Assessment Methodology

The security assessment will be performed using technologies and known threats as of the date(s) of the test. Security levels and threat models will be generated for each test, along with a prioritized list of remediation steps and actions. Indigenous recommends security assessments be performed on a periodic basis as new vulnerabilities are continually developed and operationalized by threat actors and cyber criminal elements. In addition, Indigenous recommends security assessments be regularly supplemented with internal configurations reviews and policy assessments to ensure best practices are being implemented and followed to ensure that a comprehensive security program is used to mitigate future risks, i.e. NIST 800-53, CSC-Top 20, ASD Top-35, etc…

Indigenous employs a six-phased methodology for its security assessments. Phase Zero represents the blue teaming component of our security assessment, where Phases One through Three detail the red team assessment structure and how tests are performed. Phases One through Three detail the assessment structure and how tests are performed. Phases Four through Six occur after initial testing has been completed to ensure comprehensive findings are compiled and proper remediation with follow-up occur. Our focus is first identifying critical vulnerabilities that require immediate action and working with the security team to ensure recommended mitigation steps are implemented. Smaller single purpose tests are then employed to validate the effectiveness of the fix actions and mitigation steps.

Phase 0: Threat Hunting

In keeping with advances in malware trends and advanced threat attacker capabilities, Indigenous Intel employs a host based agent solution for collecting live operating system telemetry from customer endpoint machines and networks. Endpoints include Desktop and Server infrastructures. This security telemetry is streamed back to Indigenous Intel cloud analytic server for processing, storage, and analysis. Data returned from machines is characterized for both known signature threats and unknown threats based upon behavioral characteristics. Deployed agents also allow Indigenous Intel analysts to perform continuous live monitoring, remote investigations against suspicious host artifacts, and forensics. Security telemetry collected from endpoints include:

- List of running processes, process image path, list of loaded libraries or modules, a hash value for each executable module, and start/end time for process execution
- Processes running that appear to be cloaked or hidden (anomaly detection)
- Metadata (path, size, file MAC times) on files considered suspicious (anomaly detection)
- List of domains to which DNS requests were issued (sort based based upon uniqueness)
- Metadata (IP:Port) of UDP and TCP network connections
- History of IP addresses for each endpoint
- List of registered services, drivers, and programs along with their recorded behavior
- List of programs set to auto-boot (autorun) indicative of persistence
- Metadata on files added, removed or modified into directories commonly affiliated with malicious software or threats
- Memory pages marked as executables for recognizable artifacts as suspicious

This data is continuously analyzed and leveraged to develop a profile for individual hosts and networks regarding their respective threat score within the network and identification of any indicators of compromise. Any identified threats are reported to security assessment points of contact for remediation and mitigation.

Results from threat hunting activity are leveraged to provide a holistic report on supported customer network security architecture, not only from conducting red team security auditing and benchmarking to security best practices and standards, but also identification of any threats or threats gaps from a blue teaming perspective.

Phase I: Reconnaissance

Each aspect of the assessment begins with a reconnaissance phase, where information gathering techniques are employed to gather data used to develop a plan of action and effectively prosecute identified targets of interest. This phase is particularly important for establishing attack vectors that are most likely to succeed. This phase relies heavily on open source intelligence gathering tools and methodologies, such as Maltego, Search Engines, Shodan, and other information harvesting tools and techniques with a goal of disclosing as much information as possible about target systems and networks of interest. Harvested information is used to identify vulnerabilities and identify security weaknesses to move toward exploitation and detection evasion. Each targeted technology type of the test security controls will be tested to determine if an attack may result in sensitive data disclosure, vulnerability discovery for gaining local or remote access, and inappropriate or unauthorized viewing, altering, copying, deletion of information and data. Two types of users are mimicked during this phase: (1) unauthorized users attempting to gain access to sensitive data, information systems, and networks; and (2) authorized users attempting attempting to acquire or utilized enhanced or inappropriate privileges to gain access to sensitive data, information systems, and networks. The following will be tested during this phase:

