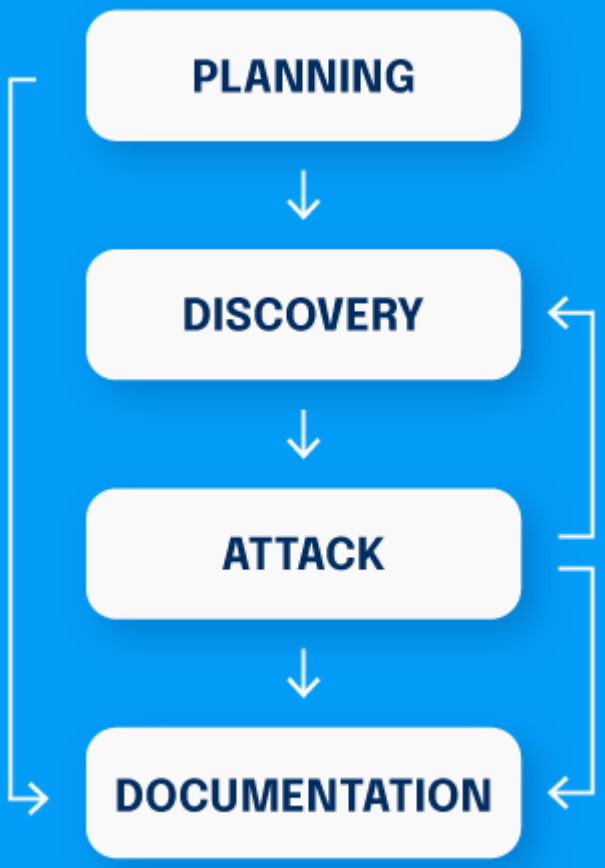
360ADVANCED

360 ADVANCED PENETRATION TESTING SERVICES

INFO@360ADVANCED.COM | 360ADVANCED.COM | (866) 418-1708

Table of Contents

At a high level, 360 Advanced leverages a **four-phase** approach to penetration testing services. This includes Planning, Discovery, Attack, and Documentation. **Clients can also opt for an additional phase** which includes remediations and re-testing.



Penetration Testing Overview

360 Advanced bases their penetration test methodology on the NIST SP 800-115 Technical guide to information security and assessments.

Depending on the components involved in testing, supplemental definitions, strategies, and techniques are based on the Pen Test Execution Standard, OWASP Testing Guide (v4.2), OWASP API Security Top 10, OWASP MASVS, and OWASP MASTG.

Penetration Testing services offered by 360 Advanced include:

- Vulnerability Scanning
- External Network Penetration Testing
- Internal Network Penetration Testing
- Unauthenticated Web Application Testing
- Authenticated Web Application Testing
- Unauthenticated API Testing
- Authenticated API Testing
- Unauthenticated Mobile Application Testing
- Authenticated Mobile Application Testing
- Social Engineering
- Physical On-Site Testing

1. Planning

Defining the rules of engagement and overall project goals.

Upon agreement of contractual items, the 360 Advanced team will reach out to the client and schedule a planning call to identify the testing dates, gather detailed scope information, and validate and restrictions that the penetration testing team must abide by. This information will be captured within our Rules of Engagement (RoE) document and sent to the client for approval and signature. This document will serve as the waiver authorizing the penetration testing team to complete the testing during the specified timeframe under the constraints contained within the RoE.

2. Discovery

Gather system information and identify potential vulnerabilities
Prioritize vulnerabilities for exploitability

The penetration team will begin the discovery phase of testing on the start date (within any time constraints defined) agreed upon within the RoE. An email will be delivered to the client indicating that testing is about to commence and will contain any relevant contact information of the involved 360 Advanced Point of Contacts (POCs) as well as the source of the testing (i.e. source IP).

This phase will leverage automated tools and vulnerability scanners to identify low-hanging and well-known targets of opportunity. Automated scanning is intended to have a low impact on client assets and infrastructure. Our goal during the entire penetration test is to keep our clients' systems operational. This phase is designed to give the testers a snapshot of the intended target scope and a baseline of potential exploitable vulnerabilities to be prioritized for use in the next phase.

