STACKTITAN

TACTICAL ASSESSMENT CATALOG

VULNERABILITY ASSESSMENT

The Vulnerability Assessment produces actionable data, curated and analyzed by experienced, specialized professionals in a non-intrusive manner. Introducing contextual and human analysis results in improved network security posture understanding and prioritization.

STACKTITAN

VULNERABILITY ASSESSMENT

INFORMATION GATHERING AND INTELLIGENCE DERIVATION

Information within public domain (e.g., search engine caches), and abstracted data (e.g., dark / deep web repositories) often provide the necessary details to assist in cataloging details for relevant targets of interest. Further, the information gleaned from these sources will often provide usable and actionable intelligence that may be leveraged to position further adversarial campaigns. The output of this exercise will enable the Threat Profiling and Modeling.

THREAT PROFILING AND MODELING

A variety of criteria such as industry vertical, incentive, capability, and opportunity cost, for example, can enable a motivated adversary. Therefore, the significance of understanding the overall objective in conjunction with a relevant threat actor is paramount to establishing threat models that will replicate actual venerable attack pattern models. The output of this exercise will project a viable Exploitation and Post Exploitation lifecycle.

RISK IDENTIFICATION AND EVALUATION

The collective of details observed throughout the engagement are analyzed and evaluated for impact to the information systems, surrounding networks, policies and procedures, software design, and vulnerability management, for example. The severity of each respective issue is weighed within the context of actual risk exposure, severities may be adjusted as a result, and the results prioritized for remediation. The output of these activities will produce the necessary input for all formal reporting requirements.

VULNERABILITY ASSESSMENT

EVIDENCE COLLECTION AND REPORTING

The evidence collected throughout the engagement is provided in a manner that proves the empirical risk of each detected vulnerability. The evidence is provided in conjunction with the required data for recreating and remediating the vulnerable state. A final set of reports is provided to exemplify the engagement appropriate for executive and technical leadership as well as those responsible for risk treatment.