- OSINT Information Gathering
- Initial Target Review, Identification, and Verification
- Social Engineering
- War Dialing
- Network and Wireless Network Scanning and Enumeration
- Website Mapping and Web Application Enumeration
- On-site Physical Site Surveillance and Reconnaissance
- Wireless Data Collection for Password Cracking
- Brute Force Authentication Techniques
- Credential, Authentication, and Cookie Testing
- Source Code Review and Backdoor Testing
- Input Validations for Data Disclosure

Phase II: Verification

Following the initial reconnaissance phase, the verification phase begins where the majority of data manipulation and active prosecution against devices, applications, and sites begin using both automated and manual tools and processes. Results are meticulously reviewed by Indigenous analysts, where each test is validated and furthermore tested again to validate results through detailed introspection. For example, now that system identification and positive identification of a target has been achieved with an initial vulnerability review, we can now begin to modify and retest identified vulnerabilities in an attempt to further abuse and validate the severity of the findings. Indigenous attempts to identify security risks resulting from weaknesses, such as:

- Vulnerability Scanning and Mapping
- Port Scanning and Host Fingerprinting (In-Depth)
- Alternate Route & Backdoor Identification (Web Shells)
- Weak or No Encryption/SSL Vulnerabilities

- Obtain Unprotected Source Code
- Cookie Poisoning
- Code and Form Vulnerabilities
- Hidden Field Manipulation
- Parameter Tampering
- Exploitation of State Variables
- SQL Injection
- Source Code/Banners
- Input Validation Errors
- Malicious Code or Command Injection
- Capture Traffic
- Executable Code vulnerabilities such as Buffer Overflow Conditions/IIS or Apache Weaknesses
- Identification and Exploitation of Business Logic

Phase III: Exploitation

Finally, the assessment escalates to active exploitation, where Indigenous assessors attempt to fully compromise identified target(s) (e.g. web infrastructure, wireless access points, etc…). Prior to any assessment, Indigenous works with the specified web site owner to determine ground rules for vulnerability exploitation. Within the realm of exploitation of identified vulnerabilities, Indigenous performs services based upon the type of target, such as, in the case of a web server: (1) we will identify and exploit the implemented security controls or lack of controls, (2) for applications with sensitive data, we will attempt to gain unauthorized access and transfer data between test accounts and/or perform other transactions without providing the appropriate authentication, or (3) for web applications that use downloadable code, we will attempt to identify vulnerabilities associated with installing and operating the executable code. Prior to exploitation we will coordinate with the network owner per instructions in the rules of engagement, where identified vulnerabilities will be used to gain access to internal systems and networks. This phase typically utilizes many tools that may be available in the public domain and are used by actual adversary threat actors. The methods utilized during this phase are tightly controlled per the assessment agreement; the highest consideration is always paid to avoid damaging or disrupting customer computing resources and information. All activities are extensively logged.

Below is a high level description of Indigenous's phases 1 - 3 methodology for performing an assessment:

