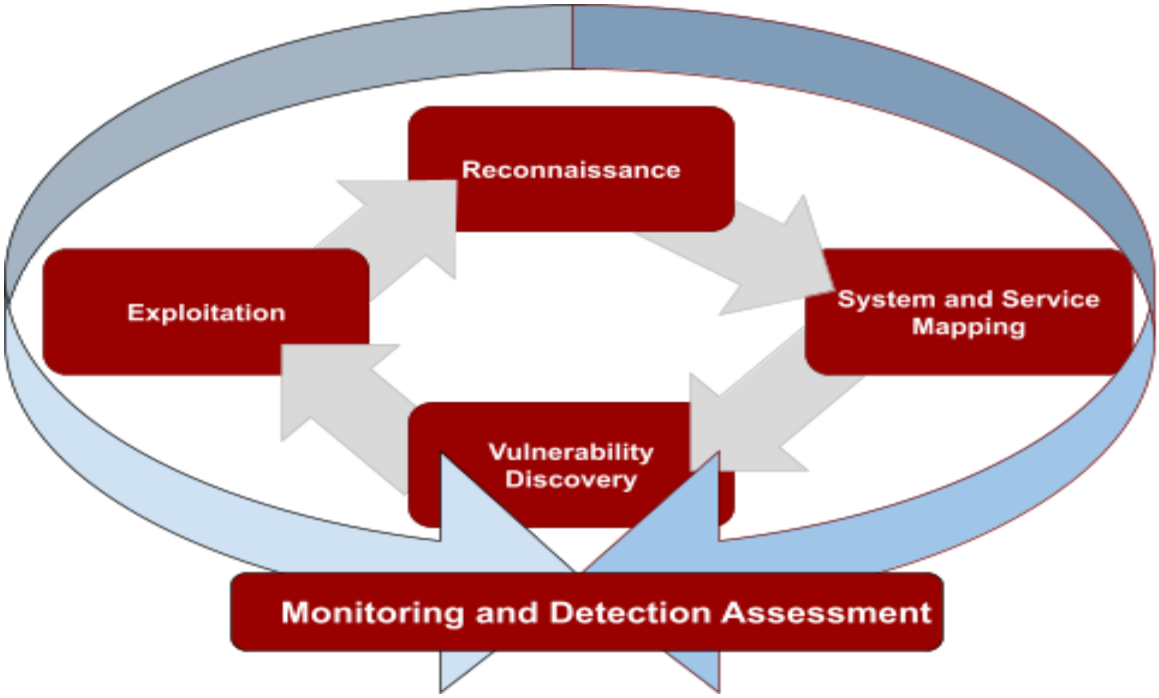
Secure Ideas follows an industry standard methodology for testing the security of network infrastructure, clients and applications. This methodology is a four-step process as follows:



Note that the methodology is cyclical in nature. Successful exploitation may lead to additional iterations through the methodology. Also, the entire methodology is surrounded by our monitoring and Detection Assessment.

A red team and penetration testing assessment is an ongoing long-term engagement designed to simulate an attack by a modern sophisticated attacker. Secure Ideas offers these in 30, 60 and 90 day sizes. The methodology we follow is explained below.

Reconnaissance:
During reconnaissance, Secure Ideas staff will search public sources for information regarding the target organization and its infrastructure, systems, and applications. Examples of information that is gathered during reconnaissance include:

- Lists of users, for potential use in account harvesting and takeover attacks as well as social engineering if it is in scope
- Lists of hosts associated with the target organization
- Host configuration information
- Vulnerabilities that have been publicly disclosed in the past

Secure Ideas will include information discovered as part of the final report if it is relevant to any of the exploitable findings found during the penetration testing.

System and Service Mapping:
The next step in the methodology is mapping, which is where Secure Ideas will study the systems and services provided by the target network. Examples of items that are covered during application mapping include:

- Understanding the network architecture and segmentation (e.g. flat vs. strictly segmented)
- Services exposed to the Internet and/or internal network
- Fingerprinting operating systems and applications used on the target network
- Analysis of services and applications mapped
- Detection of known applications and services within the target network
- Identify sensitive data visible within the network services and shares

Note the above list is not exhaustive. If Secure Ideas encounters network behavior or services that fall outside of the usual, it will be treated as an area of interest and scrutinized accordingly.

Discovery:
During the discovery stage of the network penetration test, Secure Ideas will use the information gathered in the previous two steps to assist our staff in finding the vulnerabilities within the target systems and services. Using this information combined with both automated tools and manual testing, Secure Ideas will provide thorough coverage for all common vulnerabilities and will also seek out less common vulnerabilities depending on the network architecture and features (e.g. web services or the use of certain client applications). Testing may be divided into the following categories:

Category	Testing
Authentication, Authorization, and Session Management Testing	Most of this category must be tested manually, as automated scanners have difficulty understanding context within the application: • Discovery of default passwords within available services • Testing of all authentication features such as login, registration, and forgot password. • Testing of authorization across sensitive functionality and services • Seek out horizontal and vertical privilege escalation opportunities • Validate existence and effectiveness of Single-Sign On controls and systems • Assess the Active Directory (AD) infrastructure
Encryption and Configuration	Scan the network for flaws related to encryption and configuration. This includes: • The use of components (both server and client side) with known vulnerabilities. • Use and configuration of SSL

	• Evaluating encryption at-rest systems discovered during mapping
Server and Services Testing	Using a combination of automated and manual techniques, test server and services exposed on the target network. This testing includes items such as: • Discovering known vulnerabilities based on service identification • Assessing services for misconfigurations that can be exploited • Evaluating shared datastores or applications for access to sensitive data • Explore services for potential pivoting capabilities and flaws
Client System and Application Testing	Using a combination of automated and manual techniques, test inputs on the client systems. This testing includes items such as: • Testing for exploitable applications • Testing misconfigured end-points • Assess end-points for exposure to lateral movement and pass-the-hash attacks
Other Testing	Test for other common flaws that fall outside of the above, such as: • Segmentation issues and flaws • Authorization token capture via MitM or poisoning attacks • Social Engineering possibilities due to internal system exposures • Data exposure within services and applications • Testing of any other features not otherwise mentioned

Exploitation:
Exploitation is the final step of the network penetration test. By exploiting the vulnerability, Secure Ideas is able to provide a realistic understanding of the business exposure from the target. Exploitation exercises are often limited to the minimum required to build a proof of concept so that developers and security staff may reproduce the issue. Secure Ideas may go beyond a proof of concept if pivoting and post-exploitation is in scope for the test. Secure Ideas will not conduct exploitation of Denial of Service vulnerabilities without written prior permission.

Monitoring and Detection Assessment:
As Secure Ideas performs the four steps that make up the methodology, our staff work with the target organization to determine the capabilities for monitoring the network for attacks. Secure Ideas also determines the thresholds at which the organization will detect an attack. The result of this assessment is that the client is provided information on how a real-world attacker would assess and exploit the system as well as a metric for how capable and well the detection and monitoring capabilities function. Secure Ideas will also work with the organization to provide recommended fixes or improvements based on these assessments.