail messages dangerous?

HTML can contain malicious scripts.

b) What is spam?

Spam is unsolicited commercial email.

c) What three problems does spam create?

Spam clogs mailboxes, slows user computers, and annoys users by requiring them to spend time deleting the unwanted messages.

d) Why is spam filtering dangerous?

Spam filtering is dangerous because valid email will eventually be affected.

e) For what legal reason should companies filter sexually or racially harassing message content?

Filtering explicit message content shows that the company does not tolerate this type of action and tries to stop it. (In case of lawsuits, this may help.)

f) What is extrusion prevention?

Preventing certain information from leaving the company

g) Why is extrusion prevention needed for intellectual property?

It prevents the loss of trade secrets.

h) What is PII, and why must it be prevented from leaving the firm?

PII is Personally Identifiable Information (such as SSN, date of birth, address, etc.) that must be prevented from leaving a firm in order to avoid lawsuits related to identify theft or credit card theft.

E-Mail Encryption

16. a) Is encryption widely used in e-mail?

Encryption is not widely used in email because of the difficulties of end-to-end encryption systems.

b) What part of the e-mail process does SSL/TLS usually secure?

SSL/TLS usually only secures the transmission of email from the client to the server.

c) Is this end-to-end security? Explain.

This is not end-to-end security because unless all other links in the path are encrypted (such as between mail servers, and the POP3/IMAP connection from mail server to end user client application), there is no end-to-end security.

d) What standards provide end-to-end security?

S/MIME and PGP provide end-to-end security.

e) Compare PGP and S/MIME in terms of how applicants learn the true party’s public key.

S/MIME uses the traditional PKI to share keys. In PGP, keys are shared via circles of trust.

f) Describe the advantages and disadvantages of each approach.

Using PKI offers the strongest security, but it is labor-intensive and can be expensive to get key pairs issued to all participants. PGP is cheaper, but the possibility of misplacing trust and having bogus public key/name pairs is high. Thus, PKI has been used in corporate environments, while PGP is primarily used in person-to-person communications.

Voice over IP (VoIP) Security

Sending Voice between Phones

17. a) What is VoIP?

Voice over IP, or VoIP, is the digitization of voice and its transmission over a data network.

b) Distinguish between IP telephones and soft phones.

IP telephones are telephones that contain everything needed to attach to a VoIP network.

A soft phone is a computer with hardware and software for VoIP.

c) List in order of appearance at the receiver, the headers and message of a packet carrying voice between phones.

IP header

UDP header

RTP header

Codec byte stream

d) What does RTP add to compensate for the limitations of UDP?

RTP adds sequence numbers (for in-order delivery) and time stamps (to control jitter).

Transport and Signaling

18. a) Distinguish between transport and signaling.

In transport, data/voice is sent. In signaling, the parameters for the communication channel are determined, configured, and managed.

b) In Figure 8-25, is the packet shown a transport packet or a signaling packet?

The packet shown is a transport packet because it contains the Codec byte stream.

c) What are the two main signaling standards in VoIP?

SIP and H.323

d) What does the registrar server do? (Hint: Don’t say, “It registers things.”)

The registrar server adds the user and his location to the registration database for proxy servers to use to route calls.

e) What type of SIP message does a VoIP phone use when it wants to connect to another VoIP phone?

First, the caller’s phone sends a SIP INVITE message to the caller’s own SIP proxy server.

f) How is this message routed to the called VoIP phone?

The caller’s proxy server checks the IP telephone’s registration information, then contacts a proxy server on the destination end. The destination proxy passes the INVITE to the called VoIP phone.

g) Are SIP proxy servers involved during transport transmissions? Explain.

No, SIP proxy servers are only used in signaling.

h) What two types of communication does the media gateway translate between the VoIP network and the PSTN?

It translates between both signaling and transport standards.

VoIP Threats

19. a) What is eavesdropping?

Listening in on another’s conversations

b) Why can DoS attacks be successful even if they only increase latency slightly?

