STACKTITAN

TACTICAL ASSESSMENT CATALOG

PENETRATION ASSESSMENT

Whether the requirement necessitates compliance with regulatory mandates or security posture insight, the Penetration Assessment provides demonstrable information security controls validation through adversarial proof of concept scenarios that exemplify actual contextual risk along with thoughtful and actionable mitigation strategies.

STACKTITAN

COMPLIANCE ALIGNMENT

DOCUMENT COLLECTION AND NETWORK REVIEW

Depending on the regulatory requirement, a precursory review of documentation may be required to align the preliminary Penetration Assessment objectives. This may include network architecture diagrams, user access procedures, data handling and classification documents, and critical assets/resources, for example. The output of this exercise will clearly define targets of interest, operationalization methods, tactical techniques, area familiarity, and logical situational awareness.

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 establish a viable Exploitation and Post Exploitation lifecycle.

COMPLIANCE ALIGNMENT

EXPLOITATION AND POST EXPLOITATION

Exploitation is used to deduce the probability of a vulnerability's inherent risk exposure to be leveraged to compromise the target of interest. Further, the exploitation can lead to technical compromise of the affected asset and then be used to further penetrate into the network environment. Similarly, the compromised asset may disclose protected data such as personal or privacy information. The output of this exercise provides demonstrable impact and severity weighting based on tactical observations.

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.

COMPLIANCE ALIGNMENT

EVIDENCE COLLECTION AND REPORTING

The Penetration Assessment must be a stand-alone work document, therefore, 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.

NON-COMPLIANCE ALIGNMENT

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 establish a viable Exploitation and Post Exploitation lifecycle.

NON-COMPLIANCE ALIGNMENT

EXPLOITATION AND POST EXPLOITATION

Exploitation is used to deduce the probability of a vulnerability's inherent risk exposure to be leveraged to compromise the target of interest. Further, the exploitation can lead to technical compromise of the affected asset and then be used to further penetrate into the network environment. Similarly, the compromised asset may disclose protected data such as personal or privacy information. The output of this exercise provides demonstrable impact and severity weighting based on tactical observations.

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.

NON-COMPLIANCE ALIGNMENT

EVIDENCE COLLECTION AND REPORTING

The Penetration Assessment must be a stand-alone work document, therefore, 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.