CRITICAL FAULT

PROFESSIONALLY PARANOID

PENETRATION TESTING

ADVERSARY SIMULATION

Penetration testing takes an offensive security approach to cybersecurity. Certified security specialists assume the role of the attacker and try to locate and exploit vulnerabilities to gain unauthorized access to an organization's systems. Critical Fault's Red Team specializes in penetration testing as professionally certified hackers. We have an extensive background as developers, IT administrators, and physical security specialists.

Penetration Testing Services

- Network Penetration Testing
- Application Penetration Testing
- Mobile Device Penetration Testing
- Physical Penetration Testing

CRITICAL FAULT

PROFESSIONALLY PARANOID

WHY DO I NEED A PENETRATION TEST?

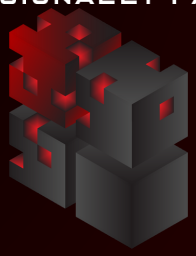
Penetration testing has become a critical element to any mature cybersecurity program. Penetration testing is crucial to identifying vulnerabilities that a standard risk assessment or vulnerability scan can miss. 95% of all data breaches are caused by human error. The goal of any penetration test is to find out where these errors are occurring and how to remediate them before a malicious attacker has a chance to exploit them.

Additionally, many regulatory bodies require regular penetration testing to maintain compliance with security standards.

Penetration Testing is a critical element for the "Identify" stage of the Cybersecurity Lifecycle.

CRITICAL FAULT

PROFESSIONALLY PARANOID



PENETRATION TEST TYPES

Penetration Testing is when an organization hires professional hackers, also known as “ethical hackers”, to identify vulnerabilities in an organization’s security architecture. Once testing is complete, a detailed report is given to the organization identifying risks and vulnerabilities found and providing remediation strategies to help reduce risk of a cyber event.

Various testing categories help to determine the risk level of the internal network and the effectiveness of security controls.

- External Network
- Internal Network
- Web Application
- Mobile Device
- Physical Security
- Social Engineering

CRITICAL FAULT

PROFESSIONALLY PARANOID

NETWORK PENETRATION TESTING

Network penetration tests simulate attacks to an organization's systems, networks, applications, or data. Network penetration testing identifies risks within the network before those risks can be exploited by unauthorized users.

Designed to mimic attacks from multiple network perspectives

Rogue Admin.

Guest

Internet Hacker

COMMON TARGETS

- SOFTWARE
- EMAIL SERVERS
- NETWORK ARCHITECTURES
- WIRELESS DEVICES
- FIREWALLS
- COMPUTER SYSTEMS

CRITICAL FAULT

PROFESSIONALLY PARANOID

NETWORK PENETRATION TESTING

EXTERNAL NETWORK PENTEST

External penetration testing targets vulnerabilities within an organization's perimeter systems such as web applications, websites, email servers, or other systems accessible from the internet. A security professional assumes the role of an outside attacker trying to gain unauthorized access to sensitive organizational data. These tests are used to determine external threats to the organization.

INTERNAL NETWORK PENTEST

Internal penetration testing targets vulnerabilities from within an organization. A penetration tester assumes the role of an attacker who has already gained access to your network and exploits vulnerabilities within an organization’s internal security architectures. These tests are used to determine internal threats to the organization, including malicious threats and accidental breaches.

CRITICAL FAULT

PROFESSIONALLY PARANOID

APPLICATION PENETRATION TESTING

Applications often rely on external security controls, such as web application firewalls, and have multiple user roles that require testing. Often, internal security controls native to the application are missing, or worse, untested. Our Red Team will test against all roles and security controls protecting applications.

Critical Fault uses two Application Penetration Testing Approaches

D.A.S.T.

Dynamic Application Security Testing

Examines the live application to find flaws and identify areas of risk.

S.A.S.T.

Static Application Security Testing

Examines the source code to find flaws hidden deep within the application.

CRITICAL FAULT

PROFESSIONALLY PARANOID

SOCIAL ENGINEERING

Often the easiest way to infiltrate an organization is through humans, not systems. Hackers know this and will use common user mistakes to infiltrate organizational systems. These Social Engineering tactics are often very effective. Our Red Team utilizes these tactics to find weak links in an organization and gain unauthorized access to secure systems and facilities by deceiving employees and tricking them into revealing critical information or allowing access to protected systems. Social Engineering is often combined with other penetration test engagements.

Social Engineering Tactics

- Phishing
- Spear Phishing
- Baiting
- Malware
- Pretexting
- Tailgating
- Vishing
- Watering Hole Attacks

CRITICAL FAULT

PROFESSIONALLY PARANOID

PHYSICAL PENETRATION TESTING

A physical security environment is tested by simulating attacks to an organization's buildings, hardware, and remote devices. Hackers will often deploy malicious hardware into an organization by breaching the building's perimeter and inserting an infected device into an organization's network. Critical Fault simulates a threat actor's attempts to physically breach the organization's perimeter through social engineering, abusing poor physical controls, or utilizing a variety of tools to gain unauthorized access to sensitive areas and systems.

PHYSICAL SECURITY CONTROLS

- ACCESS CONTROLS
- VIDEO SURVEILLANCE
- INTRUSION ALARMS
- EMPLOYEE AND MANAGEMENT TRAINING
- EQUIPMENT DOCUMENTATION