



UNIVERSITÀ DEGLI STUDI DI MILANO

Lab Sicurezza & Privacy

Network Security Tools



Setup

Virtual Environment (VirtualBox, Hyper-V, ecc)



Kali Linux
(attacker)

192.168.206.65

00-15-5d-01-02-07



VSFTPD

192.168.201.216

00-15-5d-01-02-06

Metasploitable 2
(vulnerable target)

Host internal network
(192.168.192.0/20)



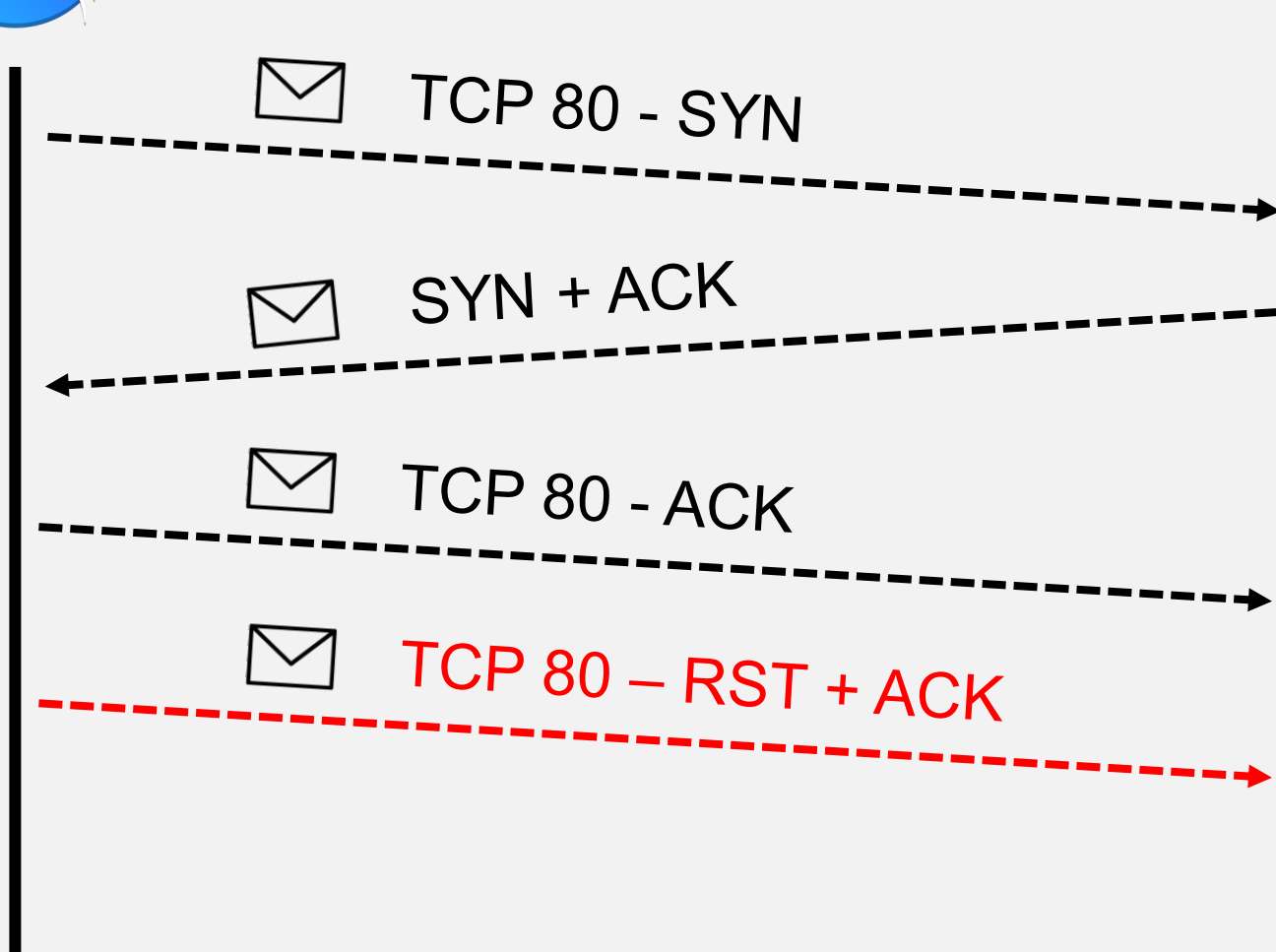
Host

192.168.192.1

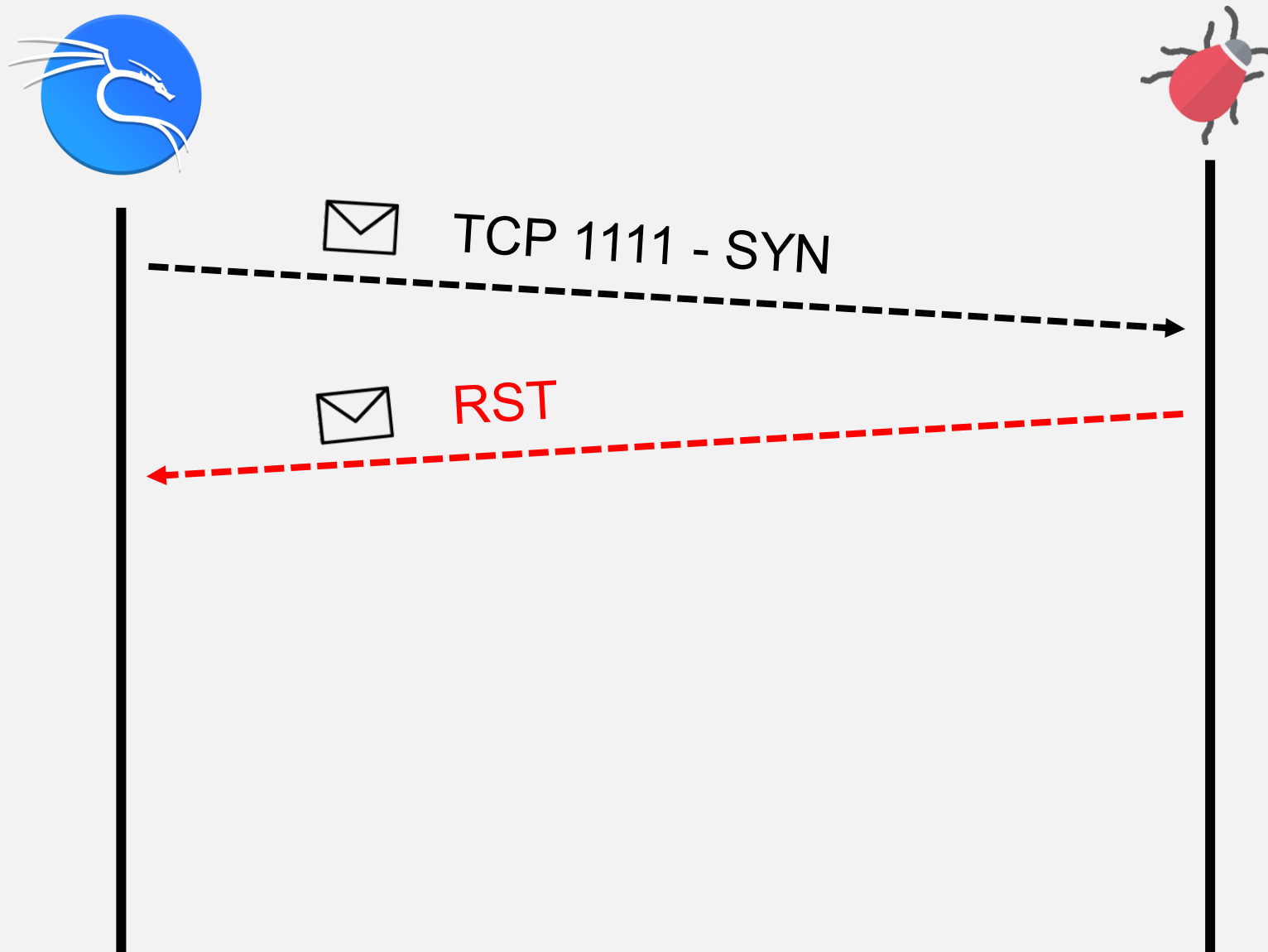
00-15-5D-9D-22-B4

172.22.56.45
(WiFi Unimi)

