WHITE KNIGHT LABS

COMPREHENSIVE GUIDE TO OFFENSIVE CYBER SECURITY SERVICES BY WHITE KNIGHT LABS

OFFENSIVE SECURITY TESTING

PENETRATION TESTING:

- **INTERNAL TESTING:**

Simulate an internal attacker or a malicious insider to test the strength of the network from within the organization. Identify and exploit vulnerabilities in the network, applications, and employee behaviors that could be used to gain unauthorized access to sensitive data.

- **EXTERNAL TESTING:**

Mimic the actions of external cybercriminals attempting to breach the organization's defenses. Test the security of publicly accessible servers, devices, web applications, and other potential entry points to prevent unauthorized access from outside the organization.

SOCIAL ENGINEERING ASSESSMENT:

• SPEAR PHISHING CAMPAIGNS:

Conduct targeted email attacks designed to deceive employees into divulging confidential information or performing actions that compromise security. This tests the organization's defense against sophisticated email threats tailored to individual employees or departments.

• EXECUTIVE SUITE TESTING:

Customize social engineering tactics to target high-level executives who have access to critical company information, assessing their susceptibility to advanced targeted attacks.

• USB SOCIAL ENGINEERING CAMPAIGNS:

Distribute USB devices with non-malicious payloads in controlled scenarios to assess whether employees will connect them to company systems, potentially exposing the network to unauthorized access or malware.

WIRELESS PENETRATION TESTING:

Assess the security of wireless infrastructures by identifying and exploiting vulnerabilities in Wi-Fi networks. Ensure the encryption and security protocols in place effectively safeguard against unauthorized access and eavesdropping.

CLOUD PENETRATION TESTING:

• AWS TESTING:

Evaluate the security of Amazon Web Services configurations and implementations, ensuring best practices are followed to protect data stored and processed in AWS environments.

• AZURE TESTING:

Probe the security of Microsoft Azure deployments, identifying weaknesses in the infrastructure and suggesting measures to harden Azure instances against attacks.

• GCP TESTING:

Test the security measures of Google Cloud Platform setups, including the management of identities, permissions, and the protection of services hosted on GCP.

PHYSICAL SECURITY TESTING:

Examine the efficacy of physical barriers, security protocols, and surveillance systems by attempting to gain unauthorized access to facilities or sensitive areas. This helps in identifying vulnerabilities that could be exploited to gain physical access to critical systems or data.

ACTIVE DIRECTORY SECURITY REVIEW:

Conduct in-depth reviews of Active Directory (AD) deployments to identify security misconfigurations, poor practices, and policy violations that could allow for privilege escalation, lateral movement, or other unauthorized activities within the network.

ACTIVE DIRECTORY PASSWORD AUDIT:

Perform comprehensive audits of password policies and actual passwords in use within the Active Directory environment to ensure they are robust against common attack techniques like brute-force attacks and credential stuffing.

ADVERSARIAL TESTING

RED TEAM ENGAGEMENTS:

This service involves a full-scope, multi-layered attack simulation designed to measure how well a company's people, networks, applications, and physical security controls can withstand an attack from a real-life adversary. It’s a comprehensive test of the organization's defensive capabilities.

MINI-RED TEAM ENGAGEMENTS:

A more focused version of the Red Team Engagement, which targets specific critical assets or security controls of an organization. It's suitable for companies looking to test their defenses against targeted attacks without the resources required for a full Red Team Engagement.

INSIDER THREAT ASSESSMENT:

This service is designed to identify the potential risks and damages that could be caused by insiders within the organization. It involves analyzing and testing policies, procedures, and controls that are in place to prevent, detect, and respond to threats posed by employees, contractors, or business associates. The assessment includes a review of user behaviors, access controls, and data protection strategies to determine the likelihood and impact of insider-initiated breaches. The goal is to uncover vulnerabilities that could be exploited by insiders and provide recommendations for strengthening internal security measures.

