CERTCOP

CERTIFIED CYBER COP

Red Team

Certcop CertTips

CERTCOP

RED TEAM CERTIFIED - OFFENSIVE SECURITY

www.Certcop.com

Android Rooting

Rooting is a Linux word syntax term.
This indicates that the user has the special privilege of using a mobile phone.
Users may take control of their phone's SETTINGS, FEATURES and PERFORMANCE.

Application Framework

It offers numerous key classes for the creation of an Android app.
It offers a general summary of hardware access and helps to manage application resources in the user interface.

Android architecture

It comprises many components to satisfy all the requirements of Android devices.
An open-source Linux kernel with a set of C/C++ library

Application/Server Level Vulnerabilities

Credentials stored locally stolen through local file inclusion (LFI) or remote code execution (RCE).
Credentials stolen through a servers metadata through server-side request forgery (SSRF) or RCE

Availability

IT refers to the ability of a user to access information or resources in a specified location and in the correct format.

Red Team

Broad Network Access

Red Team

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.

Red Team

Blue Keep

Red Team

Blue Keep is a Microsoft RDP vulnerability that allows attackers to remotely log in to a victim's computer.

Red Team

Burp

Red Team

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.

Red Team

Block Storage

Red Team

Space in Blocks File storage has a hierarchy of folders and file.

Red Team

Bluetooth

Red Team

Bluetooth is a technology that allows wireless connection.

Buffer Overflows

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

Bootrom Exploit

©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

Baiting

©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

Red Team

Confidentiality

©Certcop

Red Team

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

©Certcop

Red Team

Cloud Carrier

©Certcop

Red Team

The intermediary that provides connectivity and transport of cloud services between

©Certcop

Red Team

Cloud Security

Red Team

Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion. Methods of providing cloud security include firewalls, penetration testing, obfuscation, tokenization, virtual private networks (VPN), and avoiding public internet connections.

Red Team

Cloud Service Provider (CSP)

Red Team

A company that offers cloud computing to businesses or individuals (Amazon, Google, Microsoft)

Red Team

Cloud Security Broker

Red Team

Third party individual or business that acts as intermediary between cloud consumer and cloud provider

Red Team

Cloud Auditor

Red Team

Conducts independent assessments of cloud services, information system operations and performance and security

Red Team

Computer Exploits

Red Team

Exploits are commonly classified as one of two types: known or unknown.
Known exploits have already been discovered by cyber security researchers.
Unknown exploits or zero-day exploits, in contrast, are created by cybercriminals as soon as they discover vulnerability.

Crunch

To crack a password, we must test a large number of passwords until we find the one that works.
There is no guarantee that any of those millions of possibilities will work.

Communications Lead

Leads the effort on messaging and communications

Cloud Security Alliance (CSA)

Cloud Security Alliance is a not-for-profit organization with the mission to “promote the use of best practices for providing security assurance within cloud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing.”

Cloud Workload Protection Platforms (CWPP)

Primarily used to secure server workloads in public cloud infrastructure as a service environment .

Clicking Jacking

Clicking Jacking fooling people to click something else they believe they click. Attackers obtain sensitive information or take device control

Config Manipulation

Red Team

Apps can utilize external files and libraries, alter them, or influence the ability of apps to manipulate the settings.

©Certcop

Red Team

Computer Incident Response Team (CIRT)

©Certcop

Red Team

A computer incident response team (CIRT) is a group that handles events involving computer security breaches.

©Certcop

Red Team

Carrier-loaded Software

©Certcop

Red Team

Pre-installed software or apps on devices may be vulnerable to criminal actions, such as deleting, altering, stealing of device data, wake-up calling, etc.

©Certcop

Red Team

Create phase

©Certcop

Red Team

Data will continue to be generated in the cloud and by remote users.

©Certcop

Red Team

Cloud Provider

©Certcop

Red Team

PaaS Develops, tests, deploys, and manages applications hosted in a cloud environment.

©Certcop

Cryptography

Red Team

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

©Certcop

Red Team

Cloud Pentesting

©Certcop

Red Team

Cloud Penetration Testing is a permitted simulated cyber-attack against a system that is hosted on a Cloud provider. Amazon's AWS

©Certcop

Red Team

Documentation

©Certcop

Red Team

Documents all team activities

©Certcop

Red Team

Drones

©Certcop

Red Team

Drones may investigate and report on places that are not accessible by any other means UAV & UAS.
A drone might serve as a mobile sensor in an IoT environment to collect data and send it to a cloud application or some other analysis service.

©Certcop

Red Team

Drive by Downloading

©Certcop

Red Team

Unintentional Internet download of software.
This exploit affects Android

©Certcop

Data Caching

Red Team

Caching in mobile devices used to interact with web apps, attackers attempt to exploit the data caches

©Certcop

Red Team

Destroy phase

Red Team

Furthermore, we would need to delete data from the production process and then sanitise the media.

