JDS SECURITY

NETWORK PENETRATION TESTING

JDS is CREST (International) certified as a penetration testing service provider, offering expert advice and consulting for a range of security requirements. We utilise the latest globally recognised standards, benchmarks and methodologies to ensure our tests and audits are relevant to today's security risks. JDS uses proactive, detailed and industry-best practice threat intelligence to increase your organisation's resilience against cyber threats, on time and on budget.

EXTERNAL NETWORK PENETRATION TESTING

The JDS External Network Penetration Testing methodology utilises both manual and automated testing of your organisation's external-facing infrastructure to determine if an external attacker can breach your perimeter.

What is the outcome of this service?

Identify exploitable vulnerabilities in the publicly accessible network access – i.e., Kiosks, Guest Wi-Fi, Access Ports found in accesible areas.

Gain visibility on how a remote attacker could compromise your public network systems and services such as firewalls and VPN services, as well as network devices.

Allow your organisation to assess its current security posture and formulate an incident response plan that is relative to your likely risks.

Uplift the security capabilities of your IT team through our recommended remediation.

INTERNAL NETWORK PENETRATION TESTING

The JDS Internal Network Penetration Testing methodology involves simulating an internal attacker, potentially in the form of a rogue employee, contractor, guest user, or other onsite attacker via malware, viruses, infected applications, or unattended devices.

What is the outcome of this service?

An understanding of how an internal attacker could compromise your internal network ranging from employee access, and access points, to local servers.

Identify existing weaknesses in access controls within the internal infrastructure, and testing of the security controls of applications and databases.

Gain insights into the potential resulting damage and business risk from an attack.

A comprehensive report outlining the security exposures of your internal network, including high-impact recommendations and root causes.

WIRELESS NETWORK PENETRATION TESTING

Wireless technology is the entry to the perimeter network, hence an unsecured wireless network can enable attackers to enter and cause catastrophic damage to an organisation's reputation and safety. At JDS Security, wireless penetration testing is all-encompassing. We work with your team to assess wireless technologies for exploits and vulnerabilities, helping to validate the effectiveness of defensive controls and determine what is required to strengthen them.

In a Wireless Network Penetration Test, JDS examines the following:

- Rogue Access Point Detection - Validates that the alerting systems in place are detecting unauthorised access points in your environment correctly.
- Encryption Key and Password Strength - Assess the strength and complexity of your wireless keys and their vulnerability to be 'brute force' or dictionary attacked.
- Network segmentation - Identify any vulnerabilities between your corporate/guest wireless environments and physical networks.
- Router Configuration Review - Identify any weak configuration settings in routers.

VIRTUAL DESKTOP BREAKOUT ASSESSMENT

A Virtual Desktop Breakout Assessment will identify how an attacker can compromise your Virtual Desktop environment and perform unwanted actions.

During a Virtual Desktop Breakout Assessment, the JDS Security team will identify and exploit configurations that bypass virtual desktop restrictions, access other unintended or restricted assets on the same network, enumerate and access other connected networks, or even exfiltrate data.

The following actions are assessed:

Vertical and Horizontal Privilege Escalation

Gaining command prompt and / or PowerShell access

Executing code through Microsoft Office macros (i.e. Excel, Word)

File-system access on the Virtual Desktop server

Enumerating and possibly accessing other hosts on the same network

Accessing a restricted desktop or application

HOST-BASED SECURITY ASSESSMENT

When a particular host, device or asset is critical to the function of your organisation, it is imperative to assess its depth of security. A JDS Host-Based Security Assessment will provide full visibility of the existing weak points of a specific asset, as well as the potential impact to other assets and the network.

An example of hosts we can target, but are not limited to:

Desktops and Laptops
Printers and Scanners
Network Devices (i.e, Routers, Switches)
Firewalls
VPNs
Servers
Databases
Any other devices that may be network connected (i.e, Smart TV, Security Camera)

Providing a full report of reproducible exploits and vulnerabilities, JDS Security can assist in determining the best remediation options to keep your essential assets secure.

STOLEN ASSET SIMULATION

Smartphones, tablets, and laptops are essential in corporate environments because they enable your staff to be productive in any place, and at any time. However, if one of these assets is stolen, cybercriminals will have direct access to some of the most sensitive systems and information you have. In order to determine your organisation's level of readiness to handle these risks and gauge the efficacy of your current security measures, a stolen device assessment is required.

The following are typically evaluated in a Stolen Asset Simulation assessment:

Device/disk encryption
Absent security patches
Insecure storage
Insecure password management
Cached credentials
Boot process analysis
Information leakage
Mobile Device Management (MDM)

The JDS Security team will simulate a cyberattack using a "stolen" device, determining how much information can be retrieved from the device, and any other vulnerabilities that would aid an attacker to achieve remote access to the organisation's internal network. We also analyse the device configurations and any associated risks.

OPEN SOURCE INTELLIGENCE GATHERING

OSINT, or Open Source Intelligence, refers to collecting data and information from openly available sources online such as media or social networks. At JDS, we use OSINT to identify potential vulnerabilities and weaknesses in networks, before an attacker has the chance to exploit them using the same tools and techniques.
We collect and analyse information from online sources via various techniques such as data mining, data extraction, and data washing. JDS utilises OSINT as part of our security services such as Red Teaming exercises, Wireless Penetration Testing and Application Penetration Testing.

JDS consult OSINT to discover the following information from publicly available sources:

Physical/Online Infrastructure and networking detail

Full DNS listings of all associated assets; Netblock owners and email records, mail address structure.

Lists of compromised accounts from previous breaches, and passwords that are associated with these accounts that if reused, could be applied to gain access.

Any other information relating to the organisation and/or employees, which could potentially be used in future exploits.

Established in 2003, JDS Australia delivers specialist services in a set of technologies and capabilities that ensure critical IT systems work.

JDS focuses on IT Monitoring (Observability), Security, Service Management, Quality Assurance and Automation as areas that enterprises and government departments need to increase the value of their investments. With an entirely local team of 100+ employees, JDS has the trusted skills and experience to ensure IT works and Australian business carries on.

jds CREST PEN TEST

Melbourne
Level 8, 2 Russell Street
Melbourne VIC 3000

Sydney
Level 10, 50 Park Street
Sydney NSW 2000

Brisbane
Level 37, 123 Eagle Street
Brisbane QLD 4000

Toll Free
1300 780 432

Email
contactus@jds.net.au

Web
www.jds.net.au