Behavioral Analysis – Networking Edition

Malware

Shamoon – August 2012

- Cyber warfare against Saudi Aramco and Qatar RasGas
- Capabilities
  - Dropper – Creates 'NtsSrv' for persistence. 32 and 64 bit versions
  - Worm – Spreads computer-to-computer across network
  - Locate targeted files, exfiltrates them, and then erases them
  - Overwrites the master boot record of system 😈
  - "Logic bomb" – Data wiping payload scheduled to execute on all systems on Aug 15 2012 at 11:08am – Right before Ramadan holiday to delay detection
- Impact
  - 30,000 Windows computers overwritten at Saudi Aramco (75% of enterprise systems)
  - Weeks of downtime and system restoration fun for IT staff

Shamoon – Politically Motivated

"We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action. One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people. In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours."

The Full Shamoon

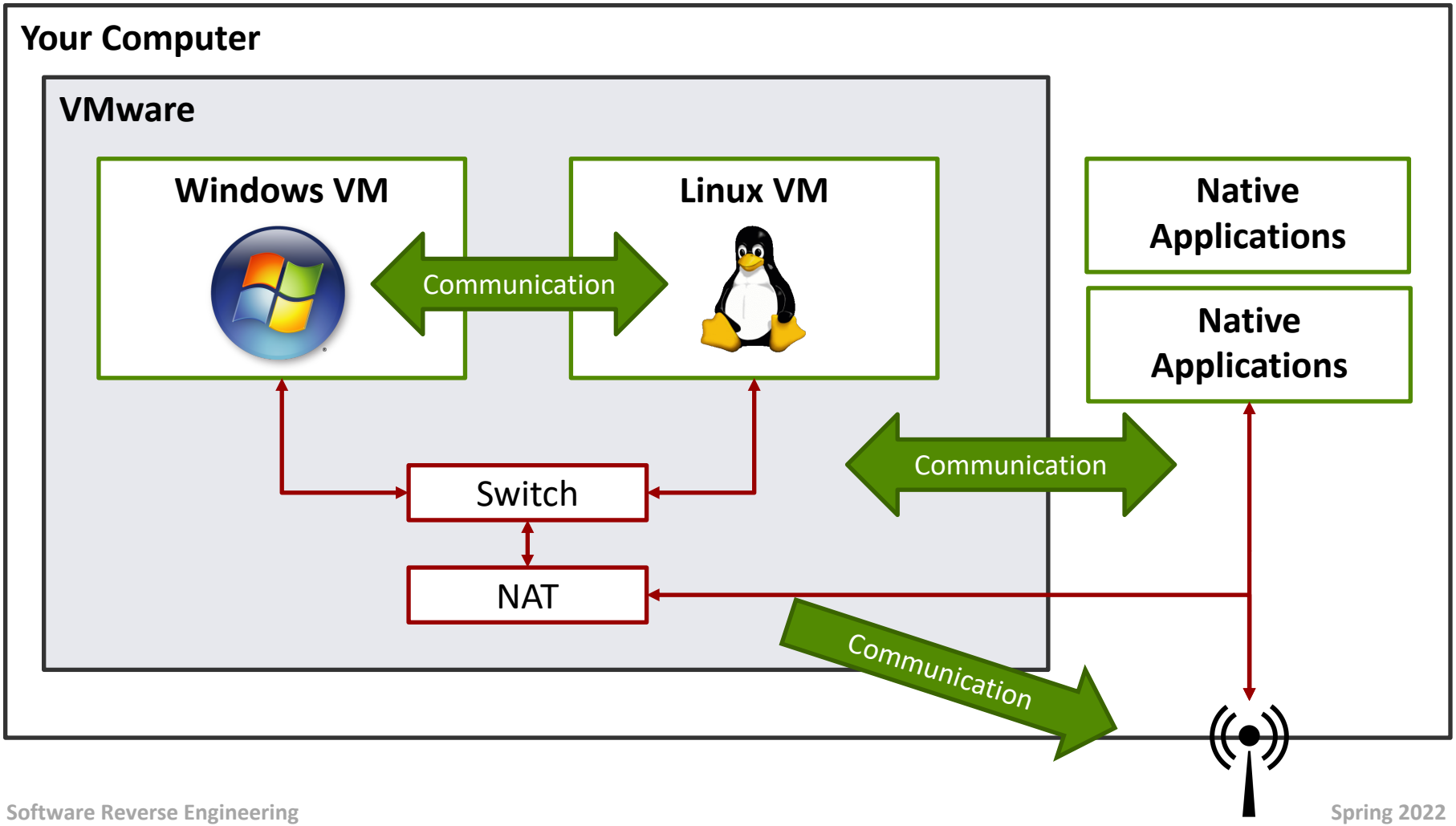
https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/