©Certcop

©Certcop

Red Team

Dynamic Runtime Injection

Red Team

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

Digital Authentication

Red Team

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

DNS Poisoning

Red Team

Attackers utilize DNS servers, forward website users to another attacker's website DNS Poisoning.

©Certcop

©Certcop

Diversion Theft

Red Team

In this sort of attack, social engineers deceive a delivery or courier business into travelling to the incorrect pickup or drop-off location, intercepting the transaction.

©Certcop

Red Team

Dumpster diving

©Certcop

Red Team

It is a term used to describe the act of going This is a social engineering assault in which a person examines the garbage of a corporation for information, such as passwords or access codes scrawled on sticky notes or pieces of paper, that might be used to penetrate the organization's network.

©Certcop

Red Team

Databases

©Certcop

Red Team

Databases in the cloud, like their conventional counterparts, have some kind of framework for stored data.

©Certcop

Red Team

Data Portability

©Certcop

Red Team

The ability to transfer data from one system to another without being required to recreate or re-enter data descriptions or to modify significantly the application being transported.

©Certcop

Red Team

Degrees Monitoring (DLP)

©Certcop

Red Team

Which involves looking at data as it exits the production environment. These are commonly referred to as DLPs.

©Certcop

Examples of PaaS

- AWS Elastic Beanstalk
- Windows Azure
- Heroku
- Force.com

Examples of IaaS

- Digital Ocean
- Linode
- Rackspace
- Amazon Web Services

Examples of SaaS

- Google Apps
- Dropbox
- Salesforce
- Cisco WebEx

Evil Twin

Creating an evil twin is one of the most common techniques used by wireless network attackers.
In other words, attackers obtain a wireless access point and configure it to function as the current network.
One of the simplest methods to prevent evil twins from stealing your organization's information is to use data encryption.

Encryption

Encryption can be used to secure data when it is in transit, at rest, and in use.

Firewalls

Red Team

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

Red Team

First Aid Drones

©Certcop

Red Team

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

Red Team

FIDO Alliance

©Certcop

Red Team

FIDO Authentication enables password-only logins to be replaced with secure and fast login experiences across websites and apps.

©Certcop

Red Team

Firewalls

©Certcop

Red Team

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

Red Team

File Storage

©Certcop

Red Team

The data is stored and viewed as files and directories, with all of the same hierarchical and naming features as in a conventional environment.

©Certcop

Framing

Red Team

Website combined with iFrame components in HTML in another webpage

©Certcop

Red Team

Google Vulnerability Reward Program (VRP)

©Certcop

Red Team

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

Red Team

Git Repositories

©Certcop

Red Team

Misconfigured repositories leaking sensitive data
Mistakes in commits, publishing sensitive data

©Certcop

Red Team

Gaining Access

©Certcop

Red Team

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

Red Team

Hashing

©Certcop

Red Team

Using a one-way cryptographic function to create a digest of the original data

©Certcop

HR/Legal Representation

Legal and HR guidance and participation

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.

Integrity

It provides assurances that data has not changed, been one has modified, tampered with, or corrupted the data.

Infrastructure as a Service (IaaS)

Organization outsource equipment requirements, hardware, VMs, etc . Provider owns equipment, data centre

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.

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.

Red Team

IaaS Use

It has authority over operating systems; storage, installed applications, and maybe limited authority over some networking components (e.g., host firewalls).

©Certcop

Red Team

IaaS Delivery

- IaaS delivers cloud computing infrastructure through virtualization technology.
- IaaS clients can still access their servers and storage directly, but it is all outsourced through a “virtual data center” in the cloud.

©Certcop

Red Team

IaaS manages

- Servers
- hard drives
- Networking
- Virtualization
- Storage

©Certcop

Red Team

IaaS Advantages

- The most flexible cloud computing model
- Hardware purchases can be based on consumption
- Clients retain complete control of their infrastructure
- Resources can be purchased as-needed
- Highly scalable

©Certcop

Internal Employees

Employees getting compromised, then bringing that to your environment
Employees mistake leading to unintended consequences

IaaS Limitations and Concerns

- Security
- Legacy Systems Operating in the Cloud
- Internal Resources and Training
- Multi-Tenant Security

Intrusion Prevention Systems

Intrusion prevention systems (IPSs) used to monitor network traffic looking for suspicious activity. Solutions can detect, in real time, suspicious activity on a network.

Incident Handling

To handle an event, a set of predetermined processes and procedures are used.
Before, during, and after an event is identified, it involves the planning and actionable phases.

Incident response team

Assists in reducing the impact of security risks by responding quickly and effectively. Due to the increasing amount of security risks, companies must have a specialized incident response team to deal with them.

Indicators Of Compromise (Ioc)

Red Team

These detect potentially malicious behaviour on a system or network
Information security and IT workers can use indicators of compromise.

