STACKTITAN

TACTICAL ASSESSMENT CATALOG

ADVERSARIAL SIMULATION

STACKTITAN has successfully been executing complex Adversarial Simulations for nearly a decade, and understands that each organization is comprised of unique requirements or objectives. The ability to understand the true capabilities of deployed security controls is paramount when measuring the organization's security readiness and attack resiliency. Further, it is necessary to perform actual unconventional attack simulations that exceed techniques and subsequent results of the typical penetration test. This collection of services enables the organization with simulated, unconventional, adversarial attack campaigns as a method to demonstrate impact (e.g., red teaming). In conjunction with collaborative interaction (e.g., threat hunting), analysis of kill chain metrics, and educational knowledge sharing, Adversarial Simulation services can enhance an organization's introspection of security readiness.

ADVERSARIAL SIMULATION

SERVICE DESCRIPTION

The Adversarial Simulation is planned, executed and operationalized using tools and techniques along with skilled operators proven to remotely (i.e., sourced from the Internet), locally (i.e., insider) and/or physically breach some of the world's most difficult environments. A breach of security controls is not accomplished using automated means, but rather purpose built tool-chains, manual examination and precision relevant to the overall target objective. STACKTITAN's operators have a diverse tactical background comprised of Red Team and esoteric specialized capabilities.

The evolution from traditional Penetration Testing to Adversarial Simulations facilitates the introduction of more advanced assessment techniques. Additionally, each Adversarial Simulation, although unique, should strive to achieve mission or business critical objectives. Adversarial Simulations allow defense teams (e.g., Threat Hunt, Incident Response, Sec-Ops) to better understand and prepare for actual attacks through the use of live-fire exercises and subsequent telemetry data. The following sections describe some of the more pertinent and relevant aspects as applicable to all simulation engagements.

ADVERSARIAL SIMULATION

PRE-ENGAGEMENT PLANNING

The demonstration of actual risk through adversarial testing employs unconventional techniques, which requires absolute precision during the preplanning phase. Prior to project initiation, STACKTITAN and the client will collaboratively define overall project goals, operational escalation/de-escalation protocols, exclusionary criteria, timelines, milestones, etc. in order to ensure all details are adequately addressed and the overall project is positioned for success.

OSINT – DEEP/DARK WEB – THREAT INTEL DERIVATION

The Remote Adversarial Engagement starts with information collection relevant to the target objective. The information often comprises logical, physical, and social data sets obtained through public, private, and commercial sources. All of the data is then analyzed to construct a profile that is intended to derive actionable intelligence. The intelligence is used to facilitate and enable attack campaigns throughout the engagement.

ADVERSARIAL SIMULATION

THREAT PROFILE AND MODELING

Adversaries or Threat Agents possess varying objectives, depending on their motive and capacity. Therefore, prior to commencing with the first attack chain it is important to define a valid threat profile and model the proposed course of action to be taken during the adversarial simulation. The Threat Profile and Threat Model used within the Remote Adversarial Simulation is a culmination of various known Threat Agents and their respective historical threat campaigns to provide a unique perspective of attack resiliency, mitigation capabilities, and security readiness.

NON-ATTRIBUTABLE TESTING ARCHITECTURE

The ability to accurately demonstrate a motivated and capable adversary while maintaining anonymity is dependent upon both skill and appropriate tooling. STACKTITAN leverages a combination of both proprietary and commercial methods of establishing various geographically-distributed, cloud-based abstraction nodes. This infrastructure known as “Fast Ready Destroy (FRD)” is considered unique to each Adversarial Assessment and is highly adaptive to a variety of tactical requirements and conditions. As a result, each FRD maintains a discrete distributed point of origin making threat hunting and overall detection capabilities a formidable attribution effort.

ADVERSARIAL SIMULATION

RED TEAMING

The Red Team exercise provides the actual tactical live-fire demonstration built upon prior stages in the Adversarial Simulation. The Red Team attack chain leverages gathered intelligence, threat profiles and models, and unconventional attack techniques. As a result, this exercise provides ample opportunity for educational transfer between both adversarial and defending teams, which will enhance overall security operational capabilities.

ADVERSARIAL SIMULATION

REMOTE ADVERSARIAL SIMULATION

SERVICE DESCRIPTION

The Remote Adversarial Simulation (RAS) encompasses the core adversarial methodology as a means to emulate a viable Internet-sourced threat campaign against a target organization. Emphasis is always on the skilled, covert breach of perimeter security controls, whether through logical or social means, and the subsequent attack chain and overall course of action. Observations are made throughout the progressive threat campaign to identify effective block points and deficiencies that should have prevented attack proliferation.

ONSITE ADVERSARIAL SIMULATION

SERVICE DESCRIPTION

The Onsite Adversarial Simulation (OAS) extends upon the prior reconnaissance and information gathering phases mentioned during the Remote Adversarial Simulation as a means to prepare for the breach of a physical location. The emphasis is on unauthorized or unlawful entry into a physical dwelling through unconventional tactical breach techniques. The use of proven surreptitious and covert techniques is leveraged as a means to accurately assess both technical (i.e., physical deterrents) and social (i.e., human) controls. Further, this simulation is often combined with the Remote Adversarial Simulation in order to illustrate a complex threat campaign against the target organization while providing a high-level perspective of actionable observations and mitigation strategies.

ADVERSARIAL SIMULATION

INSIDER ADVERSARIAL SIMULATION

SERVICE DESCRIPTION

The Insider Adversarial Simulation (IAS) is planned and executed under the premise that an adversary has already gained initial entrenchment within the organization. This introduces the shift in mindset, to not if an adversary is going to gain unauthorized enterprise access, but rather to what extent can an adversary operate within the environment. The IAS, similar to all STACKTITAN Adversary Simulations, leverage unconventional techniques to emulate an insider threat campaign (e.g., rogue employee, phishing victim, malicious contractor, etc.) while assessing the organization's mitigation capabilities.

DECOMPOSED ADVERSARIAL SIMULATION

SERVICE DESCRIPTION

As industry-wide, public breaches are more frequently occurring, organizations often want to understand the relevance of their assets and resources targeted by specific threat campaigns. The intent of the Decomposed Adversarial Simulation (DAS) is to align the target organization's operational faculties with the motive and capacity of a formally-documented threat agent. An adversary's respective threat campaign is deeply analyzed, decomposed into a tactical adversarial simulation emulating the actual historical threat campaign, mapped to a granular threat model, and executed to assess mitigation capabilities and overall attack resiliency.