Memo

To: Shelby Clair

From: Joseph Subrath

Date: February 8, 2025

Subject: Rules Of Engagement Summary

The rules of engagement section identify the operational guidelines of accepted practices in the selling and marketing of performing testing work, handling the results of testing engagements, and testing.

(A) Deception, uncertainty, and fear may not be used in the sales or marketing materials for the purpose of providing or selling security tests. *It is not permissible to offer free services for failure to penetrate target.* Public contests of hacking, trespass, and cracking to promote security assurance for the marketing or sales of security products or testing is not permissible. *It is only permissible to name present or past clients in the sales or marketing for potential customers if the job for the client is specifically the same as being sold or marketed and the client being named has given written permission to name them.* In regards to security measures and security, clients must be advised factually and truthfully, ignorance is not an excuse for not doing so.

(B) Explicit written permission from target owner or proper authority is required before performing security tests. Security testing of highly insecure infrastructure is not allowed until the proper security infrastructure is installed.

(C)Regardless of an NDA(Non-Disclosure Agreement) non-disclosure and confidentiality is required of the security analyst regarding customer information and test results. Contracts must clearly explain the dangers and limits of the security test, and generally limit liability to the cost of the job unless there is proven malicious activity. The client must give a signed statement which gives testing permission exempting the security analyst from trespass within the scope. Emergency contact names and numbers must be within the contract. *Clear permissions for tests involving denial of service*, social engineering, process testing, and survivability failures *must be in the contract.* Contracts must contain verified conflicts of intrest for a factual report and security test, and the process for future statement of work and contract changes.

(D)Contractually, the scope must be clearly defined before verifying vulnerable services. And according to the scope, the audit must explain clearly limits of any security tests.

(E)Techniques, procedures, plans, and processes outside the area of competence level of the analyst may not be contained within the test plan.

(F)Safety, welfare, health, and privacy must be maintained by the security analyst. The analyst must always operate within the law of where they are. Only key people are to be notified about testing. If needed for privileged testing, two separate access tokens must be provided by the client, being typical to the users whose privileges are being tested. Analysts must know details about their tools and have them tested within a restricted test area before using the tools on the client. *The conduct of tests explicitly meant to test* process or survivability or *denial of service can only be done with explicit permission and only to the scope where no damage is done outside the community or scope where the scope resides.* Tests including people can only be done to those identified in the scope. Verified limitations discovered during testing has to be reported to the customer with a practical solution as soon as they are identified. Over non-privately owned channels, flood testing of any sort where a scope is overwhelmed from a larger and stringer source is not allowed. The analyst can not leave the scope in a state of less actual security than it was provided with.

(G)The analyst, for all results, must respect and maintain the privacy of all individuals. Results involving non-security personnel can only be reported through statistical or non-identifying means. Regarding test results and audit reports an analyst is not directly involved in, they may not sign them. Reports must remain objective and truthful. Client notifications are required hen there are changes in the testing plan, source test venue, has low trust findings, or if any testing issues occur. Notifications also must be given before running dangerous, high traffic, or new tests. Regular progress updates must e given. Solutions in the report must be practical and valid. Unknowns and anomalies must be clearly marked in the report. Loss of controls and failed and successful security measures must be clearly stated in the report. Reports must include only factual quantatative security metrics when measuring security. To confirm receipt or delivery and to expect it’s arrival, the client must be notified when the report is being sent. Delivery channels for delivery of report must be end to end confidential. Reports and results can never be used for commercial gain beyond the interaction with the client.