©Certcop

Red Team

IOT Devices

©Certcop

Red Team

IoT is an Internet-connected gadget which can interact with other devices and networks.
Depending on their design and functions, these gadgets may do a wide range of activities.

©Certcop

Red Team

Industrial processes

©Certcop

Red Team

ICS assets are digital equipment. All the important components (power network, water treatment, etc.), the production process and comparable applications are included.

©Certcop

Red Team

Improper SSL validation

©Certcop

Red Team

Security Laps in applications The process of SSL validation can allow attackers to bypass data security

©Certcop

Red Team

iOS Jailbreaking

©Certcop

Red Team

Removal of apple-based security measures to avoid harmful code

©Certcop

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.

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.

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

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.

Lead Investigator

Collects and analyzes all evidence and implements rapid system and service recovery.

Linux Kernel

The core of the Android architecture is Linux Kernel. It manages all drivers accessible, such as Display controls, Camera ports

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.

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.

Man in the Middle

An attacker has connections between two systems across the current network

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

NIST Security Working Group

Red Team

The NIST Cloud Service Public Working Group (PWG) provides guidance for better understanding and categorizing cloud services

Red Team

Nmap

Red Team

Nmap is characterized as a tool used by a network administrator. It uses to discover and troubleshoot services operating on a networked machine.

Red Team

NotPetya

Red Team

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

Red Team

No encryption / faint encryption

Red Team

Unsecured or weakly encrypted data transmission applications are capable to attack, for example hijacking session

Red Team

NGINX

Red Team

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

Nikto

Nikto is a free software command-line vulnerability scanner.
This scans webservers for dangerous files/CGIs, outdated server software and other problems.

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.

Object-Based Storage

Data is saved in the form of objects rather than files or blocks.

Penetration Test Methodology and Requirements

- API Testing
- Mobile Application Testing
- Network Testing

Public Cloud

A cloud deployment model (see SSP Table 8-2). The cloud services and infrastructure support multiple organizations and agency clients.

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

Performance Audit

Systematic evaluation of a cloud system by measuring how well it conforms to a setoff established performance criteria

©Certcop

Red Team

Packet Sniffing

Includes all the physical resources used to provide cloud services, most notably the hardware and the facility

©Certcop

Red Team

Privacy

Information privacy is the assured, proper, and consistent collection, processing, communication, use and disposition of disposition of personal information (PI) and personally identifiable information (PII) throughout its life cycle.

©Certcop

Red Team

Platform Libraries

Platform Libraries comprises several fundamental C/C++ libraries and Java-based libraries, such Media, Graphics, Surface Manager, OpenGL etc.

©Certcop

Red Team

Private Cloud

Red Team

The cloud services and infrastructure are dedicated to a specific organization/agency and to no other clients.

Red Team

Phishing

Red Team

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.

Red Team

Pangu

Red Team

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.

Red Team

Pharming

Red Team

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.

Red Team

Password Cracking

Red Team

THC Hydra uses brute force attack to crack virtually any remote authentication service.

PaaS Characteristics

- Provides a variety of services to assist with the development, testing, and deployment of apps
- Accessible to numerous users via the same development application
- Integrates web services and databases

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.

Platform vulnerabilities

Exploiting vulnerabilities in the OS, Server software, or app modules running on the web server

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.

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.

Password Reuse

An old 3rd party database is compromised; your users are still using a compromised password
Users using the same password across many accounts

Red Team

Penetration Testing

You can carry out penetration tests against resources on your AWS account per the policies and guidelines at Penetration Testing.

Red Team

Platform as a Service (PaaS)

Capability to deploy applications in the cloud, Languages, libraries, services, some control by user

Red Team

Resource Change

Adjusting configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud

Red Team

Regulatory Compliance

The DLP solution can define particular forms and types of data and the distribution of that data can be regulated appropriately to better conform to regulatory mandates.

Randomization

Red Team

The replacement of the data with random characters.

©Certcop

Red Team

Redundancy

©Certcop

Red Team

A component is duplicated so if it fails there will be a backup. Redundancy has a negative connotation when the duplication is unnecessary.

©Certcop

Red Team

Resource Pooling

©Certcop

Red Team

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model.

©Certcop

Red Team

Risk mitigation

©Certcop

Red Team

Reduces the chances that a threat will exploit a vulnerability by implementing controls

©Certcop

Red Team

Rainbow Crack

©Certcop

Red Team

Rainbow Crack is a tool that cracks password hashes using the time-memory trade-off technique. To crack password hashes, it use rainbow tables.
It does not crack passwords using the typical brute force method.

©Certcop

Remote Terminal Unit (RTU)

Red Team

RTU is a microprocessor-controlled electronic device. This uses telemetry data and messages from its Master Supervisory System to control connected objects to interface objects.
Remote telemetry unit and remote control unit may also be used in other words for RTU.

