Description

What is ethical hacking?

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers. This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

Also known as “white hats,” ethical hackers are security experts that perform these assessments. The proactive work they do helps to improve an organization’s security posture. With prior approval from the organization or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.

What Is A Red Team?

A red team consists of security professionals who act as adversaries to overcome cyber security controls. Red teams often consist of independent ethical hackers who evaluate system security in an objective manner.

They utilize all the available techniques to find weaknesses in people, processes, and technology to gain unauthorized access to assets. As a result of these simulated attacks, red teams make recommendations and plans on how to strengthen an organization’s security posture.

How Does A Red Team Work?

You might be surprised to learn that red teams spend more time planning an attack then they do performing attacks. In fact, red teams deploy a number of methods to gain access to a network.

Social engineering attacks, for example, rely on reconnaissance and research to deliver targeted spear phishing campaigns. Likewise, prior to performing a penetration test, packet sniffers and protocol analyzers are used to scan the network and gather as much information about the system as possible.

What Is A Blue Team?

A blue team consists of security professionals who have an inside out view of the organization. Their task is to protect the organization’s critical assets against any kind of threat.

They are well aware of the business objectives and the organization’s security strategy. Therefore, their task is to strengthen the castle walls so no intruder can compromise the defenses.

How Does A Blue Team Work?

The blue team first gathers data, documents exactly what needs to be protected and carries out a risk assessment. They then tighten up access to the system in many ways, including introducing stronger password policies and educating staff to ensure they understand and conform to security procedures.

Monitoring tools are often put in place, allowing information regarding access to the systems to be logged and checked for unusual activity. Blue teams will perform regular checks on the system, for example, DNS audits, internal or external network vulnerability scans and capturing sample network traffic for analysis.

In this Course we will Learn all the below in one course only:

What is Cyber Security ?

Basic Linux Commands

Kali Linux Command Line (CLI)

Netcat (nc) Essentials

Wireshark

Bash Scripting (Shell Scripting)

Passive Information Gathering Techniques

Active Information Gathering Techniques

Scanning with Nmap

Web Application Attacks

The Metasploit Framework Essentials

Buffer Overflow

Active Directory Attacks

Hands-On Practice Labs

Who this course is for:

Cyber Security Engineers

DevSecOps Engineers

Ethical Hackers

Penetration Testers

System Administrators

Requirements

Eager to Learn and Patience !!!