# CERTIFIED CYBER COP

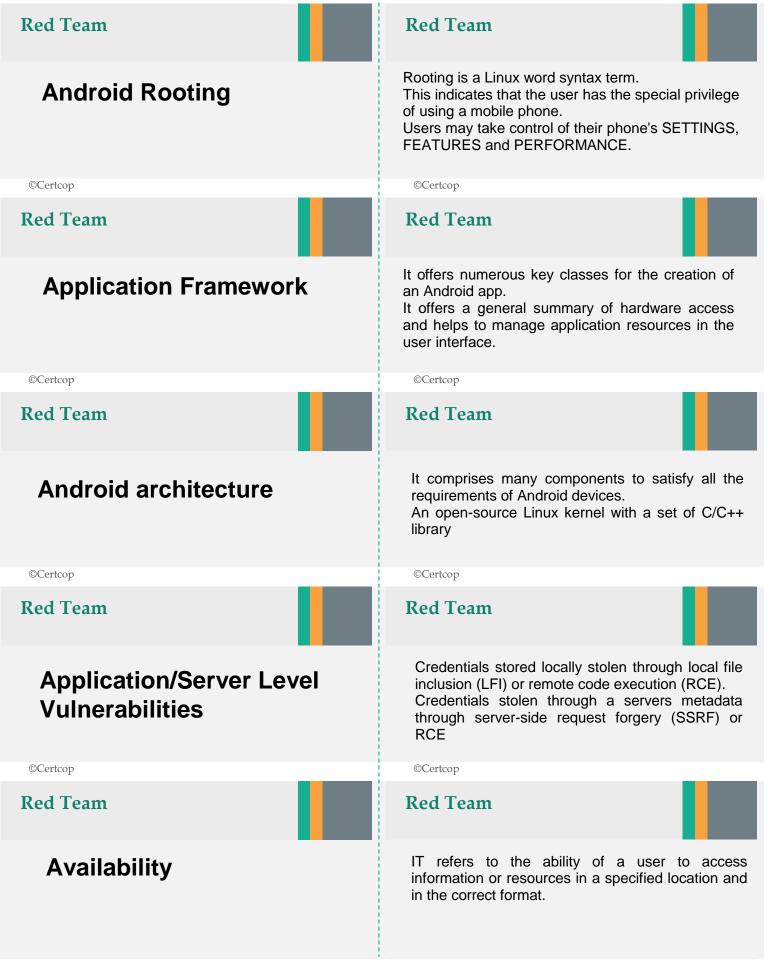
57

# Red Team Certcop CertTips



Copyrights @ 2022 Certcop, All rights reserved





Red Team	Red Team
Broad Network Access	Broad network access refers to resources hosted in a private cloud network (operated within a company's firewall) that are available for access from a wide range of devices, such as tablets, PCs, Macs and smart phones. These resources are also accessible from a wide range of locations that offer online access.
©Certcop	©Certcop
Red Team	Red Team
Blue Keep	Blue Keep is a Microsoft RDP vulnerability that allows attackers to remotely log in to a victim's computer.
©Certcop	©Certcop
Red Team	Red Team
Burp	Burp is a suite of tools used to test online applications for security flaws, or "pen testing." It was created by a business called Port swigger.
©Certcop	©Certcop
Red Team	Red Team
Block Storage	Space in Blocks File storage has a hierarchy of folders and file.
©Certcop	©Certcop
Red Team	Red Team
Bluetooth	Bluetooth is a technology that allows wireless connection.
©Certcop	©Certcop

# **Buffer Overflows**

©Certcop

Red Team

# **Bootrom Exploit**

©Certcop

Red Team

### **Baiting**

©Certcop

**Red Team** 

# Confidentiality

©Certcop

Red Team

### **Cloud Carrier**

#### **Red Team**



Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer.

©Certcop

#### **Red Team**



A jailbreak bootrom may break all authentications at low levels such as file system, iBoot, and NOR (custom boot logos).

In the application for discarding signature checks, this procedure discovers a flaw.

©Certcop

#### **Red Team**



To make contact with or gain access to a cloud service an attacker places a malware-infected physical item, like as a USB flash drive, at a location where it will be discovered. The victim then takes the gadget and plugs it into their computer, accidentally downloading malware.

©Certcop





Prevents the unauthorized disclosure of data, In other words, authorized personnel can access the data, but unauthorized personnel cannot access the data.

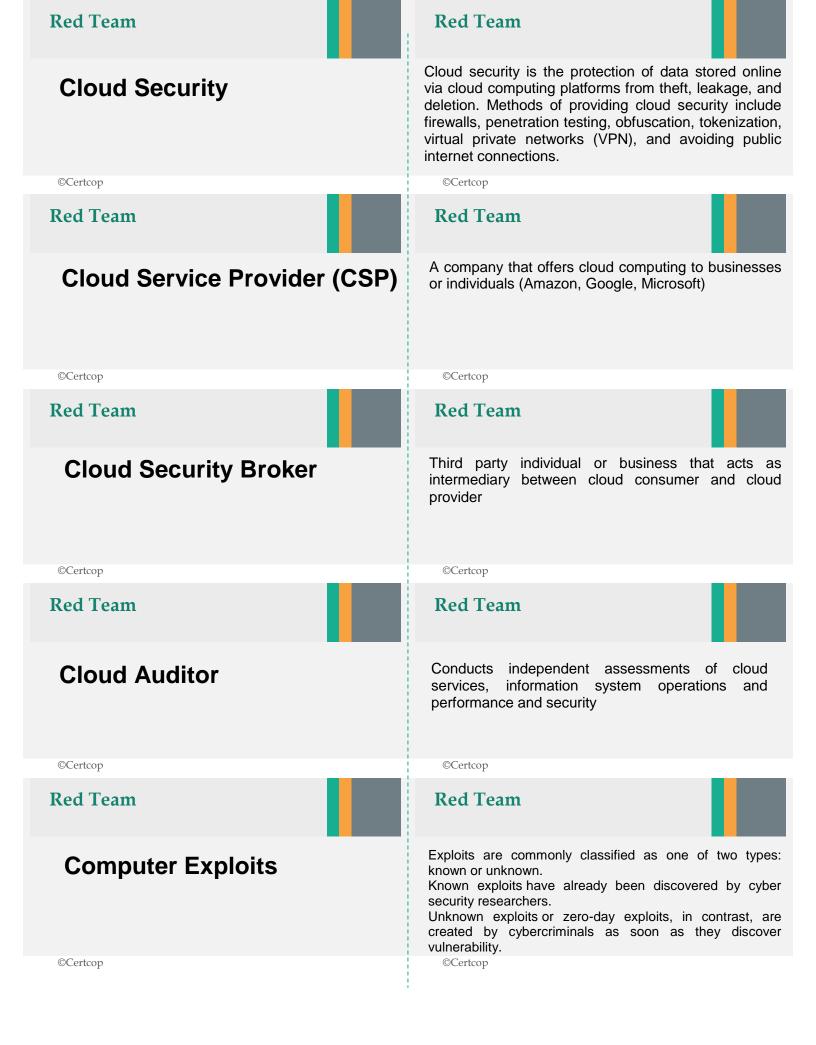
©Certcop

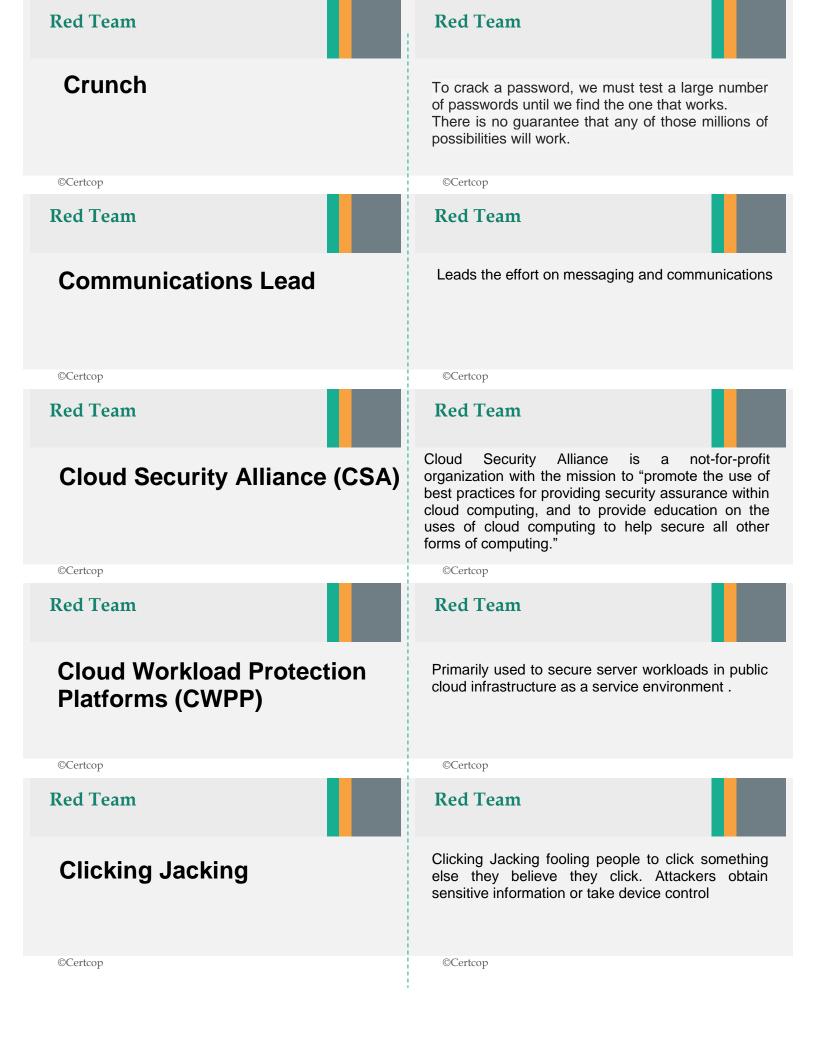


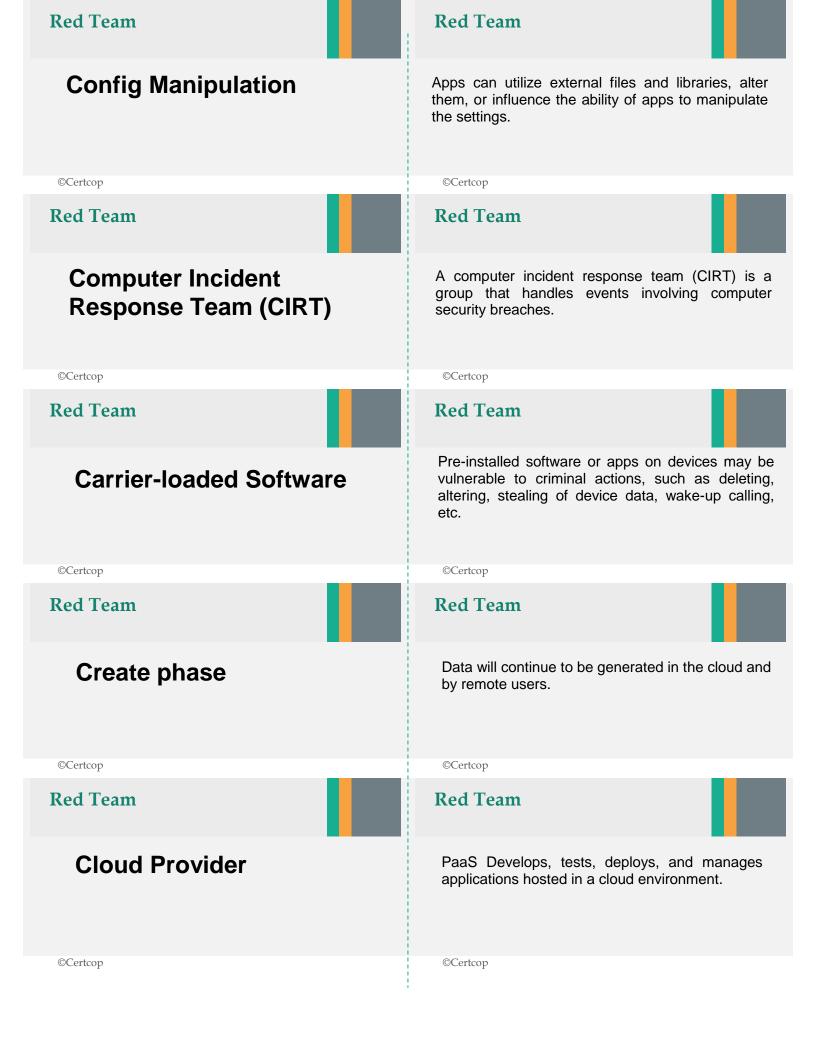


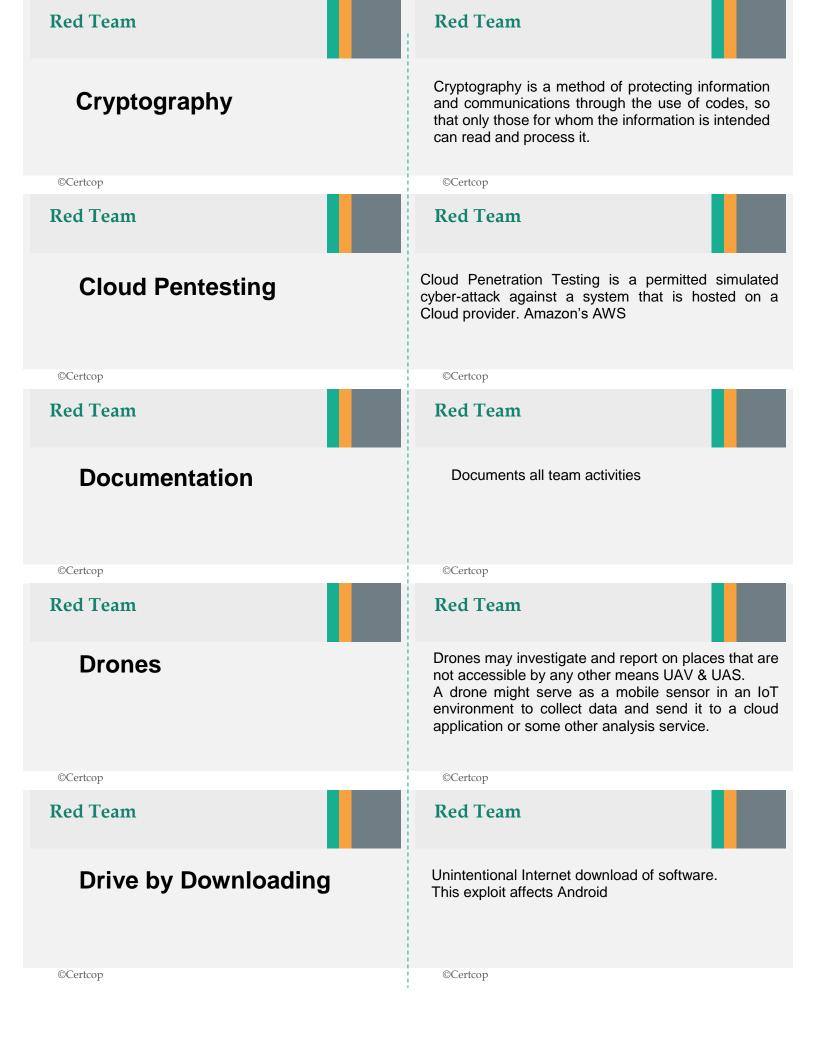
The intermediary that provides connectivity and transport of cloud services between

