ICMC USP
SÃO CARLOS

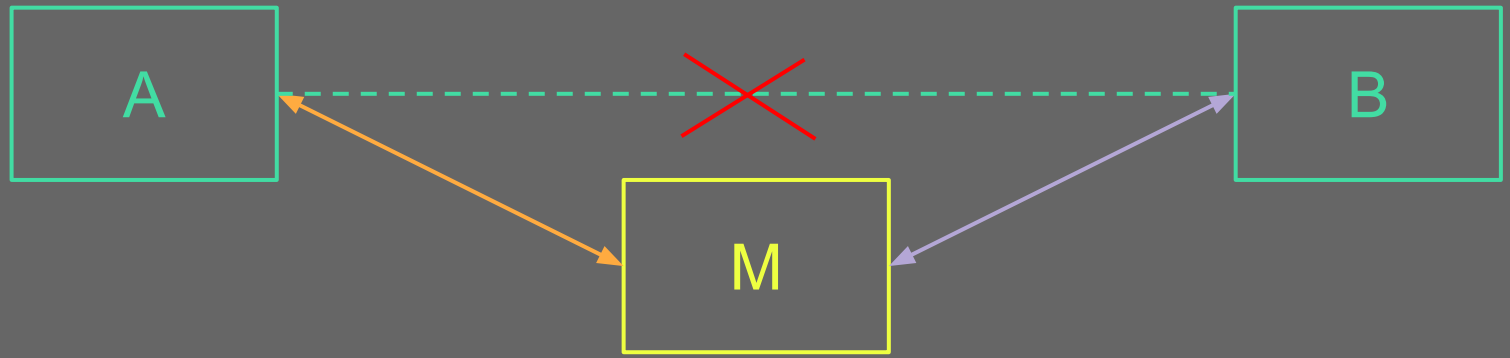
GANESH

Arp Cache Poisoning

Man in the middle

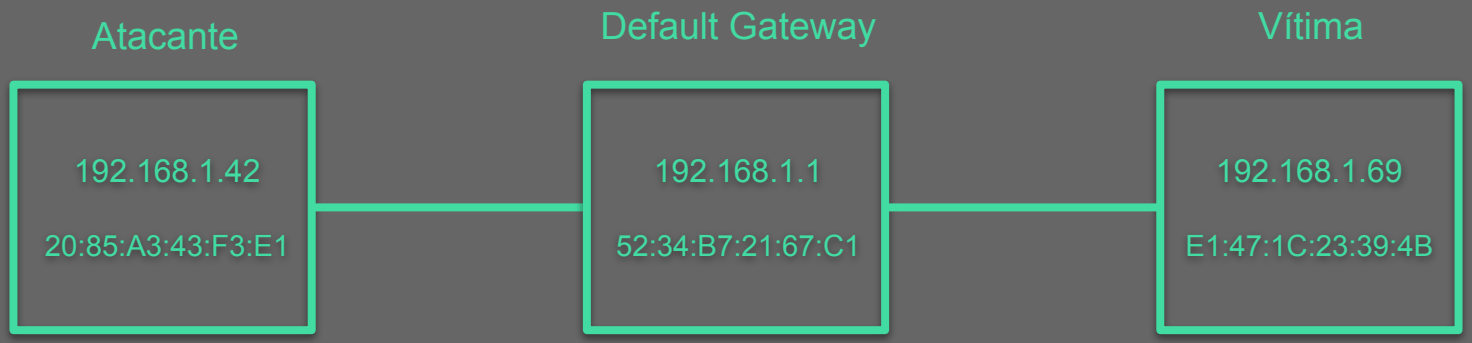
MITM - Man In The Middle

- Ataque de homem do meio
  - Dois computadores (A e B) se comunicando
  - Atacante (M) finge ser B para A
  - Atacante (M) finge ser A para B

