Service Definition
Network Penetration Testing

Introduction

Intertek NTA's *External Penetration Test* provides a vulnerability assessment and review of defined Internet-facing IP addresses, which includes testing for configuration, operating system, and software vulnerabilities, as well as unauthenticated application vulnerabilities. Security issues found are detailed in a formal report and recommendations are provided to enable the client to eliminate or mitigate the risk, thus greatly reducing the likelihood of a successful attack.

The service is engineered to ensure that no damage is caused. Limited exploitation is performed to prove exploits such as cross-site scripting, but with damaging exploits and denial of service attacks not being performed. Options are available for more exploitative testing should this be required.

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

Intertek NTA will conduct network probing to identify all systems visible from the Internet within the specified IP address range(s), including routers, firewalls, web applications, remote access systems, mail and domain name servers. Where found, these systems will undergo port scans and 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(s), to identify flaws such as insecure authentication, weak encryption, SQL injection, faulty lockout facilities and cross-site scripting.

The service utilises Intertek NTA's unique test software, which is self-scripted and maintained in-house, along with selected open source and commercial tools where appropriate. This provides the benefit of our test consultants fully understanding the inner workings of the tests being performed and thus understanding how the results are derived, greatly increasing the accuracy of the service.

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 range(s).

The below tests would be performed if the associated system type is identified:

- **Manual Check of Web Applications**
  Intertek NTA will assess the security of search functions and form submissions on the website(s), particularly with regards to data sanitisation controls (before data is submitted back-end database) to check for injection and cross site scripting vulnerabilities. Checks for default administrator pages and logins will be performed as well as insecure external libraries being used.

- **Webmail Security Test**
  Intertek NTA will search for vulnerabilities that that may allow an unauthorised user to bypass authentication and access internal mail records, monitor mail traffic or perform a denial of service attack against the mail system.

- **Email Server Checks**
  This test will check mail relay server for information leakage and if mail can be relayed through the server which would facilitate spam and phishing campaigns by malicious actors.

- **SSL VPN & Citrix Gateway Security Test**
  This test will seek to ensure that remote access portals are locked down and securely configured, checking that strong authentication and encryption is in place and that the system is not vulnerable.

- **IPSec VPN Security Test**
  The objective is to determine as much information as possible about the configuration and security of the target VPN server and to establish if it is possible to gain access to the network through this device. Vulnerabilities are usually caused by poor configuration, particularly with regard to the authentication procedure.

- **Site-to-Site IPSec VPN**
  Intertek NTA will check that the IPSec VPN system is configured for site-to-site access only and does not allow for remote access from non-specified external IPs and does not leak sensitive system information.

- **FTP/SFTP Test**
  If either type of File transfer server is discovered, Intertek NTA will seek out vulnerabilities that may allow unauthorised access to the files within, as well as attempt to upload or download files, assess associated anti-virus controls and investigate the possibility of the facility being taken offline, from an unauthorised user's perspective.

Vulnerabilities Found

Intertek 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 client 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

Testing will check for network and unauthenticated application level vulnerabilities on all systems visible from the Internet. Given the high volume of tests that are performed, NTA is familiar with testing a wide variety of system and software types. Examples of vulnerabilities found by the service include:

- Unsupported operating system detected
- Servers allow Windows Terminal Server access
- Telnet access to network devices or servers
- Firewall offers dangerous network services
- Exposed CMS admin interface
- FTP servers have world-writeable directories
- SMTP server allows relaying
- Firewall/Server offers PPTP VPN service
- Directory Listing available through PROPFIND method
- VPN system uses crackable transforms
- Microsoft Outlook Web Access URL Redirection
- Depreciated and vulnerable SSL/TLS protocols and cipher suites
- Exposed services which should not be publicly accessible

Examples of vulnerabilities found by the additional manual and application level testing provided by this service, over and above standard network vulnerability testing, include:

- Remote command execution and shell access
- Unrestricted file access and download
- Local administrator password discovered
- Access to FTP possible with re-used credentials
- SSL VPN user using weak guessable password
- Web applications have cross-site scripting vulnerability
- Web application vulnerable to URL redirection attacks
- Application backend source code disclosure
- Authentication credentials found hardcoded in web file
- Phpinfo.php file leaks information

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)

Service Definition
Network Penetration Testing

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.

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

- Technical contact details for any necessary communication during the testing (e.g. high risk issue notifications)
- A list of target Internet IP addresses (to include publicly accessible services such as web servers, FTP servers, IPsec/SSL VPN remote access
- 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
- Internet router details
- Internet firewall details