©Certcop

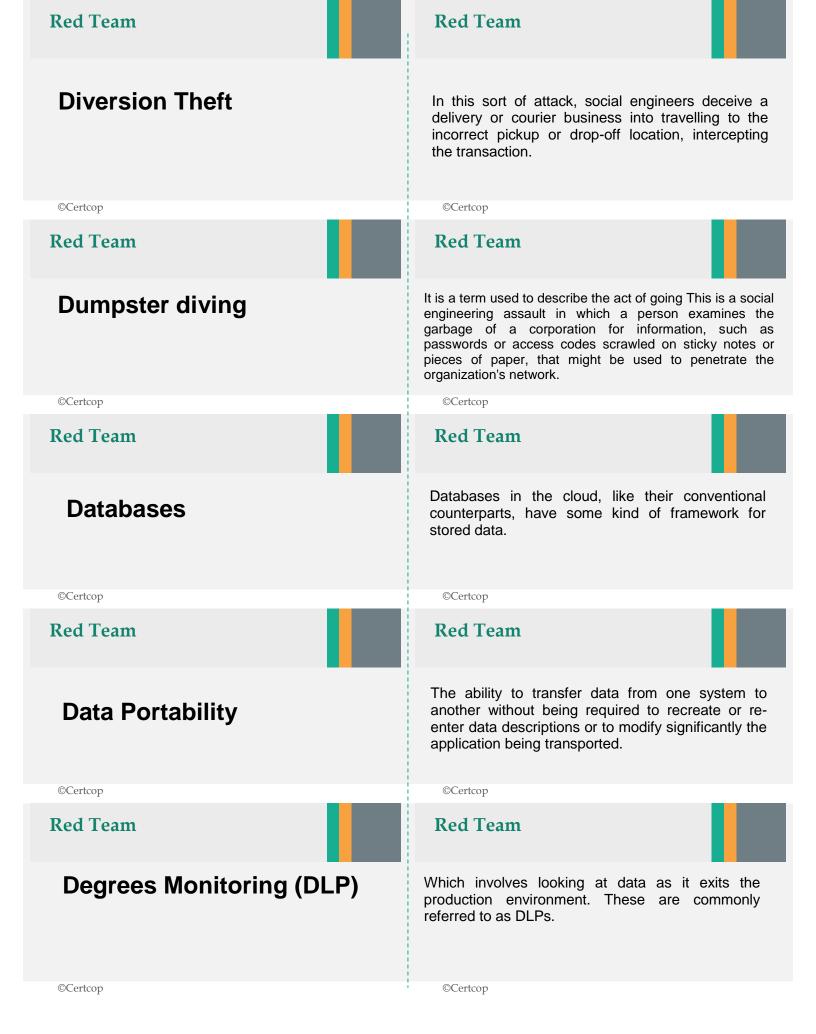


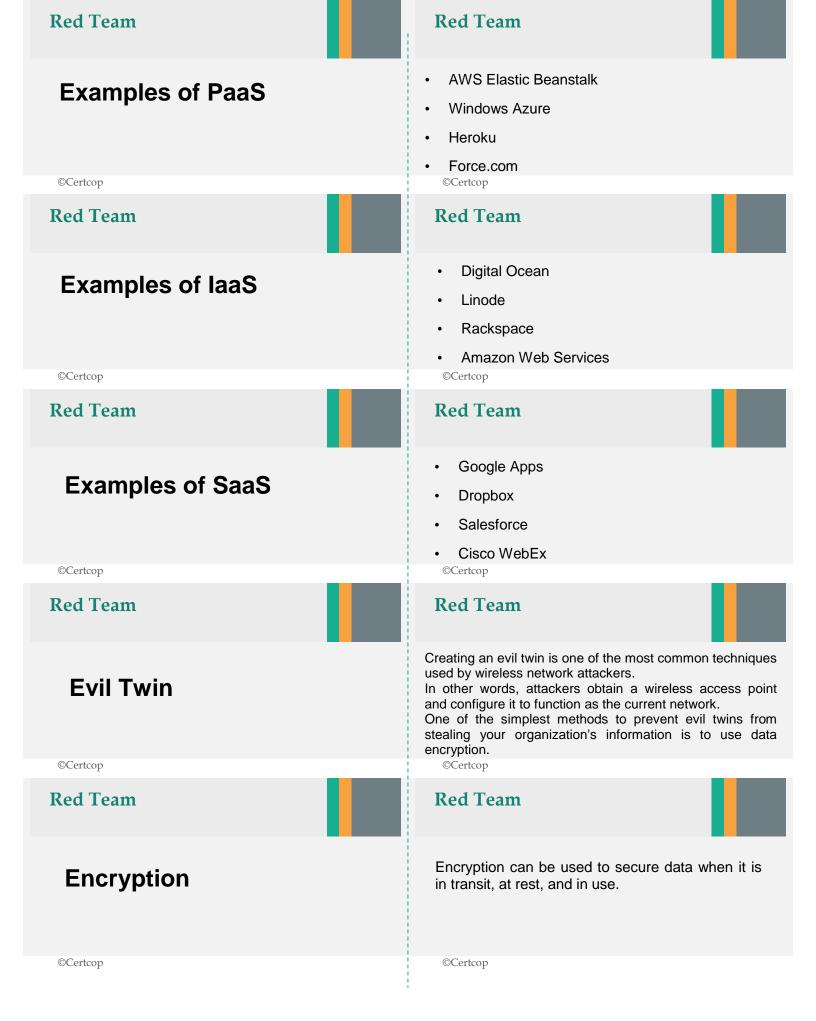






Red Team	Red Team
Data Caching	Caching in mobile devices used to interact with web apps, attackers attempt to exploit the data caches
©Certcop	©Certcop
Red Team	Red Team
Destroy phase	Furthermore, we would need to delete data from the production process and then sanitise the media.
©Certcop	©Certcop
Red Team	Red Team
Dynamic Runtime Injection	Attackers handle and misuse a program to overcome security locks, logic checks, rights access sections of the app, and rob data Runtime Injection.
©Certcop	©Certcop
Red Team	Red Team
Digital Authentication	The process of establishing confidence in user identities presented digitally to a system, which was previously referred to as Electronic Authentication (E-Authentication)
©Certcop	©Certcop
Red Team	Red Team
DNS Poisoning	Attackers utilize DNS servers, forward website users to another attacker's website DNS Poisoning.
©Certcop	©Certcop



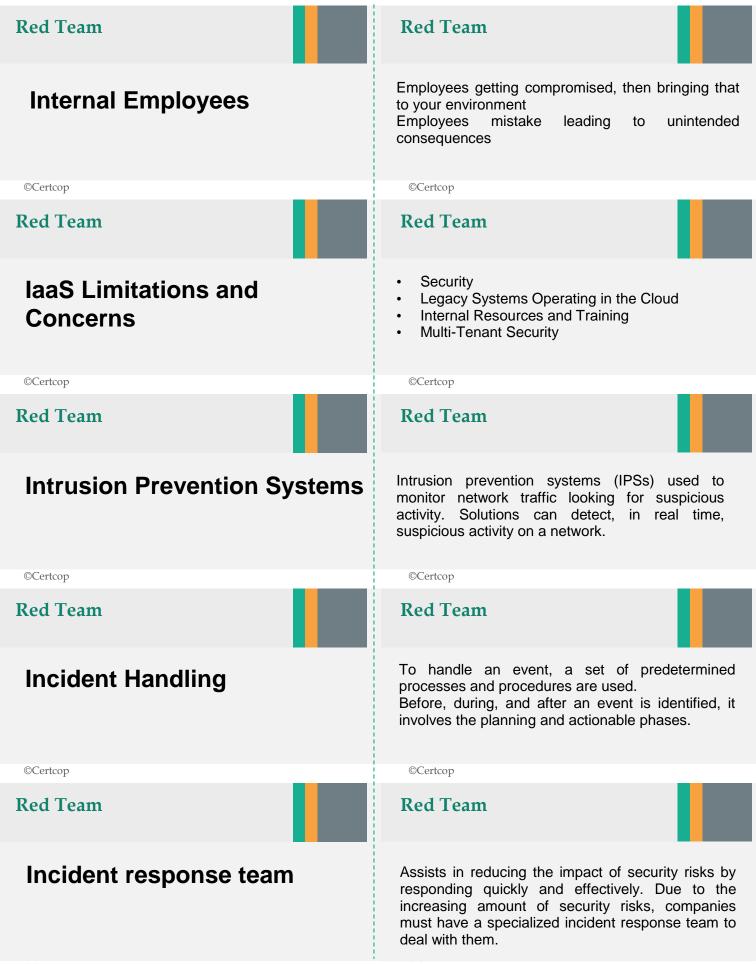


Red Team	Red Team
Firewalls	Firewalls can be classified into two broad categories: stateless or state full and can be network based or host based. Firewalls typically block or allow traffic based on ports, protocols, and service.
©Certcop	©Certcop
Red Team	Red Team
First Aid Drones	For example, if two individuals were strolling along a street and one collapses, this would be a scenario. In instances like these, abrupt heart arrest may be a life-threatening cause (SCA).
©Certcop	©Certcop
Red Team	Red Team
FIDO Alliance	FIDO Authentication enables password-only logins to be replaced with secure and fast login experiences across websites and apps.
©Certcop	©Certcop
Red Team	Red Team
Firewalls	Firewalls can be classified into two broad categories: stateless or state full and can be network based or host based. Firewalls typically block or allow traffic based on ports, protocols, and service.
©Certcop	©Certcop
Red Team	Red Team
File Storage	The data is stored and viewed as files and directories, with all of the same hierarchical and naming features as in a conventional environment.
<b>File Storage</b> ©Certcop	directories, with all of the same hierarchical and

Red Team	Red Team
Framing	Website combined with iFrame components in HTML in another webpage
©Certcop	©Certcop
Red Team	Red Team
Google Vulnerability Reward Program (VRP)	We have long enjoyed a close relationship with the security research community. To honor all the cutting-edge external contributions that help us keep our users safe, we maintain a Vulnerability Reward Program for Google-owned web properties, running continuously since November 2010.
©Certcop	©Certcop
Red Team	Red Team
Git Repositories	Misconfigured repositories leaking sensitive data Mistakes in commits, publishing sensitive data
©Certcop	©Certcop
Red Team	Red Team
Gaining Access	The goal of a modern-day attack is to gain access to resources. Extract valuable information for the attacker or to utilize the network as a launch pad.
©Certcop	©Certcop
Red Team	Red Team
Hashing	Using a one-way cryptographic function to create a digest of the original data
©Certcop	©Certcop

Red Team	Red Team
HR/Legal Representation	Legal and HR guidance and participation
©Certcop	©Certcop
Red Team	Red Team
Honey trap	In this assault, the social engineer disguises himself as an attractive person in order to engage with a person online, create an online relationship, and acquire sensitive information through that interaction.
©Certcop	©Certcop
Red Team	Red Team
Integrity	It provides assurances that data has not changed, been one has modified, tampered with, or corrupted the data.
©Certcop	©Certcop
Red Team	Red Team
Infrastructure as a Service (laaS)	Organization outsource equipment requirements, hardware, VMs, etc . Provider owns equipment, data centre
©Certcop	©Certcop
Red Team	Red Team
Incident response plan (IRP)	An incident response plan is a set of instructions designed to assist IT personnel in detecting, responding to, and recovering from network
	security issues.

