Digital
Boundary Group

EXTERNAL PENETRATION TESTING

An External Penetration Test provides independent verification of the security status of an organization's Internet presence by examining external IT systems for any weakness that could be used by an attacker to disrupt the confidentiality, availability, or integrity of the network.

HIGHLIGHTS

- Discovery of publicly available details about the organization to aid in the exploitation phase
- Exploitation of vulnerabilities (with customer's permission) to validate findings and provide an assessment of the potential threat each vulnerability may pose
- Optional electronic social engineering engagement to determine the extent to which internal users may represent an exploitable risk

INCLUSIONS

1. Public Information Disclosure
2. DNS, SMTP, and Domain Registration
3. Intrusion Prevention
4. Firewall
5. Password Strength and Authentication
6. Host Security
7. Transport Layer Security

REPORTING

The final report includes a summary of findings, prioritized recommendations, and detailed observations, implications, and recommendations for each discovered vulnerability.

COST

Based on the number of live, external-facing IPs.

Digital
Boundary Group

WEB APPLICATION PENETRATION TEST

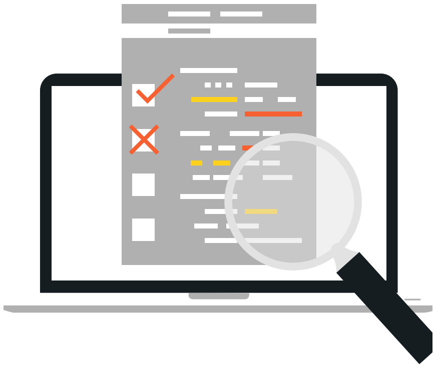
A **Web Application Penetration Test** provides independent verification of the security status of a web application and its supporting infrastructure. This test includes techniques that attempt to identify security weaknesses and logic flaws that could allow an attacker to cause harm or gain unauthorized access to the application or privileged information.

HIGHLIGHTS

- Assess application vulnerabilities, including OWASP Top 10
- Identify sensitive data exposure, workflow bypasses, and application deployment deficiencies
- Testing includes vulnerability assessment and exploitation

INCLUSIONS

1. Application Security
2. Firewall
3. Password Strength, Authentication, and Session Management
4. Host Security
5. Transport Layer Security



Controlled attacks are performed against each reported vulnerability, excluding those likely to cause denial of service.

REPORTING

The final report includes a summary of findings, prioritized recommendations, and detailed observations, implications, and recommendations for each discovered vulnerability.

COST

Based on factors including mobile operating system, number of server IP addresses, application frameworks in use, and the complexity of the application workflows. Completion of a brief scoping questionnaire may be required.

Digital
Boundary Group

MOBILE APPLICATION PENETRATION TESTING

A Mobile Application Penetration Test provides independent verification of the security status of a mobile application, its supporting infrastructure, and, optionally, the host device itself. This test includes techniques that attempt to identify security weaknesses and logic flaws that could allow an attacker to cause harm or gain unauthorized access to the application or to privileged information.

Because mobile applications operate on devices that are more likely to be stolen or connected to untrusted Wi-Fi access points, they are subject to unique additional risks as compared to traditional web applications.

HIGHLIGHTS

- Identify risks that affect mobile applications hosted on Android, iOS, and/or hybrid browser-based platforms
- Assess application vulnerabilities, including OWASP Top 10 and Mobile Top 10
- Identify sensitive data exposure, workflow bypasses, and application deployment deficiencies
- Monitor application communication to evaluate cloud- and company-hosted web service endpoints
- Testing includes vulnerability assessment and exploitation

INCLUSIONS

1. Android/ iOS Security
2. Application Security
3. Firewall
4. Password Strength, Authentication, and Session Management
5. Host Security
6. Transport Layer Security
7. Mobile Operating System Security (if device provided)

Controlled attacks will be performed against each reported vulnerability, excluding those that are likely to cause a denial of service condition.

REPORTING

The final report includes a summary of findings, prioritized recommendations, and detailed observations, implications, and recommendations for each discovered vulnerability.

COST

Based on factors including mobile operating system, number of server IP addresses, application frameworks in use, and the complexity of the application workflows. An APK/IPA file or app store link, and completion of a brief scoping questionnaire may be required.

PHISHING CAMPAIGN

Digital Boundary Group

Phishing is a form of *social engineering* that leverages emails to solicit information. The attacks are typically framed as a message from a reputable organization that the target is familiar with, such as a credit card company, mailing service, or online shopping site. To gain access to private information, the attacker formulates a convincing message to persuade a target to provide sensitive account information or credentials.