Shamoon

- MD5 for 2012 variant (Shamoon 1.0):
  `d214c717a357fe3a455610b197c390aa`
- https://www.virustotal.com/#/file/f9d94c5de86aa170384f1e2e71d95ec373536899cb7985633d3ecfdb67af0f72/
- http://contagiodump.blogspot.com/2012/08/shamoon-or-disttracka-samples.html

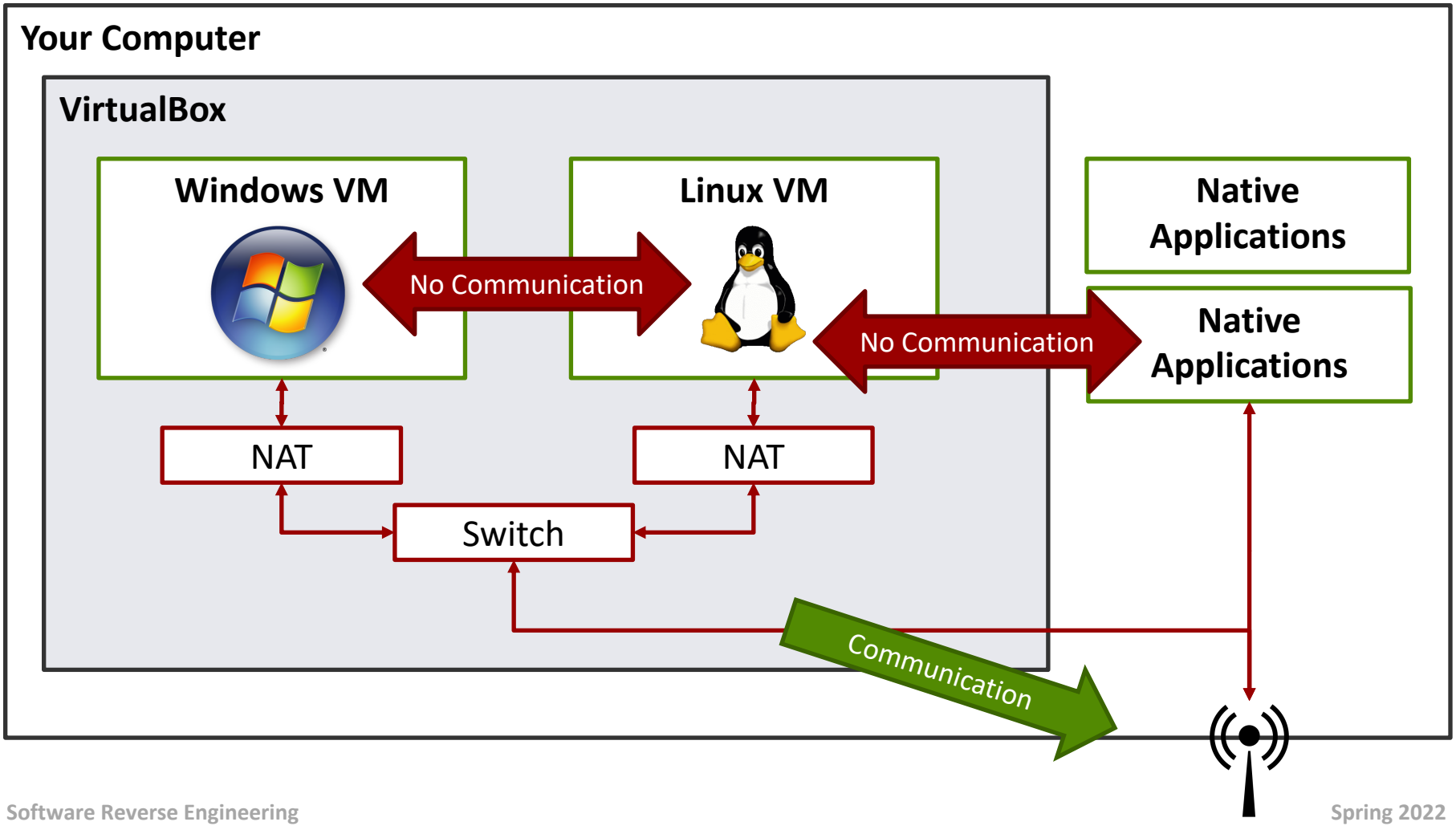
Networking

VMware Networking



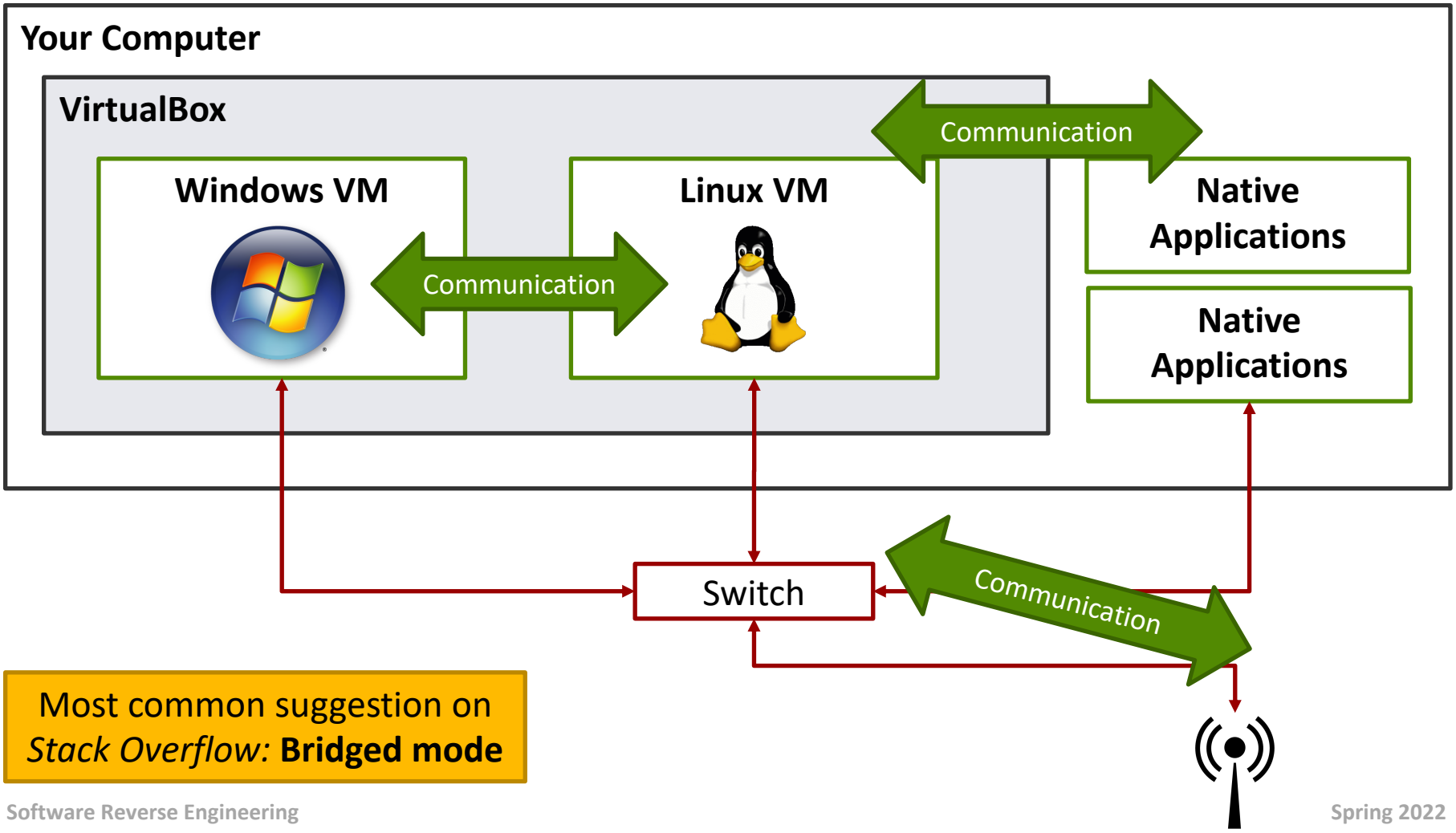
The isolation of VMs is an *intentional* design feature