Red Team	Red Team
Intrusion Detection Systems	If an attack is detected, the intrusion detection system (IDS) will notify a management system or can be programmed to send emails or SMS notifications.
©Certcop	©Certcop
Red Team	Red Team
laaS Use	It has authority over operating systems; storage, installed applications, and maybe limited authority over some networking components (e.g., host firewalls).
©Certcop	©Certcop
Red Team	Red Team
laaS Delivery	<ul> <li>IaaS delivers cloud computing infrastructure through virtualization technology.</li> <li>IaaS clients can still access their servers and storage directly, but it is all outsourced through a "virtual data center" in the cloud.</li> </ul>
©Certcop	©Certcop
Red Team	Red Team
laaS manages	<ul> <li>Servers</li> <li>hard drives</li> <li>Networking</li> <li>Virtualization</li> <li>Storage</li> </ul>
©Certcop	©Certcop
Red Team	Red Team
laaS Advantages	<ul> <li>The most flexible cloud computing model</li> <li>Hardware purchases can be based on consumption</li> <li>Clients retain complete control of their infrastructure</li> <li>Resources can be purchased as-needed</li> <li>Highly scalable</li> </ul>
©Certcop	©Certcop



©Certcop



Red Team	Red Team
iBoot Exploit	A jailbreak iBoot permits access to the file system and level iboot. If a fresh boot-rom is in place, this sort of exploit can be semi-tethered. This is used mostly for reducing iOS controls at low level.
©Certcop	©Certcop
Red Team	Red Team
inSSIDer	It is comparable to the old Net Stumbler tool, except that it has been updated and works with Windows XP, Vista, and Windows 7. The program detects wireless networks and reports on their kind, maximum transfer rate, and channel utilization.
©Certcop	©Certcop
Red Team	Red Team
John the Ripper	It is a fantastic program for breaking passwords. Well-known brute-force techniques such as dictionary and bespoke wordlist attacks. It can also be used to crack hashes or passwords for zipped or compressed data, as well as locked
©Certcop	©Certcop
Red Team	Red Team
Jamming	The goal of jamming is to interrupt the network. Interference is almost unavoidable due to the wireless characteristics. Mild interference can be caused by Bluetooth headphones.
©Certcop	©Certcop
Red Team	Red Team
Lead Investigator	Collects and analyzes all evidence and implements rapid system and service recovery.

Red Team	Red Team
Linux Kernel	The core of the Android architecture is Linux Kernel. It manages all drivers accessible, such as Display controls, Camera ports
©Certcop	©Certcop
Red Team	Red Team
Multi-Tenant Security	Multi-tenancy is a software architecture that uses a single application to serve multiple customers (or tenants). By using multi-tenancy, you can create one application and then deploy it to as many customers as you want, so you don't have to recreate a separate solution for each end user.
©Certcop	©Certcop
Red Team	Red Team
Metasploit	Ethical hackers can use to investigate systemic vulnerabilities on networks and servers. It can be easily customized and used with most operating systems because it is an open-source framework.
©Certcop	©Certcop
Red Team	Red Team
Man in the Middle	An attacker has connections between two systems across the current network
©Certcop	©Certcop
Red Team	Red Team
Next Gen Firewalls	A next generation firewall (NGFW) is, as Gartner defines it, a "deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall."

Red Team	Red Team
NIST Security Working Group	The NIST Cloud Service Public Working Group (PWG) provides guidance for better understanding and categorizing cloud services
©Certcop	©Certcop
Red Team	Red Team
Nmap	Nmap is characterized as a tool used by a network administrator. It uses to discover and troubleshoot services operating on a networked machine.
©Certcop	©Certcop
Red Team	Red Team
NotPetya	NotPetya was unable to be decrypted. Users and organisations never received anything in return, even if they paid up. Petya ransomware strains, according to experts, inflicted over \$10 billion in damage as they swept
©Certcop	©Certcop
Red Team	Red Team
No encryption / faint encryption	Unsecured or weakly encrypted data transmission applications are capable to attack, for example hijacking session
©Certcop	©Certcop
Red Team	Red Team
NGINX	In addition to being used as a web server, Nginx is also utilized as a reverse proxy, HTTP cache, and load balancer. There are a number of well-known organizations that use Nginx such asAutodesk Atlassian
©Certcop	©Certcop
-	-

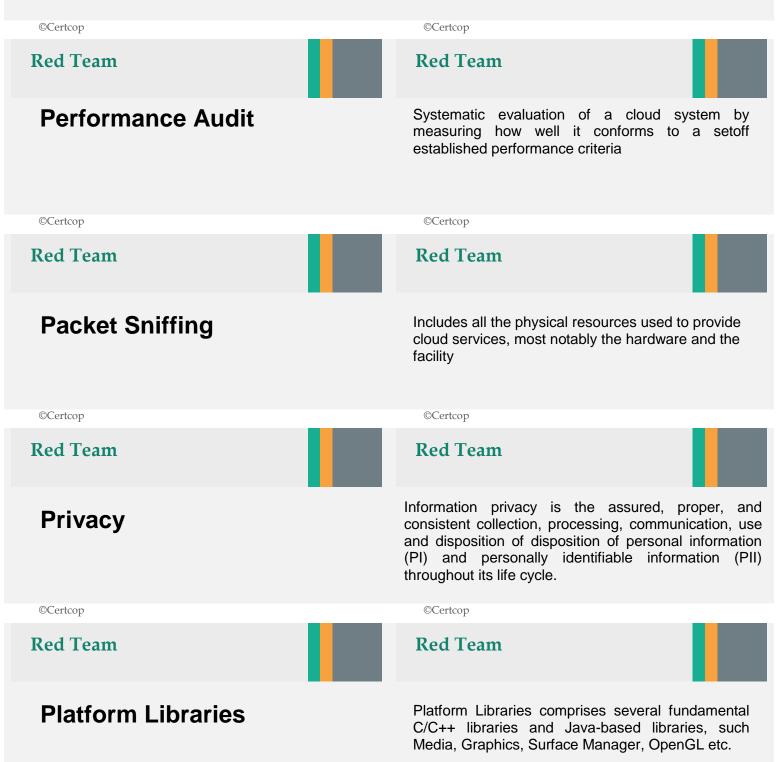
Red Team	Red Team
Nikto	Nikto is a free software command-line vulnerability scanner. This scans webservers for dangerous files/CGIs, outdated server software and other problems.
©Certcop	©Certcop
Red Team	Red Team
Nessus	Nessus examines your computer and alerts you if it finds any weaknesses. In order to do so, it runs over 1200 checks on a particular machine.
©Certcop	©Certcop
Red Team	Red Team
Object-Based Storage	Data is saved in the form of objects rather than files or blocks.
©Certcop	©Certcop
Red Team	Red Team
Ponotration Tast Mathadalagy	
Penetration Test Methodology	API Testing
and Requirements	Mobile Application Testing
	Network Testing
©Certcop	©Certcop
Red Team	Red Team
Public Cloud	A cloud deployment model (see SSP Table 8-2). The cloud services and infrastructure support multiple organizations and agency clients.
©Certcop	©Certcop

# Programmable Logic Controllers (PLCS)



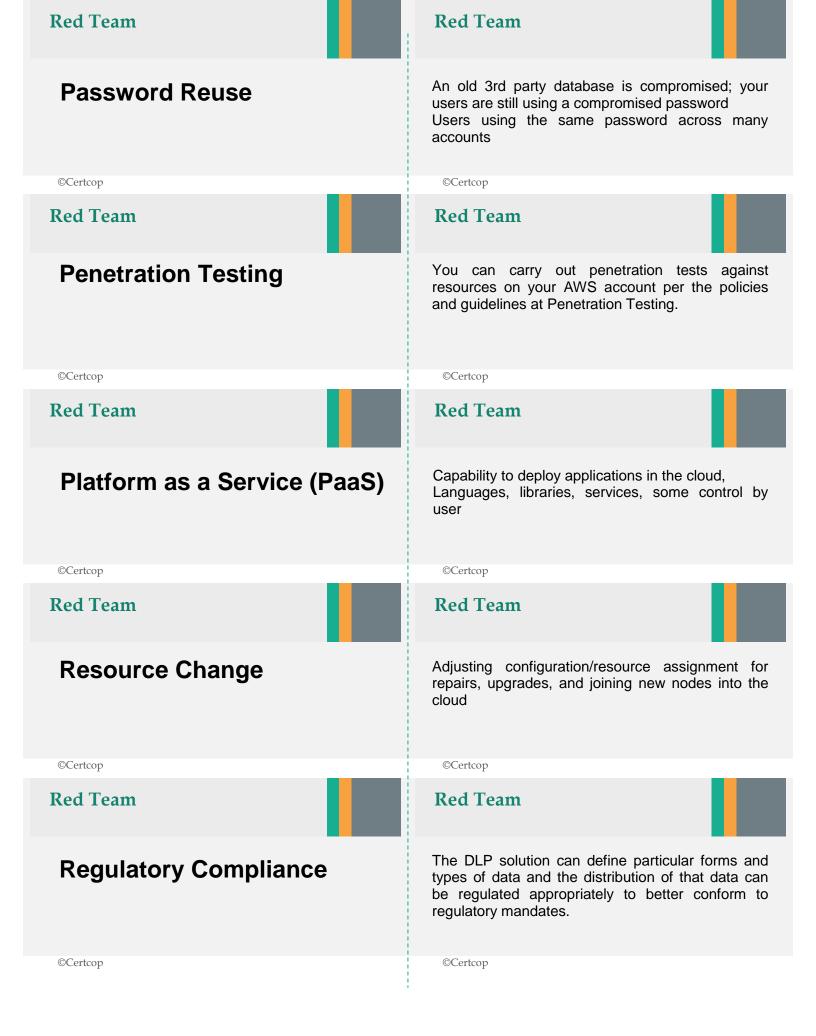
It is a digital computer used to handle common industrial electromechanical operations

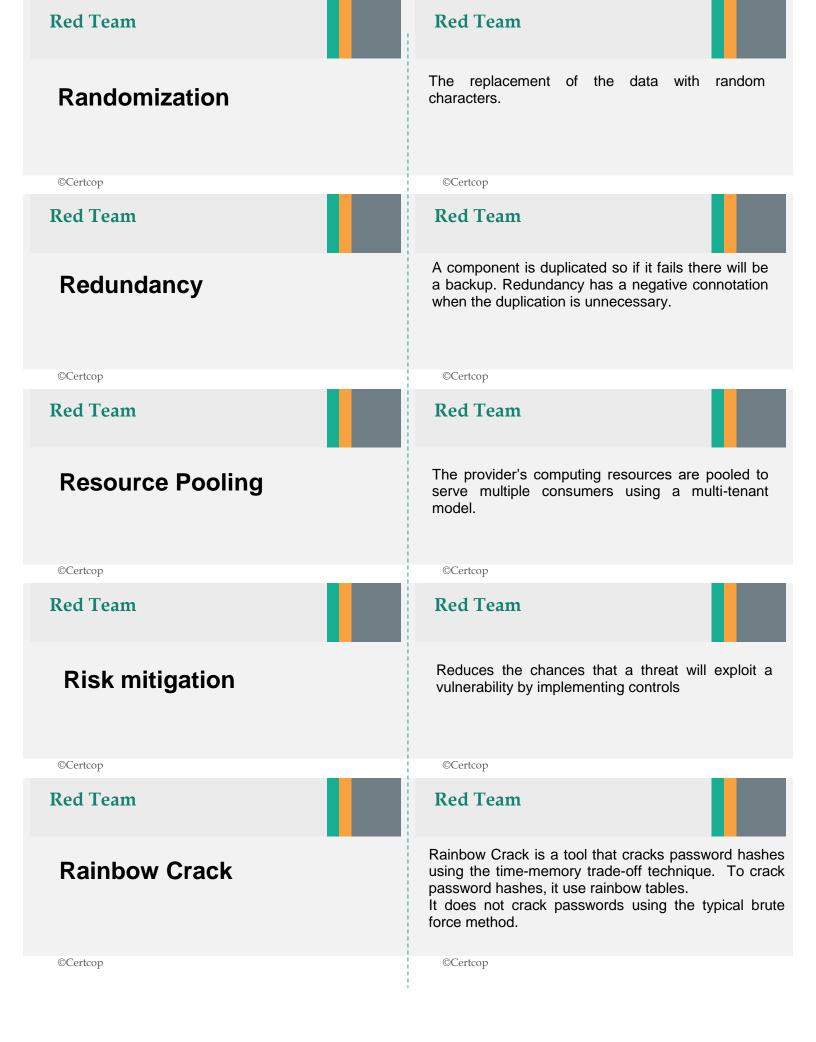
In various machines, in many sectors, practical PLCs are employed. It is intended for a variety of digital and analog inputs and outputs



Red Team	Red Team
Private Cloud	The cloud services and infrastructure are dedicated to a specific organization/agency and to no other clients.
©Certcop	©Certcop
Red Team	Red Team
Phishing	When a malevolent entity sends a fraudulent email masquerading as a real email, frequently from a trustworthy source. The message's purpose is to dupe the receiver into disclosing financial or personal information or clicking on a link that installs malware.
©Certcop	©Certcop
Red Team	Red Team
Pangu	Pangu team comprises a number of prominent security scientists and focuses on mobile security research. It is famous for several jailbreak tools released in 2014 for iOS 7 and iOS 8.
©Certcop Red Team	©Certcop Red Team
Pharming	A cybercriminal installs malicious code on a computer or server that automatically redirects the user to a phony website, where the user may be fooled into revealing personal information.
©Certcop	©Certcop
Red Team	Red Team
Password Cracking	THC Hydra uses brute force attack to crack virtually any remote authentication service.

Red Team	Red Team
PaaS Characteristics	<ul> <li>Provides a variety of services to assist with the development, testing, and deployment of apps</li> <li>Accessible to numerous users via the same development application</li> <li>Integrates web services and databases</li> </ul>
©Certcop	©Certcop
Red Team	Red Team
PaaS Delivery	This platform is delivered via the web, giving developers the freedom to concentrate on building the software without having to worry about operating systems, software updates, storage, or infrastructure.
©Certcop	©Certcop
Red Team	Red Team
Platform vulnerabilities	Exploiting vulnerabilities in the OS, Server software, or app modules running on the web server
©Certcop	©Certcop
Red Team	Red Team
Pretexting	To acquire access to sensitive data, one party lies to another. A pretexting fraud, for example, may entail an attacker pretending to request financial or personal information to authenticate the recipient's identity.
©Certcop	©Certcop
Red Team	Red Team
Petya	Petya - and its follow-up, NotPetya, were ransomware variants with humorous names. The Petya ransomware wreaked havoc on computers by encrypting the master file table.
©Certcop	©Certcop







# Red Team Social engineering

©Certcop

**Red Team** 

# **Smart cars**

©Certcop

**Red Team** 

# Supervisory Control And Data Acquisition (SCADA)

©Certcop

**Red Team** 

**Spare Phishing** 

©Certcop

Red Team

### Sensitive data storage

#### **Red Team**



Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime,

#### ©Certcop





Develop independent vehicles.

