SparkC

INTEGRATED. INNOVATIVE. IMPACT.

www.sparkcllc.com

PENETRATION TESTING CAPABILITIES

SparkC provides a variety of penetration testing capabilities and services. Below details our overall goals that we guarantee to accomplish for our clients:

- Test for susceptibility to Advanced Persistent Threats (APTs) such as social engineering or phishing vulnerability, viruses, malware, trojan horses, botnets and other targeted attack exploits. Evaluate current threat posture including antivirus and Intrusion Detection and Prevention (IDP) capabilities.
- Identify physical security vulnerabilities by attempting access to computing hardware and sensitive information using social engineering techniques.
- Perform PCI security compliance and risk assessment; provide remediation steps to meet compliance requirements.
- Review wireless network system components for security vulnerabilities, validating system specific configurations and known exploits.
- Perform vulnerability assessment of the clients network.
- Validate system-specific configurations and review for known exploits. This includes firewalls, switches and routers, Microsoft Active Directory and file servers, web servers, wireless routers, VPN, Cisco VoIP and Office 365 Email.

HOW DO WE CONDUCT OUR PEN TEST?

SparkC will perform white, gray, and/or black box network penetration testing using tools and sophisticated by-hand penetration testing to examine our clients information technology security and architecture. The penetration testing team will attempt to exploit vulnerabilities that have been identified in a customer's systems (hosts, applications, database, or other computer related resources). The results will detail the risk exposure for customer systems and demonstrate how vulnerabilities can be exploited to gain access to their systems. Suggested remediation actions to lower a customer's risk exposure will also be provided. During the penetration test, SparkC will not delete any live data, will make every attempt not to disrupt current operations, and will not perform any Denial of Service attacks. The team will only concern themselves with discovering and exploiting vulnerabilities which provide greater access to the system or network that is being tested. SparkC will be limited to the scope identified in the Rules of Engagement with the customer, even if the test team identifies access to other networks.

The following activities will be performed during our Penetration Test:

I. Perform basic open source information gathering of customer's Internet reachable network presence.
II. Perform active network host and service identification through the use of port scanning and host enumeration.
III. Perform exploitation of identified vulnerabilities. This will include automated tools and scripts that attempt to exploit systems as well as manual testing.
IV. Attempt to access customer systems, applications, and networks through identified vulnerabilities.

SparkC

INTEGRATED. INNOVATIVE. IMPACT.

www.sparkcllc.com

1. WIRELESS PENETRATION TESTING ASSESSMENT

SparkC's wireless penetration testing analyzes the current wireless infrastructure, network cryptographic protections, and the security of endpoint systems to identify weaknesses and attempt to exploit them to gain additional access to a customer network. During the wireless penetration test the SparkC Team will identify Wireless Access Points (WAPs) and attempt to exploit and gain access to the network through those WAPs. Once access is gained to the wireless network, the team will attempt to map out the network and discover vulnerabilities. The following associated activities will be performed under the wireless assessment:

I. Perform Wireless Site Survey
II. Attempt to access customer's Wireless Access Points and internal networks

2. WEB APPLICATION PENETRATION TESTING ASSESSMENT

The Web Application Assessment includes scanning, manual testing or both..The test provides a deep and detailed security look at an application. The Web Application Scan identifies web application specific vulnerabilities and assesses the security posture of selected customer's web applications against the Open Web Application Security Project (OWASP) Top Ten common vulnerabilities. The scan looks for a wide variety of vulnerabilities such as Cross-Site scripting, SQL injection, application configuration errors, and other specific application problems. The results detail the risk exposure for a customer's Web applications and demonstrate how vulnerabilities in these applications can be exploited. Suggested remediation actions to lower a customer's risk exposure will also be provided. The penetration test uses knowledge gathered from a web application scan to exploit vulnerabilities discovered during the scan. A manual look at the web application is also performed to identify flaws in business logic, application behavior, and a high-level examination the source code.

Communications between the web client and the servers which make up the web application environment is also reviewed through the use of a proxy for data manipulation/submission on different input fields. The tests will attempt to determine if application accounts are utilizing proper access controls and verify if unauthorized access to protected resources can be achieved from the web application attack vector. The tests also verify if the application properly sanitizes al data that is submitted by application users. The following associated activities will be performed under the Web Application Assessment:

I. Perform Web Application vulnerability scanning.
II. Perform Web Application penetration testing by exploiting identified vulnerabilities.
III. Perform manual Web Application security review.
IV. Perform architectural and code review.

3. DATABASE PENETRATION TESTING

Our Database Penetration Testing assesses the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities. For example, the scan will attempt to identify holes, weaknesses and threats to the information stored within the database. The SparkC Team will identify default usernames and passwords, identify patch-management issues, and review various other security vulnerabilities and configuration problems. The results identify deviations from required baselines and, insecure configurations that are applied on assessed databases. In addition, recommended remediation actions are provided. Credential, non-credential, compliance and vulnerability scans are performed under the Database Scan effort. The following activities will be associated with the Database Scan:

I. Perform network database discovery.
II. Perform automated database vulnerability scanning.

4. NETWORK PENETRATION TESTING & SCAN

Our Network Penetration Testing & Scan assesses the configuration of selected network devices, host and endpoints against configuration baselines in order to identify potential misconfigurations and/or system vulnerabilities. The SparkC Team will identify default usernames and passwords, identify patch-management issues, and review various other security vulnerabilities and configuration problems. The results identify deviations from required baselines and, insecure configurations that are applied on assessed devices. In addition, recommended remediation actions are provided. Credential, non-credential, compliance and vulnerability scan are performed under the Network Scan effort. The following activities will be associated with the network scan:

I. Perform network discovery.
II. Perform automated network vulnerability scanning.

The assessment may vary depending on the assessment plan TOEs and rules of engagement. Our general approach is:

1. Perform reconnaissance to gather information on the target system if not previously defined in the assessment plan
2. Scan the network for open ports and vulnerabilities
3. Achieve the TOEs defined in the assessment plan.