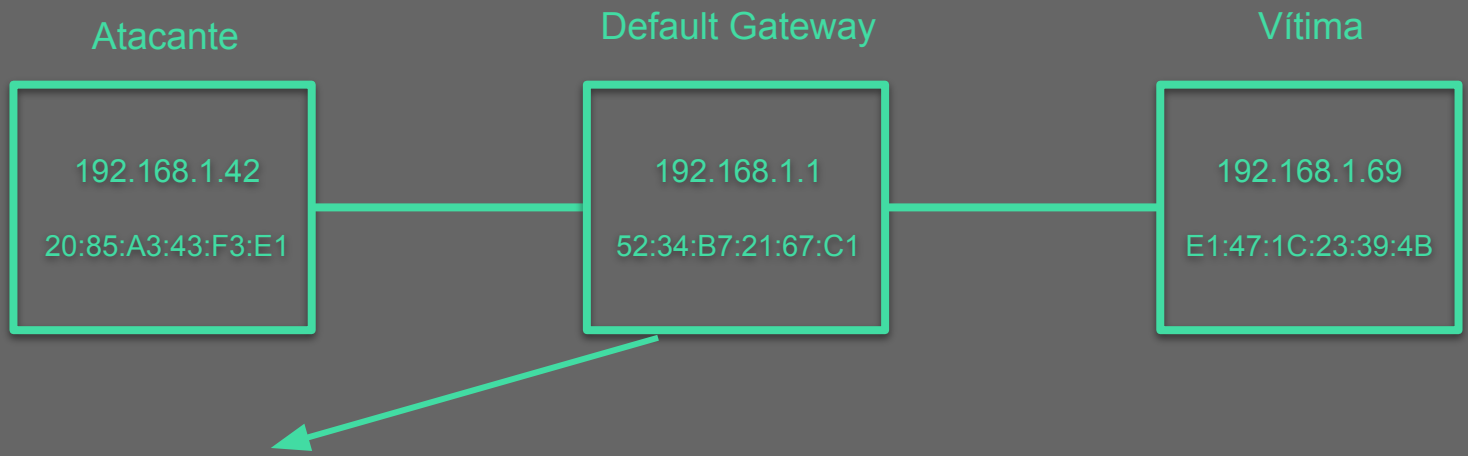


Arp Cache Poisoning

Arp Cache Poisoning

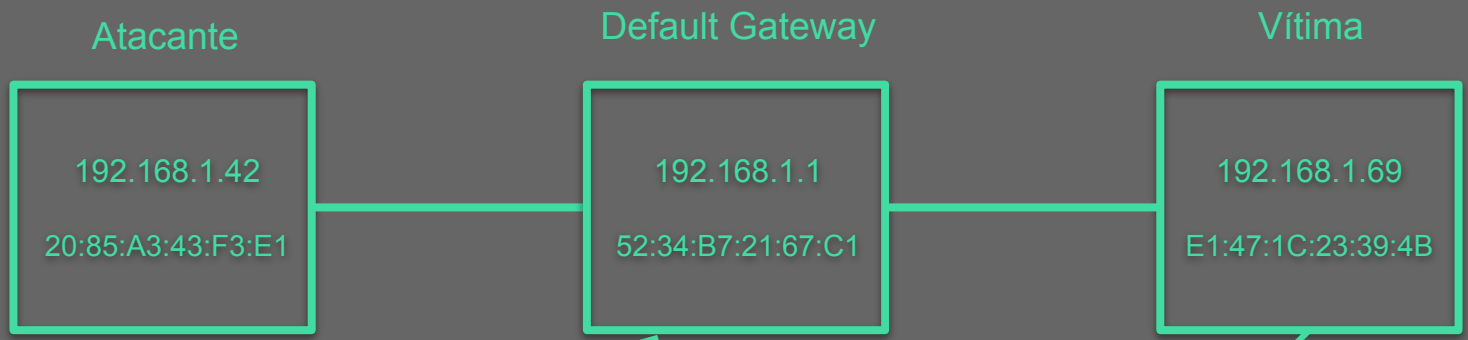


Arp Cache Poisoning



IP	MAC Address
192.168.1.42	20:85:A3:43:F3:E1
192.168.1.69	E1:47:1C:23:39:4B

Arp Cache Poisoning



IP	MAC Address
192.168.1.42	20:85:A3:43:F3:E1
192.168.1.69	E1:47:1C:23:39:4B

IP	MAC Address
192.168.1.1	52:34:B7:21:67:C1
192.168.1.42	20:85:A3:43:F3:E1

Arp Cache Poisoning

- 1º passo: Identificar o MAC Address da vítima e do default gateway

Arp Cache Poisoning

- 1º passo: Identificar o MAC Address da vítima e o default gateway
- Solução: arp request e arp reply