By increasing latency, DoS attacks can severely degrade the performance of VoIP systems, making them almost unusable.

c) Why is caller impersonation especially dangerous in VoIP?

VoIP caller impersonations can provide spoofed credentials, making the impersonation seem more realistic.

d) Why are hacking and malware dangerous in VoIP?

As with all applications, hacking and malware can render VoIP completely vulnerable to the attacker, where they can issue commands, such as SIP BYE, when they want to disrupt service or re-route data.

e) What is toll fraud?

Toll fraud is when someone breaks into a corporate VoIP system to make free long distance calls.

f) What is SPIT?

Spam over IP Telephony

g) Why is SPIT more disruptive than e-mail SPAM?

Unlike e-mail spam, which you only get when you read e-mail, SPIT causes your phone to ring, annoying you directly.

Implementing VoIP Security

20. a) What authentication mechanisms are common on IP telephones?

SIP Identity protocols authenticate across second-level domains, increasing authentication between companies.

b) What does SIP Identity ensure?

SIP Identity ensures that traffic is authenticated between two companies holding public/private keys.

c) How can eavesdropping be thwarted?

Eavesdropping can be thwarted by encrypting both transport and signaling traffic.

d) What sound quality problem may encryption create?

Encryption adds a small delay, which may impact performance.

e) Why do firewalls have problems with typical VoIP traffic?

Firewalls don’t like VoIP traffic because the packets are small, there are lots of them, they cannot be appreciably delayed to minimize latency, and they use multiple ports for signaling and transport.

f) For SIP signaling, what port has to be opened on firewalls?

SIP signaling requires port 5060 to be open.

g) Describe firewall port openings for VoIP transport.

Firewall port openings are required for SIP/H.323 messages. Additionally, the firewall must read these messages in order to open the transport ports.

h) Why is NAT traversal problematic?

NAT adds latency to VoIP packets, and VoIP relies on IP addresses between participants; using NAT may break the VoIP protocol being used.

i) How are VLANs useful in VoIP?

Placing VoIP on a separate VLAN makes it difficult for attackers to come through the data side of the network to hack VoIP, and vice versa. It also helps to reduce traffic on the network for the data side.

The Skype VoIP Service

21. a) What is Skype?

Skype is a VoIP service that currently offers free calling among Skype customers over the Internet and reduced-cost calling to and from Public Switched Telephone Network customers.

b) Why is Skype’s use of proprietary software problematic?

Skype’s use of proprietary software is problematic because Skype uses proprietary software and protocols that have not been studied by security professionals. This causes security professionals to be concerned with the existence of vulnerabilities, backdoors, and other security threats.

c) What problem is there with Skype’s encryption for confidentiality?

The problem with Skype’s encryption for confidentiality is that its method is unknown. Worse yet, Skype controls the encryption keys so that it can read traffic if it wants.

d) Does Skype control who can register a particular person’s name?

No, an attacker can use another person’s name and impersonate him or her. Skype initial registration is open and uncontrolled.

e) Why do firewalls have a difficult time controlling Skype?

Firewalls have a difficult time controlling Skype because Skype protocol is unknown and changes frequently to avoid analysis. Skype uses its structure to help users communicate through NAT firewalls. This is good for the user but bad for corporate security.

f) Does Skype’s file transfer generally work with antivirus programs?

No, Skype’s file transfer generally does not work with antivirus programs.

g) Overall, what is the big problem with Skype?

Although Skype concerns are theoretical, the fact that Skype cannot be well controlled by corporate security policies makes it unacceptable in many firms.

Other User Applications

Instant Messaging (IM)

22. a) In IM, what does a presence server do?

Presence servers allow two users to locate each other.

b) What does a relay server do?

Relay servers have all messages pass through them, allowing filtering and recording.

c) For corporate IM, what are the advantages of using a relay server instead of only a presence server?

Using a relay server allows the company to report IM messages to satisfy legal retention and other compliance regulations.