©Certcop

Red Team

SaaS Limitations and Concerns

©Certcop

Red Team

- Interoperability
- Vendor Lock-In
- Lack of Integration Support
- Data Security
- Customization

©Certcop

Red Team

SIEM- Bro (Zeek)

©Certcop

Red Team

Zeek sits on a “sensor,” hardware, software, virtual, or cloud platform that quietly and unobtrusively observes network traffic.

©Certcop

Red Team

Security Appliances

©Certcop

Red Team

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems

©Certcop

Red Team

Security Information and Event Management (SIEM)

©Certcop

Red Team

SIEM is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure.

©Certcop

Social engineering

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

Smart cars

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.

Supervisory Control And Data Acquisition (SCADA)

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.

Spare Phishing

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

Sensitive data storage

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

Software as a Service (SaaS)

Red Team

Applications accessible from client devices, web browser, email, mobile, limited configuration

©Certcop

Red Team

Services in scope

©Certcop

Red Team

In principle, any Google-owned web service that handles reasonably sensitive user data is intended to be in scope.

©Certcop

Red Team

SSLStrip

©Certcop

Red Team

MITM type attack that leverages SSL/TLS implementation flaws

©Certcop

Red Team

Session Hijacking

©Certcop

Red Team

Attacker Steal DNS Poisoning Valid Session ID

©Certcop

Red Team

Sandboxing Attacks

©Certcop

Red Team

Sandboxing helps to safeguard systems and users by restricting the resources available to the application on the mobile platform.

©Certcop

Threats

Red Team

Threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks and other attack vectors.

©Certcop

Red Team

Third Parties

©Certcop

Red Team

A 3rd party is doing malicious things that you are unaware of, a 3rd party you trust is compromised

©Certcop

Red Team

Tailgating

©Certcop

Red Team

Tailgating also known as piggybacking occurs when a hacker follows someone with an approved access card into a protected building. This assault assumes that the individual with valid access to the facility is kind enough to keep the door open for the person in front of them, presuming they are permitted to be there.

©Certcop

Red Team

TCP Trace route

©Certcop

Red Team

It is a trace route implementation that uses TCP packets. TCP Trace route follows routes via networks to determine what is obstructing traffic.
This can occur as a result of firewalls performing their job too well and accidentally blocking traffic that should be allowed through.

©Certcop

Red Team

Unintended Permissions

©Certcop

Red Team

Unknown applications sometimes allow attackers to enter doors by offering unknown permission.

©Certcop

User land Exploit

A jail broken user enables access at user-level but does not allow access at the iboot level.
This sort of exploit cannot be linked since recovery mode loops are not possible.

Vulnerabilities

Any weakness, flaw, bug, coding error

Vishing

Vishing often known as voice phishing, is the use of social engineering over the phone to get financial or personal information from a victim.

WannaCry

WannaCry was the stuff of night mare's .A wormable attack that spread exponentially over computer network. Infects 10,000 devices per hour in 150 countries. WannaCry ransomware encrypts computers, making them inaccessible.

Wireshark

Wireshark -- is a free and open source network protocol analyzer. It allows users to examine data traffic on a computer network in an interactive manner.

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.

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.

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

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.

Wireess Networking

Connecting multiple devices without any physical connection. Transfer data through Radio Frequency

WLAN

Red Team

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

WMAN

Red Team

WMAN is a wireless metropolitan area network capable of covering an entire city. It is larger than WLAN but smaller than WWAN.

©Certcop

Wired Equivalent Privacy (WEP)

Red Team

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

Wi-Fi Protected Access (WPA)

Red Team

WPA was introduced as an interim security upgrade over WEP while the 802.11i wireless security standard was being developed.
For encryption, most modern WPA implementations employ a pre-shared key (PSK).
To produce keys or certificates, WPA Enterprise use an authentication server.

©Certcop

Wi-Fi Protected Access (WPA2)

Red Team

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

Red Team

Wireless Wizard

Red Team

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.

Red Team

Wireless Key Generator

Red Team

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.

Red Team

Zero Day Exploit

Red Team

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.

Red Team

ZigBee

Red Team

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.

Red Team

Z-Wave

Red Team

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.

Red Team

Zero-day exploits

Red Team

Start an attack on a mobile OS or app, taking advantage of an undiscovered vulnerability.

Red Team

Zoho Docs

Red Team

A SaaS user productivity suite that includes features like macros.

Red Team

Access control list (ACL)

Red Team

In computer security, an access-control list is a list of permissions associated with a system resource.

Red Team

Access Management

Red Team

The part of the process that deals with managing access to resources after it has been granted is called access management.

Red Team

Additional Security

Red Team

Additional Security DLP may be used as a final control in the layered security strategy, designed to prevent inadvertent or malicious disclosure.

Advantages of PaaS

- Simple, cost-effective development
- Scalable
- Highly available
- Automation of business policy
- Easy migration to the hybrid model

APIs (application programming interfaces)

APIs are coding components that enable applications to communicate with one another, usually through a web interface and ideally in a safe and secure manner.

