ASTAARA
RISK MANAGEMENT

PENETRATION TESTING

Penetration Testing is an important element of risk management. Its job is to think like a hacker and expose risks and vulnerabilities so that they can be dealt with before a hacker can get to them. Risks are increasing in sophistication; and increasing digitisation brings with it greater risks of vulnerabilities being exploited.

- Regulations require cyber risks to be properly identified and managed by shipowners and operators.
- Penetration Tests are an important function of the risk management portfolio.
- They range in sophistication and depth and their results are only valid for a short while.
- They need to be performed frequently and by different teams to maintain credibility and they need to be performed by accredited people

WHAT DOES A PEN TEST DO?

Penetration testing involves identifying vulnerabilities in a particular website, network or system and attempting to exploit them to penetrate the system.

The purpose of a Pen Test is to determine whether a detected vulnerability is genuine. If a pen tester manages to exploit a potentially vulnerable spot, he or she considers it genuine and reflects it in the report. The report can also show unexploitable vulnerabilities as theoretical findings. Don't confuse these theoretical findings with false positives. Theoretical vulnerabilities threaten the network but it's a bad idea to exploit them as this will lead to a Denial of Service.

At the initial stage, a reputable provider of penetration testing services will use automated tools sparingly. Practice shows that a comprehensive penetration test should be mostly manual – which explains why Pen Tests cost more than Vulnerability analyses.

During the exploiting stage, a Pen Tester tries to harm the customer's network (takes down a server or installs malicious software on it, gets unauthorized access to the system). Vulnerability assessments do not include this step.

OUR DIFFERENT LEVELS OF TESTING EXPLAINED:

BRONZE Level

- Scan of external facing assets
- List of assets provided by customer
- Mostly Automated – quick
- £1000 per vessel / office

SILVER Level

- Scan of external facing assets - as for Bronze
- Some internal information
- Testing of internal network segmentation
- Some external hacking techniques
- Around £5000 per vessel / premise
- Can also form part of a wider risk management offering over a year

GOLD Level

As for silver, plus:

- Probes onto host network inside firewall
- Social engineering
- Dark web data mining
- Use of e.g. DDOS, brute force, spear phishing
- Price will depend on number of endpoints
- Requires vessel access
- Yearly budget, including a scheduled combination of grey and white hat testing, together with 6-8 black hat hacks (unannounced)

Contact us for more information **enquiries@astaara.co.uk**