TCP/IP Supervisory Applications

23. a) What is the Danvers Doctrine?

The general thrust by the IETF to add strong security to all or nearly all of its standards

b) Distinguish between security in SNMP V1 and security in SNMP V2.

SNMP v1 had no security at all. SNMP v2 introduces community strings in which a shared secret between manager and managed devices was used to authenticate messages. However, the same secret was used on all devices, making it easy to crack and lose control of the secret. Also, the secret is sent in the clear, making it vulnerable to network sniffers.

c) Distinguish between security in SNMP V2 and security in SNMP V3.

SNMP v2 security, consisting of community strings, was an improvement over SNMP v1, but still very inadequate. SNMP v3 added individual secrets shared between manager and devices for authentication. SNMP v3 also added confidentiality, message integrity, and time stamps to guard against replay attacks.

d) What still needs to be done for SNMP security?

Future versions of SNMP should include a public-key implementation to provide strongest cryptographic controls for authentication, confidentiality, and message integrity.

Incident and Disaster Response

Answer Key

Introduction

Walmart and Hurricane Katrina

1. a) Why was Walmart able to respond quickly?

Walmart was able to respond quickly because it had a disaster preparedness mechanism in place that was well established and operationally proficient. They had detailed business continuity plans, a full time staff, a crises command center, and an economic need to get back into business as soon as possible.

b) List at least three actions that Walmart took that you might not have thought of.

Three actions that Walmart took that students might not have thought of include sending additional security personnel to stores in preparation for possible looting, providing meals, ammunition, etc. to local law enforcement for free, and ordering 40 emergency power generators for stores that lacked them. Additional actions may include:

Walmart sent out bleach and mops to its stores.

Walmart sent ammunition and protective gear to police and relief workers.

Walmart developed a business continuity center that specializes in disaster planning.

Incidents Happen

2. a) Can good planning and protection eliminate security incidents?

No amount of planning can eliminate security incidents, but good planning can provide a baseline to build from in order to recover quickly.

b) Name three terms that successful attacks are commonly called?

Successful attacks are commonly called security incidences, breaches, and compromises.

Incident Severity

3. a) What are the four severity levels of incidents?

The four severity levels of incidents are false alarms, minor incidents, major incidents, and disasters.

b) What is the purpose of a CSIRT?

The purpose of a CSIRT is to respond to severe computer security incidents with impacts that are too large for the on-duty IT staff to handle.

c) From what parts of the firm do its members come?

CSIRT members come from legal, PR, IT, and senior management.

d) What is business continuity?

Business continuity is the maintenance of the day-to-day revenue generating operations of the firm.

e) Who should head the business continuity team?

A senior manager should head the business continuity team.

Speed and Accuracy

4. a) Why is speed of response important?

Speed of response is important because it can reduce damage. The attacker/s will have less time to do damage, and they cannot burrow as deeply into the system and become very difficult to detect. In these ways, speed is necessary for a more complete recovery.

b) Why is accuracy of response important?

Accuracy of response is equally as important as speed. It is a common mistake to act on incorrect assumptions. If the problem is misdiagnosed or the wrong approach is taken, things can get much worse.

c) Define incident response in terms of planning.

Incident response means reacting to incidents according to plan.

d) Why are rehearsals important?

Rehearsals improve speed and accuracy. Rehearsals are critical because no plan is useful until it is tested to find out its faults in implementation.

e) What is a walkthrough or table-top exercise?

A walkthrough or table-top exercise is when managers and other key personnel get together and discuss, step by step, what each will do during an incident. These involve people from many departments.

f) Why is a live test better?

Live tests are better than walkthroughs because live tests reveal subtleties that walkthroughs may miss or may not be able to address.

g) What is the problem with live tests?

The problem with live tests is that they are very expensive.

The Intrusion Response Process for Major Incidents

Detection, Analysis, and Escalation

5. a) Distinguish between detection and analysis.