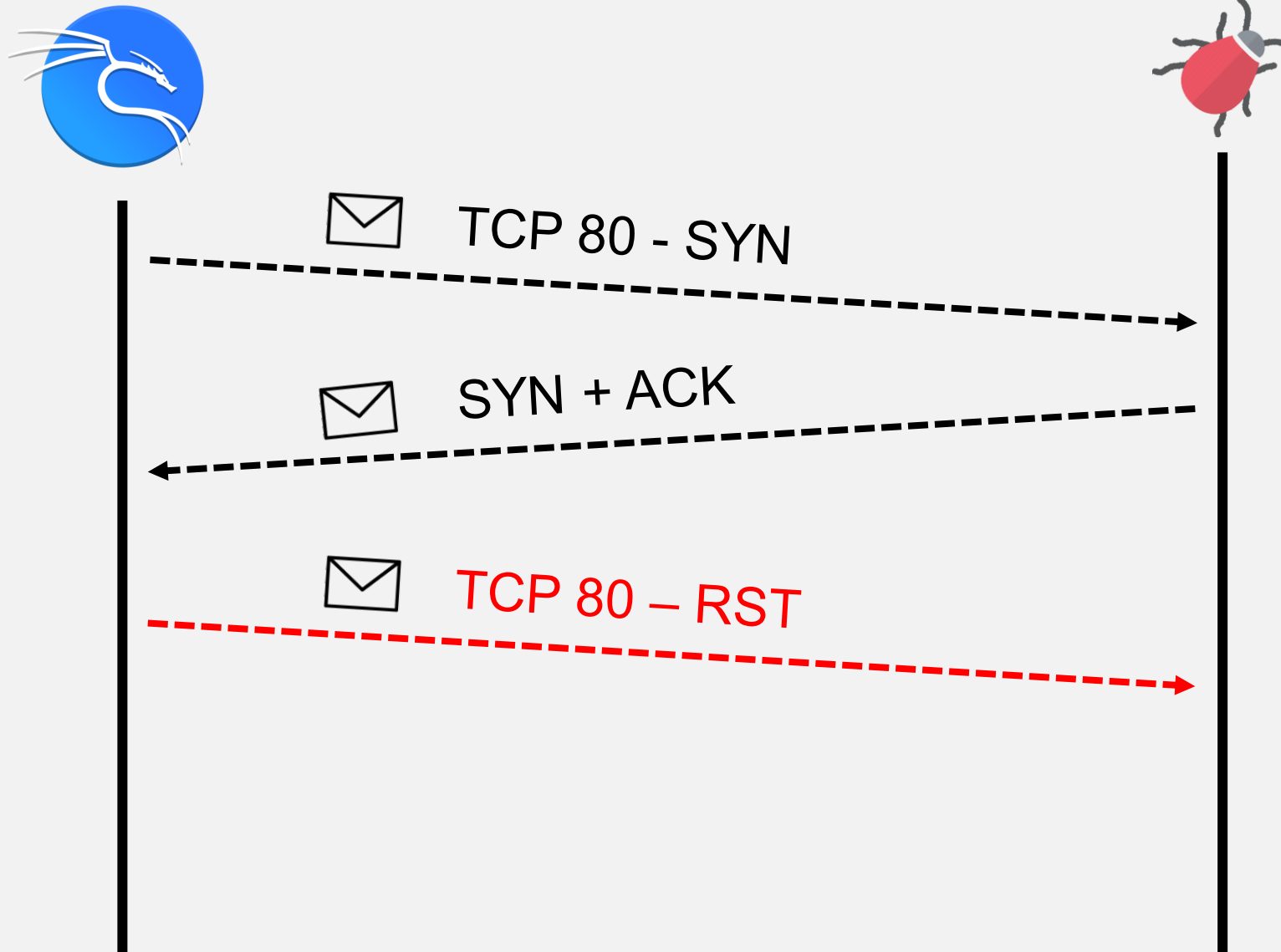
Nmap -sT 192.168.201.216 (existing service)



Nmap -sT 192.168.201.216 (non-existing service)



