Red Teaming and Social Engineering

Red Teaming and Social Engineering

The Red Team operation consists of a realistic scenario of a world-class offensive attack that is often used in the direction of large targets. The Red Team uses every documented and innovative method to infiltrate the victim's cyberspace. These standards Complies with MITRE ATT&CK and simulates all fourteen documented plans for a global cyber attack, this simulation severely tests the status of all your defense mechanisms and their performance quality, hence red team services are one of the most important and sensitive offensive security services.

CONTACT

Phone:
026 368 06249

Website:
unk9vvn.com

Email:
info@unk9vvn.com

RECONNAISSANCE

The attacker is always trying to gather information used to plan future operations. Reconnaissance operations involve techniques in which attackers actively or passively gather information. These techniques are used to support the target, and the information obtained from them may include details of the organization, infrastructure, or victim staff and personnel, and may be used by the attacker to perform other steps in the intrusion cycle in cases such as Information Gathering to help the attacker plan and execute the Initial Access step.

INITIAL ACCESS

The attacker is trying to break into your network. Primary access involves techniques that use different input vectors to obtain their initial access in a network. Techniques used to gain access include Spear Phishing and exploiting vulnerabilities in public web servers. Bases obtained through initial access can provide continuous access, such as valid accounts and external remote services.

RED TEAM AND PENETRATION TESTING

The red team differs from the penetration test: the red team is not limited to a specific domain and is not strict (for example, the access level is only within a specific web application).

Detecting access-specific vulnerabilities, some of which are only relevant to the red team, such as detecting browser vulnerabilities and deploying them in an attack scenario.

Red team operations are not limited to technical techniques, but also involve human resources (social engineering) as well as physical security (on-site physical access level).

Red Team operations should not be noisy because one of the goals, is to remain anonymous against defense mechanisms to better communicate with the hacker control and command center.

SOCIAL ENGINEERING

We carry out authorized social engineering attacks, which usually refer to the development of phishing campaigns targeting customer employees. The target of the attack may be planned individually with each client.

Other scenarios may be available for on-site Wi Fi users to be enabled by an external hardware of a rogue AP (Evil Twin). Establishing employees' first connection to the wireless network enables the MiTM (Man-in-The-Middle Attacks) scenario to inject malicious execution files into traffic or hijack downloaded files for further access.

PERSISTENCE

The attacker is trying to maintain his access. Access stability includes techniques that an attacker uses to prevent re-access to the system, change credentials, and other interruptions that interrupt access. Techniques used for stability include any performance or configuration changes that allow an attacker to retain their place in the system, such as replacing or hijacking authorized code or adding code in Startup.

PRIVILEGE ESCALATION

Privilege Escalation involves techniques that an attacker uses to obtain higher-level permissions on a system or network. Attackers can often gain access to and detect a network with unauthorized access, but they need higher access to pursue their goals. This need is addressed through routine approaches, the use of vulnerabilities or incorrect settings, and system vulnerabilities. These techniques are often accompanied by sustainability access techniques.

DEFENSE EVASION

Being invisible to defense mechanisms (Defense Evasion) includes techniques that attackers use to prevent detection during their attacks. These techniques include deleting and disabling security software or obscuring and encrypting data and scripts. Attackers also exploit trusted processes to hide their malware.

ENEMY SIMULATION

We are able to perform simulated attacks at the APT (Advanced persistent Threat) quality level using CPH (Cyber-Physical-Human) techniques. Red team operations are meant to reflect real-world cyber-attack scenarios that may be specific to an organization.

Red team exercises are used to assess the current security situation in a target company, employee awareness, as well as the response time of internal security teams such as the SOC (Security Operations Center).

The red team always tries to use its innovative methods in all the required stages of the attack, so the quality of the attack and benchmarking of the blue teams always depends on the level of knowledge used in the red team attack.

PHYSICAL AND NETWORK ATTACKS

The main purpose of physical security testing is to implement red team scenarios based on access to the organization building, restricted areas, documents, company devices and internal network. Physical attacks based on peripheral equipment can be very dangerous and out of sight of defense mechanisms.

As part of the Red Team operation, we carry out network attacks both externally and internally, where the main goal is to gain access to the company's important resources, data or a way to enter the internal network. But in most cases, after gaining initial access to the network, we use social engineering or physical access to intensify the attack.

DISCOVERY

Internal discovery includes techniques that an attacker may use to gain information about the system and the internal network. These techniques help attackers observe and orient the environment before deciding how to work. The information obtained allows attackers to discover what they can control and what is around their entry point, and to figure out how to exploit the victim system after infiltrating. In this regard, there are native operating system tools that are often used to collect information.

LATERAL MOVEMENT

Lateral movement involves the techniques that attackers use to access and control remote systems on the network. Pursuing the main goal often requires exploring the network to find your goal and subsequently achieve it. Achieving a goal often involves spinning through multiple systems and accounts to gain. Attackers may install their remote access tools to perform Lateral Movement or to use authorized credentials with local network and operating system tools (which may be hidden).

COLLECTION

This collection consists of techniques that attackers may use to gather information from targeted sources. Often, the next step after collecting data is to steal it. Sacrifice sources usually include different types of drives, browsers, audio, video and email. Common collection methods include taking screenshots and keyboard input.