## INFRASTRUCTURE SECURITY ASSESSMENTS

- External and Internal Networks
- Servers, Network Devices, DNS, Services, Other devices

## APPLICATION SECURITY ASSESSMENTS

- Web Application Security Assessment
- Mobile Application Security Assessment
- Secure Code Review (SAST)
- Grey Box and Black Box Assessments

## OTHER ADVANCED SECURITY ASSESSMENTS & SERVICES

- PCI DSS, NIST, HIPAA Compliance
- Cloud security assessment
  – Azure/AWS/Oracle
- Security baselining & controls validation

## SCOPE AND RULES OF ENGAGEMENT

- Documents customer's requirements, scope and any assumptions

## EXECUTIVE SUMMARY

- Executive-level briefing including the objectives and findings.
- Risk summary to identify both level of risk as well as level of effort required to remediate.

## RISK FINDINGS AND REMEDIATION GUIDANCE

- DREAD Scoring, CVSS scoring, OWASP TOP 10 mapping
- Summary of Findings/ Vulnerabilities, Proofs of Concept, Detailed Recommendations.

## SECURITY POSTURE ANALYSIS

- Summarized recommendations
- Concise view into positive and negative findings

## RISK SCORING: DREAD THREAT MODEL

- Uses the DREAD threat model to calculate the Risk scores
- A numeric score between 1-50 is assigned by measuring five risk categories (see below)

## ENGAGEMENT STORYBOARD (IF APPLICABLE)

- Walkthrough of multi-step exploitations to help the customer to understand risk

Sample Pricing –

External Vulnerability Testing:
- Per Public IP Address - $250
- External Website / Application - $950

External Penetration Testing:
- External Website / Application Testing - $1,999
- 5 Public IP addresses + External Website - $2,999

Pricing can be tailored to specific requirements

DREAD Threat Model

**DAMAGE**
If the threat is exploited, how much damage will be caused?

**REPRODUCIBILITY**
How easy is it to reproduce the threat exploit?

**EXPLOITABILITY**
How easy is it to exploit the vulnerability?

**AFFECTED USERS**
How many users will be affected?

**DISCOVERABILITY**
How easy is it to discover this threat?

CRITICAL 40 - 50

SEVERE 25 -39

MODERATE 11 - 24

LOW 1 - 10

Digital Beachhead is a Certified Service Disabled Veteran Owned Small Business

Digital Beachhead provides proven Cyber Risk Management techniques, processes and compliance-based assessments with the Department of Defense, State/Local Governments and Commercial Enterprises. Our team of highly trained, certified agents provides detailed reporting based on consistently updated penetration / vulnerability toolsets and best practices.

## *Our Approach*

### Scoping and Enumeration

Prior to a test, our team discusses the requirements for your device, network or infrastructure assessment to define the scope of the test.

This is followed by service enumeration, network mapping, banner reconnaissance, and threat identification.

### Reconnaissance

Our team members use both private and public methods of intelligence gathering to develop the foundation for attacks. Information is collected from multiple relevant sources pertaining to the target organization. Information of email addresses, phone numbers, previous data breach credentials, web or mobile applications along with API endpoints is collected during this process.

### Mapping and Attack Planning

The attack strategy is planned at this stage. The approach is based on the information gathered in the previous stage and includes identifying subdomains hidden environments, analyzing cloud services for possible misconfigurations, checking authentication forms for weak or default credentials and crafting other attack scenarios.

### Executing Penetration Attack

The information and intelligence gathered in the previous stages are used to launch a host of attack options across all relevant vectors. Execution includes exploiting previously identified vulnerabilities, compromising systems, exploiting client-side vulnerabilities, targeting personnel using social engineering methods, etc.

### Documentation and Reporting

Our reports provided both executive level information down to the technical details required. Each is customized to the specific scope of the engagement and outlines any vulnerabilities discovered and exploited. The reports are designed to be easily digestible but complete in the findings, giving both the exploitation likelihood, potential impact and DREAD risk score.