Annual Third-Party Penetration Testing

With over a decade of experience working with service providers and financial institutions, AuditOne LLP has been providing top-tier analysis and testing services at cost-effective prices.

Our penetration testing represents a method of evaluating the security of a service provider's internal (local area network) computing systems by simulating an attack by a person with malicious intent (e.g., a hacker or disgruntled employee). The process involves an active analysis of these systems for any weaknesses, technical flaws or vulnerabilities. Our tests are carried out from the perspective of a potential attacker using grey hat hacking methodologies. Unlike an information security audit, which is based on external standards, a penetration test is of variable scope with the aim of compromising a target in any way possible via selective targeting. We are here to help you secure your environment.

Methodology:

Our process follows a structured methodology to ensure a safe and thorough execution of the network vulnerability assessment. This methodology employs a series of gradually escalating steps to minimize any risks inherent in such testing. Should anything abnormal become evident, the testing would be suspended before any damage is caused.

The penetration test consists of four phases: Discovery, Enumeration, Port Scanning, and Vulnerability Mapping and Exploitation.

The discovery phase involves information gathering. Public information is used to enumerate targets. In cases where such information is questionable or lacking, we conduct ping sweeps and restricted port scans to determine potential targets.

Once potential targets are identified in the discovery phase, we obtain as much information as possible about each one. The enumeration phase provides us with the information necessary to efficiently conduct the next phase.

We then map the profile of the targets to publicly known vulnerabilities. Only appropriate vulnerability tests are applied to the target hosts (e.g., IIS vulnerabilities are not tested on Apache systems, firewall vulnerabilities are tested only on firewalls, etc.). In cases where the host is indeterminate, several tests for a wide range of vulnerabilities are used.

Finally, we attempt to exploit the identified vulnerabilities to gain access to the target systems. Our policy is to not proceed without explicit permission from service provider management if we are about to compromise the security of a system.

Results of the vulnerability mapping are analyzed for false positives and applicability to the service provider's computing environment. Every attempt is made to ensure the contents of this report are concise and the scale and scope of recommendations are realistic and achievable. Details regarding the exact timing of the tests are not known to service provider employees. Denial of service and other potentially destructive attacks are not performed.

About us:

AuditOne LLP provides a cost-effective program to deliver globally recognized third-party security audit reports. To provide independence between audit and penetration testing engagements, AuditOne LLP partners with another firm to perform all annual penetration tests. AuditOne LLP manages the entire process for you and serves as your primary contact for all associated engagements.

Robert Kluba CISM CISSP
Managing Director
Phone: 408.656.9300
Robert.Kluba@AuditOneLLP.com

https://www.AuditOneLLP.com