UISO Penetration Test

Pre-engagement documentation list

The penetration tests performed by the UISO simulate attacks by internal attackers with various levels of knowledge of IU's systems and procedures, and the system being tested. To accomplish that and best design the testing to efficiently and as completely as possible determine risks to the system, the tests are what is commonly referred to as "white box" or "crystal box." This means the testers have complete knowledge of the system before testing is started. To that end the following information should be provided to the testers before the end of the pre-engagement phase:

- List the primary and any secondary goals that will be furthered by this penetration test.
- Provide a description of any threats to the system being tested that have been active or discovered in the past twelve months. These will be considered when determining the appropriate tests to be performed.
- Provide a description of any vulnerabilities in the system or any of the system components that have been exploited or discovered in the past twelve months. These will be considered when determining the appropriate tests to be performed, even if the vulnerabilities have been patched or mitigated.
- Provide a current list of the following:
    - All assigned VLANs with all subnets and gateways.
    - All IT system components including their:
        - IP address(es)
        - Hostname (host configured and DNS if different)
        - If they are joined to Active Directory and if so the name of the Computer Object
        - Operating system and version
        - Geographic location(s) of the system component.
- Provide a current network diagram showing all connections between system components of the system being tested and those between system components of the system being tested and system components of supporting systems. A spreadsheet detailing each connection with a key that makes an easily followed link between the connection on the diagram and its description in the spreadsheet. The spreadsheet must at least include the following details:
    - Source IP address (if dynamic or unknown indicate that)
    - If applicable, source port (if dynamic indicate range)
    - Destination IP address (if dynamic or unknown indicate that)
    - If applicable, destination port (if dynamic indicate range)
    - Network protocol chain starting at most appropriate network layer. For example, a typical connection to a web site might start with the Internet layer of the Internet protocol suite model and end with the application layer: "IPv4 – TCP - HTTP"
    - Short description of the purpose of the connection.

- Provide a step by step description and diagram of the sensitive data flow through the system components to identify those components that are critical to the system and could have the greatest impact if compromised.
- If web applications are part of the system, provide the following:
    - Identify all IT system components that are involved in the delivery of the web applications. Make sure to include all system components that monitor or effect the delivery, such as proxy or reverse-proxy servers, web application firewalls, load balancers, etc.
    - Provide details on the services used by each identified IT system component to deliver or effect the web application; at least provide name of the service and version, but any major additions, such as loadable modules, should also be listed. Examples: “IIS 8”, “Apache HTTP Server ‘httpd’ 2.4.23”.
    - List the languages used to provide interactive content and/or provide web application functionality. Additional data such as versions can be useful as well. Examples: “Java”, “HTML 5, CSS3, and javascript”, “Ruby”, “PHP”
    - List the URL of each page of the web application to be tested that a user of the web application could start an interaction with the application on, and any other URLs of note.
    - Schedule a full web application vulnerability scan with UISO before the end of the per-engagement phase.
- Provide a copy of any business and/or operational procedures that are to be tested, or may help to plan the testing.
- Provide a list of all IU staff that are in-scope for the testing. Include all information needed to perform allowed testing (email address, phone number, name or address of assigned computer, geographic location of office, etc). Indicate if they are in-scope for tests that may include social engineering. If such tests are allowed during the testing, indicate if they have been informed testing may include the capture and use of their IU username and passphrase, and that if captured they will be required to change their passphrase within a reasonable amount of time.
- List all data that must be considered "off limits" to the testing. This will mean that accessing this data will be avoided, and that this data will not be used as part of information gathering, vulnerability analysis, or to further exploitation. This list should be kept to a minimum, but must include all data that is restricted by contractual agreements or governmental law as not to be accessed by the UISO testers. Also, list any data that must not be included in the final report because the access restrictions to the data and the report will be different.
- List any system components that are not owned and maintained by IU and note them in the network diagram(s) so they are avoided.