Experiment 6

Report Writing: Statements of Work, Rules of Engagement, Non-Disclosure Agreements

In penetration testing and cybersecurity projects, documents like Statements of Work (SOW), Rules of Engagement (ROE), and Non-Disclosure Agreements (NDA) are crucial for defining the scope, legal conditions, and confidentiality of the project. These documents make sure all involved parties are aware of the processes, risks, and legal requirements before, during, and after the engagement.

Statements of Work (SOW)

The SOW outlines the scope, objectives, and deliverables for the cybersecurity assessment. This document ensures that both the client and the security provider agree on the goals and outcomes. In penetration testing, the SOW details key components such as:

Scope of Work:

Defines the systems, applications, and networks that will be tested, like external IP addresses, internal networks, web apps, and databases. For instance, a file-sharing web application may be included in the scope, while production servers are excluded.

Testing Phases:

Outlines the stages of the engagement, including reconnaissance, scanning, vulnerability identification, exploitation, and reporting. The tools used, such as OSINT for reconnaissance or Metasploit for exploitation, should be specified.

Deliverables:

Details what the security provider will deliver at the end, such as vulnerability reports, exploitation success rates, or a risk assessment summary.

Timelines:

Specifies the timeframe for each phase, like scheduling scanning for a week and exploitation over a weekend to reduce disruptions.

Security Controls:

Defines how data collected during testing, such as credentials or network setups, will be securely managed and stored.

The SOW is essential throughout the cyber kill chain, ensuring each phase—Reconnaissance, Scanning, Exploitation, and Post-Exploitation—is pre-approved, minimizing legal risks and establishing a clear workflow for both client and security teams.

Rules of Engagement (ROE)

The ROE establishes the legal, technical, and operational boundaries for penetration testers. These rules ensure that the engagement is safe and lawful by defining the scope and permitted actions.

Legal Boundaries:

Specifies that the client authorizes actions like OSINT, port scanning, or password brute-forcing, providing legal protection to avoid violations such as those under the Computer Fraud and Abuse Act (CFAA).

Permitted Targets:

Lists systems, applications, or networks within scope. For example, external email servers may be included, while financial servers are not, preventing disruption of critical systems.

Allowed Attack Techniques:

Indicates approved techniques, such as exploiting known vulnerabilities with Metasploit, while prohibiting damaging actions like DoS attacks that might crash systems.

Timing:

Specifies time windows for activities, such as conducting tests during off-peak hours to minimize disruption.

Example: Reconnaissance may occur during business hours, while active exploitation is restricted to after-hours.

Fail-safe Procedures:

Includes steps for emergencies like unintended outages or critical vulnerabilities, such as immediate client notification or halting the test.

During Reconnaissance and Scanning, the ROE ensures testers operate within legal limits, performing tasks like OSINT or subdomain scanning on authorized domains. In the Exploitation phase, it restricts testers from using harmful techniques that could impact operations.

Non-Disclosure Agreements (NDA)

The NDA is a legal agreement ensuring the confidentiality of sensitive information gathered during the security assessment. It protects the client’s proprietary data, network configurations, and vulnerabilities found.

Confidentiality Clause:

Defines what information is confidential, such as credentials from password spraying, scan results, or data from breached accounts. The NDA prevents sharing sensitive data with third parties without approval.

Time Frame:

Specifies the duration of the NDA, such as during the engagement and a set period after completion.

Breach of Agreement:

Outlines consequences for breaking confidentiality terms, which could include financial penalties or legal action if unauthorized parties gain access to findings.

Importance of NDA in Cyber Kill Chain:

The NDA is vital during the Reconnaissance and Exploitation stages, ensuring sensitive data like breached credentials or Active Directory flaws are kept secure and not misused. It also helps protect the client’s reputation by keeping security issues private.