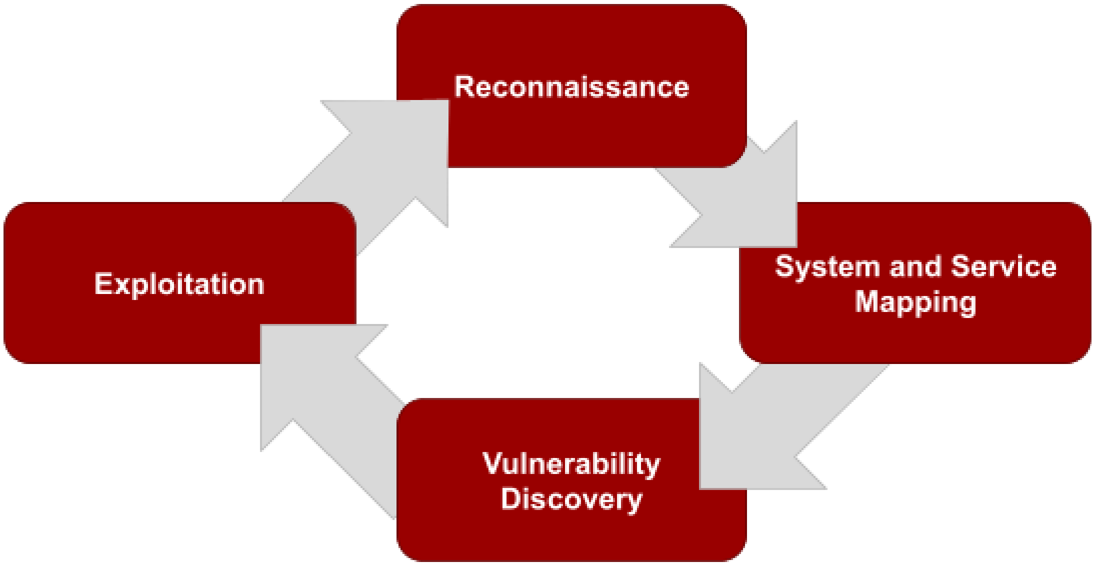
Secure Ideas follows an industry standard methodology for testing the security of network infrastructure, clients and applications. This methodology is a four-step process as follows:



Note that the methodology is cyclical in nature. Successful exploitation may lead to additional iterations through the methodology.

The specific exercises performed in each step of the penetration test vary depending on the specific attributes and scope of testing, and a complete penetration test may include several or all of the following attributes. The following table matches attributes with details and scoping notes about how this impacts a test.

Attribute	Details and Scoping Notes
External	External network penetration testing focuses on public IP space of the organization. The penetration test proceeds from the perspective of an external attacker and is focused on vulnerabilities that can be used to gain entry to the Internal network as well as exposure of sensitive information. Social Engineering may be included in the scope of external testing.
Internal	Internal network penetration testing focuses on the private IP space of the organization. The penetration test proceeds from the perspective of an internal attacker, usually by simulating a compromised workstation. This type of test aims to identify risks specific to this type of inside threat and is centered around the attacker's ability to gain elevated user credentials, access to important systems, and access to sensitive information. Social Engineering is typically not included for Internal testing as it is assumed to have already succeeded.

Black box	Black box penetration testing begins by providing the testing team with only very limited information about the test. This type of test is designed to better reflect a realistic attack scenario. A significant portion of the test is spent performing reconnaissance activities, and the testing team must frequently verify scope before proceeding with attack scenarios. Black box testing is typically also performed in a more stealthy manner, takes longer, and is more costly than gray box testing.
Gray box	Gray box testing begins by providing the testing team with details such as specific network ranges and domains that are in scope. User accounts may also be provided. Gray box testing is more efficient than Black box testing as it shortcuts most of the reconnaissance activities. Gray box testing is typically also less stealthy, shorter, and less expensive than Black box testing. Gray box testing also usually provides a more comprehensive assessment of risk.

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 servers 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	Using a combination of automated and manual techniques, test inputs

Application Testing	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. Rather than just stating that a vulnerability exists, Secure Ideas attempts to determine the actual risk the vulnerability presents. This happens by exploiting the flaw and then looking for opportunities to escalate privileges and pivot onto other systems. These post-exploitation processes usually involve determining what access the exploited system or user has and whether it can be further tested. This often restarts the methodology's cycle by opening new avenues for reconnaissance, mapping, and discovery. When multiple vulnerabilities are found with similar potential results, exploitation exercises are often limited to the minimum required to gain access and demonstrate the risk. Secure Ideas will not conduct exploitation of Denial of Service vulnerabilities without written prior permission.