



## a&o Service Offerings

<b>Offering</b>	<b>Network Penetration Testing</b>
<b>Description</b>	<p>With the advent of increasingly sophisticated hacking tools that are ever more readily available, it has never been more important for companies to evaluate the intruder threat to their business.</p> <p>The a&amp;o <b>Network Penetration Testing</b> service is delivered by experienced networking and security professionals who employ “ethical hacking” techniques to evaluate the security of target networks.</p> <p>Penetration testing of a customer’s network will be performed both internally and externally to actively evaluate your information security measures and identify vulnerability of the network. This is an active real world test of the security measures in place rather than a theoretical paper based audit.</p> <p>The results of the penetration testing are documented in a report along with recommendations to address any vulnerability discovered.</p>
<b>Methodology</b>	<p>An a&amp;o Technical Consultant will use the common hacking tools and techniques that are available to a real intruder to undertake a network penetration assessment and determine security vulnerabilities of the customer network.</p> <p>Testing will be carried out from an external perspective, typically via the company’s Internet connections, and also from key internal network segments. In this way our consultant will build a comprehensive view of the network, key target systems and the existing security mechanisms.</p> <p>Whilst the exact testing plan may vary, it will typically encompass the following steps:</p> <ul style="list-style-type: none"> <li>• Network Footprinting           <p>Footprinting is the starting point of the security test or assessment. Output from this activity will include a list of domain names, IP addresses, a theoretical network topology map and information regarding ISPs/ASPs, system and service owners.</p> </li> <li>• Port Scanning           <p>Port scanning is used to identify which TCP and UDP ports on externally visible hosts are accepting connections from the Internet. Various techniques and hacking tools will be used to port-scan and to attempt bypass of the firewall.</p> </li> </ul>



Empowering Technology



## a&o Service Offerings

	<ul style="list-style-type: none"> <li>• Detection of operating systems By analysing the TCP and UDP packets to and from the testing host and target, the operating system can be identified.</li> <li>• Enumeration Connecting to computers in the target network to identify network and host accounts and poorly protected computing resources.</li> <li>• System Hacking Using hacking techniques to attempt to gain control of systems in the target network:             <ul style="list-style-type: none"> <li>• Operating System hacking</li> <li>• Dial-up and VPN hacking</li> <li>• Wireless Network hacking</li> <li>• Firewall hacking</li> <li>• Denial of Service (DOS) attacks</li> <li>• Remote control, Trojan Horse and back doors</li> <li>• Internal user hacking</li> <li>• Web Server hacking</li> <li>• Session Hijacking</li> <li>• Virus &amp; Worms</li> </ul> </li> </ul> <p>a&amp;o will then provide a report document that details the testing results, identifies risks and vulnerabilities, and provides recommendations.</p>
<p><b>Deliverables</b></p>	<ul style="list-style-type: none"> <li>• Best practice “ethical Hacking” testing of the target networks</li> <li>• Configuration review of key device configurations and security systems</li> <li>• Report documenting risks and vulnerabilities found with recommendations for remediation and countermeasures</li> </ul>
<p><b>Supported Environments</b></p>	<p>The Network Penetration service is equipment and environment agnostic. Our consultant will require a suitable level of access to:</p> <ul style="list-style-type: none"> <li>• Network design and IP schema</li> <li>• ISP and public addressing information</li> <li>• Equipment configurations</li> <li>• Key IT personnel</li> </ul>



Empowering Technology



## a&o Service Offerings

<p><b>Resource Model</b></p>	<p>Resourcing for this service will be dependent upon a number of specific network topology factors and customer specific requirements, hence a scope and pricing process will be applied on an individual basis. An indicative example for a single site with one Internet link and up to 500 users would be:</p> <p>Technical Consultant : <b><u>3 days</u></b></p> <ul style="list-style-type: none"> <li>• Assessment 1.0 day</li> <li>• Analysis 1.0 day</li> <li>• Report Generation 1.0 day</li> </ul>
<p><b>Related Services</b></p>	<ul style="list-style-type: none"> <li>• Network Health Check</li> <li>• Wireless LAN Planning &amp; RF Survey</li> </ul>