3. Attack

Validate potential vulnerabilities and repeat discovery phase for any newly gained access

During the attack phase, 360 Advanced will look to manually leverage any vulnerabilities identified during the discovery phase to attempt to exploit targets in scope. This also aids to identify any potential false positives that the automated scanner identified and enables 360 Advanced to eliminate these items before final reporting.

During this phase, the penetration testers may also leverage additional in-house scripts or manual assessment techniques to identify vulnerabilities that may not have been alerted by automated tools such as brute force or default credential issues. As new information is discovered, the attack phase will cycle continuously with the previous phase to move through exploited vulnerabilities or identify new ones.

Within this phase of testing, if at any point a vulnerability is determined to be “critical” (i.e., exploitation is very likely and the impact of exploitation could cause major issues to the company or systems in scope), testing will be paused and immediately reported to the client. It will be upon the client to determine if the penetration testing team is allowed to continue testing, halt testing, or continue to other areas of scope, that does not impact the affected asset while remediations are performed.

4. Documentation

Capture successful attacks in a formal report.

As each vulnerability is confirmed and is determined to exist via exploitation or other means of validation, the penetration team will capture details. This includes information about the vulnerability that is pertinent to assigning severity, proof of concept, and recommendations for proper remediations. Each finding will be documented to include: Finding Title, Severity, Tools, Affected Systems, Description, Risk (Likelihood and Impact), Additional Guidance, Evidence, and References.

Severity rankings for documentation are based upon the likelihood and impact of exploitation.

Likelihood is determined based on how easily the vulnerability is identified, accessed, and exploited. Mitigating controls such as whitelisted access, required authentication, multi-factor authentication (MFA), or patching can help to reduce the likelihood.

Impact is determined by what is perceived during the testing. Each environment is different, and exploitation does not always imply a high impact to the target system of underlying infrastructure. As an example, a host could be exploited but is found to be isolated from talking to any other hosts and does not have any relevant data to be gathered once system level access has been achieved. This device would not have as high of an impact as a domain connected device with administrative users and data.

Upon testing completion, a condensed PDF version of the findings and their details will be provided to the client for review, so that remediation efforts may begin if desired. During this time, the full technical report and executive summary report will go through a quality control (QC) process to be approved for final release.

Remediations and Re-Testing

Capture successful attacks in a formal report.

Remediations and re-testing are included in our Penetration Testing procedures. 360 Advanced remains available for questions if needed and allows the CLIENT up to 90 days to complete remediation efforts against the reported vulnerabilities. The baseline is 30 days and can be extended based on CLIENT needs, resource availability or remediation difficulty.

At the conclusion of the remediation period, 360 Advanced will complete re-testing of the items identified remediations. Each validated remediation effort will be documented in the final report as a status update to the associated finding. No findings are removed from the report, but an update will be made to the report to show the current status after remediation. Details will be provided for each led remediation or mitigation efforts. This ensures proper documentation of reported vulnerabilities (360 Advanced level of effort) and remediated vulnerabilities (CLIENT level of effort).

Penetration Testing Services Overview

Penetration Testing is a point-in-time service. Meaning, the testing itself is restrained by the testing window agreed upon via the Rules of Engagement (RoE). It is a common misconception that a penetration test will be a full-proof identification of anything and everything wrong with the components being tested. This is not feasible in a confined window of testing. Rather, it is the priority of the penetration testing team to provide highly actionable items to the CLIENT. Testing is focused on prioritizing the identification of vulnerabilities that could be the most harmful and based on the highest likelihood of impact to ensure that these items are targeted for remediation by the CLIENT.

Vulnerability Scanning

Vulnerability scanning is the entry point to a pentest. This includes automated scanning of the target scope via Nessus Professional. No manual intrusion attempts, or validation of exploitable vulnerabilities are performed. Vulnerabilities identified by the automated scanner will be presented in XLSX report format. A formal PDF report can be created to outline vulnerabilities identified if client facing reporting is required.

External Network Penetration Testing

External testing is conducted from the open web. No internal systems or access to them is required. The 360 Advanced Penetration Testing Team will conduct both automated and manual identification of vulnerabilities as well as eliminating as many false positives as possible prior to reporting. One of the goals of an external test is to achieve access through the external posture to the internal network. However, our main concern is identifying as many vulnerabilities as possible from a level of Critical to Low and aiding our clients in remediating and hardening the external facing network posture.