Authenticator Assurance Level (AAL)

A category describing the strength of the authentication process.

Android operating

Android operating system is a Google mobile operating system. Its design allows users to intuitively use mobile devices. Google uses Android software also with a distinct user experience for TVs. automobiles and wristwatches.

Cloud Access Security Broker (CASB)

A cloud access security broker is on-premises or cloud-based software that sits between cloud service users and cloud applications, and monitors all activity and enforces security policies.

Cloud Security Posture Management (CSPM)

Cloud Security Posture Management (CSPM) automates cloud security management across the SaaS, PaaS, IaaS.

Common Vulnerabilities and Exposures (CVE)

The Common Vulnerabilities and Exposures system provides a reference-method for publicly known information-security vulnerabilities and exposures.

Computer Emergency Response Team (CERT)

A computer emergency response team is a historic term for an expert group that handles computer security incidents.

CSA STAR Certification

The CSA STAR Certification is a third-party independent assessment of the security of a cloud service provider.

Computer Exploits

Exploits are commonly classified as one of two types: known or unknown.
Known exploits have already been discovered by cyber security researchers.
Unknown exploits or zero-day exploits, in contrast, are created by cybercriminals as soon as they discover vulnerability.

Device Vulnerabilities

- Reverse Engineering
- Jailbroken iPhones
- Rooted Devices

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)

Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol is a network management protocol used on Internet Protocol local area networks. A DHCP server must be present on the network.

Evasi0n7

Evasi0n7 is an iPhone, iPod touch, iPad, and iPad mini devices running iOS 7.0 to 7.0.6 is suitable as a junk tool (Devices that have been updated Over The Air [OTA] should be restored with iTunes first).

Future of Mobile Device Security

- Mobile Application Pen testing
- Dynamic Application Security Testing (DAST)
- Static Application Security Testing
- Smartphone Pen testing Framework

How Can Biometrics Secure SaaS?

Red Team

Biometrics as a Service is useful for many applications in the Cloud Authentication, Identity Services & Identity Duplication Detection

©Certcop

Red Team

Host Based IDS

©Certcop

Red Team

HIDS tools monitor the log files generated by your applications, creating a historical record of activities and functions allowing you to quickly search them for anomalies and signs an intrusion may have occurred.

©Certcop

Red Team

Host Based IPS

©Certcop

Red Team

It is a built-in software package which operates a single host for doubtful activity by scanning events that occur within that host.

©Certcop

Red Team

Hybrid Cloud

©Certcop

Red Team

The cloud services and infrastructure are made up of two or more distinct cloud infrastructures that remain distinct entities but are linked by standardized or proprietary technology that allows data and application portability.

©Certcop

Red Team

Interoperability

©Certcop

Red Team

The capability to communicate, to execute programs, or to transfer data among various functional units under specified conditions

©Certcop

Identity and Access Management (IAM)

IAM is concerned with the people, processes, and processes used to create, maintain, and destroy various kinds of identity.

Identity Management

Identity management is the method of associating user rights with a given identity to grant individuals access to system services.

Identity Services

Identity servers are databases that store information or attributes about people.

IaaS Characteristics

- Resources are available as a service
- Cost varies depending on consumption
- Services are highly scalable
- Multiple users on a single piece of hardware
- Dynamic and flexible

Jump Bag

Response times should be as short as feasible when an issue occurs. As a result of every minute that passes, a danger artifact is lost, or the attackers cause additional harm.

Red Team

JavaScript Object Notation

Red Team

An open-standard file format that uses human-readable text to transmit data objects consisting of attribute-value pairs and array data types.

Red Team

Key Management

Red Team

How and where encryption keys are stored has a significant impact on the overall risk of the data.

Red Team

Media Access Control (MAC) Address

Red Team

A unique identifier assigned to a network interface controller that uniquely identifies each device on a network.

Red Team

Multifactor Authentication

Red Team

Multi-factor authentication is a type of electronic authentication in which a device user gains access to a website or application only after successfully submitting two or more pieces of evidence to an authentication mechanism.

Red Team

Mobile Endpoints

Red Team

A physical device, frequently carried by the user, that served as a man/machine interface to cloud services and apps. To connect to cloud services and apps, a Mobile Endpoint may employ a variety of technologies and protocols.

Monitoring and Reporting

Discovering and monitoring the virtual resources, monitoring cloud operations and events, and generating performance reports

Masking

Hiding the data with useless characters; for example, showing only the last four digits of a Social Security number: XXX-XX-1234.

Mobile Device Security

Mobile Device Security refers to the safeguards put in place to protect sensitive data kept on and transferred by laptops, smart phones, tablets, wearable's, and other portable devices.

Nulls

Deleting the raw data from the display before it is represented, or displaying null sets.