Investments in autonomous vehicles have reached over \$100 billion, According to the International Business Times, as automotive companies are the first companies to produce an automotive vehicle.

©Certcop

#### **Red Team**



SCADA is an industrial control system

It usually uses geographical dispersed assets that are often spread across long distances.

Control and acquisition control is an industrial control system. It is for process control and in order to regulate equipment and circumstances from remote places in real time.

©Certcop

**Red Team** 



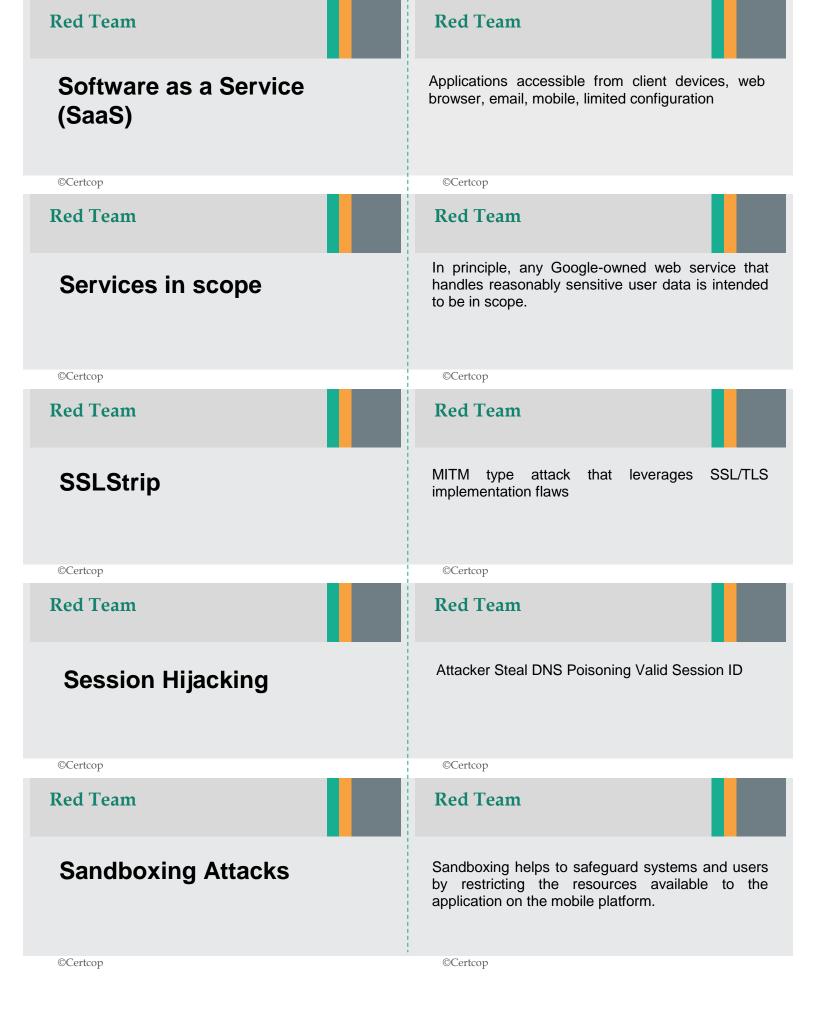
It is a type of deception. This is similar to phishing, except the rootkit or malware is customized to a specific person or organization.

©Certcop

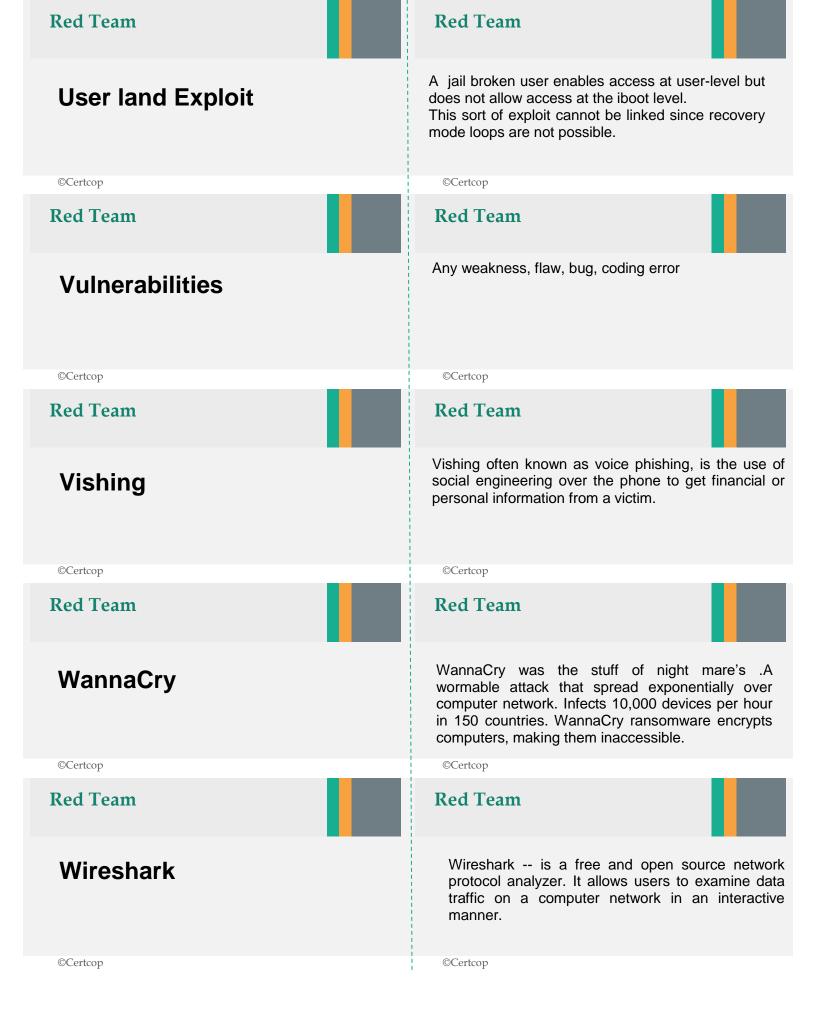
**Red Team** 



Some applications utilize a poor security system in their database design, such that attackers may hack and steal sensitive user information.



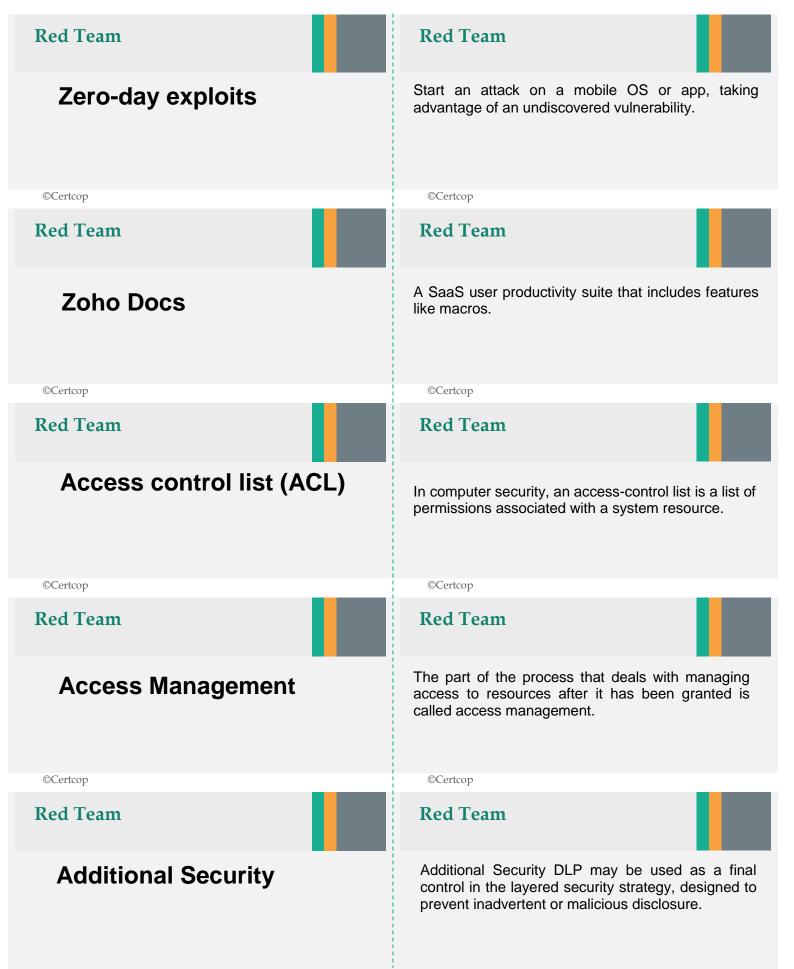


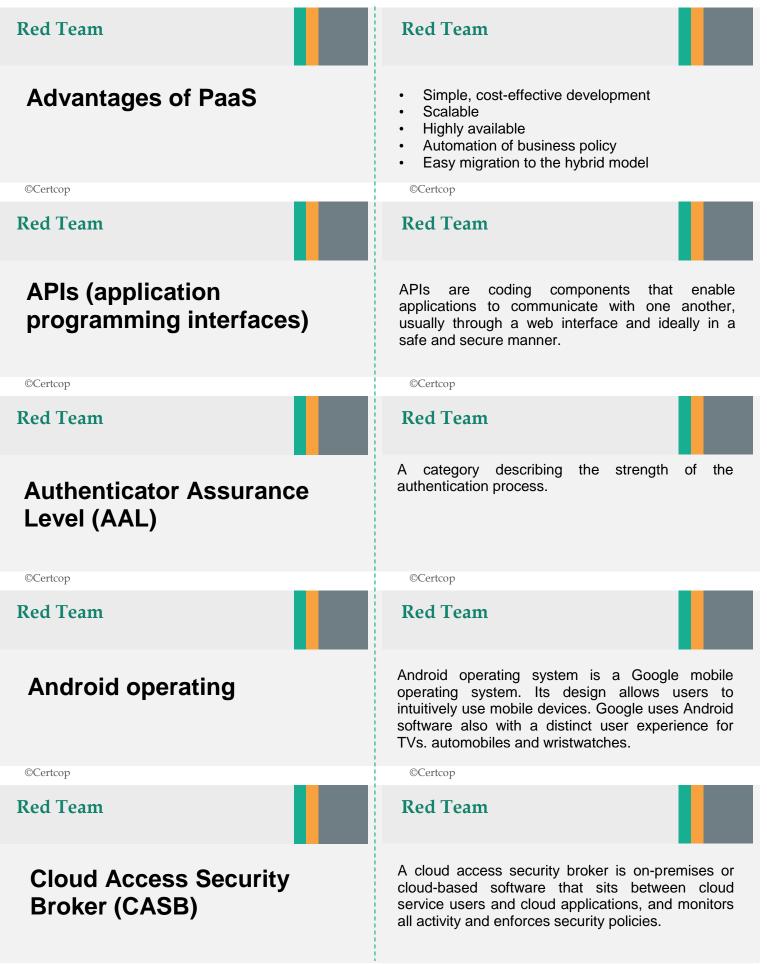


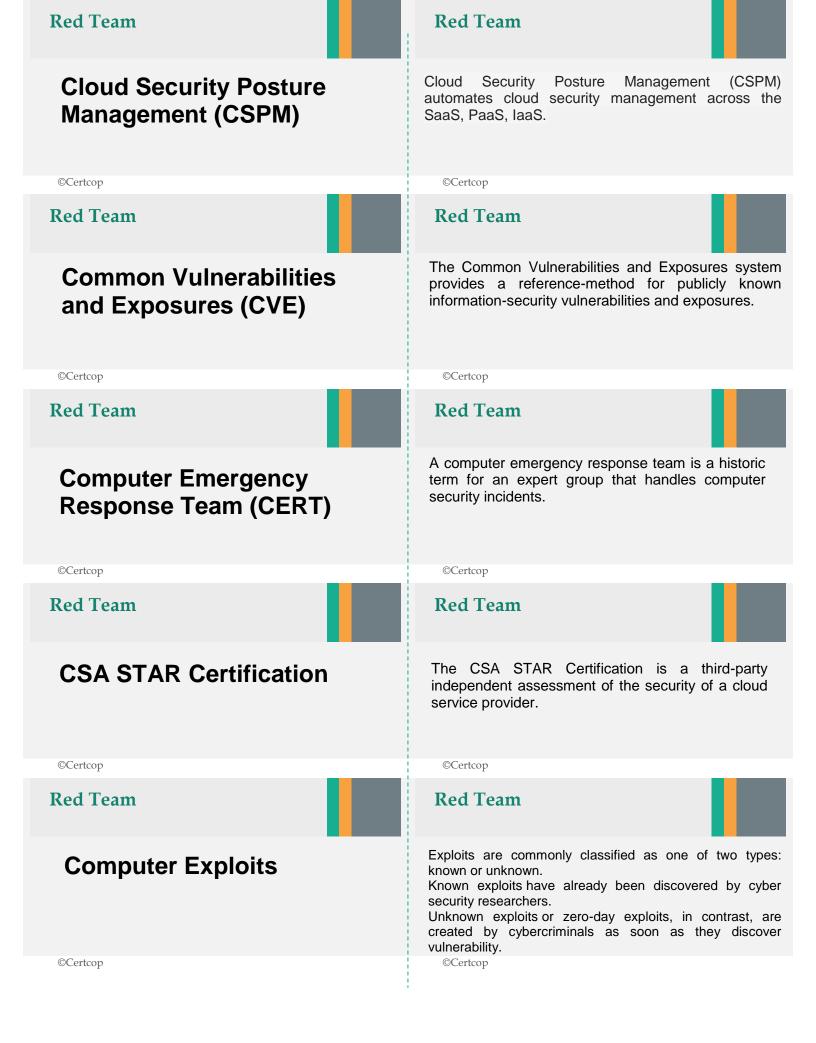
Red Team	Red Team
Whaling	A whale assault is a sort of phishing attack that targets high-profile workers, such as the chief financial officer or CEO, in order to deceive the targeted employee into giving critical information.
©Certcop	©Certcop
Red Team	Red Team
Watering hole	In order to acquire network access, the attacker attempts to compromise a specific group of individuals by infecting websites they are known to visit and trust.
©Certcop	©Certcop
Red Team	Red Team
WEB Servers	It is a machine on which the content of the web is kept. There are several types of web servers available, including Gaming, Storage, FTP
©Certcop	©Certcop
Red Team	Red Team
WPScan	WPScan is a free and open-source security scanner for the WordPress platform. You can check for known vulnerabilities in the WordPress core. You can also check for known vulnerabilities in plugins and themes.
©Certcop	©Certcop
Red Team	Red Team
Wireess Networking	Connecting multiple devices without any physical connection. Transfer data through Radio Frequency
©Certcop	©Certcop

