From Reactive to Proactive – 4D5A Security

4D5A Security

http://4D5Asecurity.com/ • help@4D5Asecurity.com • (208) 283-7010 • 11578 Shelburne Ct • Caldwell, ID 83605

Security Assessment Services

Assessments of critical assets should take place on an annual basis to identify both known and unknown services and risk. Assessments offered by 4D5A Security use industry trusted security tools and tactics for multiple types of assessments. A blind external assessment of all 65,535 ports on a server typically takes 10-16 hours of total time. *Discounts may be available for 50+ hours of assessment hours and/or new customers.*

Blind External Vulnerability Assessment

A comprehensive assessment of all ports on a server to identify both known (to the client) and possibly unknown open and filtered ports and associated services. This includes banner checks and associated vulnerabilities to identify potential risk to any external actor attempting reconnaissance or exploitation on an external host. Blind External Scans do not include attempted intrusion, exploitation, or other forms of infiltration. Any areas of moderate to critical risk concern found in an assessment include recommendations for mitigation of risk. A **penetration test** may also be implemented with tools such as MetaSploit to attempt exploitation. An **informed external vulnerability assessment** is similar to a blind external vulnerability assessment but is limited to specific ports.

Internal Vulnerability Assessment

Internal assessments are an excellent follow on to an external assessment, for external facing assets, to validate findings and further map out areas of risk management opportunity. Internal assessments have many options from which to select as well as customization to meet your unique business needs:

a) Internal vulnerability assessments of specific ports or services for validation of an external vulnerability assessment report
b) comprehensive scan of all ports and services
c) validation of service pack levels and other details on a host (authentication required)
d) credentials cracking to identify non-compliant or weakly defended passwords in use
e) network topology and architecture
f) admin auditing: who has admin, and to what, and how should roles and responsibilities be managed for optimal risk management
g) policy management: reviewing policy, performing interviews, and providing recommendations for improved security governance
h) social engineering assessments of trusted insiders, including longitudinal metrics, to lower user based risk

Web Application Security Assessment

A web application security assessment involves an in-depth security review of a web application and web services. This assessment involves a comprehensive set of test cases to review an application for common web vulnerabilities such as SQL injection, cross-site scripting (XSS), sensitive information disclosure, input sanitization, session management issues, weak encryption, and intricate business logic flaws. Web applications are the front door to your enterprise, make sure they're secure.

Mobile Application Security Assessment

A mobile application security assessment involves an in depth security review of a mobile application and associated web services. This assessment involves a comprehensive review of the security around the mobile application including proper authentication, local storage of sensitive data, proper binary protections, log analysis, data leakage and insecure inter-process communications. Mobile applications are ubiquitous and their security is critical to ensure your data is not exposed on a large scale.

Espionage Assessment

This assessment is beyond technical assessments of hosts and networks, focused more upon information, relationships, and areas of risk related to being targeted or subject to espionage attacks from competitors and nation/state based attacks. Open source intelligence is aggressively searched for data on target(s) or entity(s) assessed for information that helps map out business relationships, permissions and access to sensitive data, potential social engineering angles, and other data relevant to reconnaissance and/or attempted exploitation for espionage activity.