14.1.6 Cloud Attacks Facts

Cloud services offer a variety of resources for clients, often less expensively than an organization can implement in-house. However, cloud security is a big concern. Hackers are constantly trying to exploit technology vulnerabilities. A successful exploit could compromise data confidentiality and integrity, as well as the availability of resources and services.

This lesson covers the most prominent attacks on the cloud.

Prominent Cloud Attacks

The table below describes some of the most prominent attacks hackers make on cloud services.

Attack	Description
Service hijacking through social engineering	Service hijacking through social engineering entails the attacker using approaches such as pharming, phishing, and exploitation of software to steal credentials from either a Credential Service Provider (CSP) or the client. After stealing a client's credentials, an attacker is able to access the cloud and perpetrate exploits.
Service hijacking through network sniffing	When service hijacking through network sniffing, the attacker uses packet sniffers such as Wireshark or Cain and Abel to intercept and monitor traffic transmission between two cloud nodes. The attacker's intent is to discover and then use sensitive data such as passwords, session cookies, and other security configurations such as UDDI, SOAP, and WSDL.
Session hijacking through XSS attack	In an XSS attack, the hacker uses cross-site scripting to gain elevated access to session cookies, web page content, and other sensitive information.
Session hijacking through session riding	In a session riding attack, the hacker tricks a user with an active computer session into visiting a malicious website. When the user logs in, the malicious website executes the request so that the user can't tell anything is wrong. The hacker then uses the information obtained to steal data.
DNS poisoning	In this attack, the hacker replaces legitimate sites on the DNS server or the user's DNS cache with fake websites. When the user enters the URL of a legitimate site, the system is directed to a malicious site.
Cybersquatting	In this attack, the hacker uses a phishing scam that contains a domain name that is almost the same as the cloud service provider in an attempt to direct the user to a malicious website.
Domain hijacking	This attack works by stealing the domain name of the cloud service.
Domain snipping	This attack works by registering an elapsed domain name.
Side channel or cross-guest VM breaches	This kind of attack typically puts a malicious virtual machine close to a target cloud server to obtain leaked data from CPU buffer zones and data processing operations. Inside the attack, the hacker runs a virtual machine on the physical host of a user's virtual machine. Then the hacker is able to access the physical resources, such as the cache, to obtain data and perform malicious acts.
Cryptanalysis	All potentially sensitive data in the cloud should be protected by encryption. However, if the encryption is weak or flawed, attackers are able to break the encryption and access the data. There are many methods for breaking cryptography.
Wrapping attack	A wrapping attack involves duplicating the body of a Simple Object Access Protocol (SOAP) message in the TLS layer, then sending it to the server as a legitimate user.
Denial of service (DoS) and distributed denial of service (DDoS)	A Denial of Service (DoS) attack is intended to overwhelm a system so that it is inaccessible. DoS attacks are executed by flooding the cloud infrastructure, such as CPU and memory, with so many malicious requests that the server stops processing legitimate requests and users are unable to gain access. If the attack is completed using a network of compromised machines (a botnet), then it is a DDoS.
Man-in-the-cloud attack	These attacks are very similar to man-in-the-middle attacks made in non-cloud environments. Man-in-the-middle attacks often involve stealing data from synchronization services such as Dropbox.