

# Demonstrating Network Traffic Replay with Scapy

---



**Sean Wilkins**

Network Engineer & Author

[swilkins@infodispersion.com](mailto:swilkins@infodispersion.com)

[www.infodispersion.com](http://www.infodispersion.com)



# Engineering Knowledge

**Python/Scapy for Traffic  
Replay**

**Attack assessment knowledge  
is important**



# Overview



- **Covering the Basics of Traffic Replay**
- **Concepts Demonstration - Traffic Replay**



# Traffic Replay



---

## Methods include:

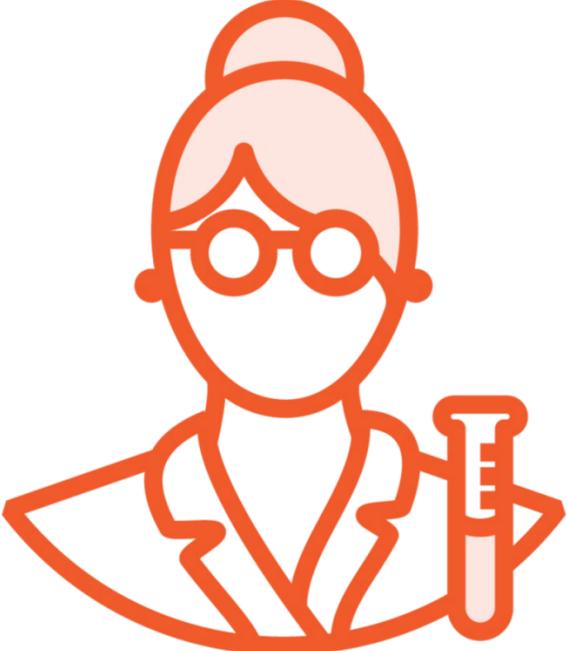
- **Direct traffic replay**
- **Indirect, used with overall solution**



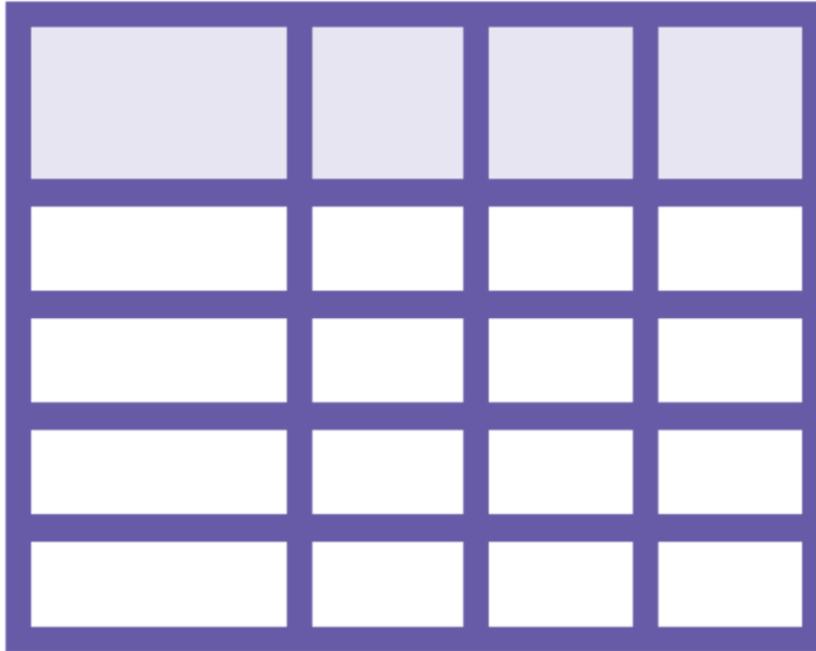
# Direct Traffic Replay



**Sends traffic as captured**



**Used to test other processes**



**Example would be to test TCP session management**



# Direct Traffic Replay

**Replay rate is not static**

**Could choose to speed up  
traffic rate**



# Indirect Traffic Replay

**Most interesting for network security  
engineers**

**Can be used to help break into systems**



# Example of Indirect Traffic Replay



Uses FTP for a clear understanding

Logic can be translated to many technologies



Authentication information is  
sent over network to be  
captured



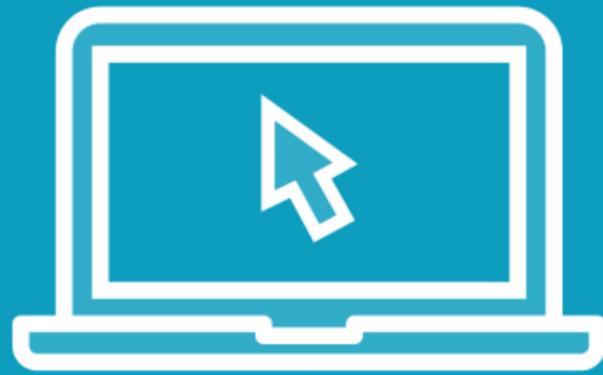
# Problems with Direct Transmission

**Direct transmission will not likely work**

**Alteration of session is required**



Demo



**Direct Replay**

**Indirect Replay**



# Summary



- **Covering the Basics of Traffic Replay**
- **Concepts Demonstration - Traffic Replay**

