Phantom RFID Exploitation Toolkit

Phantom RFID Exploitation Toolkit (RFID7343)

A selection of easy to operate tools that enable a user to exploit common types of 'Radio Frequency Identification' based Access Control Systems (ACS).

RFID technology is often employed as a convenient way in which to implement monitored/controlled access within secured facilities, hotels and offices. The 'Phantom RFID Exploitation Toolkit' is designed to provide an easy method in which to exploit some common types of these systems enabling capabilities such as the following;

- RFID Analyser – Key to exploiting a system is first knowing what frequency and type of RFID is being employed. This toolkit contains equipment capable of providing this information.
- Cloning of access card/fob to a second physical card
- Electronic emulation of a target card/fob (simulation of target card)
- Privilege escalation of a target card – Enabling access to additional readers within the same facility
- Stay-behind reader logging device with Bluetooth egress – This device is designed to record key information from any access attempts enabling a user to replay this same information on demand via a mobile application and therefor gaining access.

The 'Phantom RFID Exploitation Toolkit' is designed to exploit some of the more commonly found ACS at present such as 'Mifare Classic 1K, Mifare Classic 4K, HID ProxCard II'. However, future firmware releases can be issued enabling increased functionality and compatibility with additional RFID types helping to ensure longevity of use of this equipment as part of a client's capability and skillset.

Important Note: An understanding of what types of systems this equipment can effectively be deployed against is key to success of this capability. Thus, a 1-day training package is extremely recommended for any users upon purchase.