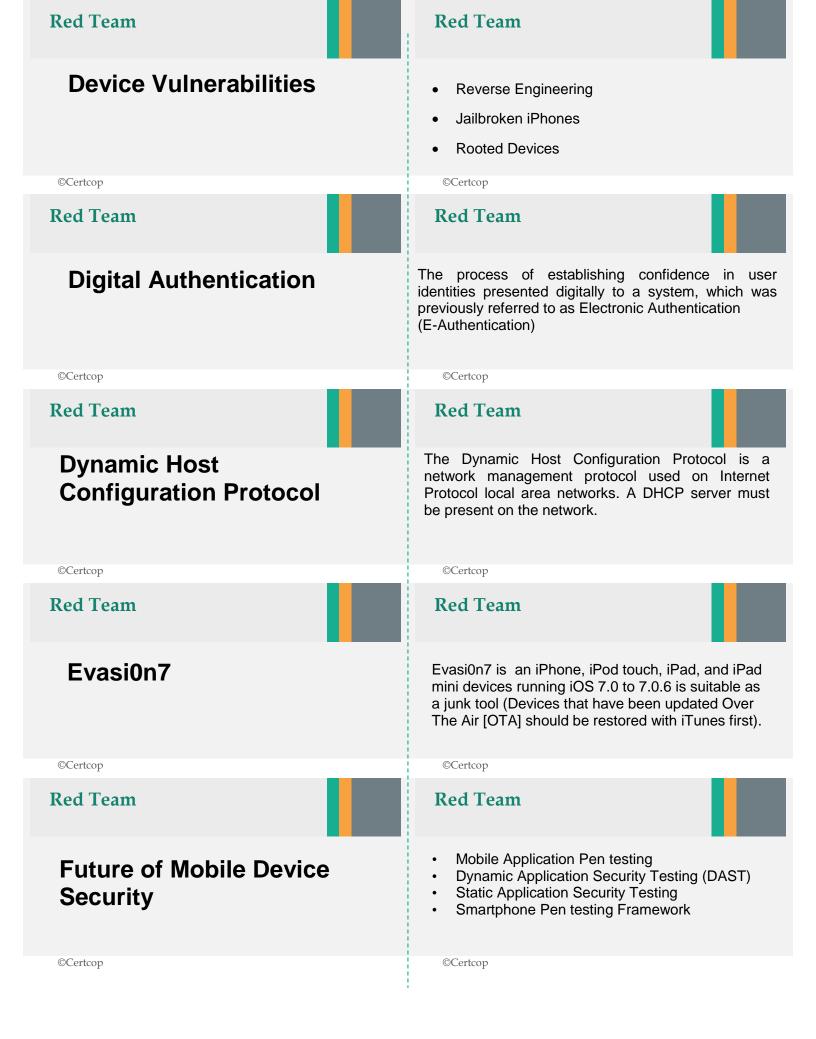
Red Team	Red Team
WLAN	WLAN is a network that connects two or more computers using a wireless distribution mechanism. They have high-frequency radio waves and an internet access point (AP).
©Certcop	©Certcop
Red Team	Red Team
WMAN	WMAN is a wireless metropolitan area network capable of covering an entire city. It is larger than WLAN but smaller than WWAN.
©Certcop	©Certcop
Red Team	Red Team
Wired Equivalent Privacy (WEP)	WEP was accepted as a Wi-Fi security standard after being created for wireless networks. The first encryption system designed specifically for wireless networks WEP, on the other hand, has several well-known security vulnerabilities, is complex to configure, and is readily cracked.
©Certcop	©Certcop
Red Team	Red Team
Wi-Fi Protected Access (WPA)	<ul> <li>WPA was introduced as an interim security upgrade over</li> <li>WEP while the 802.11i wireless security standard was being developed.</li> <li>For encryption, most modern WPA implementations employ a pre-shared key (PSK).</li> <li>To produce keys or certificates, WPA Enterprise use an authentication server.</li> </ul>
©Certcop	©Certcop
Red Team	Red Team
Wi-Fi Protected Access (WPA2)	A wireless security standard based on the 802.11i wireless security standard WPS assaults remains significant in contemporary WPA2-capable access points, as is the case with WPA.
©Certcop	©Certcop

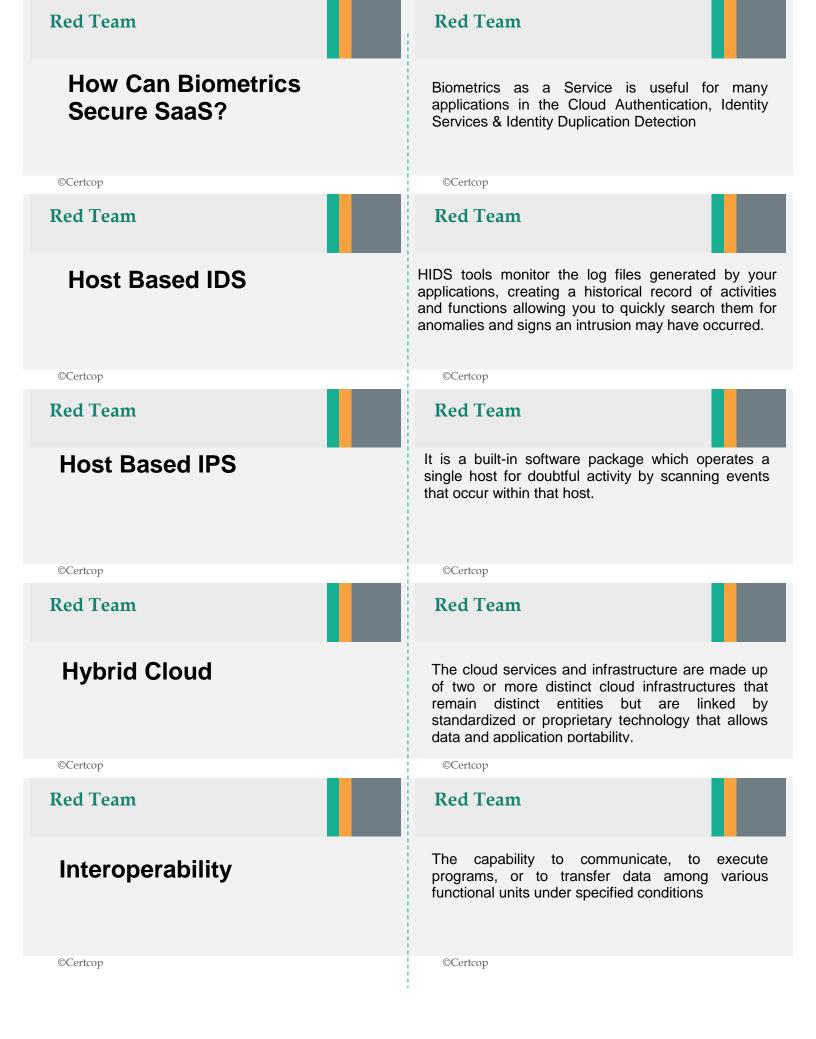
Red Team	Red Team
Wireless Wizard	Wireless Wizard is a free tool that will assist you in getting the greatest performance out of your wireless network connection. The program also includes a set of diagnostic tests that you can use to determine how well your wireless network is working.
©Certcop	©Certcop
Red Team	Red Team
Wireless Key Generator	It is a basic application for enhancing network security in the Wireless Key Generator. It invites you to choose the security type and key strength that you use on your wireless network. Then a random encoding key is generated for you to utilize.
©Certcop	©Certcop
Red Team	Red Team
Zero Day Exploit	Zero-day attacks target victims without warning by exploiting software defects that are unknown to the software's authors. Every year, these attacks become more widespread, therefore it's critical to be aware of the dangers.
©Certcop	©Certcop
Red Team	Red Team
ZigBee	Zigbee is a protocol used to link smart devices like lights, plugs, and smart locks to a home network. You can use this home network as-is with remote controls, like a Tradfri remote from IKEA.
©Certcop	©Certcop
Red Team	Red Team
Z-Wave	When it comes to wireless, radio frequency (RF) based communications. Z-Wave is one of the most popular options. A complete mesh network is supported by Z-Wave. Allowing many devices to interact with each other concurrently.
©Certcop	©Certcop

