PENTESTING-AS-A-SERVICE

"HELPING BUSINESSES TO IDENTIFY THE VULNERABILITIES IN THEIR IT INFRASTRUCTURE"

F7Digital

Penetration Testing, aka Pen Testing, is a simulation of a real-world cyber-attack. Penetration Testing-as-a-Service helps you discover the weaknesses in your IT infrastructure by simulating an attack on a computer system or network from external and internal threats. F7 Digital Bluetooth-Attacklates the same tools, know-how, and methodologies malicious hackers use. The difference between a real attack and F7 Digital's simulation of a real-world cyber-attack is that a real attack vanishes your business within minutes. Still, F7 Digital Penetration Testing attacks find vulnerabilities in a controlled system, helping you discover and fix problems before an attacker does. The output is a comprehensive report identifying where to close security holes and how to improve security posture.

DID YOU KNOW?

- **363 high-risk vulnerabilities with CVSSv3 10.00 and RCE access were found in 2022**
- **Fixing a critical vulnerability took companies 193.1 days on average in 2021(AppSec stats Flash - Year in Review)**

Provided internal/external facing IPs (or range(s)), internal/external exposed/accessible hosts, web properties, sites, etc.

SCOPING

START OF ASSESSMENT

Query of breach databases (TBs) for potential data exposure; this includes company affiliated properties or data sets.

BREACH DATA

Open-sourceinformation gathering and intelligence assessment on potential data exposure; this includes company affiliated properties or data sets.

OSINT

WEB APP SCAN

Scan of internal/ external accessible web applications and/or properties

MANUAL VERIFICAITION

Manual confirmation of potential issues (e.g.,MFA bypass, credential spraying).

ASSUMED BREACH

where low privileged internal access 1• sprovided to testing team

ASSESSMENT FINISH

Report of issues identified along with potential mitigations

F7Digital

TYPES OF PENETRATION TESTING SERVICES

EXTERNAL PENETRATION TESTING

Securing internet-facing assets such as web, mail, and FTP servers is a huge concern. An attacker is always drawn to the company's assets that are accessible over the internet. Hence, knowing your perimeter weaknesses is critical before threat actors attempt to exploit them. F7 External Penetration Testing helps identify vulnerabilities in internet-facing infrastructure, enumeration & exploitation.

INTERNAL PENETRATION TESTING

Securing assets within an internal network is vital to prevent attackers from infecting the entire network. Internal Penetration Testing helps to determine the extent of an attacker's access and the sensitive resources they can obtain if they are already inside the network. This can prevent major security breaches.

WIRELESS PENETRATION TESTING

The entry-point for a malicious actor can be your insecure wireless networks like Wi-Fi or Bluetooth network. Wireless Penetration Testing helps identify the vulnerabilities in the wireless network that an attacker can exploit to become an uninvited guest in a network and keep an eye on all sensitive communications without revealing his presence

WEB APPLICATION PENETRATION TESTING

If an attacker successfully breaks into the web application or server, he may also gain access to sensitive information and other applications. Web Application Penetration Testing helps apply remediation against undiscovered vulnerabilities and make sure source code is as per the best practices.

MOBILE APPLICATION PENETRATION TESTING

Mobile applications are increasing with the increase in the count of smart devices.However, a vulnerable mobile application may affect not only the organisation but the users too. A single bug or vulnerability can cause data theft, including the user's personal information. F7 performs comprehensive mobile penetration testing to identify such security and privacy issues.

DOS AND DDOS

To prevent attackers from crashing servers by sending large amounts of data packets, it's important to implement a counter strategy. F7 can help by testing the performance of vulnerable servers with simulated Denial-of-Service (Dos) / Distributed Denial-of-Service (DDoS) attacks, so you can formulate effective countermeasures and be prepared for cyber warfare.

SOCIAL ENGINEERING ASSESSMENT

People are the most vulnerable assets in any organisation. Hence, organisations must conduct Social Engineering Assessments to test human vulnerabilities and train their employees, so they don't fall prey to attackers. F7's Social Engineering Assessment helps you test employees and associated security policies to identify the weakest link in the security strategy.

TYPICAL LENGTH OF ENGAGEMENT 1-4 WEEKS

HOW OFTEN DO YOU TEST IT INFRASTRUCTURE FOR VULNERABILITIES?

IT'S RECOMMENDED TO CONDUCT PEN TESTING AT LEAST TWICE A YEAR TO STAY CURRENT WITH VULNERABILITIES AND POTENTIAL THREATS. THE FREQUENCY OF TESTING CAN VARY DEPENDING ON A NUMBER OF FACTORS, INCLUDING:

- **COMPANY SIZE**: LARGER COMPANIES MAY REQUIRE MORE FREQUENT TESTING TO ENSURE THE SECURITY OF A LARGER INFRASTRUCTURE.
- **POTENTIAL EXPOSURE TO ATTACK VECTORS**: COMPANIES WITH A HIGHER RISK OF ATTACK, SUCH AS THOSE HANDLING SENSITIVE DATA OR OPERATING IN A REGULATED INDUSTRY, MAY REQUIRE MORE FREQUENT TESTING.
- **INDUSTRY**: DIFFERENT INDUSTRIES MAY HAVE SPECIFIC REGULATIONS OR COMPLIANCE REQUIREMENTS THAT REQUIRE MORE FREQUENT TESTING.
- **INFRASTRUCTURE TYPE/SIZE:** THE COMPLEXITY AND SIZE OF A COMPANY'S IT INFRASTRUCTURE CAN ALSO IMPACT THE FREQUENCY OF TESTING.
- **INDUSTRY-SPECIFIC REGULATORY ENVIRONMENT**: COMPANIES OPERATING IN A REGULATED INDUSTRY, SUCH AS HEALTHCARE, FINANCE, AND GOVERNMENT, MAY HAVE SPECIFIC REGULATORY REQUIREMENTS THAT MANDATE MORE FREQUENT TESTING.

ALWAYS A GOOD PRACTICE TO REVIEW AND UPDATE THE COMPANY'S SECURITY POSTURE AND CONDUCT A RISK ASSESSMENT TO DETERMINE THE MOST APPROPRIATE FREQUENCY OF TESTING.

F7 PENTESTING-AS-A-SERVICE GLOBAL LOCATIONS