Detection is learning that an incident has occurred. Analysis is a deeper understanding of the incident needed to determine its potential damage and gather information to begin containment and recovery.

b) Why is good analysis important for the later stages of handling an attack?

When proper analysis is done and gives good information, the company can proceed effectively through later stages of handling an attack.

c) What is escalation?

Escalation means passing the incident up to the CSIRT or business continuity team.

Containment

6. a) What is containment?

Containment means stopping the damage.

b) Why is disconnection undesirable?

Disconnection is undesirable because it prevents legitimate business users from getting to a necessary server, which amounts to lost revenue.

c) What is black holing?

Black holing the attacker’s IP address means to drop all future packets from that IP address.

d) Why may it only be a temporary containment solution?

Black holing is usually only effective against attacks from amateur hackers who do not have the resources to use bots or other agents to continue an attack.

e) Why might a company allow an attacker to continue working in the system for a brief period of time?

A company may allow an attacker to continue working in a system for a brief period of time in order to collect data on what the attacker is doing and/or collect evidence for prosecution.

f) Why is this dangerous?

The longer attackers are in a system, the more invisible they become through the deletion of IDS logs, and the more backdoors and other damage the attackers can create.

g) Who should make decisions about letting an attack continue or disconnecting an important system?

Senior business executives should make the decision whether to let an attack continue.

Recovery

7. a) What are the three major recovery options?

1. Repair during continuing server operation

2. Restoration from backup tapes

3. Total software reinstallation

b) For what two reasons is repair during continuing operation good?

Repair during continuing server operation might be good because doing this on a server with a critical function keeps those services available to users. It also means that no data is lost because there is no need to resort to backup tapes, which only contain information since the last backup.

c) Why may it not work?

Unfortunately, it is very difficult to root out all of the Trojan horses, registry entries, rootkits, and other unpleasant surprises planted by an attacker. For a virus or worm attack, there are programs that remove the specific artifacts created by the specific attack. For handcrafted break-ins, however, there is no general detection program, leaving a strong concern that “we may have missed one.”

d) Why is the restoration of *data* files from backup tapes undesirable?

Restoration of data files from tapes takes a long time and data collected after the last backup will be lost.

e) What are the potential problems with total software reinstallation?

Total software reinstallation does not address lost data since the last backup and the software will have to be re-baselined to proper security, which is a time consuming process.

f) How does having a disk image reduce the problems of total software reinstallation?

Disk imaging reduces the problem of having to re-baseline the system to proper security levels.

Apology

8. What are the three rules for apologies?

The three rules for apologies are acknowledge responsibility and harm, explain what happened, and explain what action will be taken to compensate, if any.

Punishment

9. a) Is it easier to punish employees or to prosecute outside attackers?

It is easier to punish employees than to prosecute outside attackers.

b) Why do companies often not prosecute attackers?

Companies do not often prosecute attackers because prosecutions are expensive, with a low probability of success. There is also the possible loss of reputation from a public prosecution, showing that the company could not prevent the attack in the first place, which is made worse if they lose the case.

c) What is forensics evidence? Contrast what cybercrimes the FBI and local police investigate.

Forensic evidence is evidence that is acceptable for court proceedings. The FBI mostly investigates matters of interstate commerce. Local police investigate violations of local and state laws.

d) Why should both be called?

Both should be called because one or both may have jurisdiction based on the circumstances of the incident.

e) Under what conditions will you need to hire a forensics expert?

In civil lawsuits, the company must use a certified forensics expert to collect data and interpret it in court. If it attempts to collect evidence on its own, the evidence will probably not be permissible in court.

f) Why should you hire a forensics expert rather than doing your own investigation?

A forensic expert should be hired because they are experts in the field and know how best to handle evidence once detected. Also, they are allowed to give interpretative testimony.

g) What is the chain of evidence, and why is documenting it important?