External testing will follow the 360 Advanced four phase methodology (Planning, Discovery, Attack, Documentation). Testing will target the network level to identify issues within exposed ports and services and the overall external security configuration. As a part of those exposed services, if any user interfaces are discovered, these will be leveraged for potential vulnerabilities and assessed for routes to compromise as well. Anything exposed to the public internet and defined as in scope, is a potential target vector for an attacker.

Internal Network Penetration Testing

Internal testing is completed on the private network space. It is conducted to emulate an on-network attacker or insider threat.

Testing can be completed in one of three ways:

VPN ACCESS

Testing of the internal network via VPN only limits the ability to properly assess the network for layer 2 vulnerabilities.

VPN TO PHYSICAL OR VM

The CLIENT will stand up a physical or virtual appliance with Kali Linux installed and provide the penetration testing team access via secure VPN.

360 ADVANCED SUPPLIED DEVICE

360 Advanced can ship out an Internal Testing Device (ITD) that is then attached to the CLIENT network for testing.

Once granted access to the internal network, the penetration testing team will work to enumerate the target scope and associated vulnerabilities. Aside from well-known vulnerabilities that may be returned by automated scanners, the penetration testing team will manually go through the internal network to discover additional means of compromise. These can include default credentials, unauthenticated services, misconfigured services, or weaknesses within device configurations.

If access is achieved to any service or device (foothold), the penetration testing team will work to identify routes to sustained access, enumerate the device for sensitive information that could aid in additional access or exploitation, elevation of privileges, and pivoting within the network. Each portion of testing will be documented with proper screenshots and evidence to show how the penetration testers were able to exploit, gather data, or pivot through the network. If domain administration level access is achieved, the penetration testing team will document the attack chain and then revert testing to identify additional routes that may exist to sustained or elevated access. The overall goal is to identify as many high-level vulnerabilities as possible in the time allotted by the RoE.

Unauthenticated Web Application Testing

Unauthenticated web application testing is performed without the use of credentials supplied by the CLIENT. Testing follows the same four phase approach of Planning, Discovery, Attack, and Documentation. Overall guidance for the testing is supplemented from the OWASP TOP 10; however, 360 Advanced does not conduct this in a "check-the-box" manner. Every application is different and relies on the expertise of the penetration testers to root out potential attack vectors, some of which may come from insecure coding or user error.

Unauthenticated testing is completed from outside of the application. It is up to the client whether mitigating controls such as Web Application Firewalls (WAFs) or whitelisting are to be removed to allow the tester to complete the engagement. Initial testing will begin with the application being scanned with Burp Suite Pro for well-known or common vulnerabilities. This initial scan will be used by the penetration tester as an initial indicator of possible issues within the application. Automated application scanners are highly prone to false positives and must be evaluated manually to determine the true validity of any findings.

All endpoints identified during the reconnaissance leveraged by the application, that fall within the defined scope (i.e. the scoped domain), will be assessed for vulnerabilities. This can include API endpoints that the application relies on for functionality.

During manual testing the Penetration Testing Team will look to evaluate the application for the following issues:

- Authentication Bypass, Brute Force, or Enumeration
- Cross-site Scripting Vulnerabilities (XSS)
- Default or Weak Passwords
- Encryption Issues
- Front End Code Issues or Information Disclosures
- Injection Vulnerabilities
- Indirect Object References
- Local or Remote File Inclusion Vulnerabilities
- Misconfigured or Missing Security Headers
- Out of Date or Vulnerable Software
- Security Misconfigurations
- Sensitive Data Exposure
- Web Application Firewall Bypass
- Web Directory Bypass

Authenticated Web Application Testing

Authenticated web application testing is performed with credentials provided by the CLIENT to simulate compromised accounts and/or insider threats. **All authenticated testing engagements start as unauthenticated to first evaluate the external facing portions of the application.** Testing follows the same four phase approach of Planning, Discovery, Attack, and Documentation. Overall guidance for the testing is supplemented from the OWASP TOP 10; however, 360 Advanced does not conduct this in a "check-the-box" manner. Every application is different and relies on the expertise of the penetration testers to root out potential attack vectors, some of which may come from insecure coding or user error.

