

filename:comptia-secplussy0601-1-12-network\_attacks\_mitm\_and\_mitb

Showname: Security+ (SY0-601)

Topic: Threats, Attacks and Vulnerabilities

Episode: Network Attacks - MiTM and MiTB

Learner Objectives:

Given a scenario, analyze potential indicators associated with network attacks.

Description: In this episode, the viewer will identify the characteristics of man-in-the-middle attacks or MiTM as well as man-in-the-browser or MiTB attacks. The viewer will see how an MiTM attack could be executed.

- MiTM
- MiTB
- Demo
  - Use Kali's nmap to identify open ports
  - Launch Wireshark to capture FTP login info
  - Connect to 192.168.0.131 (msf) with FTP
  - Authenticate and run the dir command and cd ../../..
  - Stop Wirehark and view FTP stream, identify clear text
  - Start Wireshark
  - Connect with SSH
  - Stop Wireshark and view encrypted information