NIST Cloud Computing Attributes

- Elasticity
- On-Demand
- Pooled Computing at provider's site
- Monitored and measured service usage
- Broad network access

Network Basic Input /Output System (NetBIOS)

Red Team

Provides services related to the session layer of the OSI model, allowing applications on separate computers to communicate over a local area network. As strictly an API, NetBIOS is not a networking protocol.

©Certcop

Red Team

Network Based IPS

©Certcop

Red Team

It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy Violations

©Certcop

Red Team

NIDS: SNORT

©Certcop

Red Team

Snort performs protocol analysis, content searching and matching.

©Certcop

Red Team

NIDS: OSSEC

©Certcop

Red Team

OSSEC is the world's most popular open-source host-based intrusion detection system (HIDS).

©Certcop

Red Team

Network Based IDS

©Certcop

Red Team

A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.

©Certcop

Obfuscation

The term "obfuscation" refers to the use of any of these techniques to make data less relevant, detailed, or readable in order to protect the data or the data's subject.

On Demand Self Service

A consumer can unilaterally provision computing capabilities. Such as server time and network storage, as needed automatically without requiring human interaction with each service provide

OWASP

A community dedicated entirely to identifying and reporting web application security flaws. The Open Web Application Security Project (OWASP) was founded in 2004.They recognized list of the top 10 security. There are publications and security tools that are widely used by OWASP.

Privacy-Impact Audit

Systematic evaluation of a cloud system by measuring how well it conforms to a set of established privacy-impact criteria

Provided by Customer

A control where the customer needs to provide additional hardware or software in order to meet the control requirement

Provisioning/Configuration

Red Team

The process of preparing and equipping a cloud to allow it to provide services to its users.

©Certcop

Red Team

Process transformation level

©Certcop

Red Team

The maturity level at which an organization is able to leverage cloud computing to improve its business processes.

©Certcop

Red Team

Plan-Do-Check-Act (PDCA)

©Certcop

Red Team

Plan-Do-Check-Act, also known as the Deming cycle, is an iterative cyclical management technique popularized by Edward Deming for quality control. PDCA involves planning, execution, evaluation, and change and is utilized in project management,

©Certcop

Red Team

Personally identifiable information (PII)

©Certcop

Red Team

Data that can be used to uniquely identify a person. Contact information, financial information, online account usernames, and government-issued identity documents are all examples of PII.

©Certcop

Red Team

Public Key Infrastructure (PKI)

©Certcop

Red Team

PKI is a hierarchical set of digital security certificates that are issued to people or computers for authentication and data security.

©Certcop

Quality of Service

There is often a trade-off between security and efficiency; any control that provides a security advantage to an enterprise will hinder productivity, often by lowering service quality (QoS).

Quid pro quo

What you get in exchange for what you get out of it. This is a social engineering assault in which the attacker claims to give something in return for the target's information or help.

Resource Abstraction and Control Layer

Entails software elements, such as hypervisor, virtual machines, virtual data storage, and supporting software components, used to realize the infrastructure upon which a cloud service can be established

Return on investment (ROI)

An SaaS enterprise's return on investment (ROI) is a performance metric used to assess the efficiency of an investment or to compare the efficiency of many investments. suite of management tools

Rich Internet application (RIA)

An RIA is a web application with an extensive feature set rivaling that of traditional desktop software.

Rogue Access Points

Attackers build physically illegal wireless access points that enable them to access a secure network by depriving network users' connections

Rouge security software

This is a form of virus that dupes victims into paying for phony malware eradication.

Rouge access point

Any illegal access point (AP) on a network is referred to as a rouge access point. It might be caused by an attacker or a misunderstanding on the part of an employee.

Secure Sockets Layer (SSL)

Encryption for secure web communications that uses a strong asymmetric key to establish a connection and a lighter-weight symmetric key for the session, creating an encrypted tunnel between a web client and web application through which data can be transmitted over public networks.

Service-level agreement (SLA)

A service-level agreement is a contract between customers and service suppliers that specifies the levels of service and service qualities that the client can request and the vendor is accountable for providing.

Service-oriented architecture (SOA)

Red Team

A set of interface programming standards that allow software-to-software interoperability between applications written using differing API standards.

©Certcop

Red Team

Sharding

©Certcop

Red Team

Database sharding involves the separation of large or complex data sets into smaller shards for simultaneous processing or analysis across distributed cloud resources.

©Certcop

Red Team

Shazam

©Certcop

Red Team

A SaaS application that can identify an overhead song.

©Certcop

Red Team

SkyDrive

©Certcop

Red Team

An IaaS file storage service by Microsoft.

©Certcop

Red Team

Staffing benefit

©Certcop

Red Team

The ability to reduce or retask staff due to improvements in efficiency.

©Certcop

Security Assertion Markup Language (SAML)

SAML is an XML method of exchanging user or computer authentication and authorization messages between identity providers and relying parties.