This component of testing relies on credentials to evaluate the portions of the application that are protected via the authentication mechanism. 360 Advanced generally asks for at least two sets of credentials to be provided for testing. This ensures that checks can be completed for potential cross-data access, escalation, and cross-tenant access if applicable. If it is determined that multiple scenarios exist such as different privilege levels and a multi-tenanted environment, more accounts may be requested to ensure all account related vulnerabilities can be evaluated. Initial testing will begin with the application being scanned/crawled with Burp Suite Pro for well-known or common vulnerabilities. This initial scan will be used by the penetration tester as an initial indicator of possible issues within the application. Automated application scanners are highly prone to False Positives and must be evaluated manually to determine the true validity of any findings.

All endpoints identified during the reconnaissance leveraged by the application, that fall within the defined scope (i.e. the scoped domain), will be assessed for vulnerabilities. This can include API endpoints that the application relies on for functionality.

During manual testing the Penetration Testing Team will look to evaluate the application for the following issues:

- Account Takeover
- Authentication Bypass, Brute Force, or Enumeration
- Cross-data Access Between Accounts
- Cross-site Scripting Vulnerabilities (XSS)
- Cross-tenant Access
- Default or Weak Passwords
- Encryption Issues
- Front End Code Issues or Information Disclosures
- Injection Vulnerabilities
- Indirect Object References
- Input Validation
- Local or Remote File Inclusion Vulnerabilities
- Malicious or Unrestricted File Upload
- Misconfigured or Missing Security Headers
- Out of Date or Vulnerable Software
- Privilege Escalation
- RBAC Misconfigurations
- Security Misconfigurations
- Sensitive Data Exposure
- Web Application Firewall Bypass
- Web Directory Bypass

Unauthenticated API Testing

Unauthenticated API testing is performed without the use of credentials supplied by the CLIENT. Testing follows the same four phase approach of Planning, Discovery, Attack, and Documentation. Overall guidance for the testing is supplemented from the OWASP TOP 10 API Security Risks; however, 360 Advanced does not conduct this in a "check-the-box" manner. Every API is different and relies on the expertise of the penetration testers to root out potential attack vectors, some of which may come from insecure coding or user error.

Testing of API endpoints, unauthenticated, the client will need to provide a list of endpoints in scope. If public API documentation is available, the Penetration Testing Team may leverage this to get open-source information about the API to aid in testing as it would also be available to any would-be attacker.

Initial reconnaissance of API endpoints will be completed, leveraging tools such as POSTMAN and Burp Suite Pro.

During manual testing the Penetration Testing Team will look to evaluate the application for the following issues:

- Authentication Bypass, Brute Force, or Enumeration
- Broken Object Authorization
- Encryption Issues
- Excessive or Unintended Data Exposure
- Improper Authorization Validation
- Improper Inventory Management
- Injection Vulnerabilities
- Misconfigured or Missing Security Headers
- Security Misconfigurations
- Unrestricted Access to Business Flows
- Unrestricted Resource Consumption

Authenticated API Testing

Authenticated API testing is performed with the use of credentials, keys, or tokens supplied by the CLIENT to simulate compromised accounts and/or insider threats. All authenticated testing engagements start as unauthenticated to first evaluate the external facing portions of the API. Testing follows the same four phase approach of Planning, Discovery, Attack, and Documentation. Overall guidance for the testing is supplemented from the OWASP TOP 10 API Security Risks; however, 360 Advanced does not conduct this in a "check-the-box" manner. Every API is different and relies on the expertise of the penetration testers to root out potential attack vectors, some of which may come from insecure coding or user error.

Testing of API endpoints from an authenticated perspective requires that the client provide API documentation to ensure the pentest team understands all parameters and/or specialized headers required to be successful. POSTMAN or SWAGGER documentation also allows for easier ingestion of testing details into tools. Manually having to input each method and parameter for APIs requires a considerable amount of time and may result in extended hours for testers to complete.

Initial reconnaissance of API endpoints will be completed leveraging tools such as POSTMAN and Burp Suite Pro.

