General Discussion on Cloud for CISSP.

Threats & Vulnerabilities.

Session 2 9/5/2020 Classroom-1

NOTES

Threats and Vulnerabilities

Threat (NIST Definition)

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Asset

Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).

The Official Study Guide by Sybex dedicates a few handful of pages for Cloud and Cloud Threats and Vulnerabilities. While there are some specific types of threats that are identified with cloud computing, the threats that affect on premise computing can affect the cloud computing infrastructure as well. But here are some of the top 12 threats. It is not necessary to remember them in any order. Every year hundreds of security companies do surveys and research to put together a security report. If this year, Data breach was number 1, next year it could be APTs.

For the CISSP Exam, having a high level understanding of the top 10 threats and vulnerabilities will help in answering the questions in the exam.

Data Breach:
A data breach is a security incident in which information is accessed without authorization.
A data breach is an incident that exposes confidential or protected information. A data breach might involve the loss or theft of your Social Security number, bank account or credit card numbers, personal health information, passwords or email.

Insufficient Identity, Credential and Access Management
The lack of scalable identity access management systems, failure to use multifactor authentication, weak password use, and a lack of ongoing automated rotation of cryptographic keys, passwords and certificates can all contribute to this condition of Insufficient Identity, Credential and Access Management. An organization has to be diligent when moving from on premise to cloud and if they are not considering the various aspects of cloud computing such as data security, identity access management they could land into some serious issues.

System Vulnerabilities
- Lack of input validation on user input
- Lack of sufficient logging mechanism
- Fail-open error handling
- Not closing the database connection properly

Account Hijacking
Cloud account hijacking is a process in which an individual or organization's cloud account is stolen or hijacked by an attacker. Think of Phishing attacks. One good example I can think of in my area of work is most vendors in the Industrial control system used to often reuse credentials and passwords, which obviously amplifies the impact of such attacks.

Malicious Insiders
Malicious insiders can be employees, former employees, contractors or business associates who have legitimate access to your systems and data, but use that access to destroy data, steal data or sabotage your systems. It does not include well-meaning staff who accidentally put your cyber security at risk or spill data.

Advanced Persistent Threats (APTs)
Like other attackers, APT groups try to steal data, disrupt operations or destroy infrastructure. Unlike most cyber criminals, APT attackers pursue their objectives over months or years. They adapt to cyber defenses and frequently retarget the same victim.

- Advanced:
    - Using latest techniques
    - Using multiple methods, tools and techniques
    - Brute force vulnerability discovery
- Persistent:
    - Targeted
    - Long-term access to the target
    - Dormant potential, Go Unnoticed for a long period of time.
    - Follow up and attack again.
- Threat:
    - Specific objective
    - Skilled actors

Data Loss:
Data loss is also known as data leakage
Data loss is any process or event that results in data being corrupted, deleted and/or made unreadable by a user and/or software or application. It occurs when one or more data elements can no longer be utilized by the data owner or requesting application.

- Accidental Deletion of Data
- Overwriting of data
- Malicious action resulting in Data deletion, corruption or encryption.

Insufficient Due Diligence
When management creates business strategies for growth and to support their business, cloud technologies and CSPs must be considered in order to meet customer needs and be competitive. Developing a good roadmap and checklist for due diligence when evaluating technologies and CSPs is essential for the greater chance of success and also to avoid pitfalls.

Abuse and Nefarious Use of Cloud Services
Poorly secured cloud service deployments, free cloud service trials and fraudulent account sign-ups via payment instrument fraud expose cloud computing models such as IaaS, PaaS, and SaaS to malicious attacks.

Insecure Interfaces and APIs

Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services.

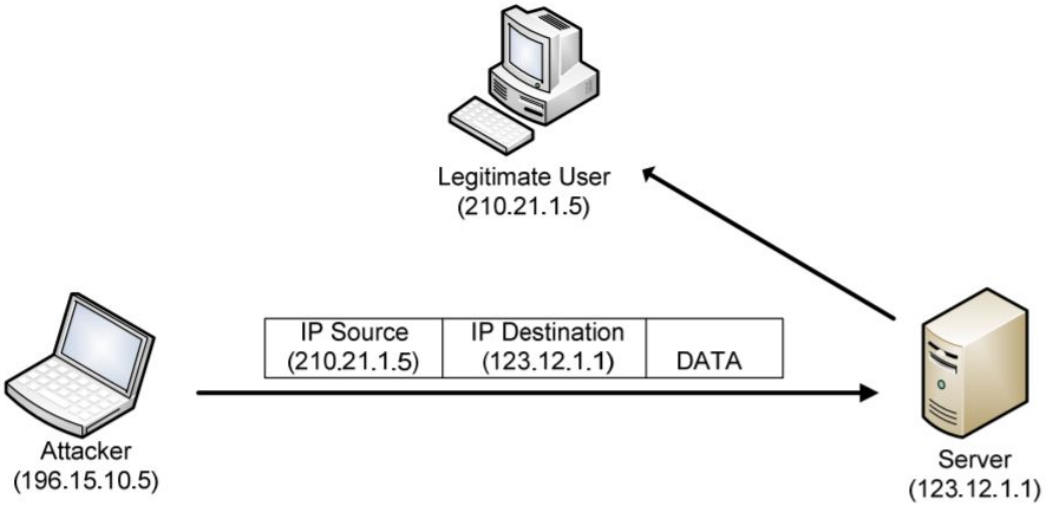
- developers create APIs without authentication
- Open source software used by developers and end users.