Arp Cache Poisoning

- 1º passo: Identificar o MAC Address da vítima e o default gateway
- Solução: arp request e arp reply

origem: 20:85:A3:43:F3:E1
destino: FF:FF::FF:FF:FF

operação: “who-has”

ip destino: 192.168.1.69

…

arp request (vítima)

Arp Cache Poisoning

- 1º passo: Identificar o MAC Address da vítima e o default gateway
- Solução: arp request e arp reply

origem: 20:85:A3:43:F3:E1
destino: FF:FF::FF:FF:FF

operação: “who-has”

ip destino: 192.168.1.1

…

arp request (default gateway)

Arp Cache Poisoning

- 1º passo: Identificar o MAC Address da vítima e o default gateway
- Solução: arp request e arp reply

origem: E1:47:1C:23:39:4B
destino: 20:85:A3:43:F3:E1

operação: “is-at”

ip origem: 192.168.1.69

…

arp reply (vítima)

Arp Cache Poisoning

- 1º passo: Identificar o MAC Address da vítima e o default gateway
- Solução: arp request e arp reply

origem: 52:34:B7:21:67:C1
destino: 20:85:A3:43:F3:E1

operação: “is-at”

ip origem: 192.168.1.1

…

arp reply
(default gateway)

Arp Cache Poisoning

- 2º passo: “envenenar” o arp cache da vítima na linha do default gateway, preenchendo com o meu MAC address

Arp Cache Poisoning

- 2º passo: “envenenar” o arp cache da vítima na linha do default gateway, preenchendo com o meu MAC address
- Solução: fake arp reply

Arp Cache Poisoning

- 2º passo: “envenenar” o arp cache da vítima na linha do default gateway, preenchendo com o meu MAC address
- Solução: fake arp reply

origem: 20:85:A3:43:F3:E1
destino: E1:47:1C:23:39:4B

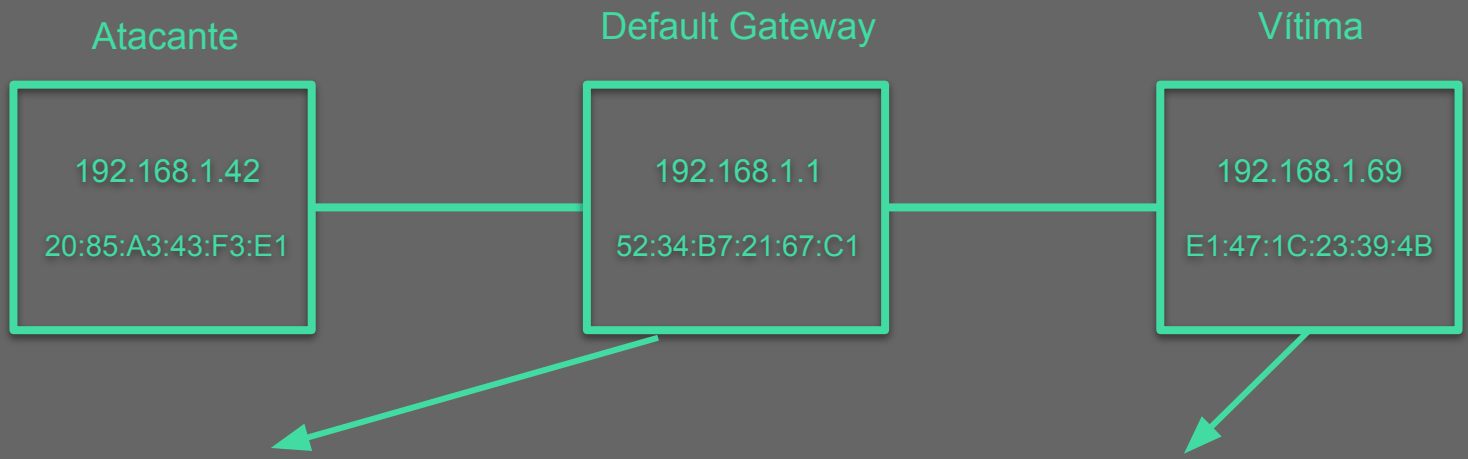
operação: “is-at”

