Ethical Hacking

Overview

Ethical Hacking enables clients to quickly identify, assess and remedy security holes. Devices attached to the network are evaluated to detect technical vulnerabilities. Ethical Hacking is accomplished by performing scheduled and selective probes of the network's communication services, operating systems, key applications, and network equipment in search of those vulnerabilities. Our specialists analyze the vulnerability conditions and provide a detailed report including corrective actions.

Benefits

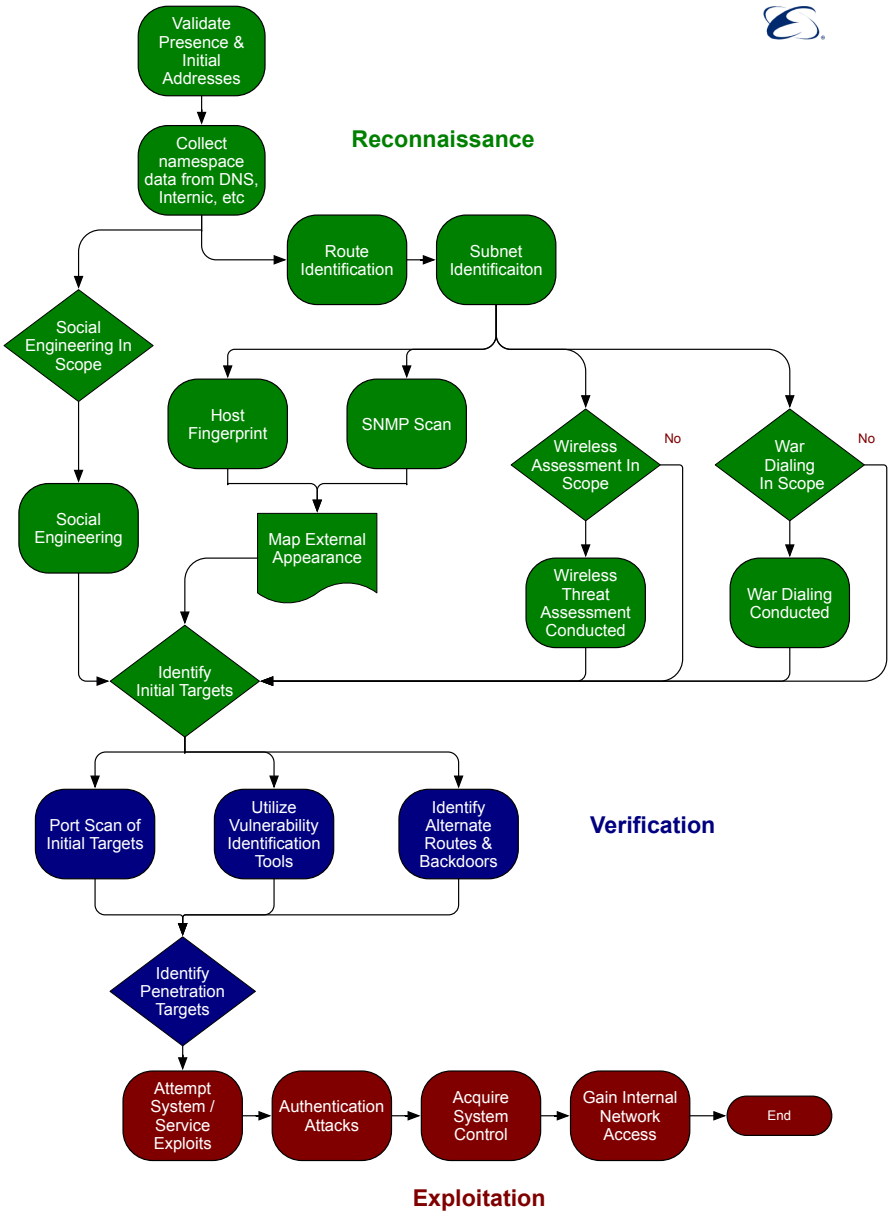
Ethical Hacking is a battle simulation to determine what vulnerabilities have not been addressed in your network. By locating vulnerabilities before the bad guys do, Ethical Hacking will increase the level of confidence of the company's security measures. In particular, Ethical Hacking:

- Provides a "battle-test" for your network, systems, and applications
- Provides a more "realistic" test than a paper-based assessment
- Provides a proactive approach to mitigating risk
- Enhances the quality assurance process
- Demonstrates the need for and effectiveness of security

Description of Service

Network Penetration Test

There are three phases to a Network Penetration Test:



Phase1) Reconnaissance:
The initial phase of any security review involves extensive data collection and penetration studies are no exception. The following methods may be used as part of this information-gathering phase:

- Web searches and newsgroup browsing
- DNS zone transfers, internic queries
- IP scanning and SNMP sweeps
- Network mapping with traceroute and other tools
- Social Engineering (if allowed)
- Initial target identification