Denial of Service (DoS)

There is also another term, DDoS. Let's first look at DoS.
A DoS attack is a denial of service attack where a computer is used to flood a server with TCP and UDP packets. A DDoS attack is where multiple systems target a single system with a DoS attack. The targeted network is then bombarded with packets from multiple locations.

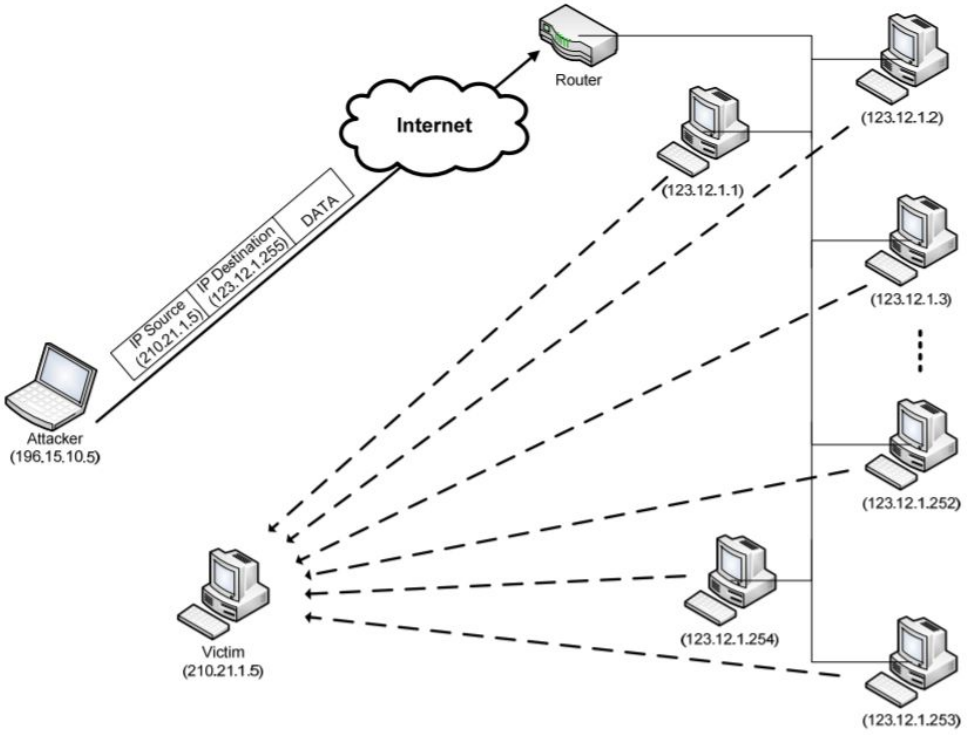
IP spoofing attack :

In the Internet Protocol (IP) spoofing attack, packet transmissions between the end user and the cloud server can be intercepted and their headers modified such that the IP source field in the IP packet is forged by either a legitimate IP address, as shown in Figure below, or by an unreachable IP address



Smurf attack :

In a smurf attack, the attacker sends a large number of Internet Control Message Protocol (ICMP) echo requests. These requests are spoofed such that its source IP address is the victim's IP, and the IP destination address is the broadcast IP address, as shown in Figure below. As a result, the victim will be flooded with broadcasted addresses. The worst case occurs when the number of hosts who reply to the ICMP echo requests is too large.



Buffer overflow attack:

Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information. For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.

