Penetration testing

Owner: Ho Yeung, Lee

Classification: Secret

FIPS-199 SC administrative information = {(confidentiality, HIGH), (integrity, LOW), (availability, LOW)}

Standard: NIST 800-115, OWASP

**Approval from senior management**

Planning includes agreement upon the scope of the test and the rules of engagement. This is an extremely important phase because it ensures that both the testing team and management are in agreement about the nature of the test and that the test is explicitly authorized.

Information gathering and discovery uses manual and automated tools to collect infor- mation about the target environment. This includes performing basic reconnaissance

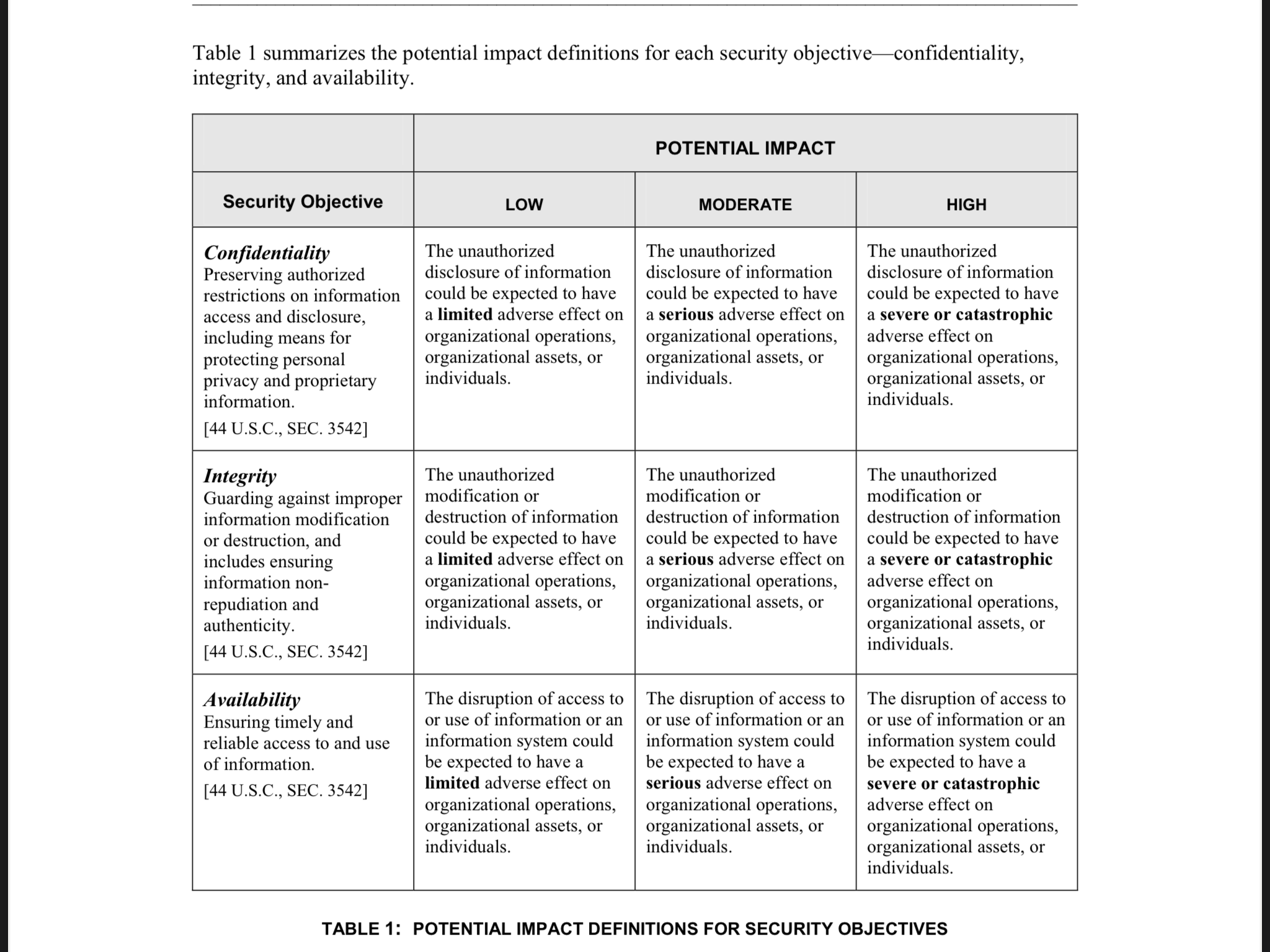
to determine system function (such as visiting websites hosted on the system) and con- ducting network discovery scans to identify open ports.

Vulnerability scanning probes for system weaknesses using network vulnerability scans, web vulnerability scans, and database vulnerability scans.

Exploitation seeks to use manual and automated exploit tools to attempt to defeat sys- tem security.

Reporting summarizes the results of the penetration testing and makes recommenda- tions for improvements to system security.

**Appendix**

**FIPS-199**