VirtualBox Networking



"VirtualBox makes me sad..."
~ The Cat

VirtualBox Option: Bridged Network



Most common suggestion on *Stack Overflow:* **Bridged mode**

VirtualBox Option: Bridged Network

- **Bridged = "As if you had 3 computers all plugged into the same network switch"**
- **Pros**
  - Everyone (VMs, host OS, even remote PCs) can communicate
  - No annoying NAT in the way
- **Cons**
  - All your VMs are *directly* on the network (e.g. PacificNet)
    - Isolation? Protection? Easier to make a mistake
  - If you *manually* configure the IP address assignment – such as to force Windows to use Linux as a default gateway – it will be very easy to accidentally pick an IP already in use by a classmate
  - Wireshark will capture more *external* noise
  - Will need to reconfigure manual addresses each time you change physical network (e.g. lab WiFi to home WiFi)
  - Not all network administrators tolerate multiple hosts on same interface

VirtualBox Options

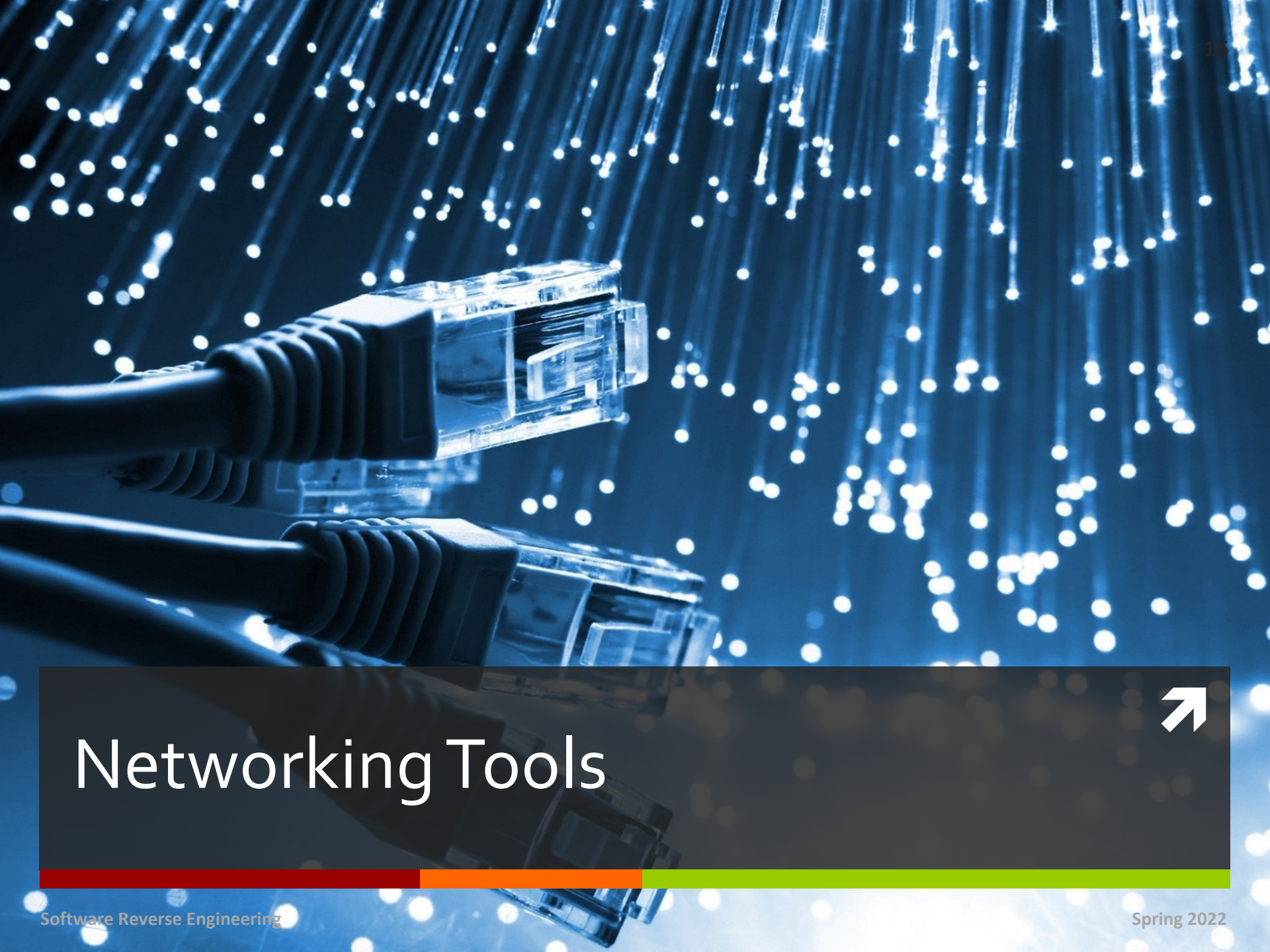
	VM ↔ Host	VM ↔ VM	VM -> Internet	VM <- Internet
NAT			✅	Port Forwarding
Bridged	✅	✅	✅	✅

