You have been hired as a security consultant to help recommend the best cloud model or type to use for an organization as they migrate from self-hosted services to a cloud-based model. The organization’s current network is used to host a lot of confidential information, so the Chief Information Officer has stated that whatever cloud solution you recommend should focus on providing secure services and paying a higher price for security is acceptable. Which cloud model would you recommend to the organization?

Public cloud

Private cloud

Hybrid cloud

Community cloud

Answer: B

Explanation: Since security is the main requirement you have been provided, you should recommend a private cloud. A private cloud is designed for a single organization to use, provides the organization with the most control over the infrastructure and data, and is generally more secure than a public, hybrid, or community cloud model.

You have been asked to pick the right “as a service” solution for your company. Your boss would like you to find a solution that provides the server load balancing, routing, and hosting, but will allow the company to install its own operating system, backend applications, and custom-built web application into the cloud service. Which “as a service” would best meet these requirements?

Platform as a Service (PaaS)

Security as a Service (SECaaS)

Infrastructure as a Service (IaaS)

Software as a Service (SaaS)

Answer: c

Explanation: Infrastructure as a Service (IaaS) provides an organization with the network, servers, load balancing, routing, and VM hosting required for a service. The organization can then choose their own operating system (usually Windows or Linux), install backend applications (like Apache or MySQL), and any custom-built applications they would like to install and utilize. With IaaS, you get the most control over the “as a service”, but you also have the most responsibility for its inner workings and design.

Which type of server is often targeted as part of the privilege escalation or lateral movement phase of an attack?

Domain Controller

Email Server

File Server

Web Server

Answer: A

Explanation: A domain controller or directory service (such as Active Directory in Windows and LDAP in Linux) is often targeted as part of the privilege escalation or lateral movement phases of an attack. These servers contain all the user accounts, computer accounts, and groups for a particular network. The creation and use of a Golden Ticket are often used as a form of privilege escalation inside a Windows network and exploit a vulnerability in the Kerberos ticketing system used by the Active Directory domain controller.