Single sign-on (SSO)

SSO passes authentication information from a single authentication sequence to computing services that would each normally require their own separate authentication.

SOAP (Simple Object Access Protocol)

SOAP is a protocol specification for exchanging structured data or information in web services.

Sandboxing

A physical sandbox is a test environment of isolated devices and cabling, completely distinct from the production environment.

Service Provider System Specific

A control specific to a particular system when the control is not part of the service provider corporate controls

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.

TRIAD- CIA

- Confidentiality
- Availability
- Integrity

Three models of cloud service

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS).

Third Party Assessment Organizations (3PAO)

- Verify Cloud Provider's Security Implementations
- Plan and Perform Security Assessments of the CSP Systems
- Review Security Package artifacts IAW FedRAMP requirements
- 3PAO creates the Security Assessment Report (SAR)

Types of threats

- Internal
- External
- Trusted
- Untrusted

Total cost of ownership (TCO)

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

Time-sharing

©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

Thick client

©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

Thin client

©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

Time to market

©Certcop

Red Team

The amount of time from product conception to release.

©Certcop

Unified Threat Monitoring (UTM)

UTMisa single security appliance, that provides multiple security functions at a single point on the network.

Utility level

The level of maturity at which an organization experiences immediate usefulness from cloud computing, such as reduction in costs.

Vendor lock-in

Vendor lock-in, also known as proprietary lock-in, is a circumstance in which an organization is required to remain using a certain set of technologies or products from a certain vendor in order to avoid considerable expenses associated with shifting to other counterparts.

Vertical hybrid cloud

Vertical hybrid models bring together all services required for a particular task.

Vertical scaling

Adding resources to a single node, such as memory, processing power, or redundant components. Also referred to as scale up.

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.

VMware vCloud

VMware vCloud is a VMware suite of products used to manage private clouds.

Vulnerability Management

- Vulnerability Scanning
- Key Component of Risk Assessment
- Risk that a threat actor is going to exploit a vulnerability
- Risk Mitigation

Vulnerability Types

- Unpatched Systems
- Misconfigured Systems
- Zero Days, web application vulnerabilities
- Injection attacks

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.

Wireless Attack Tools

Red Team

Aircrack-ng is one of the best wireless password hack tools for WEP/WAP/WPA2 cracking utilized worldwide!It works by taking packets of the network, analyses it via passwords recovered.

©Certcop

Red Team

When to use SaaS

©Certcop

Red Team

- Short-term projects that require quick, easy, and affordable collaboration
- Applications that aren't needed too often, such as tax software
- Applications that need both web and mobile

©Certcop

Red Team

Android Package Kit (APK)

©Certcop

Red Team

A packaged file format that includes the necessary files to run an application on the Android operating system.

©Certcop

Red Team

Authorization

©Certcop

Red Team

The procedure or action involved in identifying the proper access levels for a user or process.

©Certcop

Red Team

Authentication

©Certcop

Red Team

The process or action of confirming an identity used to interact with or log in to an information system.

©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.

©Certcop

Red Team

Biometrics

©Certcop

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 facility.

©Certcop

Red Team

Bluesmack

©Certcop

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.

©Certcop

Red Team

Bluebugging

©Certcop

Red Team

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

©Certcop

Red Team

Brute force attack

©Certcop

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 dictionaries.

©Certcop

Red Team

Clickjacking

Using numerous transparent or opaque layers to trick a user into clicking on a web button or link on a website where he or she had no intention of navigating or visiting.

Red Team

Command injection

An attack in which the attacker attempts to run instructions on a system that he or she is not meant to be able to execute using a vulnerable application.

Red Team

Cold boot attack

An attack method developed nearly a decade ago by Princeton University researchers who demonstrated the potential to recover disk encryption keys from random access memory (RAM) when the device's power is cycled in cooled or frozen temperatures.

Red Team

Credentialed vulnerability scanning

A scan conducted by a vulnerability scanner that has been given access to the system with the same rights as an authorized user.

Red Team

Cross-site scripting (XSS)

A very common web application vulnerability that can lead to installation or execution of malicious code, account compromise, session cookie hijacking, revelation or modification of local files, or site redirection. There are three major types of XSS: reflected XSS, stored (persistent), and DOM-based XSS.

Red Team

Data mining

©Certcop

Red Team

The process of analyzing large data sets to reveal patterns or hidden anomalies.

©Certcop

Red Team

Dictionary attack

©Certcop

Red Team

A type of password guessing attack that uses lists of possible passwords as the source for its guesses.

©Certcop

Red Team

Document the threats

©Certcop

Red Team

A step in the threat modeling process where the organization will match each threat, threat actor, and respective vulnerability relevant to the organization.

©Certcop

Red Team

Dumpster diving

©Certcop

Red Team

An unauthorized individual searches for and attempts to extract sensitive information from garbage.

