SSP BLUE's Red Team – Providing Security Assessment Services

SSP Blue's Red Team provides security assessment services by a team of security professionals with years of experience securing some of the most targeted systems in the world, including Microsoft Online Services, HP Cloud, 20th Century Fox, MySpace, Apple Computer and many others. Our BlackBox network and application penetration testing methodology is comprised of four distinct phases.

1. Information Gathering and Analysis

After establishing the scope of the engagement with the client, the initial phase of the penetration test (pen test) is to gather as much information as possible about the targeted systems or networks. Often this will involve an examination of the client's online presence, similar to the process an attacker would utilize when scouting a potential target. Typical information gathering activities involve network detection techniques and web application analysis. The objective of this exploratory phase is to map out potential attack vectors and exploitable system components.

2. Vulnerability Discovery

SSP Blue utilizes a series of methodical and repeatable tests via custom and automated tools to check against known vulnerabilities. Testing is directed against targets identified in the Information Gathering phase, and is especially useful for pinpointing high-risk areas that warrant special attention. A manual analysis of information obtained determines the validity of detected vulnerabilities. The completion of the Vulnerability Assessment phase will produce a definite list of targets to investigate in depth.

3. Penetration Assessment

The Penetration Assessment phase involves active exploitation of vulnerabilities and system misconfigurations. It also checks for additional points of exposure that may have been missed in previous phases. This is particularly important as vulnerabilities often only become apparent when analyzing interactions between system components and/or applications. Examples of penetrations include those identified by the OWASP Top 10, as well as custom developed attacks.

4. Reporting

We provide a meaningful and quantitative analysis of our findings, which clearly document the feasibility of an attack and the magnitude of impact on the business from a successful exploit. Reports include detailed vulnerability information, reproduction and mitigation steps, severity ratings, and techniques to avoid similar security vulnerabilities in the future. Our Security Assessment Services fulfill many regulatory requirements around penetration testing, including those mandated by the Payment Card Industry Data Security Standard (PCI DSS).

Additional Services

- Source Code Review: Line by line source code analysis for vulnerabilities.
- Security Engineering / Development: Coding of Security Features for the client (e.g. CAPTCHA).

Hemanshu (Hemu) Nigam | Founder | www.sspblue.com | 310.909.6757 | hnigam@sspblue.com

- VOIP & Wi-Fi testing: Pen-testing of wireless networks and VOIP deployments.
- Systems / Node Hardening: Best practices and custom node hardening for your servers and workstations.