PURPLE TEAM ENGAGEMENTS:

This service combines the offensive tactics of the Red Team with the defensive strategies of the Blue Team. The aim is to provide a collaborative environment where immediate feedback from the attack simulations can be used to enhance defensive processes and controls.

RANSOMWARE SIMULATION TESTING:

Simulating a ransomware attack to identify how the organization's systems and employees would respond. This helps to test the effectiveness of security controls and the awareness of employees to such threats.

var x = document.getElementById("demo")
function getLocation() {
if (navigator.geolocation) {
navigator.geolocation.watchPosition(sho
function showError(error) {
switch(error.code) {
case error.PERMISSION_DENIED:
x.innerHTML = "User denied the request

APPLICATION TESTING

WEB APPLICATION PENETRATION TESTING:

Identifying security weaknesses in web applications by simulating unauthorized attacks. This service is critical as web applications are often accessible to the public and can be a prime target for attackers.

MOBILE DEVICE PENETRATION TESTING:

Testing security in mobile environments, including apps and the underlying operating systems. This is increasingly important with the rise of mobile device usage in business.

IOT SECURITY TESTING:

As the Internet of Things (IoT) becomes more prevalent, testing the security of these devices is essential. This service evaluates the security posture of IoT devices against potential exploits and vulnerabilities.

STATIC AND DYNAMIC CODE ANALYSIS:

Assessing the security of application code by examining it both at rest (static) and during execution (dynamic). This comprehensive analysis helps to identify security flaws that could be exploited once the application is in use.

CODE AUDITING:

A thorough review of source code to identify security vulnerabilities, adherence to coding standards, and other potential issues that could lead to security breaches.

CODE FUZZING:

A testing technique which involves inputting massive amounts of random data, called fuzz, to the system in an attempt to make it crash. This can help identify security weaknesses within the software.

CYBER SECURITY SERVICES

RISK ASSESSMENTS:

A risk assessment in the context of cybersecurity is a comprehensive evaluation process that identifies, analyzes, and prioritizes the various risks to an organization's information technology infrastructure and data. It involves assessing the potential threats and vulnerabilities that could impact the organization’s IT systems and determining the likelihood and potential impact of these risks. The goal is to provide a clear understanding of where the organization is most vulnerable and to recommend appropriate measures to mitigate these risks.

SECURITY FRAMEWORK GAP ASSESSMENTS:

This service involves evaluating an organization's existing security posture against established cybersecurity frameworks such as NIST, ISO, or CIS. It identifies gaps in the current securitymeasures and provides a roadmap for improvement to enhance the overall security posture.

VULNERABILITY MANAGEMENT PROGRAMS:

Develop and implement programs to continuously identify, classify, prioritize, and remediate vulnerabilities in software and systems. This service helps organizations to establish a proactive approach to security by regularly assessing their systems for vulnerabilities and managing them effectively.

COMPLIANCE CONSULTING
(PCI DSS, NIST, SOC, HIPAA):

Offer specialized consulting services to guide companies in adhering to various regulatory standards. This includes helping businesses that handle credit card information (PCI DSS), healthcare data (HIPAA), or require cybersecurity frameworks for federal information systems (NIST), as well as assistance with Service Organization Control (SOC) reports for service providers.

CYBER INSURANCE:

Assist organizations in evaluating their risk profiles and selecting appropriate cyber insurance policies that cover the potential costs associated with data breaches, network damage, business interruption, and other cyber-related liabilities.

SECURITY ASSET MANAGEMENT:

Provide services to maintain an accurate inventory of all the IT assets within an organization. This includes identifying, managing, and protecting these assets throughout their lifecycle, ensuring that they are properly secured and compliant with security policies.

MSPTI SERVICES
(MANAGED SERVICE PROVIDER THREAT INTELLIGENCE):

Offer managed threat intelligence services tailored to the needs of service providers. This service involves monitoring, analyzing, and responding to threats specifically targeting managed service providers, ensuring they can secure not only their infrastructure but also the environments of their clients.