ip origem: 192.168.1.1

…

fake arp reply (default gateway)

Arp Cache Poisoning



IP	MAC Address
192.168.1.42	20:85:A3:43:F3:E1
192.168.1.69	E1:47:1C:23:39:4B

IP	MAC Address
192.168.1.1	20:85:A3:43:F3:E1
192.168.1.42	20:85:A3:43:F3:E1

Arp Cache Poisoning

- 3º passo: “envenenar” o arp cache do default gateway na linha da vítima, preenchendo com o meu MAC address
- Solução: fake arp reply

origem: 20:85:A3:43:F3:E1
destino: 52:34:B7:21:67:C1

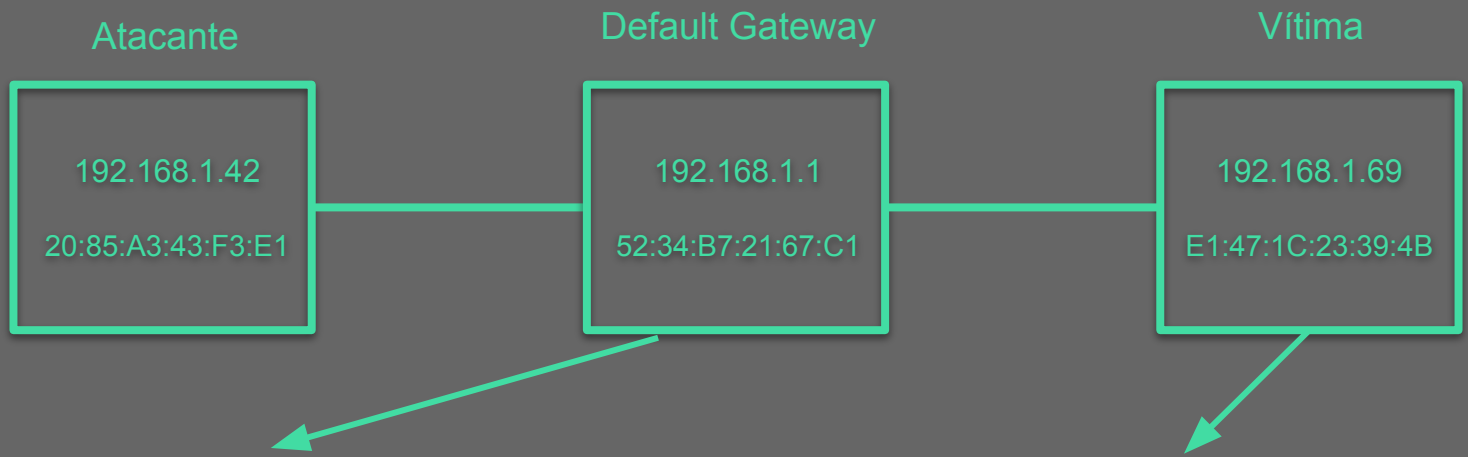
operação: “is-at”

ip origem: 192.168.1.69

…

fake arp reply (default gateway)

Arp Cache Poisoning



IP	MAC Address
192.168.1.42	20:85:A3:43:F3:E1
192.168.1.69	20:85:A3:43:F3:E1

IP	MAC Address
192.168.1.1	20:85:A3:43:F3:E1
192.168.1.42	20:85:A3:43:F3:E1

ICMC USP SÃO CARLOS

Ganesh

Grupo de Segurança da Informação
ICMC / USP - São Carlos, SP
ganesh.icmc.usp.br
ganesh@icmc.usp.br