Nmap -sS 192.168.201.216



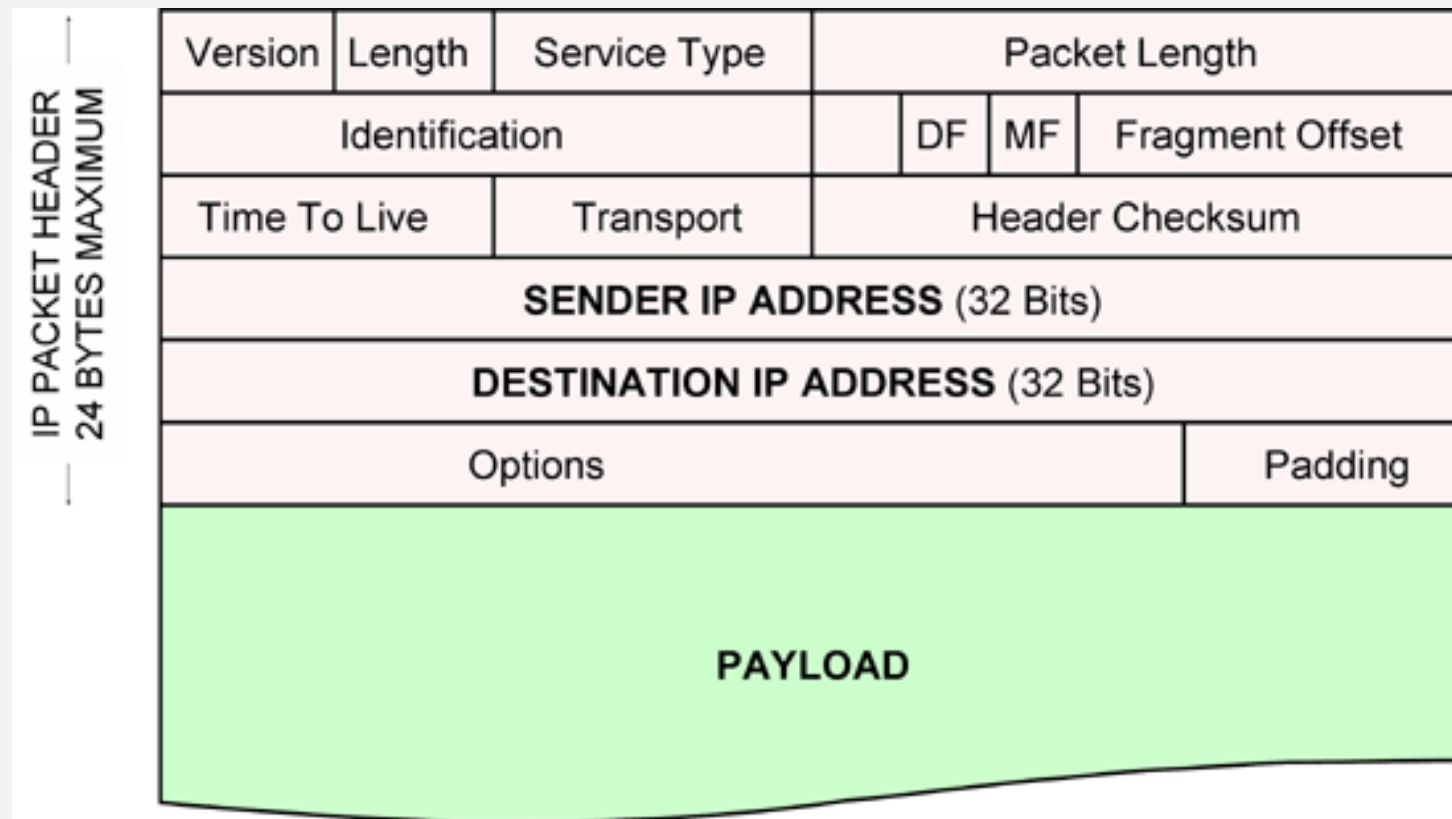


Nmap Idle Scan

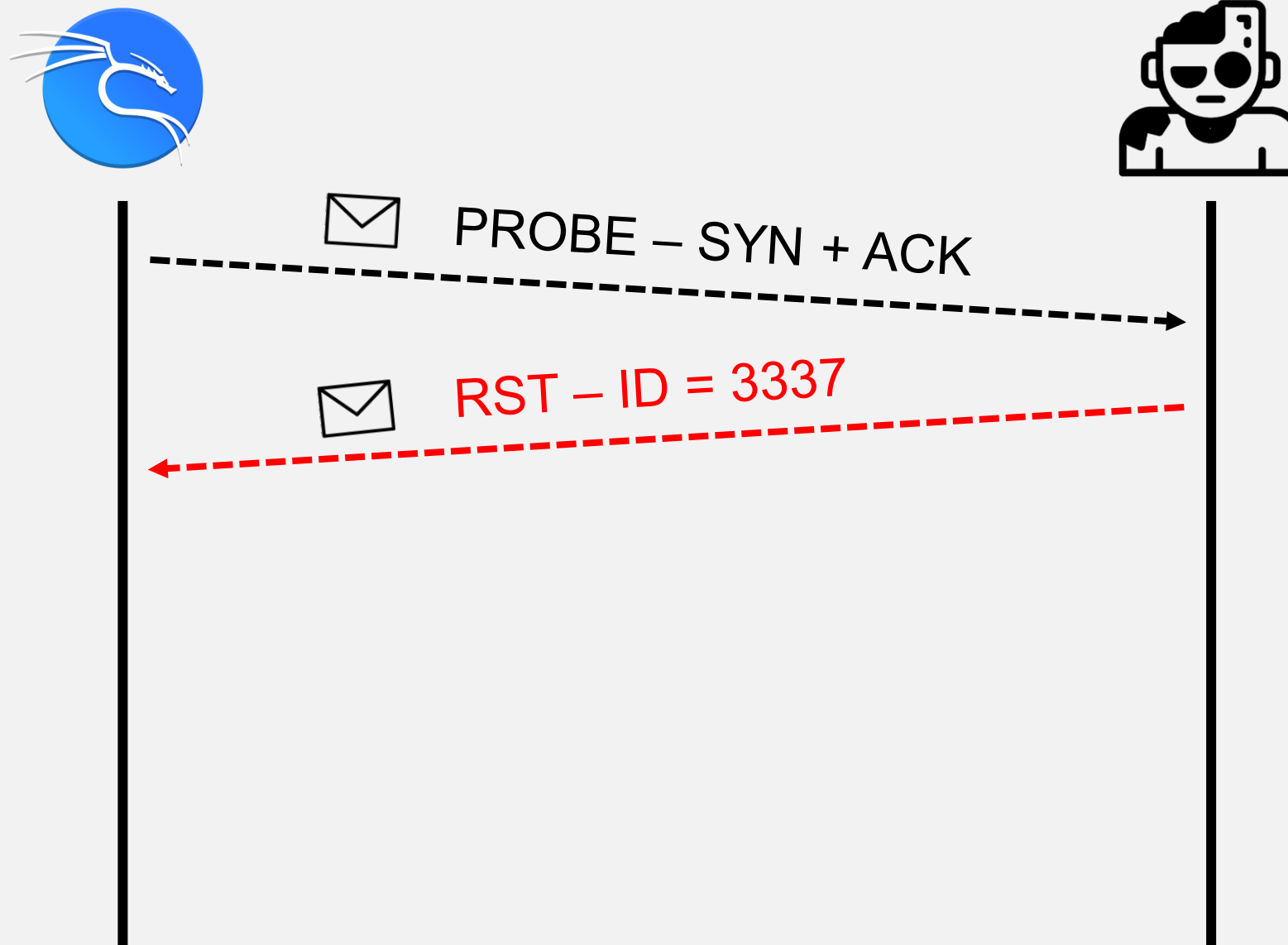
- Sfrutta la segmentazione IP per capire, tramite un host detto ***zombie***, se una determinata porta di un host che vogliamo *attaccare* è aperta/chiusa
- L' host *attaccato* non riceve nessun pacchetto con ip sorgente dell' *attaccante*
- “Side-channel attack” perche valutiamo gli effetti che ha la comunicazione *attaccato-zombie* su alcuni header

IP Segmentation

- ID usato per gestire la frammentazione quando il payload supera la *MTU*
- In alcune implementazioni è un *global counter*




Probe Primitive




Port Status Deduction – Open Port



 SYN (Source: zombie)

 SYN + ACK

 RST- ID = 3338

Attacker probes zombie a second time



Port Status Deduction – Close Port



SYN (Source: zombie)



RST



Attacker probes zombie a second time

MITM



192.168.206.65

00-15-5d-01-02-07

HOST: 00-15-5D-9D-22-B4

METASPLOIT: 00-15-5D-01-02-06



192.168.201.216

00-15-5d-01-02-06

HOST: 00-15-5D-9D-22-B4

KALI: 00-15-5D-01-02-07

METASPLOIT: 00-15-5D-01-02-06

KALI: 00-15-5D-01-02-07



192.168.192.1

00-15-5D-9D-22-B4

MITM



192.168.206.65

00-15-5d-01-02-07

HOST: 00-15-5D-9D-22-B4

METASPLOIT: 00-15-5D-01-02-06



192.168.201.216

00-15-5d-01-02-06

HOST: 00-15-5D-01-02-07

KALI: 00-15-5D-01-02-07

ARP POISONING

METASPLOIT: 00-15-5D-01-02-07

KALI: 00-15-5D-01-02-07



192.168.192.1

00-15-5D-9D-22-B4