PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Study Planner

# Cert Guide

Advance your IT career with hands-on learning

CompTIA®

# Cybersecurity Analyst (CySA+)

CS0-002

TROY McMILLAN

# Special Offers

- ***Internet Key Exchange (IKEv2):*** Also sometimes referred to as IPsec Key Exchange, IKE provides the authentication material used to create the keys exchanged by ISAKMP during peer authentication. This was proposed to be performed by a protocol called Oakley that relied on the Diffie-Hellman algorithm, but Oakley has been superseded by IKEv2.

IPsec is a framework, which means it does not specify many of the components used with it. These components must be identified in the configuration, and they must match in order for the two ends to successfully create the required SA that must be in place before any data is transferred. The following selections must be made:

- The encryption algorithm, which encrypts the data
- The hashing algorithm, which ensures that the data has not been altered and verifies its origin
- The mode, which is either tunnel or transport
- The protocol, which can be AH, ESP, or both

All these settings must match on both ends of the connection. It is not possible for the systems to select these on the fly. They must be preconfigured correctly in order to match.

When configured in tunnel mode, the tunnel exists only between the two gateways, but all traffic that passes through the tunnel is protected. This is normally done to protect all traffic between two offices. The SA is between the gateways between the offices. This is the type of connection that would be called a site-to-site VPN.

The SA between the two endpoints is made up of the security parameter index (SPI) and the AH/ESP combination. The SPI, a value contained in each IPsec header, helps the devices maintain the relationship between each SA (and there could be several happening at once) and the security parameters (also called the transform set) used for each SA.

Each session has a unique session value, which helps prevent

- Reverse engineering
- Content modification
- Factoring attacks (in which the attacker tries all the combinations of numbers that can be used with the algorithm to decrypt ciphertext)

With respect to authenticating the connection, the keys can be preshared or derived from a public key infrastructure (PKI). A PKI creates public/private key pairs that are associated with individual users and computers that use a certificate. These key pairs are used in the place of preshared keys in that case. Certificates that are not derived from a PKI can also be used.

In transport mode, the SA is either between two end stations or between an end station and a gateway or remote access server. In this mode, the tunnel extends from computer to computer or from computer to gateway. This is the type of connection that would be used for a remote-access VPN. This is but one application of IPsec.

When the communication is from gateway to gateway or host to gateway, either transport or tunnel mode may be used. If the communication is computer to computer, transport mode is required. When using transport mode from gateway to host, the gateway must operate as a host.

The most effective attack against an IPsec VPN is a man-in-the middle attack. In this attack, the attacker proceeds through the security negotiation phase until the key negotiation, when the victim reveals its identity. In a well-implemented system, the attacker fails when the attacker cannot likewise prove his identity.

### SSL/TLS

***Secure Sockets Layer (SSL)/Transport Layer Security (TLS)*** is another option for creating VPNs. Although SSL/TLS has largely been replaced by its successor, TLS, it is quite common to hear it still referred to as an SSL/TLS connection. It works at the application layer of the OSI model and is used mainly to protect HTTP traffic or web servers. Its functionality is embedded in most browsers, and its use typically requires no action on the part of the user. It is widely used to secure Internet transactions. It can be implemented in two ways:

Key Topic

- **SSL/TLS portal VPN:** In this case, a user has a single SSL/TLS connection for accessing multiple services on the web server. Once authenticated, the user is provided a page that acts as a portal to other services.
- **SSL/TLS tunnel VPN:** A user may use an SSL/TLS tunnel to access services on a server that is not a web server. This solution uses custom programming to provide access to non-web services through a web browser.

TLS and SSL/TLS are very similar but not the same. When configuring SSL/TLS, a session key length must be designated. The two options are 40-bit and 128-bit. Using self-signed certificates to authenticate the server's public key prevents man-in-the-middle attacks.

SSL/TLS is often used to protect other protocols. Secure Copy Protocol (SCP), for example, uses SSL/TLS to secure file transfers between hosts. Table 8-2 lists some of the advantages and disadvantages of SSL/TLS.