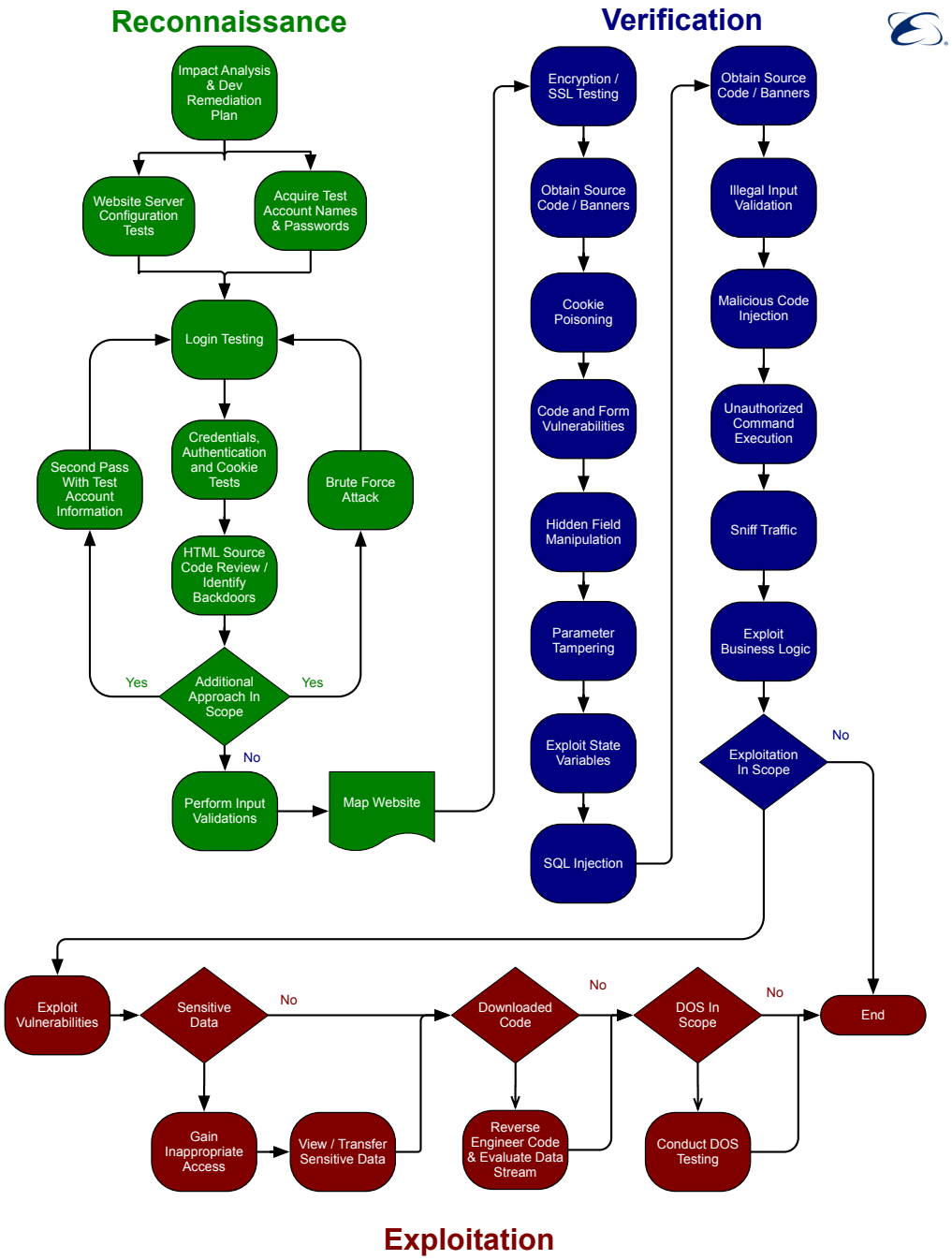
Phase 2) Verification:
Once the verification phase is begun, targets are more likely to be alerted to suspicious activity. This phase serves to identify potential or known vulnerabilities that could be exploited by intruders. This is the main analysis phase that correlates the information gathered in the first two stages. Methods of performing this phase can include:

- Vulnerability scanning
- Port scanning

Phase 3) Exploitation:
The exploitation phase is typically only used when a client needs to demonstrate actual data or system compromises. This phase involves actually utilizing identified vulnerabilities to gain access to internal systems and networks. This phase typically utilizes many tools that may be available in the public domain and are used by actual intruders. This methods used during this phase are tightly controlled by the penetration agreement and activities are extensively logged.

Web Application Penetration Test

Similarly, there are three phases to a Web Application Penetration Test:



Phase1) Reconnaissance:
The Web Application Ethical Hack begins with Passive Website Mapping that can be designed to evade detection. During this phase the application's security controls are tested to determine if an attack may result in inappropriately viewing, altering, copying or deleting information. During passive website mapping, testing is performed mimicking two types of users:

- Unauthorized User attempting to gain access
- Authorized User trying to acquire and utilize enhanced or inappropriate privileges

Phase 2) Verification:
The assessment then moves into verification where the majority of website manipulation takes place. Through an automated and manual process, websites are reviewed for many security risks. The risk review begins by first performing system identification. Once determined the operating system, web server versions and other associated systems have been determined, we are able to quickly evaluate well-known system vulnerabilities. Our process examines for security risk such as:

- Encryption / SSL Testing
- HTML Code & Form Vulnerabilities
- Hidden Field Manipulation
- Parameter Tampering
- Cookie Poisoning
- Executable code testing such as buffer overflows and IIS weaknesses

Phase 3) Exploitation:
Finally, the assessment escalates to exploitation where attempts are made to fully compromise the web infrastructures. Within the realm of aggressive penetrations, we perform services based on the type of website:

- The basic service attempts to exploit the implemented security controls or lack of controls
- For web financial applications, attempts are made to gain inappropriate access and transfer financial data between test accounts and/or perform other transactions without providing appropriate target authentication
- For web application that use downloadable code, attempts are made to identify vulnerabilities associated with the installation and operation of the executable