During manual testing the Penetration Testing Team will look to evaluate the application for the following issues:

- Account Takeover
- Authentication Bypass, Brute Force, or Enumeration
- Broken Object Authorization
- Cross-data Access Between Accounts
- Cross-tenant Access
- Default or Weak Passwords
- Encryption Issues
- Excessive or Unintended Data Exposure
- Improper Authorization Validation
- Improper Inventory Management
- Injection Vulnerabilities
- Input Validation
- Malicious or Unrestricted File Upload
- Misconfigured or Missing Security Headers
- Privilege Escalation
- RBAC Misconfigurations
- Security Misconfigurations
- Unrestricted Access to Business Flows
- Unrestricted Resource Consumption
- Web Application Firewall Bypass

Unauthenticated Mobile Application Testing

Unauthenticated Mobile Application testing is performed without the use of credentials supplied by the CLIENT. Testing follows the same four phase approach of Planning, Discovery, Attack, and Documentation. Overall guidance for the testing is supplemented from the OWASP MASVS and OWASP MASTG; however, 360 Advanced does not conduct this in a "check-the-box" manner. Every mobile application is different and relies on the expertise of the penetration testers to root out potential attack vectors, some of which may come from insecure coding or user error.

Mobile application testing from an unauthenticated perspective is focused on the front-end compiled version of the application. This can come from the penetration testers retrieving the application from their relative stores or the CLIENT providing 360 Advanced with the files such as APK and IPA.

Initial reconnaissance and decompiling of mobile applications will be completed leveraging tools such as mobile devices, emulators, MobSF, APKTool, Objection, and Frida.

During manual testing the Penetration Testing Team will look to evaluate the application for the following issues:

- Authentication Bypass, Brute Force, or Enumeration
- Authentication Mechanism Implementation
- Exposed Libraries
- Identity Pinning
- Improper Data of Log Storage
- Improper Key Management
- Insecure Cryptography
- Network Traffic Security Controls
- Resiliency Testing
- Sensitive Data Exposure
- Privacy Controls
- Versioning and Update Requirements
- Vulnerable Software or Dependencies
- WebView Configuration and Implementation

Authenticated Mobile Application Testing

Authenticated Mobile Application testing is performed with the use of credentials supplied by the CLIENT. Testing follows the same four phase approach of Planning, Discovery, Attack, and Documentation. **All authenticated testing engagements start as unauthenticated to first evaluate the external facing portions of the mobile application.** Overall guidance for the testing is supplemented from the OWASP MASVS and OWASP MASTG; however, 360 Advanced does not conduct this in a "check-the-box" manner. Every mobile application is different and relies on the expertise of the penetration testers to root out potential attack vectors, some of which may come from insecure coding or user error.

Authenticated Mobile application testing is focused on the front-end compiled version of the application and the portions of the application accessible once authenticated. This typically includes API or WebView testing. Access to the application itself can be achieved by retrieving it from the relative store or the CLIENT providing 360 Advanced with the files such as APK and IPA.

Initial reconnaissance and decompiling of mobile applications will be completed leveraging tools such as mobile devices, emulators, MobSF, APKTool, Objection, and Frida. Once authenticated, the underlying API associated to the application will be scraped for endpoints and analyzed for vulnerabilities as well *(see section for Authenticated API Testing for more details)*.

During manual testing the Penetration Testing Team will look to evaluate the application for the following issues:

- Account Takeover
- Authentication Bypass, Brute Force, or Enumeration
- Broken Object Authorization
- Cross-data Access Between Accounts
- Cross-tenant Access
- Default or Weak Passwords
- Encryption Issues
- Excessive or Unintended Data Exposure
- Improper Authorization Validation
- Improper Inventory Management
- Injection Vulnerabilities
- Input Validation
- Malicious or Unrestricted File Upload
- Misconfigured or Missing Security Headers
- Privilege Escalation
- RBAC Misconfigurations
- Security Misconfigurations
- Unrestricted Access to Business Flows
- Unrestricted Resource Consumption
- Web Application Firewall Bypass
- Authentication Mechanism Implementation
- Exposed Libraries
- Identity Pinning
- Improper Data of Log Storage
- Improper Key Management
- Insecure Cryptography
- Network Traffic Security Controls
- Resiliency Testing
- Sensitive Data Exposure
- Privacy Controls
- Versioning and Update Requirements
- Vulnerable Software or Dependencies
- WebView Configuration and Implementation

Social Engineering

Social engineering focuses on the human aspect of a network. Your employees are a common vulnerability for any business and often are the weakest point in a network. Testing is intended to check for user's clicking unknown links, divulging company information, giving up credentials, or otherwise giving the penetration testing team information or access that can be leveraged to harm the company or aid in future attacks.