**Table 8-2** Advantages and Disadvantages of SSL/TLS

| Advantages | Disadvantages |
|---|---|
| Data is encrypted. | Encryption and decryption require heavy resource usage. |
| SSL/TLS is supported on all browsers. | Critical troubleshooting components (URL path, SQL queries, passed parameters) are encrypted. |
| Users can easily identify its use (via https://). | |

When placing the SSL/TLS gateway, you must consider a trade-off: The closer the gateway is to the edge of the network, the less encryption that needs to be performed in the LAN (and the less performance degradation), but the closer to the network edge it is placed, the farther the traffic travels through the LAN in the clear. The decision comes down to how much you trust your internal network.

The latest version of TLS is version 1.3, which provides access to advanced cipher suites that support elliptical curve cryptography and AEAD block cipher modes. TLS has been improved to support the following:

- **Hash negotiation:** Can negotiate any hash algorithm to be used as a built-in feature, and the default cipher pair MD5/SHA-1 has been replaced with SHA-256.
- **Certificate hash or signature control:** Can configure the certificate requester to accept only specified hash or signature algorithm pairs in the certification path.
- **Suite B–compliant cipher suites:** Two cipher suites have been added so that the use of TLS can be Suite B compliant:
    - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

### Serverless

A serverless architecture is one in which servers are not located where applications are hosted. In this model, applications are hosted by a third-party service, eliminating the need for server software and hardware management by the developer. Applications are broken up into individual functions that can be invoked and scaled individually. Function as a Service (FaaS), another name for serverless architecture, was discussed in Chapter 6.

## Change Management

All networks evolve, grow, and change over time. Companies and their processes also evolve and change, which is a good thing. But infrastructure change must be managed in a structured way so as to maintain a common sense of purpose about the changes. By following recommended steps in a formal ***change management*** process, change can be prevented from becoming the tail that wags the dog. The following are guidelines to include as a part of any change management policy:

- All changes should be formally requested.
- Each request should be analyzed to ensure it supports all goals and polices.
- Prior to formal approval, all costs and effects of the methods of implementation should be reviewed.
- After they're approved, the change steps should be developed.
- During implementation, incremental testing should occur, relying on a predetermined fallback strategy if necessary.
- Complete documentation should be produced and submitted with a formal report to management.

One of the key benefits of following this change management method is the ability to make use of the documentation in future planning. Lessons learned can be applied, and even the process itself can be improved through analysis.

## Virtualization

Multiple physical servers are increasingly being consolidated to a single physical device or hosted as virtual servers. It is even possible to have entire virtual networks residing on these hosts. While it may seem that these devices are safely contained on the physical devices, they are still vulnerable to attack. If a host is compromised or a hypervisor that manages virtualization is compromised, an attack on the virtual machines (VMs) could ensue.

### Security Advantages and Disadvantages of Virtualization

Virtualization of servers has become a key part of reducing the physical footprint of data centers. The advantages include

Key Topic

- Reduced overall use of power in the data center
- Dynamic allocation of memory and CPU resources to the servers

- High availability provided by the ability to quickly bring up a replica server in the event of loss of the primary server

However, most of the same security issues that must be mitigated in the physical environment must also be addressed in the virtual network. In a virtual environment, instances of an operating system are *virtual machines*. A host system can contain many VMs. Software called a *hypervisor* manages the distribution of resources (CPU, memory, and disk) to the VMs. Figure 8-16 shows the relationship between the host machine, its physical resources, the resident VMs, and the virtual resources assigned to them.

