Penetration Testing

Have you ever wondered how susceptible your organization is to hackers?

The best way to answer that question is to hire a team of ethical hackers to hack your network. This process is called penetration testing and it is one of the best ways you can gauge the effectiveness of your defenses.

DGC leverages an industry-standard vulnerability assessment and penetration testing methodology based largely on the Offensive Security Certified Professional curriculum. The methodology outlined below also includes many of the key components of other standard penetration testing frameworks, including those from EC-Council and The Open Web Application Security Project (OWASP).

By having DGC act as a simulated opposing force, the penetration test (pen test) is a security exercise to identify risks to the organization. The DGC team will analyze the environment and leverage found vulnerabilities and misconfigurations, along with the functionalities available to a low privileged user. Rather than simply reporting identified vulnerabilities, the assessment team will attempt to exploit these vulnerabilities, and demonstrate the potential exposure with the goal of reaching the highest possible level of privilege while gaining access to sensitive information. The methodology presented below is broad, and a carefully defined scope will drive the actual components of the test. The penetration test, in general, includes the following components:

Methodology

- Passive Reconnaissance
- Active Reconnaissance
- Social Engineering
- Exploitation
- Post Exploitation
- Privilege Escalation
- Lateral Movement
- Maintain Access
- Cover Tracks
- Reporting

(Continued)

Our final deliverable generally includes risk-ranked findings, categorized as High, Medium, Low, and Informational, based on the intersection of impact and likelihood of exploitation by a threat actor. Each machine in question will be identified by IP address or DNS name. All findings will have corresponding recommendations for improvement and remediation. We document every action taken, both via narrative and screenshot, for each step taken during penetration tests.

Penetration Testing Areas

External Pen Test

The external assessment is the process of identifying technical vulnerabilities in externally facing computers, networks, and network appliances, as well as weaknesses in policies and practices relating to the operation of these systems. DGC uses industry-leading vulnerability assessment tools to identify known weaknesses in services running on the target network. We evaluate these vulnerabilities based on validation and the risk and likelihood that an attacker could exploit them to gain control of a system.

Internal Assessment

The internal assessment's objectives will be to identify vulnerabilities in computers, network devices, printers, Internet of Things (IoT) devices, and other networked devices, and attempt to exploit them as a proof of concept.

Web Application Pen Test

DGC performs dedicated testing of web applications for security weaknesses and misconfigurations. Industry-leading vulnerability and web application scanning tools will be used to identify vulnerabilities based on the OWASP Top 10 Most Critical Web Application Security Risks. These include tests to identify cross-site scripting, SQL injection, authentication weaknesses, vulnerable web application software components, and other application security concerns. DGC will characterize the vulnerabilities to identify the associated risk. Where possible, DGC will exploit identified vulnerabilities to demonstrate risk exposure.

Mobile Application Pen Test

DGC performs dedicated testing of mobile applications to include components of the OWASP Mobile Security Checklist, such as architecture, design, data storage and privacy, cryptography, authentication and session management, and network communications.

Source Code Reviews

DGC reviews web application source code to identify poor coding practices and security vulnerabilities. This review includes static and dynamic code analysis as well as manual code reviews to identify security weaknesses at the source code-level.

DGC is an accounting and business advisory firm with a dedicated IT Risk Assurance & Advisory practice. We offer a range of IT Audit, compliance, and cyber & information security services that can help identify, evaluate, measure and manage compliance and cybersecurity risks. For more information, contact Nick DeLena, CISSP, CISA, CRISC, CDPSE at 781-937-5191 / ndelena@dgccpa.com or Scott Goodwin, OSCP at 781-937-5722 / sgoodwin@dgccpa.com.