Chain of evidence is the documented history of all transfer of evidence between people and all actions taken to protect the evidence while in each person’s possession. Without this documentation, the evidence may be rejected from being used in court.

Postmortem Evaluation

10. Why should companies undertake a postmortem evaluation after an attack?

Conducting an after-action review allows the company to determine what went wrong or right after an attack in order to improve the response process.

Organization of the CSIRT

11. a) Why should a senior manager head the CSIRT?

Because all security decisions during a major incident are business decisions, a senior manager should head the CSIRT.

b) Why should members of affected line departments be on CSIRT?

Decisions cannot be made intelligently without an understanding of how affected line departments will be impacted.

c) Who is the only person who should speak on behalf of the firm?

The only person who should speak on behalf of a firm should be the PR director.

d) Why should the firm’s legal counsel be on the CSIRT?

The firm’s legal counsel should be on the CSIRT to place actions in the proper legal framework and advise on the legal implications of various actions.

e) Why should a firm’s human resource department be on the CSIRT?

The firms HR department should be on the CSIRT to offer guidance on labor issues and implement sanctions against employees, if required.

Legal Considerations

Criminal versus Civil Law

12. a) What different actions do criminal and civil law deal with?

Criminal law deals with violations of criminal statutes. Civil law deals with interpretations of rights and duties that companies or individuals have relative to each other.

b) How do punishments differ in civil and criminal law?

Criminal punishments include jail time and fines; civil penalties only result in fines and/or orders to a defendant *not* to take certain actions.

c) Who brings lawsuits in civil and criminal cases?

Prosecutors charge defendants in a criminal case; plaintiffs bring a case against a defendant in a civil case.

d) What is the normal standard for deciding a case in civil and criminal trials?

Criminal trials require proving a defendant’s guilt beyond a reasonable doubt; civil trials require proving a defendant’s liability with a preponderance of the evidence (more than 50%).

e) What is *mens rea*?

Mens rea is when the prosecutor must prove the defendant was in a certain mental state, such as having the intention to commit the act.

f) In what type of trial is *mens rea* important?

Mens rea is important in criminal cases.

g) Can a person be tried separately in a criminal trial and later in a civil trial?

Yes, a defendant whose actions violate both criminal and civil rules may be criminally prosecuted by the state and later civilly sued by a victim for monetary damages.

Jurisdictions

13. a) What is case law?

Decisions based on individual cases set precedents for how laws are interpreted in trials.

b) What are jurisdictions?

Jurisdictions are areas of responsibility within which authorities can make and enforce laws but beyond which they cannot.

c) What is cyberlaw?

Cyberlaw is any law dealing with information technology.

d) What are the three levels of U.S. federal courts?

The three levels of US federal courts are:

* 94 U.S. District Courts
* 13 U.S. Circuit Courts of Appeal
* The U.S. Supreme Court

e) Which levels can create precedents?

The U.S. Circuit Courts of Appeal and Supreme Court can create precedents.

f) Does federal jurisdiction typically extend to computer crimes that are committed entirely within a state and that do not have a bearing on interstate commerce?

Crimes that are committed entirely within a state do not normally meet federal jurisdiction guidelines.

g) Who is likely to investigate a cybercrime that takes place within a city?

The local police are likely to investigate a cybercrime that takes place within a city.

h) Are international laws regarding cybercrime fairly uniform?

No, they are not. Internationally, cybercrime laws vary widely.

i) Why should companies that do business only within a country be concerned about international cyberlaw?

The laws involving computers are different between countries and are changing rapidly. International law is important for multinational companies and also for companies that deal with customers or suppliers in other countries.

Evidence and Computer Forensics

14. a) Why will courts not admit unreliable evidence?

Courts will not admit unreliable evidence because there is a belief that juries cannot be trusted to evaluate unreliable evidence properly.

b) What is a computer forensics expert?

A computer forensics expert is a professional who is trained to collect and evaluate computer evidence in ways that are likely to be admissible in court.

c) What type of witness is allowed to interpret facts for juries?