©Certcop

Red Team

Ethical hacker

©Certcop

Red Team

A person who hacks into a computer network in order to test or evaluate its security rather than with malicious or criminal intent.

©Certcop

EXIF

Exchangeable image file format information from graphic files, as well as the information discovered through the URL of a scanned website.

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.

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.

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.

Red Team

Group Policy Objects (GPO)

A collection of settings that govern user and computer configurations within an Active Directory (AD) network.

Hacktivist

Red Team

A threat actor with various levels of knowledge and expertise who is politically or socially motivated.

©Certcop

Red Team

HTML injection

©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

HTTP proxies

©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

In-band SQL injection

©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

iOS app store package (IPA)

©Certcop

Red Team

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

©Certcop

Red Team

Java archive (JAR)

Red Team

A package file format that includes all of the necessary resources (i.e., class files, images, text, etc.) into one resource for a Java application to execute successfully.

©Certcop

Red Team

Joint test action group (JTAG)

©Certcop

Red Team

A type of standard used for debugging and connecting to embedded devices on a circuit board.

©Certcop

Red Team

Keylogger

©Certcop

Red Team

A program used to record the keystrokes of a victim while using a computer.

©Certcop

Red Team

Linear search

©Certcop

Red Team

A sequential process of evaluation where every value is checked until the correct value has been identified.

©Certcop

Red Team

Lock bumping

©Certcop

Red Team

A brute-force method of opening a pin tumbler lock with a bump key.

©Certcop

Locks

Red Team

Locks perform numerous locking functions (e.g., entrance locks and deadlocks) to meet various types of security requirements.

©Certcop

Red Team

Malvertising

©Certcop

Red Team

The act of incorporating malicious ads on trusted websites, which results in users' browsers being inadvertently redirected to sites hosting malware.

©Certcop

Red Team

Malware

©Certcop

Red Team

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

Red Team

Metasploit

©Certcop

Red Team

One of the most popular exploitation frameworks.

©Certcop

Red Team

Netgroup

©Certcop

Red Team

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

Red Team

Non-credentialed vulnerability scan

Red Team

Shows what the attack surface looks like to an untrusted user. Organizations could analyze the results and prioritize where to focus their initial defense tactics.

Red Team

Non ethical hacker

Red Team

A person who hacks into a computer network with malicious intent or to gain unauthorized access.

Red Team

Out-of-band SQL injection

Red Team

A type of attack in which the attacker retrieves data using a different channel. For example, an email, a text, or an instant message could be sent to the attacker with the results of the query.

Red Team

Persistence

Red Team

A technique used to maintain a presence in the target environment.

Red Team

Pivoting

Red Team

A lateral movement technique that can allow an attacker to move from host to host using remote access tools such as SSH, Telnet, FTP, RDP, VNC, etc.

PowerSploit

A collection of PowerShell modules that can be used for post exploitation and other phases of an assessment.

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.

Red Team

Red team assessment

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

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.

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.

Script kiddie

Red Team

A less risk adverse threat actor, with little to no knowledge of security, who utilizes public tools, exploits, and techniques.

©Certcop

Red Team

SMS phishing

©Certcop

Red Team

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

SSL stripping

©Certcop

Red Team

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

Red Team

Static analysis

©Certcop

Red Team

A debugging method used to examine source code, byte code, and binaries without execution.

©Certcop

Red Team

Switch spoofing

©Certcop

Red Team

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

Red Team

Stealth scan

Red Team

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.

Red Team

Sysinternals

Red Team

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.

Red Team

Threading

Red Team

Used in computer programs to execute multiple tasks in parallel in order to optimize the speed and efficiency of program execution.

Red Team

Threat actor

Red Team

An individual or group that seeks to harm a business or organization and is motivated through financial, personal, or political gain.

Red Team

Time stomping

Red Team

A technique used to modify the timestamps of a file or directory to disguise the possibility of compromise.

Unauthenticated scan

A method of vulnerability scanning that is used to perform a “black box” type of penetration test. It scans only the network services that are exposed to the network as there are no credentials used for access to the target.

User-defined function (UDF)

A way to extend MySQL with a new function that works like a native (built-in) MySQL function such as CONCAT( ), and can also be used to execute code.

Voice phishing (vishing)

A social engineering technique used to extract sensitive information from a target or to perform activities that they would not normally perform, such as resetting the password of an iTunes account that does not actually belong to the caller (pretext) or sending a wire transfer that should not be sent (fraud).

Vulnerability mapping

The process of mapping vulnerabilities to potential exploits to help prioritize testing activities in preparation for a pen test.

Warded lock

Uses obstructions (i.e., wards) around the keyhole to restrict the locking mechanism from opening when the wrong key is inserted or rotated in the lock.

Wardriving

Red Team

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

Red Team

Waterholing

©Certcop

Red Team

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

Red Team

Zero day

©Certcop

Red Team

An attack that exploits a previously unknown hardware, firmware, or software vulnerability.

©Certcop