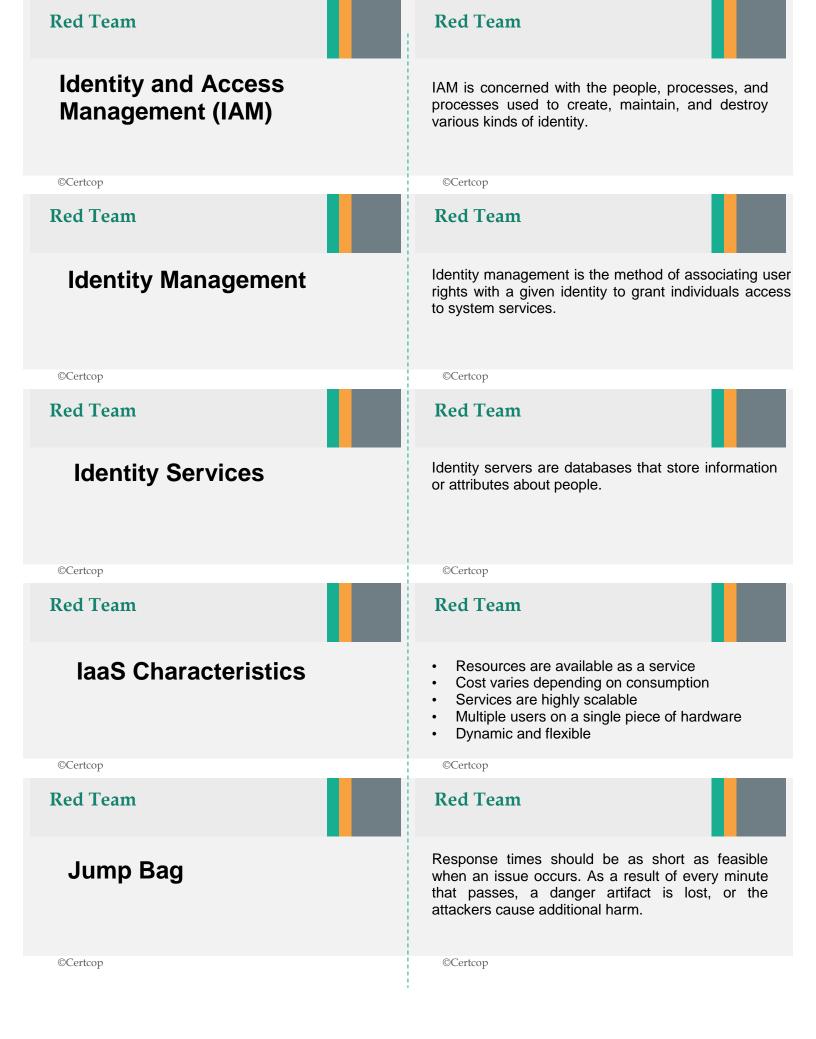


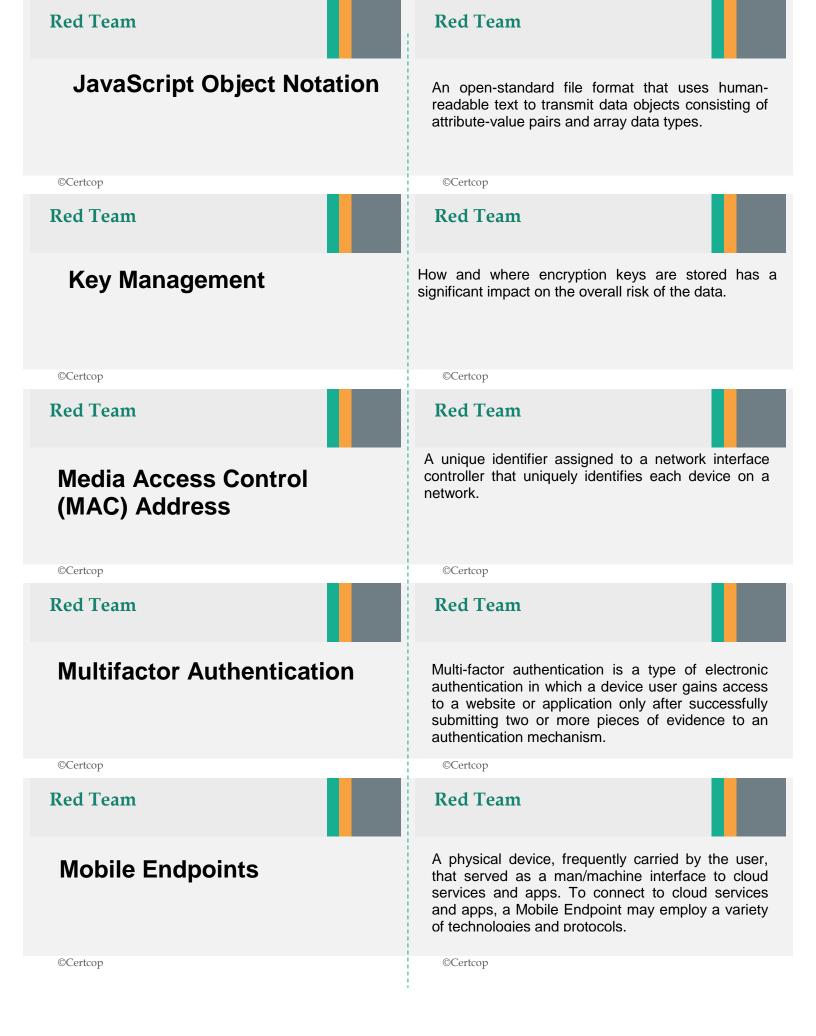


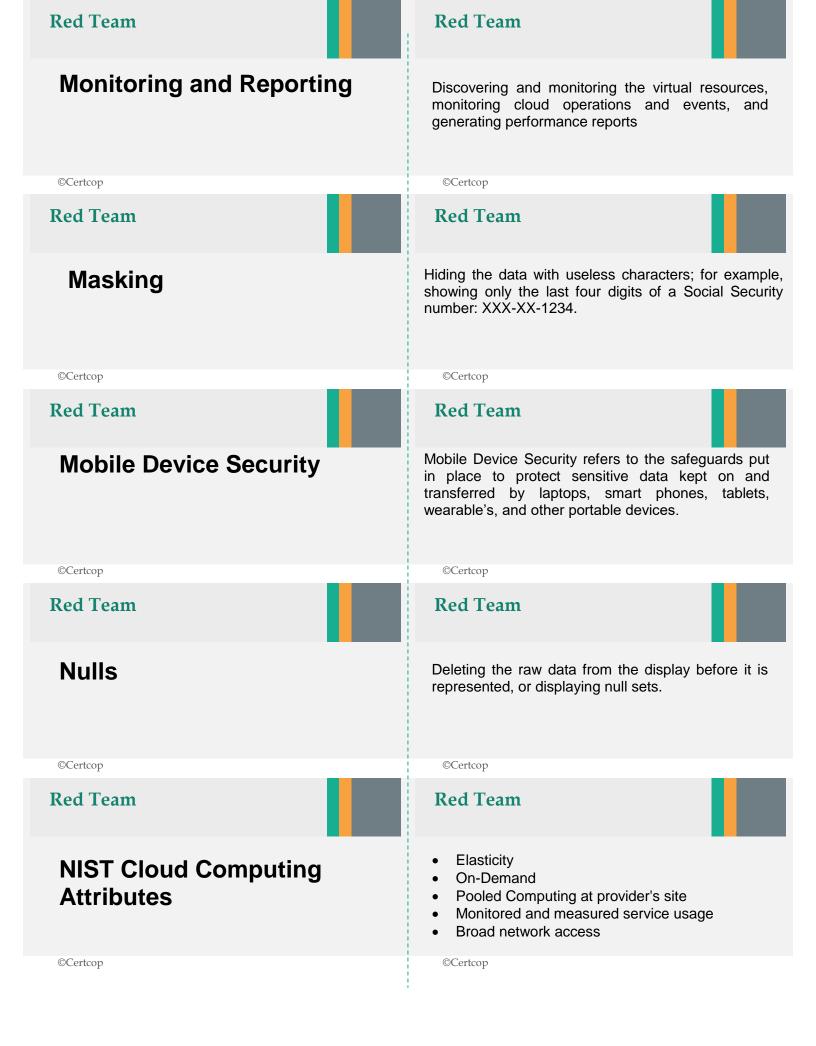


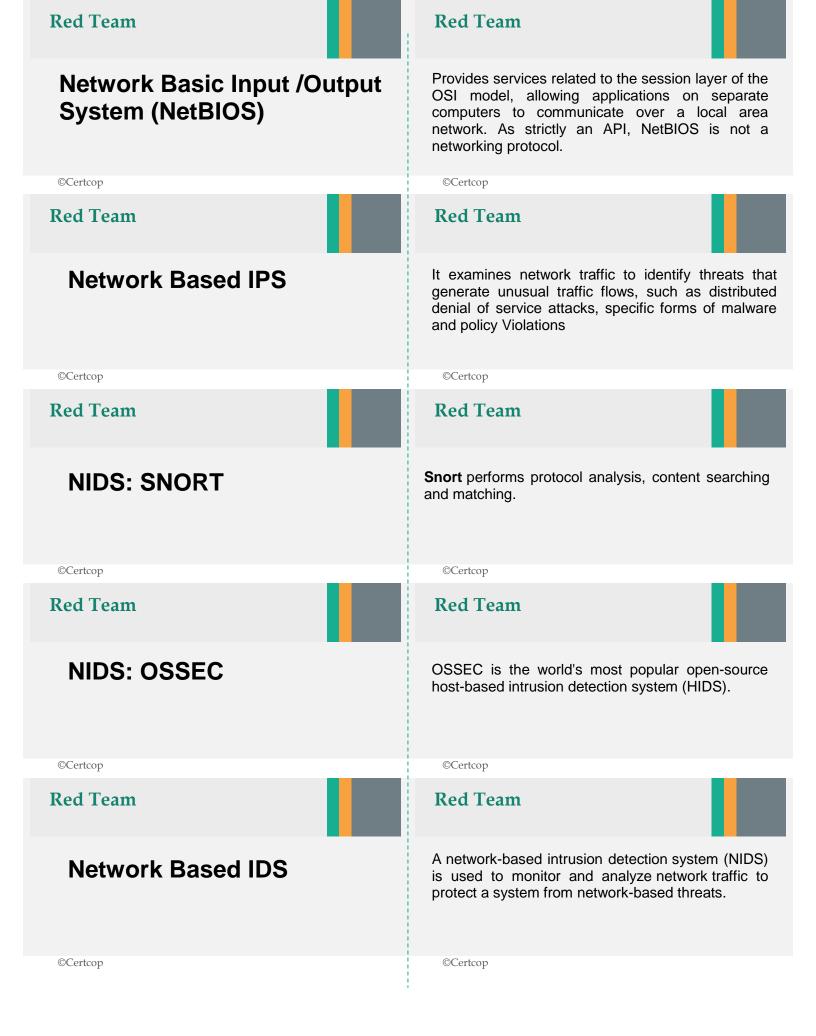


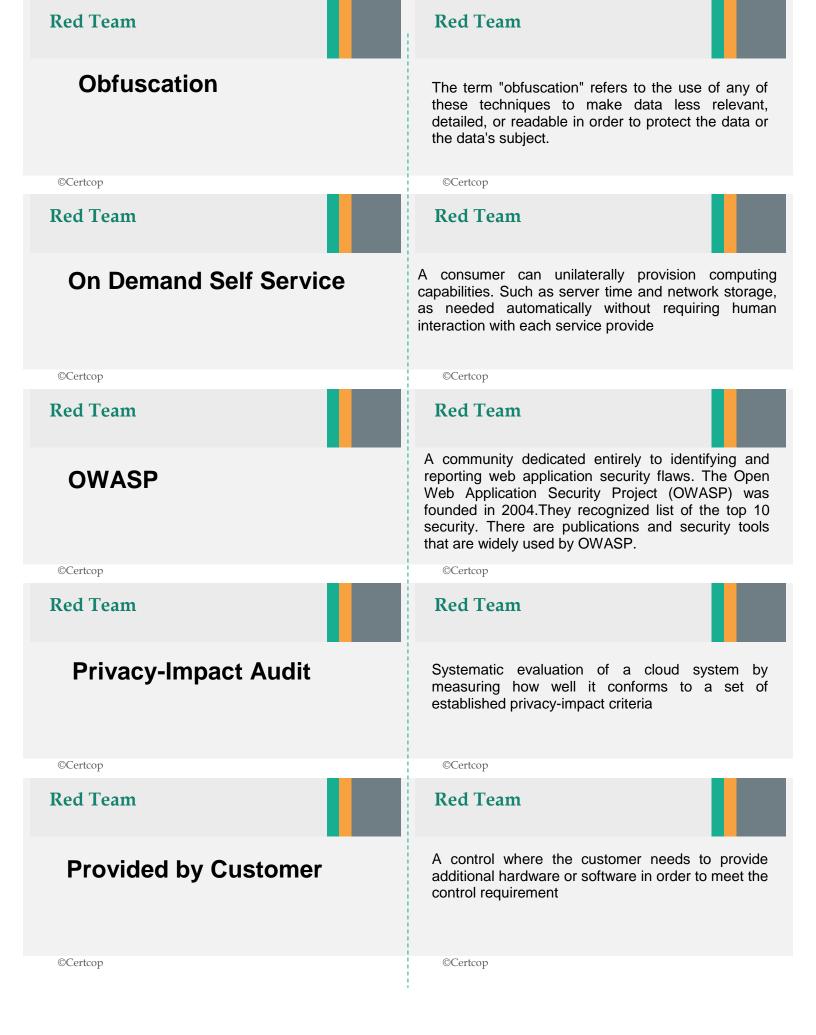


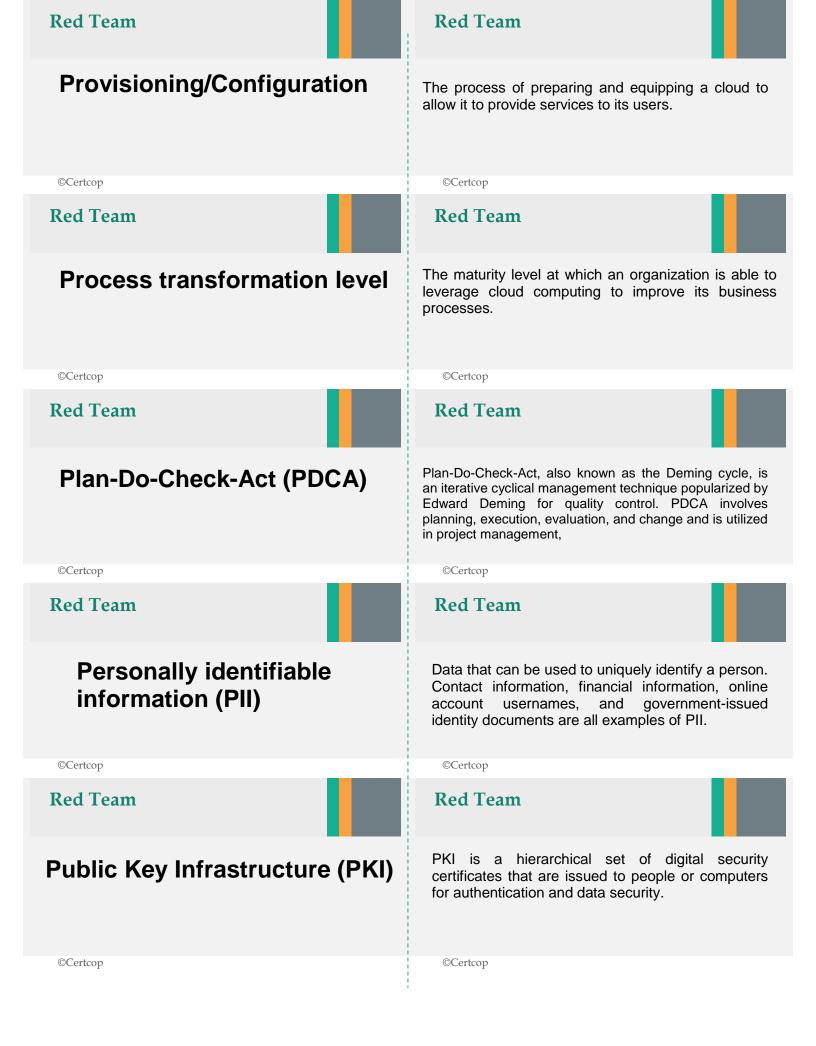




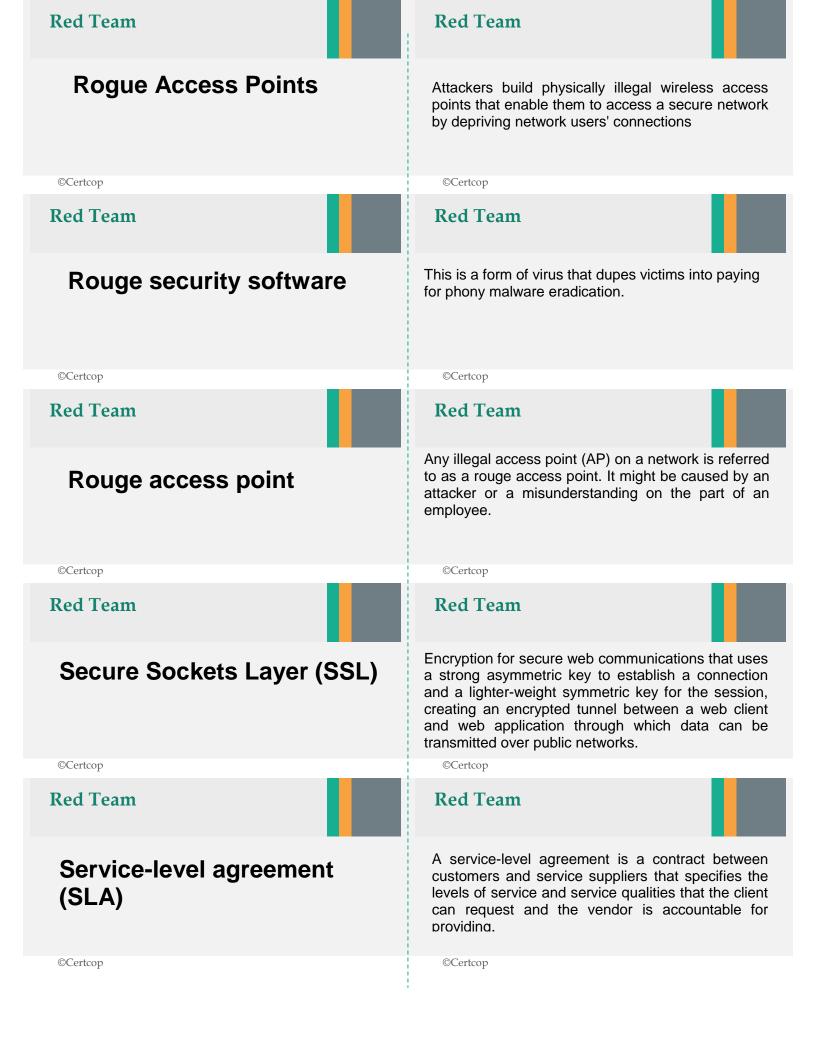




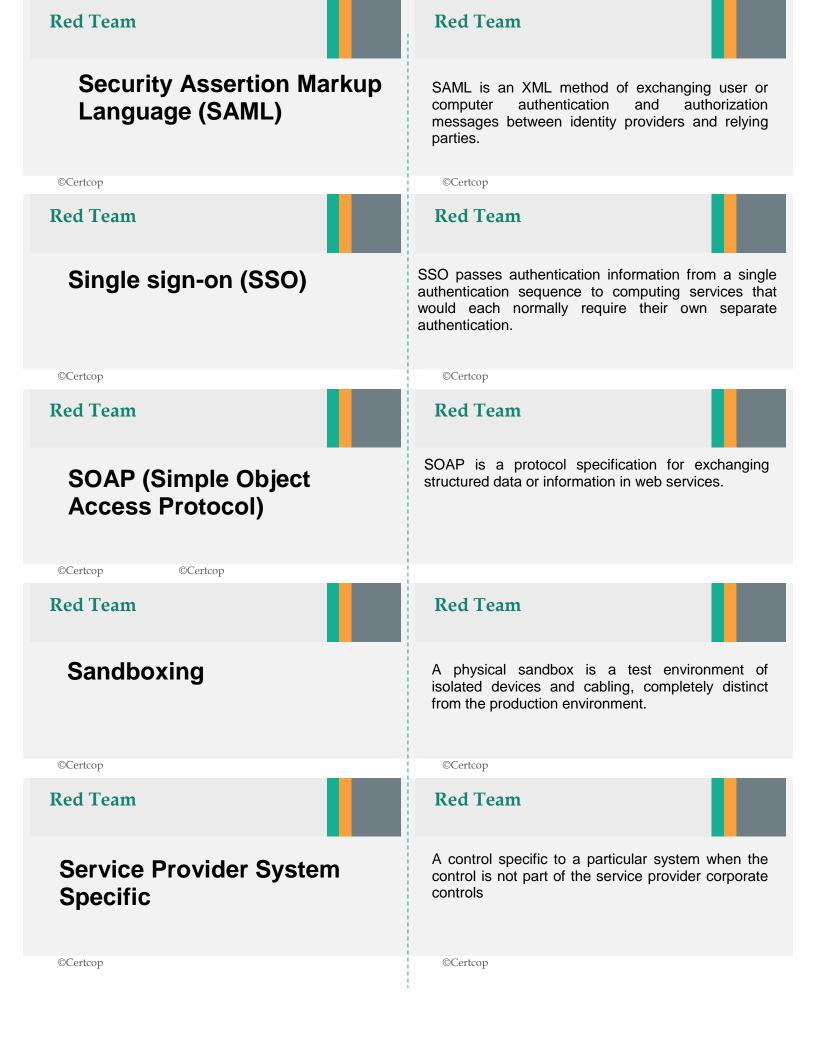








Red Team	Red Team
Service-oriented architecture (SOA)	A set of interface programming standards that allow software-to-software interoperability between applications written using differing API standards.
©Certcop	©Certcop
Red Team	Red Team
Sharding	Database sharding involves the separation of large or complex data sets into smaller shards for simultaneous processing or analysis across distributed cloud resources.
©Certcop	©Certcop
Red Team	Red Team
Shazam	A SaaS application that can identify an overhead song.
©Certcop	©Certcop
Red Team	Red Team
SkyDrive	An IaaS file storage service by Microsoft.
©Certcop	©Certcop
Red Team	Red Team
Staffing benefit	The ability to reduce or retask staff due to improvements in efficiency.
©Certcop	©Certcop



Red Team	Red Team
Threat Modeling	The IA must ensure the Penetration Test is appropriate for the size and complexity of the cloud system and takes into account the most critical security risks.
©Certcop	©Certcop
Red Team	Red Team
TRIAD- CIA	<ul> <li>Confidentiality</li> <li>Availability</li> <li>Integrity</li> </ul>
©Certcop	©Certcop
Red Team	Red Team
Three models of cloud service	<ul> <li>Software as a Service (SaaS)</li> <li>Platform as a Service (PaaS)</li> <li>Infrastructure as a Service (IaaS).</li> </ul>
©Certcop	©Certcop
Red Team	Red Team     Verify Cloud Provider's Security Implementations
Third Party Assessment Organizations (3PAO)	<ul> <li>Plan and Perform Security Assessments of the CSP Systems</li> <li>Review Security Package artifacts IAW FedRAMP requirements</li> <li>3PAO creates the Security Assessment Report (SAR)</li> </ul>
©Certcop	©Certcop
Red Team	Red Team
Types of threats	<ul> <li>Internal</li> <li>External</li> <li>Trusted</li> <li>Untrusted</li> </ul>
©Certcop	©Certcop

Red Team
----------

# Total cost of ownership (TCO)

©Certcop

Red Team

# **Time-sharing**

©Certcop

Red Team

**Thick client** 

©Certcop

**Red Team** 

# Thin client

©Certcop

Red Team

