

基于VIRTUABOX的局域网 中间人攻击

14信安 许倩玉

《识汝不识丁》番外小剧场之《请柬》

主演：



陶墨



顾弦之



崔炯



陈文帝

编剧：许倩玉

温馨提示：

直男直女请在黄大大陪同下观看收听

一场丹砂宴
只为娶一人
十月十四
敬约光临



原本，剧情应该是这样的



红衣丹砂长街宴



叩拜一生彻夜聊



“从今天起，我们将携手到老。”

“你我都不会再娶妻生子。”

“只守着彼此度过一生。”

然而，天朝广电怎么可能让你们在一起！！！！

于是乎。。。。



陈文帝：“兹事体大，弦之可要三思啊。”

顾弦之：“弦之心意已决，圣上不必再劝。”



陈文帝：“顾弦之，孤问到底你认不认错！”

顾弦之：“圣上明鉴，弦之无错。”



执手相看泪眼，竟无语凝噎

那么，问题来了：陈文帝是怎么得到消息的呢？

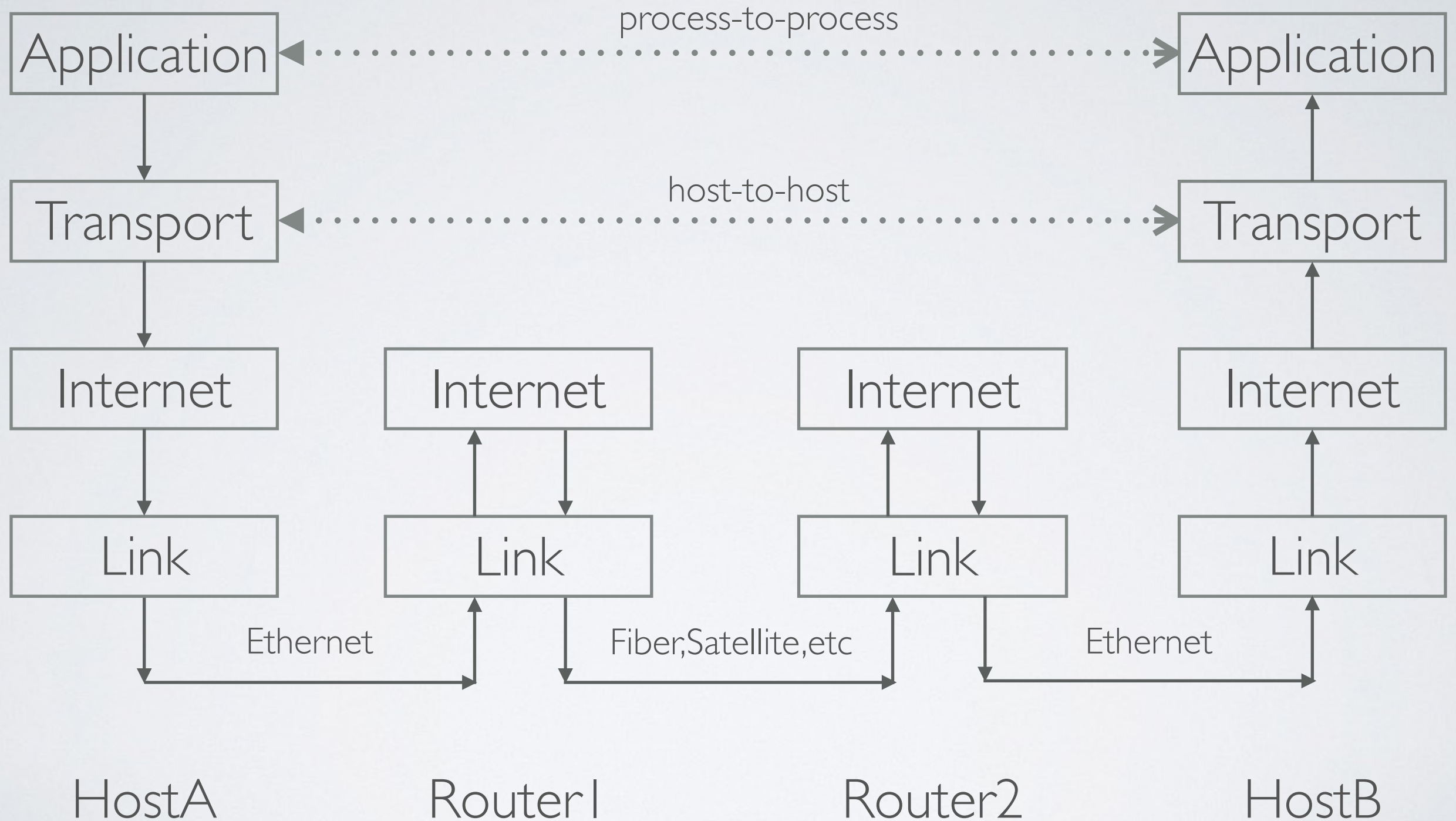


崔炯：“把你安在他们身边这么久，是时候派上用场了。”

中间人攻击

ARP缓存投毒

Data Flow



实验过程



- kali_attacker** (备份 1)
已关闭
- windows_target** (备份 1)
已关闭
- kali_gateway**
已关闭

常规

预览

VirtualBox - 网络



活动	名称
<input checked="" type="checkbox"/>	NatNetwork

☒ 启用网络(E) 仅主机(Host-Only)网络(H)

网络名称(N): NatNetwork

网络 CIDR: 10.0.2.0/24

网络选项: ☒ 支持 DHCP☐ 支持 IPv6☐ 建议默认 IPv6 路径(R)

端口转发(P)

取消

确定



取消

确定

主机音频驱动: CoreAudio
控制芯片: ICH AC97

网络

网卡 1: Intel PRO/1000 MT 桌面 (网络地址转换(NAT))

USB设备

USB 控制器: OHCI, EHCI
设备筛选: 1 (1 活动)

共享文件夹

共享文件夹: 1

描述

空

kali_attacker



命令提示符

Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\windows_xp>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

Connection-specific DNS Suffix .	:	
IP Address	:	10.0.2.15
Subnet Mask	:	255.255.255.0
Default Gateway	:	10.0.2.2

C:\Documents and Settings\windows_xp>

GateWay: 10.0.2.2

Target

IP: 10.0.2.20

MAC: 08:00:27:36:92:31

Gateway

IP: 10.0.2.10

MAC: 08:00:27:22:3d:bf

Attacker

IP: 10.0.2.5

MAC: 08:00:27:39:03:e1

实验工具： arpspoof

转发功能

剧情版权鸣谢：《识汝不识丁》剧组

实验技术鸣谢：黄玮、陈安莹、Google

谢谢观赏！