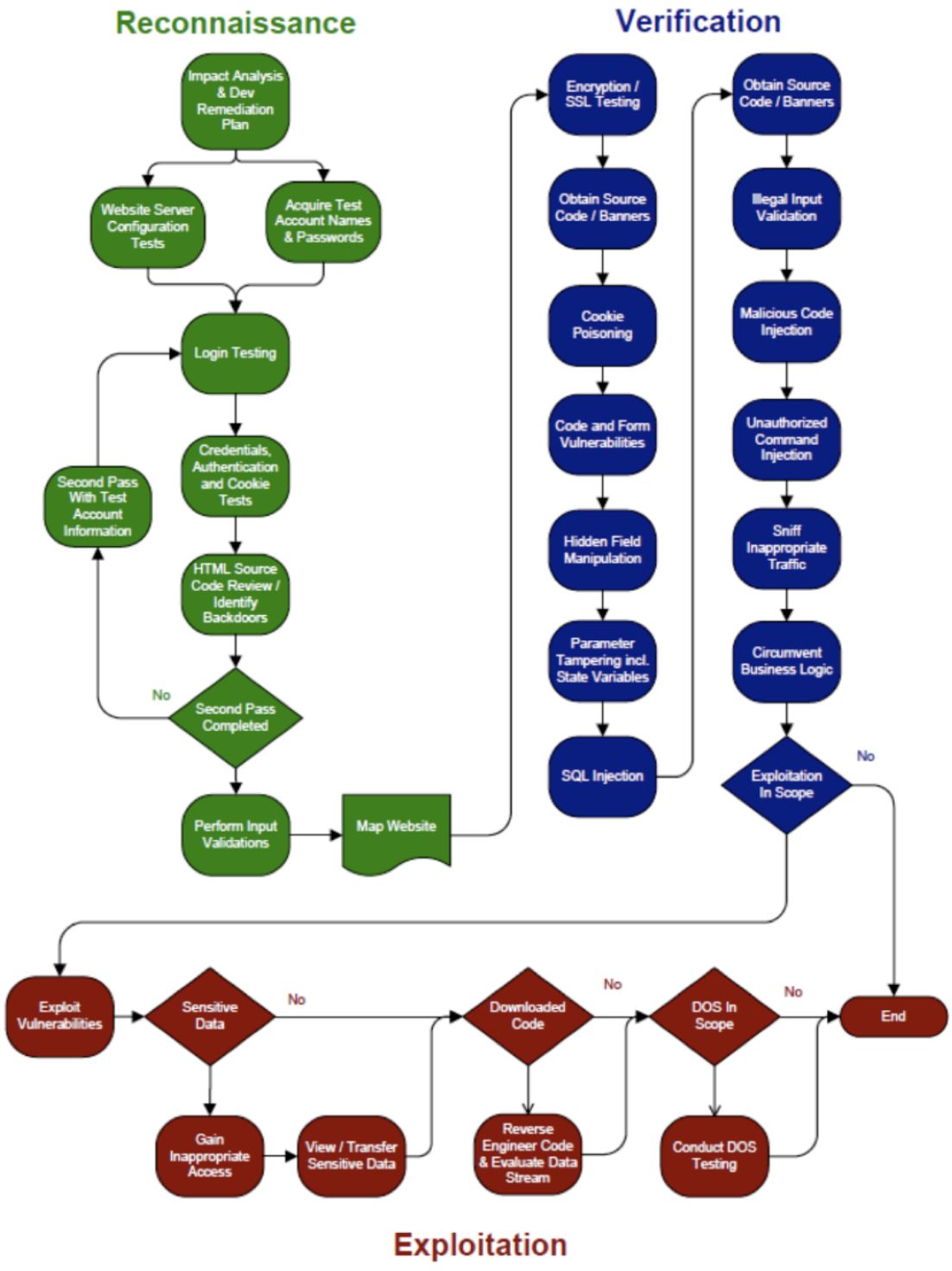

Figure 1: Web Application Methodology

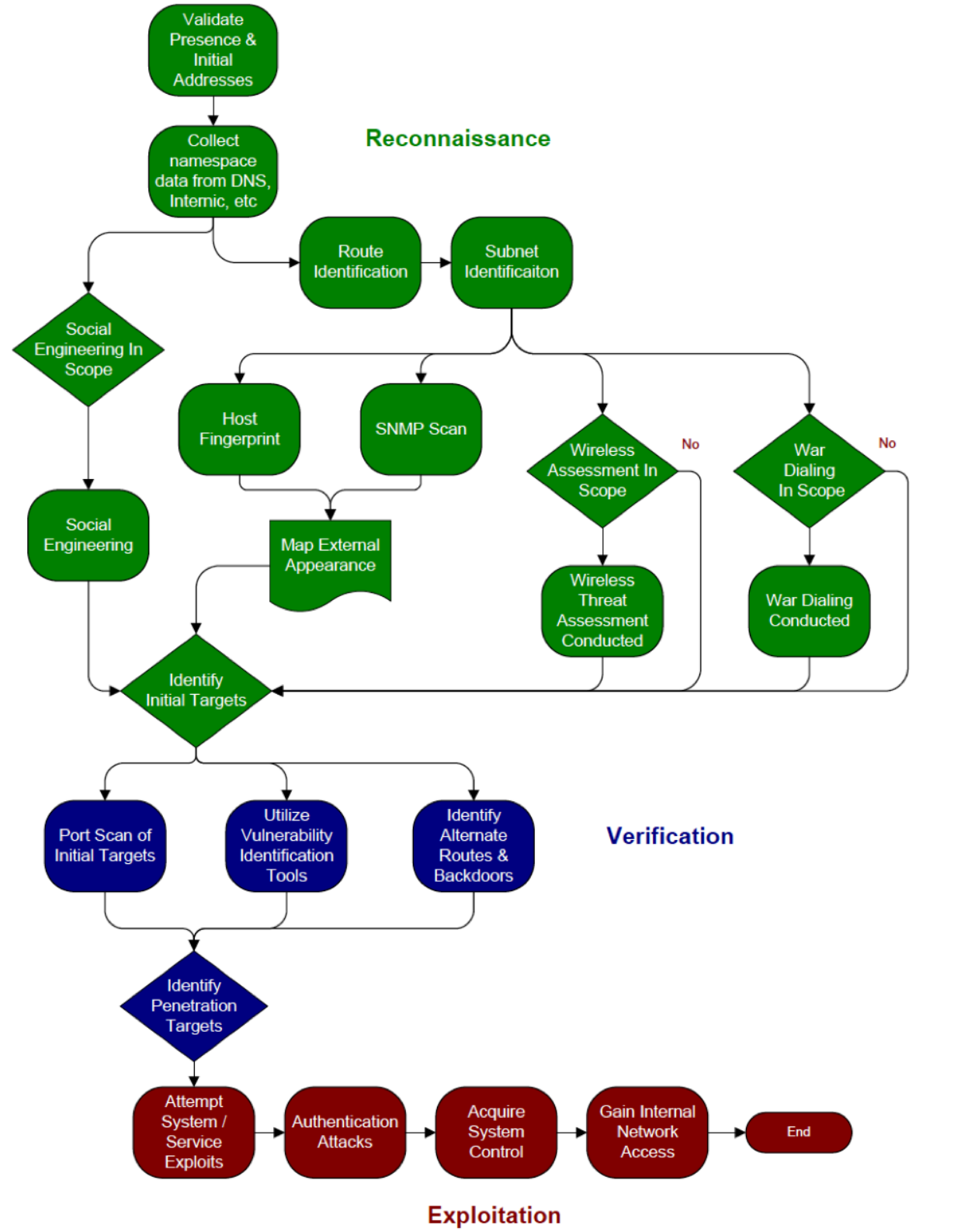

Figure 2: Network Infrastructure Methodology

Reporting and Finalization: Phases 4 – 6

In phases 4 – 6 Indigenous focuses on ensuring the customer receives the most benefit possible from its security assessment. Most companies only focus on the initial assessment. Indigenous believes that focusing on the life-cycle of a test, completing and verifying that comprehensive reporting is performed, remediation occurs and retesting of identified vulnerabilities is completed, providing customers the most value through actionable recommendations and validation of implemented security controls.

Phase 4: Report

Following completion of the exploitation phase, the project manager for the effort will provide a bulleted list with findings that covers heading and severities. This is only a preliminary findings list and early draft of results that will later be structured into a final report. This initial findings list is used to ensure that identified vulnerabilities can be rapidly fixed by appropriate IT and Security staff and retested by the Indigenous team. Additional details and findings will be added, deleted, and severities changed based upon peer reviews and further introspection of findings.

Throughout the reporting process, severity and difficulty ratings are evaluated through a peer review process with additional Indigenous assessors. The report will contain a list of IPs and/or ports to detail the location where the finding was discovered. A detailed explanation of findings is provided to give the customer a full understanding of the issues and concerns surrounding the finding and more importantly alignment with business priorities to describe how the client is affected by the finding, along with an explanation for the severity. This allows the client to more quickly incorporate and execute recommended mitigations. Evidence is further correlated and presented to provide a clear and concise understanding of findings in the report.

