Penetration Testing with the Raspberry Pi

Martin Goodfellow
@GlasgowCoder
Warning

The ideas and concepts in this talk are intended to be used for educational purposes only. The misuse of this information can result in criminal charges. Hacking is regarded as a serious crime. It’s not a case of if you get caught but when you get caught.
Why?
KALI LINUX™

“the quieter you become, the more you are able to hear”
Pen Test Drop Box
Hiding the drop box
Remote Access

- SSH
- Reverse shell through SSH
- Stunnel
Man in the Middle Attack

![Diagram of Man-in-the-middle attack]

Original connection

New connection

Man-in-the-middle, Phisher, or anonymous proxy

http://www.computerhope.com
Man in the Middle Attack

kali.home (192.168.1.81) at fc:b4:e6:af:d9:bc

bthomehub.home (192.168.1.254) at 40:f2:1:44:c4:94
Man in the Middle Attack

kali.home (192.168.1.81) at fc:b4:e6:af:d9:bc

Man in the Middle Attack

When the user submits their log-in credentials they do not realize that they are sending them in plain text.
Social Engineer Toolkit (SET)
Social Engineer Toolkit (SET)

192.168.1.7 - - [10/Dec/2015 23:21:02] "GET / HTTP/1.1" 200 -

[*] WE GOT A HIT! Printing the output:

POSSIBLE USERNAME FIELD FOUND:
email=test@test.com

POSSIBLE PASSWORD FIELD FOUND:
pass=password
Rogue Access Honeypots

- Bridgeton Library...
- Corporate
- Other...

Ask to Join Networks

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.
Reference