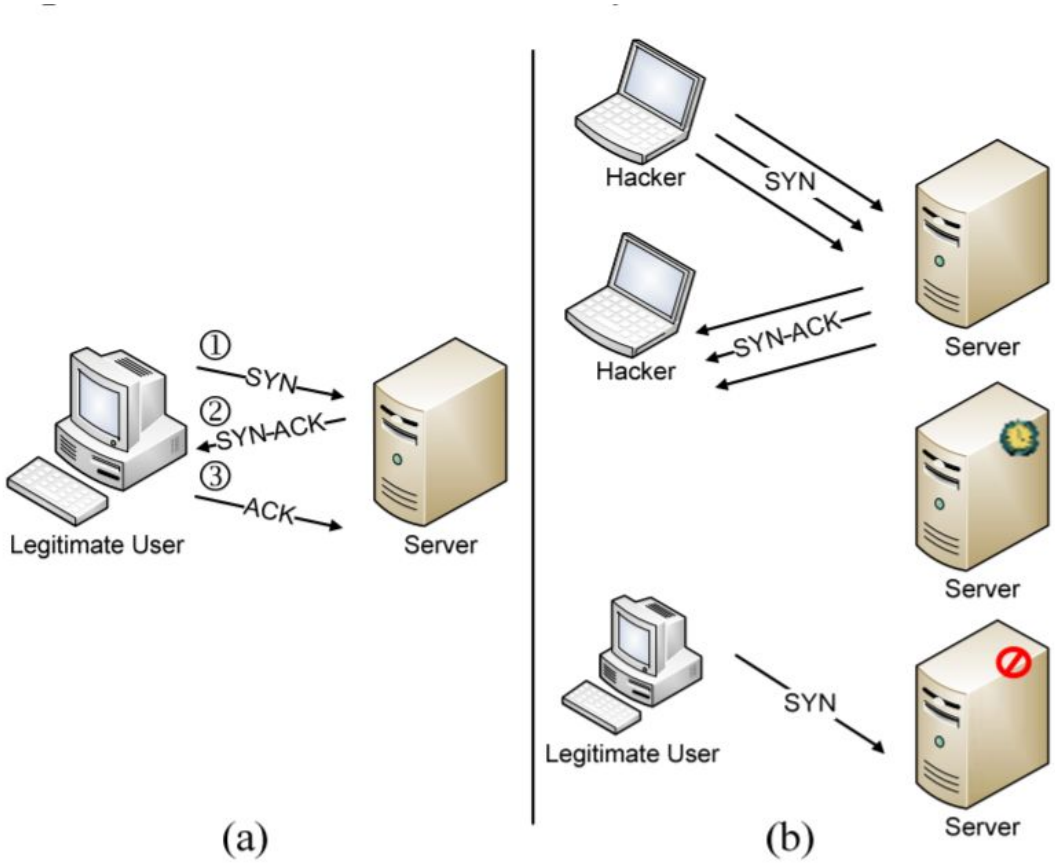
Teardrop attack :

Example system affected: Windows NT 4.0 with SP3

This kind of attack uses the “Teardrop.c” program to send invalid overlapping values of IP fragments in the header of TCP packets. As a result, the victim’s machine within the cloud system will crash in the reassembly process. Recent operating systems and network resources can handle such attacks. Therefore, teardrop attacks no longer affect any layers of cloud computing.

SYN flooding attack:

SYN flooding occurs when the attacker sends a huge number of packets to the server but does not complete the process of the three-way handshake. As a result, the server waits to complete the process for all of those packets, which makes the server unable to process legitimate requests.



Ping of death attack:

In the ping of death attack, the attacker sends an IP packet with a size larger than the limit of the IP protocol, which is 65,535 bytes, as shown in Fig. 5. Handling an oversized packet affects the victim's machine within the cloud system as well as the resources of the cloud system. Recent network resources and operating systems disregard any IP packets larger than 65,535 bytes.

Land Attack:

A **LAND** (local area network denial) attack is a DoS (denial of service) attack that consists of sending a special poison spoofed packet to a computer, causing it to lock up.

References:

Top 12 Cloud Threats
https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf

DDoS Research Paper:
https://arxiv.org/ftp/arxiv/papers/1511/1511.08839.pdf#:~:text=The%20first%20DDoS%20attack%20was,servers%20as%20reflectors%20%5B3%5D.

OWASP Cheat Sheet:
https://cheatsheetseries.owasp.org/cheatsheets/REST_Security_Cheat_Sheet.html

ISC2 2018 Cloud Security Report
https://www.isc2.org/-/media/ISC2/Certifications/CCSP/2018-Cloud-Security-Report-ISC2.ashx
2018.

ISC2 Cloud Security Report
https://www.isc2.org/-/media/ISC2/Landing-Pages/2020-Cloud-Security-Report-ISC2.ashx?la=en&hash=512D362CF94E2A69E96781698006A54369F1FE5F
2020.

Data Breaches:
https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

The NIST definition of cloud computing:
https://icsbits.com/go/clouddef
Special Publication 800-145

Process Guide:
https://icsbits.com/go/processguide
Cheatsheet for Processes in CISSP.