

The background of the slide is a solid black field. Overlaid on this are thousands of thin, vertical lines of varying heights and colors. The colors include shades of blue, teal, orange, yellow, and white. These lines are distributed across the entire width of the slide, creating a dense, textured effect that resembles a digital signal or a stylized forest of light.

# Ettercap

Pablo Andres Balbuena Rios

# Esercizio 1 Settimana 6

Utilizzando Ettercap andiamo a simulare un attacco ARP-Poisoning. La macchina web vittima è a piacere, in alternativa si può usare: vulnweb.

<http://testphp.vulnweb.com/login.php> Fare un report su:

- Cos'è il protocollo ARP.
- Cosa sono gli attacchi MITM.
- Cos'è l'attacco ARP-Poisoning.
- Le fasi dell'attacco.

# Cos'è il protocollo ARP

- ARP è un protocollo di rete utilizzato per mappare un indirizzo di livello di collegamento (come un indirizzo MAC) a un indirizzo di livello di rete (come un indirizzo IP). In sostanza, ARP consente a un dispositivo di individuare l'indirizzo MAC associato a un determinato indirizzo IP nella stessa rete locale.

# Cosa sono gli attacchi MITM

- Gli attacchi MITM (Man-in-the-Middle) sono tecniche in cui un attaccante si colloca tra due parti in comunicazione, intercettando o manipolando il flusso di informazioni tra di esse. L'obiettivo è intercettare, alterare o iniettare dati tra le due parti senza che loro ne siano consapevoli. Questo tipo di attacco può avvenire in varie forme, come l'intercettazione del traffico di rete o la creazione di reti Wi-Fi fasulle.

# **Cos'è l'attacco ARP-POISONING**

- L'attacco ARP poisoning, o ARP spoofing, è una tecnica in cui un attaccante invia pacchetti ARP falsificati nella rete locale per associare un suo indirizzo MAC a un indirizzo IP legittimo. Ciò consente all'attaccante di intercettare o manipolare il traffico di rete destinato al dispositivo legittimo.

# Le fasi dell'attacco

- 1) Avviare Ettercap con l'interfaccia primaria di rete
- 2) Scannerizzare gli host e aggiungere i due target IP
- 3) Infine avviare ARP poisoning o NDP poisoning