Expert witnesses are allowed to interpret facts for juries.

d) Why should companies work with forensics professionals before they have a need for them?

Given the importance of admissibility, companies should use forensics experts when prosecution is anticipated and they should have prior discussions with their chosen forensics experts to understand what may be required.

U.S. Federal Cybercrime Laws

15. a) What section of which title of the U.S. Code prohibits hacking?

18 U.S.C. 1030 is the U.S. Code that prohibits hacking.

b) What other attacks does it prohibit?

It also prohibits DoS and malware attacks.

c) Does it protect all computers?

18 U.S.C. 1030 only protects “protected computers” including government computers, financial institution computers, and any computer used in interstate or foreign commerce or communications.

d) What are damage thresholds?

Damage thresholds are minimum amounts of damage that must occur before attackers are in violation of the law.

e) What types of acts does 18 U.S.C. § 2511 prohibit?

18 U.S.C. 2511 prohibits the interception of electronic messages, both en route and after the message is received and stored, with the exception of e-mail systems owned by a company.

Intrusion Detection Systems (IDSs)

16. a) What is an IDS?

An intrusion detection system (IDS) is software and hardware that captures suspicious network and host activity data in event logs, and provides automatic tools to generate alarms, as well as query and reporting tools to help administrators analyze the data interactively during and after an incident.

b) Is an IDS a preventative, detective, or restorative control?

It is only a detective control. Of course, if attackers believe that they are likely to be caught by an IDS, it may have preventative benefits as well.

c) What are false positives?

False positives in an IDS are known as false alarms.

d) Why are false positives problems for IDSs?

IDSs tend to be ignored if they generate many false positives.

Functions of an IDS

17. a) What are the four functions of IDSs?

The four functions of IDSs are logging, automated analysis, administrator actions, and management.

b) What are the two types of analysis that IDSs usually do?

Two types of analysis IDSs usually perform are attack signature detection and anomaly detection.

c) What types of action did this section mention?

Actions mentioned include alarms and log summary reports with interactive manual log analysis tools.

d) What information should alarms contain?

Alarms should give the security administrator a description of what the problem is, a way to test the alarm for accuracy, and advice about what action the security administrator should take.

e) What is the purpose of log summary reports?

Log summary reports list various types of suspicious activity. They also indicate threat priority by type of threat or by statistical analysis, indicating high frequency. The purpose of log summary reports is to give IDS administrators notice of threats that aren’t high risk or detected by alarms.

f) Describe interactive log file analysis.

Interactive log file analysis allows administrators to drill down into log files to better understand an ongoing or completed attack, while filtering out irrelevant entries.

Distributed IDSs

18. a) What is the advantage of a distributed IDS?

A distributed IDS can collect data from many devices at a central manager console to allow a security manager to detect a more complex attack.

b) Name the elements in a distributed IDS.

There is a manager, an integrated log file, an agent host IDS, an agent network IDS, and an IDS vendor.

c) Distinguish between the manager and agents.

The agent collects event data and stores them in log files on the monitoring devices. The manager program is responsible for integrating the information from the multiple agents that run on multiple monitoring devices.

d) Distinguish between batch and real-time transfers for event data.

In batch transfers, the agent waits until it has several minutes or several hours of data and then sends a block of log file data to the manager. In real-timetransfers, each event’s data goes to the manager immediately.

e) What is the advantage of each type?

Batch transfer is the least expensive and has the lowest network load, while real-time transfer allows capturing of log files without worrying about attackers deleting log files.

f) What two types of communication must be secure?

Communication between IDS agents and manager should be secure in order to ensure an attacker cannot spoof either and cause mass confusion to the IDS.

Network IDSs (NIDSs)

19. a) At what information do NIDSs look?

NIDSs look at all information traveling through a network.

b) Distinguish between stand-alone NIDSs and switch-based or router-based NIDSs.