## Time to market

#### **Red Team**



The complete cost of an object or service throughout its lifetime, from purchase to disposal, including both direct and indirect costs.

#### ©Certcop

#### **Red Team**



This is when multiple users consume computing resources at the same time on the same system using independent computing sessions.

©Certcop

#### **Red Team**



A thick client, often known as a workstation, is an access device with powerful CPUs, local application storage, and connections to display and input devices. Thick clients may run apps locally while also utilizing distant cloud services as needed.

©Certcop

### Red Team



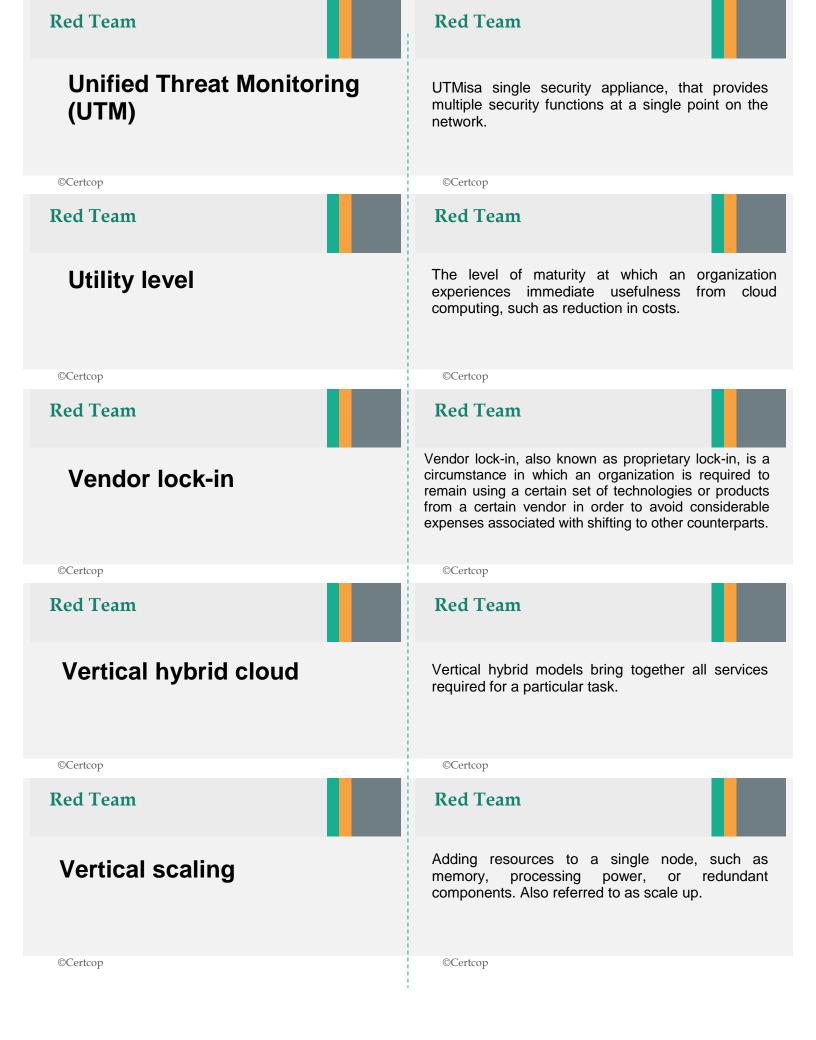
A thin client is an access device with minimal local processing power and display and input device connections but lacking local storage for applications. Thin clients require remote services to provide application functions and processing power.

©Certcop

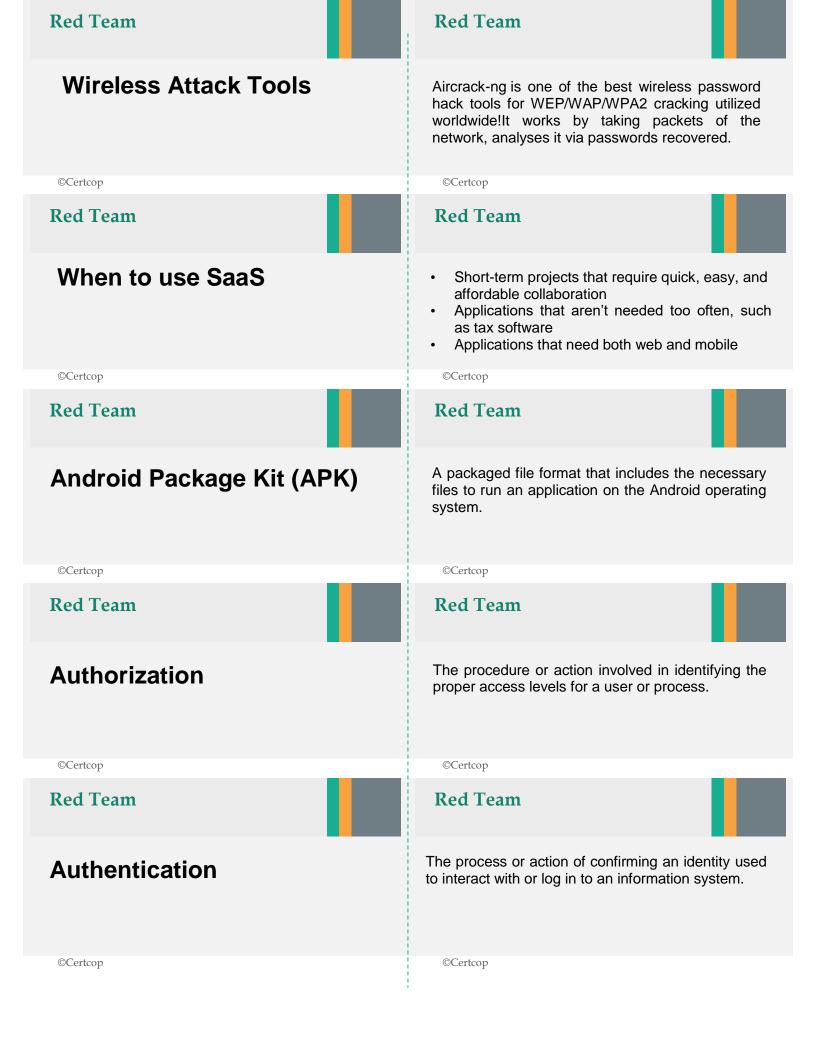
#### **Red Team**



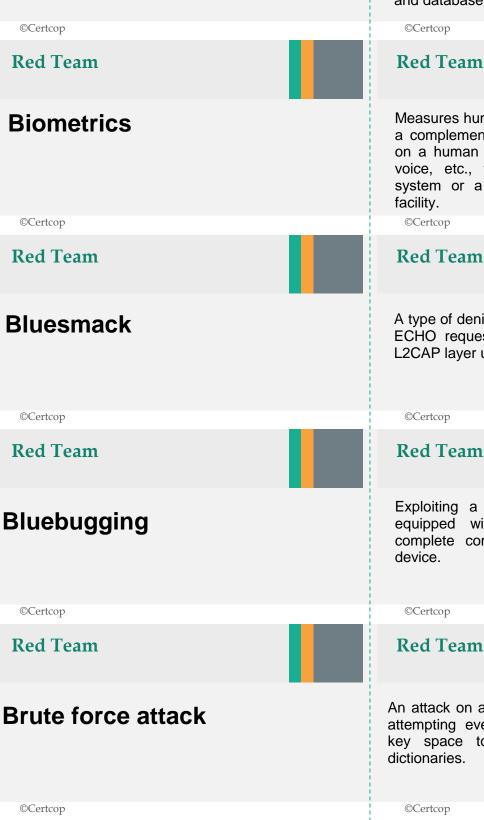
The amount of time from product conception to release.



Red Team	Red Team
Virtual firewall	A firewall developed particularly to protect virtual hosts, with varying modes of operation depending on deployment. The virtual firewall is installed within the network architecture like a typical firewall in bridge mode.
©Certcop	©Certcop
Red Team	Red Team
VMware vCloud	VMware vCloud is a VMware suite of products used to manage private clouds.
©Certcop	©Certcop
Red Team	Red Team
©Certcop	<ul> <li>Vulnerability Scanning</li> <li>Key Component of Risk Assessment</li> <li>Risk that a threat actor is going to exploit a vulnerability</li> <li>Risk Mitigation</li> </ul>
Red Team	Red Team
Vulnerability Types	<ul> <li>Unpatched Systems</li> <li>Misconfigured Systems</li> <li>Zero Days, web application vulnerabilities</li> <li>Injection attacks</li> </ul>
©Certcop	©Certcop
Red Team	Red Team
Volume Storage: File-Based Storage &Block Storage	The customer is given a storage space in the cloud, which is described as an attached drive to the user's virtual machine.
©Certcop	©Certcop



# **Blind (or inferential) SQL** injection



#### **Red Team**



An attack in which the attacker does not cause the program to display or transfer any data, but instead reconstructs the information by sending specified statements and observing the program's and database's activity.