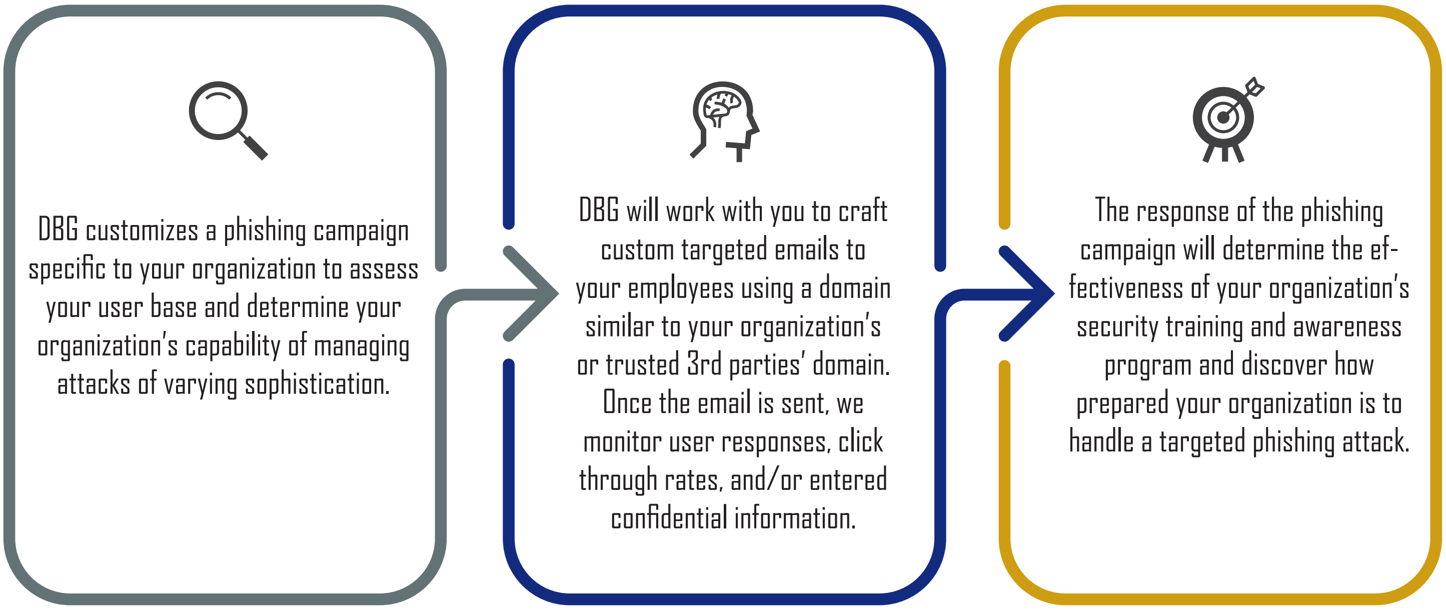
COMMON PHISHING EMAILS

Fake communications from online payment and auction services	These emails claim there is a “problem” with your account and request that you access a (usually malicious) web page to provide personal and/or account information.
Fake communications from an IT Department or Support Department	These emails will attempt to steal passwords and other information that phishers can use to penetrate your organization’s networks and computers.
Bogus business opportunities	These scams promise the opportunity to make a great deal of money with very little effort.
Health and diet scams	Prey on the insecurities some people have about the state of their well being.
Discount software offers	These scams frequently consist of advertisements for cheap versions of commercial software which can contain malware such as Trojan horses.

When the target responds with the requested information, attackers can use it to gain access to the accounts with the information provided by the victim.

THE DBG APPROACH

DBG takes social engineering to the next level.



DBG customizes a phishing campaign specific to your organization to assess your user base and determine your organization's capability of managing attacks of varying sophistication.

DBG will work with you to craft custom targeted emails to your employees using a domain similar to your organization's or trusted 3rd parties' domain. Once the email is sent, we monitor user responses, click through rates, and/or entered confidential information.

The response of the phishing campaign will determine the effectiveness of your organization's security training and awareness program and discover how prepared your organization is to handle a targeted phishing attack.

DBG's testing of your organization's resistance to human-based attacks provides you with deliverables that contain phishing metrics and recommendations on how to improve your security program. Our goal is to facilitate a clear understanding of your organization's security awareness and suggest areas for improvement.

Contact us to discuss your organizations security testing requirements.

sales@digitalboundary.net

Digital
Boundary Group

1-800-747-3557 | www.digitalboundary.net