This type of testing is targeted at users, not the surrounding infrastructure and controls in place. It is common that whitelisting and other access allowances will be required to complete testing to ensure the end users are appropriately tested. 360 Advanced leverages tools suites such as GoPhish to help in these activities.

Each social engineering engagement is intended to be interactive with the client POCs where possible to determine the best approach to surface users that may need additional training. This can be accomplished by targeting specific users or determining the types of threats that are most likely to trick the end user or have been problems in the past. The 360 Advanced penetration testing team will work to identify and plan social engineering events that are non-generic to provide the best results.

Social Engineering can be done in a variety of ways to include:

PHISHING

Emails campaigns intended to get users to divulge information, interact with malicious attachments or links, or provide sensitive information such as credentials when provided with landing pages or redirects.

VISHING

Phone calls placed throughout the test to try and gain company information, get users to divulge passwords, or instigate interactions that would cause the user to interact with accompanying emails that may ask them to click links or install software.

SMISHING

SMS text messages intended to get users to divulge information, interact with malicious attachments or links, or provide sensitive information such as credentials when provided with landing pages or redirects.

Physical (On-Site)

On-site testing can be a great way to check your overall physical security posture. The Penetration Testing Team will work to gain access to restricted spaces, after hours entry by means of unlocked doors, left open windows, etc., access to unattended devices, access to devices via a quick plug-in of a removable device, and other means of gaining information or access to pertinent company data.

On-site testing requires adequate planning and lead time. Planning will include determining the location of the on-site testing, when it will occur, any restrictions, and how many days the penetration tester will have to complete the engagement.

Blackbox, Greybox, and Whitebox Testing

Blackbox Testing

Blackbox testing simulates a real-world scenario where the testing team is not given any information about the targets in scope. The purpose is to simulate an attacker that has stumbled on to the client environment or actively set the client to be targeted with no other information than who the target is. For the purposes of legality and liability within ethical hacking, it is generally sought that the scope is defined prior to testing, only to include targets that are owned by the client that the penetration team is legally allowed to preform attacks against. If the scope is not to be given, the Penetration Testers will have to deconflict potential targets with the client after the reconnaissance phase, prior to moving any further with enumeration and attacks. No credentials or information about the environment are to be given for testing purposes. Penetration testers must work to gather the footprint of the environment, enumerate for open ports, and identify what services are available for potential attacks. This type of testing is the most commonly seen and requested.

Greybox Testing

Greybox testing allows for a little bit more information to be provided to the testing team to ensure that appropriate targets are properly assessed. This also helps reduce the time taken during reconnaissance for the penetration testing team. This type of testing will often include the use of credentials or extended access (authenticated web application testing / internal network testing). The purpose of greybox testing is not to fully allow the tester all the way in but to place them in areas that will allow for deeper testing of the components in scope that a normal attacker may not have immediate access to without credential compromise or a foothold. This style of testing helps to give the client a more in depth look at their tested scope while also creating some efficiencies for the testers.

Whitebox Testing

Whitebox testing is aimed at giving the penetration testers as much information about and access to the target environment as possible. This can include the full scope, versioning, software in use, usage documentation, network diagrams, and credentials to name a few. The aim is to ensure that the pentester has enough knowledge about the tested resource that they can dive fully into looking for issues and exploitable vulnerabilities while leveraging as many attack vectors as possible in the time given.

Let’s chat to see if we’re the right fit.

(866) 418-1708 | INFO@360ADVANCED.COM

360ADVANCED

200 Central Avenue, Suite 2105,
St. Petersburg, FL 33701