What is Cobalt Strike? How do security researchers use Cobalt Strike?

Cobalt Strike is mainly used by security researchers to evaluate security vulnerabilities in the environment.

Vulnerability testing is performed to detect and classify security holes in the system. With the rise of cyber attacks, vulnerability assessment has become central in the fight against security threats.

And when it comes to vulnerability assessment, a paid tool called Cobalt Strike stands out. Cobalt Strike is mainly used by security researchers to evaluate security vulnerabilities in the environment.

However, what is Cobalt Strike and how does it help security researchers detect vulnerabilities? Does Cobalt Strike come with any special features? Let's find out with TipsMake through the following article!

What is Cobalt Strike?

To prevent external threats, most businesses and organizations hire a team of security experts and researchers. Sometimes, companies can also hire white hat hackers or IT savvy people who want to hunt for bounty to find the weak points of the network.

To perform these tasks, most security professionals use threat simulation software services to find out exactly where vulnerabilities exist and fix them before an attacker has a chance. exploit them.

Cobalt Strike is one such tool. It is loved by many security researchers for performing real penetration scans to find out the exact locations of vulnerabilities. In fact, Cobalt Strike is designed to accomplish the 'one arrow two goals' goal: Vulnerability assessment and penetration testing.

Difference between vulnerability assessment and penetration testing

Most people confuse vulnerability scanning with penetration testing. They sound similar, but their meanings are completely different.

Vulnerability assessment simply scans, identifies and reports found vulnerabilities, while penetration testing attempts to exploit vulnerabilities to determine if there is any unauthorized access or malicious activity. other or not.

Pentests typically include both network penetration testing and application-level security testing along with associated controls and processes. For successful penetration testing, everything should be conducted from the internal network as well as from the outside.

How does Cobalt Strike work?

Cobalt Strike's popularity is mainly due to its beacons or payloads that work silently and are easily customizable. If you don't know what a beacon is, you can think of it as a direct stream into the network, controlled by an attacker to perform malicious activities.

Cobalt Strike works by sending beacons to detect vulnerabilities in the network. When used as intended, it simulates an actual attack.

Additionally, a beacon in Cobalt Strike can execute PowerShell scripts, perform keylog operations, take screenshots, download files, and generate other payloads.

How Cobalt Strike helps security researchers

It is often difficult to detect vulnerabilities or problems in a system that you have created or used for a long time. Using Cobalt Strike, security professionals can easily identify and fix vulnerabilities and rank them based on the severity of the problem they can cause.

Here are a few ways that tools like Cobalt Strike can help security researchers:

Network security monitoring

Cobalt Strike can help monitor corporate cybersecurity on a regular basis using a corporate cyberattack platform that utilizes multiple attack vectors (e.g. email, Internet browsing, web application vulnerabilities, Social

Engineering attacks) to detect vulnerabilities that can be exploited.

Detect outdated software

Cobalt Strike can be used to detect if a company or business is using outdated versions of software and if any patches are required.

Identify weak domain passwords

Most of today's security breaches involve weak and stolen passwords. Cobalt Strike is very useful in identifying users with weak domain passwords.

Overall security analysis

Cobalt Strike provides an overview of a company's security, including what data might be particularly vulnerable, so security researchers can prioritize risks that need attention. right away.

Validate the effectiveness of the endpoint security system

Cobalt Strike can also provide testing against controls such as email security sandboxes, firewalls, endpoint detection, and antivirus software to determine effectiveness against advanced and common threats.

Special Features Provided by Cobalt Strike

To detect and fix vulnerabilities, Cobalt Strike offers the following special features:

Attack Pack

Cobalt Strike offers a variety of attack packages to launch a web drive or convert an innocuous file into a trojan horse for a simulated attack.

Here are the different attack packs offered by Cobalt Strike:

1. Java Applets Attacks

2. Microsoft Office Documents
3. Microsoft Windows Programs
4. Website Clone Tool

Browser Pivoting

Browser Pivoting is a technique that essentially leverages an exploited system to gain access to browser authenticated sessions. It's an effective way to demonstrate risk with a targeted attack.

Cobalt Strike implements Browser Pivoting with a proxy server that feeds into 32-bit and 64-bit Internet Explorer. When you browse this proxy server, you inherit cookies, authenticated HTTP sessions, and SSL client certificates.

Spear Phishing

A variant of phishing, Spear Phishing is a method of intentionally targeting specific individuals or groups within an organization. This helps to identify weak targets within the organization, such as employees who are more vulnerable to security attacks.

Cobalt Strike offers a Spear Phishing tool that allows you to type messages by replacing links and text to create a convincing phishing scam. It allows you to send the perfect phishing message, using an arbitrary message as a template.

Reporting and logging

Cobalt Strike also provides reports summarizing the progress and indicators of violations detected in the operation. Cobalt Strike exports these reports both as PDF and MS Word documents.

Is Cobalt Strike still the preferred choice for security researchers?

A proactive approach to mitigating cyber threats includes implementing a cyber simulation platform. While Cobalt Strike has all the potential for a powerful threat emulator, threat actors have recently found a way to exploit it and are using Cobalt Strike to carry out attacks. secret network.

Needless to say, the same tools used by organizations to improve security are now being exploited by cybercriminals to help circumvent their own security.

Does this mean that the days of using Cobalt Strike as a threat mitigation tool are over? Not really. The good news is that Cobalt Strike is built on a very powerful framework and with all the outstanding features it offers, hopefully Cobalt Strike will remain on the list of favorites of security professionals.