

Matta Assessment Services



Wireless Security Assessment Service Overview and Information

Introduction

As an independent Information Risk Management company, **Matta** represents the new breed of Security Consultants. Through combining best practice wireless scanning and security assessment tools and hardware with hands-on vulnerability qualification and reporting, **Matta** provides its clients with a comprehensive wireless security assessment service.

Wireless security assessment involves emulation of highly determined wireless attackers with access to high gain antennae and equipment capable of sniffing 2.4GHz 802.11b traffic from a distance. Low level analysis of wireless traffic is undertaken, including attempts to crack WEP encryption and compromise keys used to protect wireless data.

Risk Identification & Classification

An important first step in improving the security of any network is to correctly identify areas of risk and set clear priorities in-line with business drivers. **Matta** understands real world network risk and business impact, focusing primarily on three key areas during a wireless security assessment:

- Low-level network security, ARP spoofing and other threats
- Assessment of encryption and intrusion prevention techniques
- Assessment of accessible servers and devices at IP level

The **Matta** assessment methodology comprehensively covers each layer of the 7 layer OSI model. **Matta** is the first security consultancy to tackle technical network security in this manner, and offers world-class assessment of both application, network & physical layer devices to ensure complete end-to-end security.

Bespoke Assessment Application

A **Matta Wireless Security Assessment** is not simply a sniffing exercise, or a vulnerability assessment. **Matta** assessment services are offered to clients with a specific business goal or driver in-mind. Examples of bespoke **Matta** assessment services being used by our clients over the last year include:

- Emulation of a determined attack to assess WEP encryption
- Low-level assessment of wireless AP configuration in public areas
- Denial of Service attack emulation to assess defensive strategy

Matta assessment services are geared completely around the client network type and requirement. A plethora of different offensive technologies are used depending on the goal and deliverable, ensuring that true value is realised and network security is effectively improved.

Matta Assessment Services



Wireless Security Assessment Service Overview and Information

Methodology

A standard **Matta Wireless Security Assessment** methodology used to assess a given 802.11b network includes the following components:

- Use of wireless sniffing equipment (usually a Linux laptop with a Cisco Aironet network card and a series of high gain antennae) to effectively identify and categorise all 802.11b traffic emanating from a given site.
- Low level assessment of wireless network topology and integrity using a plethora of tools including Kismet, Ethereal and in some cases commercial Windows packages such as ISS Wireless Scanner, NAI Sniffer Wireless and Wildpackets AiropEEK.
- Offline assessment of encryption through dictionary attacks against ASCII derived WEP keys and exhaustive keyspace searches against strong 40 and 104-bit key lengths.
- Use of tools such as Ettercap to modify the MAC address of the wireless network card to override MAC filters on access points and other low level security features.
- Upon compromising WEP encryption, simple application of **Matta Network Security Assessment** methodology to enumerate IP devices and networks, and assess the level of access to internal network spaces.

The tools and systems selected are best of breed for a comprehensive wireless security assessment to be carried out. Cisco Aironet firmware allows for sniffing of all fourteen 802.11b channels continuously, as the signals are multiplexed and handled correctly. Many security companies use ORINOCO based wireless network cards to perform assessment, which can only sniff a single channel at a time, resulting in a degree of data loss. 14 dBi gain directional Yagi antennae are used, allowing for signal to be siphoned from up to 4 miles line-of-sight.

Client deliverables include a hand written report, clearly documenting the current state of wireless network security, and recommendations for improvement to access point configuration and use of security mechanisms such as IPsec VPN technologies, intrusion detection systems (IDS) and filtering devices. Due to the fact that **Matta** reports are hand written, the findings and recommendations are tailored with both the client business drivers, and technical network configuration in mind.