

## **Case Study: Configuration Review – IDS/IPS**

### **Industry Sector: Manufacturing**

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are crucial components of an organisation's security infrastructure. However to maximise the effectiveness of an IDS or IPS, a finely-tuned configuration is required. The oversensitive IDS threatens its effectiveness by flooding even the most sophisticated log correlation engines, resulting in actual attack attempts being lost within the noise. Conversely, a poorly-configured IDS lacking the appropriate attack signatures results in legitimate attack attempts going entirely unlogged.

In contrast to our other configuration review services, IRM takes a network-based testing approach to IDS assessment. Through the transmission of a variety of security test cases including both stealthy and noisy network probes targeting client systems, IRM assesses configuration of the IDS or IPS systems in place.

A thorough examination of the logs generated during the testing process allows IRM to identify what types of attacks were matched against and flagged as a concern, and which techniques were successful in evading detection.

Using the results and recommendations of these assessments, our clients are able to assess their current configuration and then perform a fine-tuning process on their IDS and IPS systems. This allows them to achieve the necessary balance between minimising noise and maximising effectiveness with respect to their particular requirements.

#### **Case #1 – Maximising return on investment**

IRM was asked to undergo a configuration review against an IPS recently deployed into the network of a leading food manufacturer due to concerns over the lack of alerts generated by the system since deployment. The implementation was an out-of-the-box IPS solution installed by a leading network security product vendor.

IRM employed various network probing techniques combined with a targeted analysis of the generated logs. IRM consultants determined that the IPS was largely unchanged from its default configuration and attack techniques, exploits and tools commonly used by attackers were found to go undetected by the IPS.

For example, basic attack techniques such as simple network scanning attempts were confused with other intrusion attacks or went totally undetected due to out-of-date signatures. Higher level issues such as vulnerability scanning attempts or launching commonly known exploits against system services went completely unlogged by the IPS. Furthermore well-known IPS evasion techniques were performed and also went undetected.

Our client was able to use the information presented in the detailed report to fine-tune their system to provide a significantly increased level of alerting that remained sensitive to their business requirements given their relatively small operational security team.

#### **About IRM**

Information Risk Management Plc (IRM) is a vendor-independent information security consultancy. Founded in 1998 to work alongside global enterprises in understanding the security risks inherent in an increasingly interconnected business environment, IRM has become a leader in penetration testing, risk assessment and security auditing.