Service Definition
Network Penetration Testing

Introduction

NTA's Penetration Testing service provides an examination of defined Internet facing IP addresses, testing for configuration, operating system and software vulnerabilities, as well as unauthenticated application level vulnerabilities. All security issues found are detailed in a formal report and recommendations are provided to enable the customer to eliminate or mitigate the risk, thus greatly reducing the likelihood of a successful attack.

This service allows organisations who have procured services via the Digital Marketplace, or who are using cloud hosted software, infrastructure or platforms, to gain independent analysis and information security assurance regarding the governance and controls that are in place to protect these services and systems. Such assurance is vital for cloud based services which possess specific security considerations due to their on-demand, remotely accessible and multi-tenanted attributes.

This specialist testing service provides customers with governance support in relation to the integration of cloud based services and systems into their organisations.

Scoping

A scoping conversation will be held prior to delivery to fully understand requirements and expectations, the size of the network to be tested and the type of systems that may be visible to the Internet. A recommended number of units/days will then be provided to enable requirements to be met.

Service Overview

This service may be purchased either individually or as a collection of services offered by NTA Monitor.

The service involves network probing to identify all systems visible from the Internet within the IP address ranges provided, including routers, firewalls, web application, remote access systems, mail and domain name servers. Where found, these systems will be tested for vulnerabilities within the operating system, the software and their configuration.

Unauthenticated application level testing will also be conducted against any web-based applications, remote access or file transfer systems found within the specified IP range, to identify flaws such as insecure authentication, weak encryption, SQL injection and cross-site scripting.

A test consultant will assess and correlate the findings of the initial automated stage and perform manual verification and further testing of any results that look unusual, any systems that appear to be complex or offering multiple ports, or systems for which there are conflicting results. A key focus of manual testing would be on web applications and remote access systems within the target IP address ranges.

NTA frequently identify vulnerabilities that could allow attackers to deface a web site, take control of a server, access the internal network, interrupt Internet connectivity or gain unauthorised access to corporate or other user's sensitive data. If such events were to arise, the cost to the organisation could include loss, corruption or disclosure of data, the inability to send or receive email, a damaged reputation and the man hours required to get systems up and running again.

Service Definition
Network Penetration Testing

Deliverables
The output is a tailor-written formal report containing:

- An executive overview with business implications
- A summary of risks identified, ordered from high to low severity
- Technical details of each issue found
- Recommendations for closing holes found
- Full listing of test results tables including background information/evidence to support results
- Issue history to allow for comparison against previous test results (where regular testing is performed by NTA)

The style and format of the report is designed with clarity and ease of use in mind. Features include hyperlinks to relevant sections of the document as well as external sources where applicable.

A technical telephone debrief is available and included as standard following delivery of the report, to explain the areas covered during the testing and the key findings and potential business implication (severity) of the issues found. This will include suggested priorities for the customer to take action against.

Service Management
You will be appointed a dedicated account manager and provided with points of contact for commercial and technical questions, to ensure that the service is properly executed.

NTA has a Service Level Agreement that is monitored by a R.A.G system to ensure that delivery standards are met on all projects. The SLA includes timeframes for project delivery with technical staff working to targets to ensure that deadlines are met.

Additionally, NTA has a customer services department that is responsible for the key administrative aspects of delivery such as liaising with you to confirm site details, scheduling the test, ensuring reports are sent out in a timely manner, scheduling follow up tests and debriefs etc. This is documented and monitored through the use of an internal database system, and links into other key processes regarding the correct method of sending the report according to the protective marking of the contents.

Ordering and Invoicing Process
Once the scope of work and number of units/days required has been agreed between the customer and NTA, a valid purchase order is required to enable scheduling and delivery.

An invoice will then be raised upon delivery of the service.

Customer Responsibilities
The customer is responsible for the completion of a Technical Details Form (TDF) prior to delivery. The provision of appropriate information will ensure that delivery meets expectations and requirements.

Service Definition
Network Penetration Testing

Technical Requirements

The resources typically required from the customer to ensure the service is performed as efficiently as possible include:

1. Technical contact details for any necessary communication during the testing (e.g. high risk issue notifications)
2. A list of target Internet IP addresses
3. Details of all Fully Qualified Domain Names (FQDNs) and any other unique entryways into applications, remote access or other systems for the entire in-scope infrastructure