Phase 5: Remediation

The remediation phase consists of two parts:
Part 1: vulnerabilities are remediated by supported customer approved network and security staff based on the information providing in the findings portion of the report.
Part 2: the assessment team will review the initial findings and verify the remediation provided per vulnerability was appropriately implemented and the vulnerability was appropriately mitigated. Additional remediation may be validated through screenshots (images) and configuration files if acceptable by both parties.

Phase 6: Clean Up

Indigenous professionals understand that security information is extremely sensitive to an organization. As a result, we ensure assessment details are removed from test systems. Following completion of the assessment, test systems are re-imaged and customer data is only stored on encrypted file systems with full disk encryption.

Findings Severity Classification

Each vulnerability identified through out the engagement will be provided with a severity (risk) factor.

- **Critical** Findings designated as critical may be used to immediately breach the integrity of the supported organization. This level of severity should be addressed immediately. In addition to addressing the issue, action should be taken to ensure a compromise has not already taken place.

- **High** Findings with this level are serious deficiencies that have already, or most likely will result in a series breach within the hosting infrastructure's ability to maintain an appropriate security posture. The system or data that would be compromised is considered critical to the operation of the organization. The system or data that would be compromised is considered critical to the operation of the organization. An example of this type of system or data would include credit card data or personal identifiable information, administrative passwords, or control of a primary server. Findings within this category should be remediated immediately.

- **Medium** Findings at this level of severity could have a moderate impact to the organization if an attack were successful. The system or data that would be compromised are considered sensitive and should not be in the public domain, but are considered as critical. Examples of these types of findings are anonymous FTP servers or organization phone lists. Findings in this severity should be remediated quickly but are not as important a priority as those in the high findings severity.

- **Low** Findings at this level of severity allow an attacker to gain knowledge of the organization. They do not constitute a direct threat to the organization itself, but are the building blocks attackers use to wage a successful assault against an organization of interest. Examples include header leaks from web servers that provide attackers with direct knowledge of the server type, version and languages used so that they may reduce the amount of work needed in the attack. These findings are a lessor priority, but should be fixed within a reasonable timeline.

In addition, each finding identified throughout the assessment will be categorized according to the level of difficulty required to successfully exploit the vulnerability. The difficulty of exploitation is divided into the following categories:

- **Easy** Includes findings, which can be easily exploited by commonly available tools on the Internet, well-known exploits, and/or where little to no technical expertise is required.

- **Moderate** A finding, which requires a degree of technical competence in the subject and an effort to reproduce the finding, goes beyond the simple execution of an automated tool or script.

- **Hard** A finding, which requires the use of custom developed tools and procedures, programming skills, and detailed technique expertise.

  It is important to note that the severity of the classification and the difficulty of the exploitation are generally independent. While, a given finding may result in significant business risk (high severity), the findings may be quite easy to exploit. That said, a high severity finding could also be extremely difficult to exploit, requiring specialized expertise. This is where a threat model is important to provide a level of context and meaning behind each finding to ensure management has the appropriate level of understanding of risk and impact.

Testing Tools

Indigenous will use a variety of automated and manual tools to increase the thoroughness and efficiency of phases one through three of the assessment. The following tools may be used throughout the duration of the assessment.

- Burp Suite Pro
- Various Web Browsers and Plugins
- Kali Linux (associated tools/suites)
- Tenable Nessus
- Rapid 7 NeXpose
- Rapid 7 Metasploit Pro
- Peensy/Teensy
- BadUSB
- Rubber Ducky
- Pwnie Express
- Cobalt Strike Pro
- Social Engineering Toolkit
- Custom Scripts
- Elastic Search
- Logstash
- Logbeat
- Wazuh
- Kibana
- OSSEC

Penetration Testing and Security Assessment Standards and Guidelines:

- NIST Risk Management Framework
- NIST 800.53
- CSC Top 20
- ASD Top 35
- PTES (Penetration Testing Execution Standard)
- OSSTMM v3
- OWASP (Open Web Application Security Project)
- NIST SP800-115
- PCI/DSS Penetration Testing Guidance
- FedRAMP Penetration Test Guidance