Stand-alone NIDSs are boxes located at various points in a network. They read and analyze all network frames that pass by them. They are essentially corporate-owned sniffers. Switch NIDSs and router NIDSs are switches and routers that have IDS software. Typically, these capture data on all ports.

c) What are the strengths of NIDSs?

The strength of NIDSs is that they can see all packets passing through some locations in the network. Often, these packets are highly diagnostic of attacks.

d) What are the two weaknesses of NIDSs?

The two weaknesses of NIDSs are that they leave blind spots on the network where no NIDSs are placed, and they cannot read encrypted data.

Host IDSs

20. a) What is the major attraction of a HIDS?

The main attraction of HIDSs is that they provide highly specific information about what happened on a particular host. This is important for problem diagnosis.

b) What are the two weaknesses of host IDSs?

The two weaknesses of HIDSs are that they have limited views of what is happening on a network because they can only see on a particular host, and they can be compromised if the system is owned by an attacker.

c) List some things at which host operating system monitors look.

Some things host operating system monitors look at are multiple failed logins, creating new accounts, adding new executables that may be attack programs, modifying executables (installing Trojan horses does this), adding registry keys (changes how system works), and changing or deleting system logs and audit files.

Log Files

21. a) Why are integrated log files good?

Integrated log files are good because they are an aggregation of event logs from multiple IDSs.

b) Why are they difficult to create?

They are difficult to create because of format incompatibilities.

c) Explain the time synchronization issue for integrated log files.

If the times on the various IDSs are off by even a few thousandths of a second, it will be extremely difficult to see what is happening at a particular moment in time—especially if the attack is automated and occurs quickly.

d) How do companies achieve time synchronization?

Companies achieve time synchronization using the Network Time Protocol (NTP) service.

e) What is event correlation?

Event correlation is the analysis of suspicious patterns in a series of events across multiple devices.

f) Distinguish between aggregation and event correlation.

Aggregation is the collection of all log files, whereas event correlation requires analysis to determine related attack patterns.

g) Why is analyzing log file data difficult?

Analyzing log file data is difficult because the relevant event exists in much larger event streams than are logged.

h) In Figure 10-19, how long is the delay between the first attempted login and the second?

The delay is 44.28 seconds.

i) Does this indicate that the attack is a human attack or an automated attack?

This is most likely a human attack (based on memory of the logs) because the attack is done in a reasonably human amount of time.

Managing IDSs

22. a) What is precision in an IDS?

Precision in IDS means that the IDS should report all attack events and report as few false alarms as possible.

b) What are false positives, and why are they bad?

False positives are also known as false alarms and are bad because they will outnumber true alarms ten-to-one or even more. In fact, the large number of false positives generated by IDSs is the major problem with IDSs today, causing many firms to stop using them after a trial period.

c) What are false negatives, and why are they bad?

False negatives are failures to report true attack activities. They are bad because they fail to notify the user of a valid attack.

d) How can tuning reduce the number of false positives?

Tuning turns off unnecessary rules, and reduces the severity level of alarms generated by other rules, in order to limit the total number of false positives.

e) What does an IDS do if it cannot process all of the packets it receives?

IDSs that are overwhelmed by packets will simply skip packets and possibly miss a valid, suspicious attack packet.

f) What may happen if a system runs out of storage space?

When the system nears the point of running out of storage space, the IDS will transfer the log file to backup and start a new log file.

g) Why is limiting the size of log files necessary but unfortunate?

Limiting the size of log files is necessary to avoid exceeding storage capacity, and this limits the amount of log file data available for historical analysis.

Honeypots

23. a) What is a honeypot?

A honeypot is a fake server or entire network segment with multiple clients and servers.

b) How can honeypots help companies detect attackers?

Because legitimate users will not access the honeypot network assets, honeypot activities are normally attacker activities.

c) Could a honeypot attract unwanted attention from attackers?

Yes, due to the number of ports being faked, a honeypot could attract additional attention from attackers looking for a specific service, operating system, or port.