Key Topic

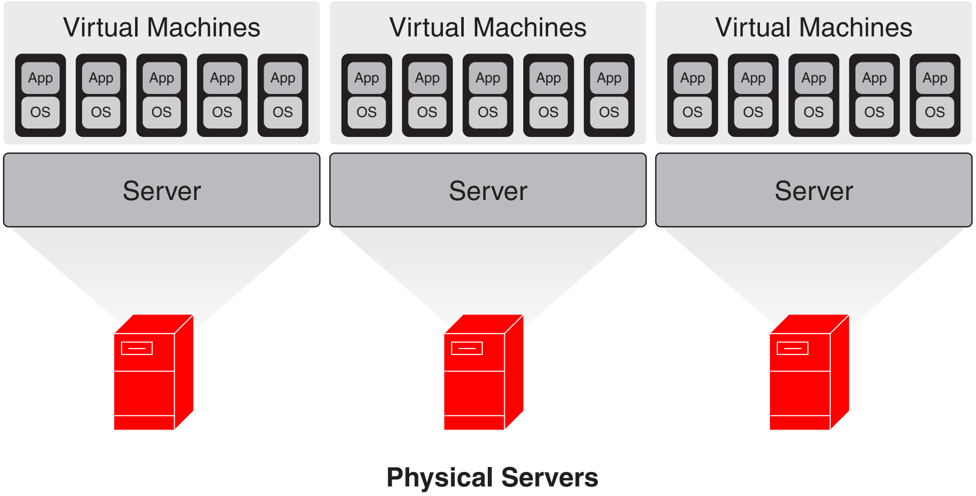

**FIGURE 8-16** Virtualization

Keep in mind that in any virtual environment, each virtual server that is hosted on the physical server must be configured with its own security mechanisms. These mechanisms include antivirus and anti-malware software and all the latest patches and security updates for all the software hosted on the virtual machine. Also, remember that all the virtual servers share the resources of the physical device.

When virtualization is hosted on a Linux machine, any sensitive application that must be installed on the host should be installed in a chroot environment. A chroot on Unix-based operating systems is an operation that changes the root directory for the current running process and its children. A program that is run in such a modified environment cannot name (and therefore normally cannot access) files outside the designated directory tree.

Key Topic

### Type 1 vs. Type 2 Hypervisors

The hypervisor that manages the distribution of the physical server's resources can be either Type 1 or Type 2:

- ***Type 1 hypervisor:*** A guest operating system runs on another level above the hypervisor. Examples of Type 1 hypervisors are Citrix XenServer, Microsoft Hyper-V, and VMware vSphere.
- ***Type 2 hypervisor:*** A Type 2 hypervisor runs within a conventional operating system environment. With the hypervisor layer as a distinct second software level, guest operating systems run at the third level above the hardware. VMware Workstation and Oracle VM VirtualBox exemplify Type 2 hypervisors.

Figure 8-17 shows a comparison of the two approaches.

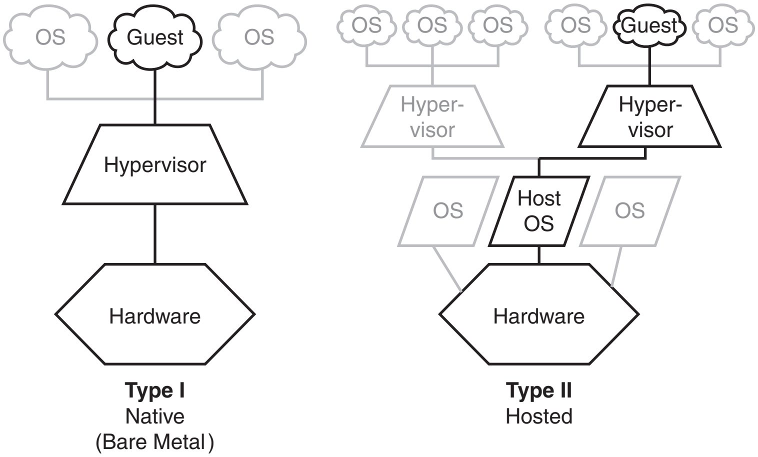

**FIGURE 8-17** Hypervisor Types

### Virtualization Attacks and Vulnerabilities

Virtualization attacks and vulnerabilities fall into the following categories:

Key Topic

- ***VM escape:*** This type of attack occurs when a guest OS escapes from its VM encapsulation to interact directly with the hypervisor. This can allow access to all VMs and the host machine as well. Figure 8-18 illustrates an example of this attack.