#### **Red Team**



Measures human characteristics that can be used as a complementary authentication solution. They rely on a human attribute such as a retina, fingerprint, voice, etc., to permit access to an information system or a restricted area in an organization's

#### **Red Team**



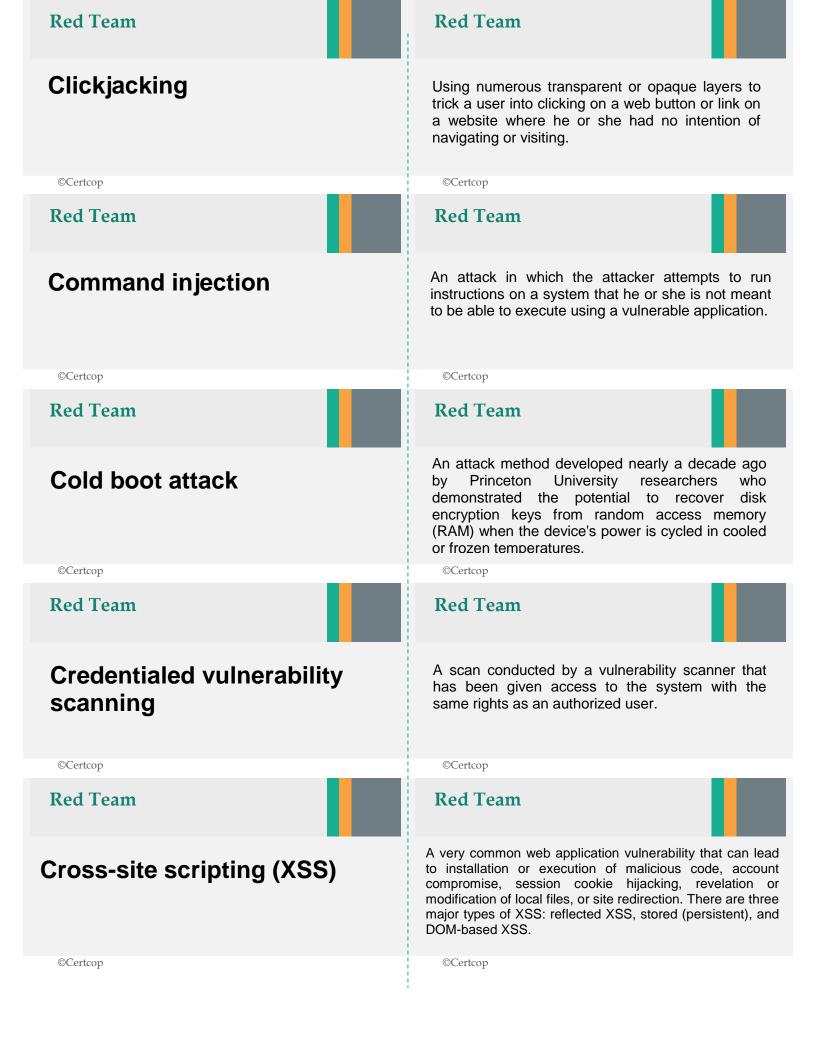
A type of denial-of-service (DoS) attack that targets ECHO requests from a Bluetooth peer over the L2CAP layer using an L2CAP ping.

Exploiting a weakness in older phone models equipped with Bluetooth technology to gain complete command and control of the mobile

#### **Red Team**



An attack on a hash, for example, would consist of attempting every possible combination inside the key space to break the hash, regardless of



Red Team	Red Team
Data mining	The process of analyzing large data sets to reveal patterns or hidden anomalies.
©Certcop	©Certcop
Red Team	Red Team
Dictionary attack	A type of password guessing attack that uses lists of possible passwords as the source for its guesses.
©Certcop	©Certcop
Red Team	Red Team
Document the threats	A step in the threat modeling process where the organization will match each threat, threat actor, and respective vulnerability relevant to the organization.
©Certcop	©Certcop
Red Team	Red Team
Dumpster diving	An unauthorized individual searches for and attempts to extract sensitive information from garbage.
©Certcop	©Certcop
Red Team	Red Team
Ethical hacker	A person who hacks into a computer network in order to test or evaluate its security rather than with malicious or criminal intent.
©Certcop	©Certcop

Red Team	Red Team
EXIF	Exchangeable image file format information from graphic files, as well as the information discovered through the URL of a scanned website.
©Certcop	©Certcop
Red Team	Red Team
Foot printing	Reconnaissance is the process of determining the nature of systems or organizations. It is how you structure your recon efforts and evaluate the outcomes.
©Certcop	©Certcop
Red Team	Red Team
Fuzzing	A security testing technique that sends unexpected, random data to an input control within an application or network service to generate errors in hopes of discovering or exposing security weaknesses that could be exploited.
©Certcop	©Certcop
Red Team	Red Team
Gray box testing	Broadly, a combination of black-box and white-box testing methodologies. Gray box testing assumes partial knowledge or understanding of the internal mechanisms of a system, network, or application.
©Certcop	©Certcop
Red Team	Red Team
Group Policy Objects (GPO)	A collection of settings that govern user and computer configurations within an Active Directory (AD) network.
©Certcop	©Certcop

# Hacktivist

©Certcop

**Red Team** 

# **HTML** injection

©Certcop

**Red Team** 

**HTTP** proxies

©Certcop

**Red Team** 

# **In-band SQL injection**

©Certcop

©Certcop

**Red Team** 

# iOS app store package (IPA)

©Certcop

**Red Team** A threat actor with various levels of knowledge and expertise who is politically or socially motivated. ©Certcop **Red Team** A vulnerability that occurs when an unauthorized user is able to control an input point and inject arbitrary HTML code into a web application. Successful exploitation could lead to disclosure of a user's session cookies, which could be used to impersonate a victim or to allow the attacker to modify the web page or the application content seen by victims. ©Certcop **Red Team** Proxies that make web server requests on behalf of other customers. They enable HTTP transfers over firewalls and can also provide HTTP message caching. Proxies can also play other roles in complicated systems, such as network address translation (NAT) and HTTP request screening. ©Certcop **Red Team** An attack in which the attacker acquires data through the same route used to inject SQL code. This is the most fundamental type of SQL injection attack, in which data is pushed directly into a web site.

©Certcop

#### **Red Team**



A Zip-compressed archive containing the necessary files to run an application on the Apple iOS mobile architecture.





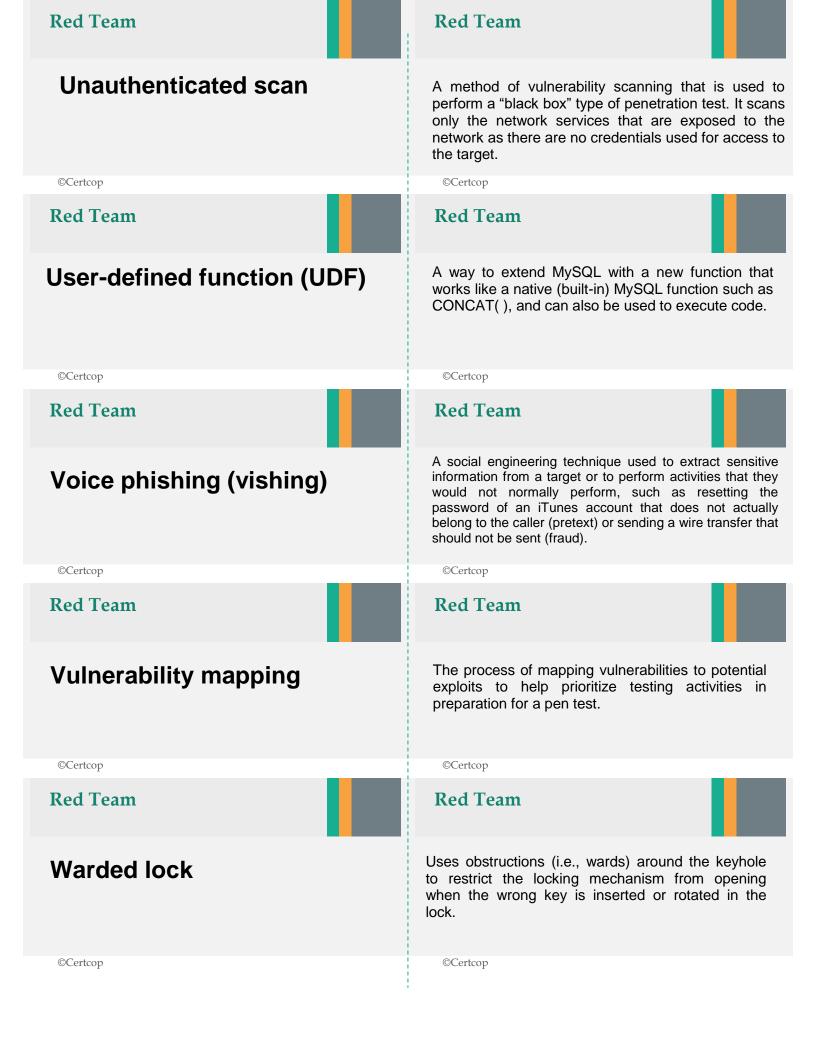
Red Team	Red Team
Locks	Locks perform numerous locking functions (e.g., entrance locks and deadlocks) to meet various types of security requirements.
©Certcop	©Certcop
Red Team	Red Team
Malvertising	The act of incorporating malicious ads on trusted websites, which results in users' browsers being inadvertently redirected to sites hosting malware.
©Certcop	©Certcop
Red Team	Red Team
Malware	A computer program that is covertly placed onto a computer with the intent of compromising the privacy, accuracy, or reliability of the computer's data, applications, or operating system.
©Certcop	©Certcop
Red Team	Red Team
Metasploit	One of the most popular exploitation frameworks.
©Certcop	©Certcop
Red Team	Red Team
Netgroup	A group of users or hosts used for permission checking when permitting remote operations such as mounting file shares, remote logins, remote execution, etc., in Linux and Unix network domain (e.g., NIS or LDAP) environments.
©Certcop	©Certcop



Red Team	Red Team
PowerSploit	A collection of PowerShell modules that can be used for post exploitation and other phases of an assessment.
©Certcop Red Team	©Certcop Red Team
Ransomware	A type of malicious software that either encrypts or steals the target's data and holds it for ransom until the threat actor is paid.
©Certcop	©Certcop
Red Team	Red Team
Red team assessment         ©Certcop	Involves stealth and blended methodologies to conduct scenarios of real-world attacks and determine how well an organization would fare given the use of the customer's existing counter-defence and detection capabilities.
Red Team	Red Team
Risk transfer	A process an organizations follows when it wants to shift risk liability and responsibility to other organizations. It is often accomplished by purchasing a cyber insurance policy.
©Certcop	©Certcop
Red Team	Red Team
Scarcity	A technique used to create a feeling of urgency in a decision-making context, to manipulate clients and in social engineering. It may involve telling a customer that an the offer is valid for one day only or that there are limited supplies.
©Certcop	©Certcop

Red Team	Red Team
Script kiddie	A less risk adverse threat actor, with little to no knowledge of security, who utilizes public tools, exploits, and techniques.
©Certcop	©Certcop
Red Team	Red Team
SMS phishing	A social engineering technique used to target victims through SMS messages and may use different motivational techniques like scarcity or fear to entice the victim to perform an action, like clicking on a malicious URL within the message.
©Certcop Red Team	©Certcop Red Team
SSL stripping	A man-in-the-middle (MiTM) attack technique used to force the user to connect to an endpoint over plaintext communication. This technique can be used to capture login credentials or other sensitive information that is typically protected when the communication is encrypted.
©Certcop	©Certcop
Red Team	Red Team
Static analysis	A debugging method used to examine source code, byte code, and binaries without execution.
©Certcop	©Certcop
Red Team	Red Team
Switch spoofing	A type of VLAN hopping attack that occurs when an attacker can emulate a valid trunking switch on the network by speaking 802.1Q.
©Certcop	©Certcop

Red Team	Red Team
Stealth scan	The process of running a scan without alerting the defensive position of the environment. It involves implementing a vulnerability scanner in such a manner that the target is unlikely to detect the activity.
©Certcop	©Certcop
Red Team	Red Team
Sysinternals	A suite of tools that allows administrators to control Windows-based computers from a remote terminal. It is possible to use Sysinternals to upload, execute, and interact with executables on compromised hosts.
©Certcop	©Certcop
Red Team	Red Team
Threading	Used in computer programs to execute multiple tasks in parallel in order to optimize the speed and efficiency of program execution.
©Certcop	©Certcop
Red Team	Red Team
Threat actor	An individual or group that seeks to harm a business or organization and is motivated through financial, personal, or political gain.
©Certcop	©Certcop
Red Team	Red Team
Time stomping	A technique used to modify the timestamps of a file or directory to disguise the possibility of compromise.
©Certcop	©Certcop



Red Team	Red Team
Wardriving	A tactical process for surveying an area for wireless access points while in a moving vehicle. The goal is preliminary reconnaissance and to pinpoint wireless networks and potential targets in a certain area of interest.
©Certcop	©Certcop
Red Team	Red Team
Waterholing	A technique used to infect websites with malicious software (malware) in order to capitalize on a target's or target group's trust relationship with websites they commonly visit.
©Certcop	©Certcop
Red Team	Red Team
Zero day	An attack that exploits a previously unknown hardware, firmware, or software vulnerability.
©Certcop	©Certcop