For REM labs, we don't need VM ↔ Host or VM<-Internet

https://www.virtualbox.org/manual/ch06.html#networkingmodes

VirtualBox

- Oracle VM VirtualBox: Networking options and how-to manage them
  - https://blogs.oracle.com/scoter/networking-in-virtualbox-v2
- Manual
  - https://www.virtualbox.org/manual/ch06.html#networkingmodes



Networking Tools

Networking Tricks

- We're already configured our Windows VM (running malware) to use the REMnux Linux VM as its *default gateway* and as its *default DNS server*
- We *could* just forward to the public Internet, but that is an uncontrolled environment 😈
- **What can we do with the network traffic within our VM sandbox?**
  - Intercept and monitor all traffic
  - Tamper with DNS
  - Tamper with HTTP
  - Tamper with <any service>

accept-all-ips

- Shell script that configures Linux network stack. OS will accept data to *any* IP address as-if it was its own
- Purpose?
  - Malware tries to communicate with <IP in Russia> but is really communicating with REMnux
- Usage
  - `accept-all-ips start`
  - `accept-all-ips stop`

httpd

- Built-in Nginx webserver in REMnux
- Purpose?
  - Malware wants to communicate with a webserver – let's give it one and see what happens next
- Usage
  - `httpd start`
  - `httpd stop`

fakedns

- DNS emulator
- Purpose?
  - Malware wants to communicate with `suspect-domain.com`
  - Instead of querying public DNS, just return <IP of REMnux> and have the malware communicate with Linux
- Usage
  - `fakedns` (CTRL-C to exit)

inetsim

- Internet Services Simulation Suite
  - Simulates common network services
  - HTTP/HTTPS, SMTP, POP3, DNS, FTP, TFTP, NTP, IRC
- Purpose?
  - Malware sends HTTP to download `malware.exe` – inetsim can respond with its own binary
- Usage
  - `inetsim` (CTRL-C to exit)

wireshark

- Network packet capture
- *Just a reminder that it's preferrable to run Wireshark in Linux, as opposed to in the Windows VM running the malware*
  - Less noise produced in tools like Process Monitor
  - One less tool for the malware executable to detect and be suspicious of
- Usage
  - `wireshark`

Lab 3

Now you can proceed to the networking section! ☺