National College of Ireland

NETWORK SECURITY AND PENETRATION TESTING

Lab 1:
Pentesting Lab Setup

Dr. Arghir-Nicolae Moldovan
arghir.moldovan@ncirl.ie

National College of Ireland

OVERVIEW

- In this lab we will look at how we can setup a virtual pentesting lab for practicing penetration testing skills and gaining practical experience.
- **By next week**, you must have a functional lab with at least an attacking VM and a target VM
- Key elements of setting up this environment will be gaining skills and experience in areas such as:
  - Virtualisation
  - Operating system installation and configuration
  - Virtual network configuration

National College of Ireland

MOTIVATION

- **Hacking devices you don't own without permission is illegal!**
- You should not perform pentesting on systems/networks that you do not own or do not have explicit written permission to attack!
  - There are vulnerable systems/networks that may crash on port scan.
  - There are security administrators within NCI and in most other IT infrastructures.
  - Your pentesting environment is **NOT** a malware analysis environment and generally will not be sufficiently secured to prevent virulent malware from escaping.
- **So how can we safely practice and learn pentesting?**
  - Setup your own pentesting lab (incl. understand virtual machine networking)
  - Pentesting labs as a service

SETTING UP YOUR OWN LAB

PENTESTING LAB SETUP

- **Why to do it?**
  - Get to practice additional skills (virtualisation, networking, etc.)
  - Get to better understand why networks/systems are vulnerable by having to setup/install and configure them.
  - You own it, and have complete freedom to choose the pentesting distros, tools, etc.
  - You can start small and add complexity as you need it.
  - Understanding every element of your own network will greatly assist you in pentesting other networks.

National College of Ireland

PENTESTING LAB SETUP

- We will cover the following critical areas which are part of the lab setup
  - Pen testing lab environment types
  - Hardware requirements
  - Planning and scoping
  - Operational security
  - Backup

PENTESTING LAB TYPES

- Few options to setup your own pentesting lab
  - **Basic lab:** multiple VMs on your laptop (1 HW machine)
  - **Hardware lab:** if you have spare hardware (more than 1 PC)
  - **Cloud lab:** uses cloud computing (IaaS, PaaS)

- For a 10 min overview of different options check:
  - https://systemoverlord.com/2017/10/24/building-a-home-lab-for-offensive-security-basics.html

HARDWARE REQUIREMENTS

- If you have multiple laptops, desktops or a server or two you can create an excellent and diverse home network of virtual and physical machines.
- While the above is great, to complete this module you can get by with a basic setup of two VMs (attacking + target) on one decent laptop.
- To effectively setup this testing environment the laptop requirements are.
  - 8GB of RAM (16GB are recommended)
  - a modern 64-bit x86 multi-core processor (Intel i5 or superior)
  - 100+ GB of available space on the hard disk
    - If short on space you can use an external hard disk or large USB for storing the VMs
- If you CPU supports virtualising instructions this should be activated in the BIOS as it will increase performance.
  - https://en.wikipedia.org/wiki/X86_virtualization
  - How to tutorial: https://www.youtube.com/watch?v=mFJYpT7L5ag

National College of Ireland

PLANNING AND SCOPING

- Once you understand the capability of the hardware you have access to you can begin to plan your new testing environment.
- Your planning should include a document detailing the following:
  - IP ranges, subnets, DHCP range and static IP address
  - Virtual machine resource allocation including RAM, vCPU and HDD
  - User IDs, functions and passwords
  - VM Operating System, VM name and VM services (HTTP, FTP, etc.)
  - Detailed network/infrastructure diagram including IP addressing
  - Backup and data storage requirements
- Note that it is up to you if (and how detailed) you do the planning document as you are not required to submit and do not get marks for it.

National College of Ireland

BACKUP AND RECOVERY

- From time to time experimenting with your environment may break VMs, corrupt operating systems, or even damage the overall virtual machine hosting environment.
- You should:
  - Regularly take snapshots of virtual machines, and periodically take full backups of the virtual hard drives.
  - Backups are useless if they are not capable of restoring data correctly. Periodically preform a test restore from a sample backup to confirm it is functioning as intended.
  - Also preform regular backups of your primary laptop and its contents to an external hard disk.
  - If your primary laptop is encrypted, confirm that you have a copy of the encryption key stored on a separate device.

INSTALLING THE HYPERVISOR

- A hypervisor is the name given to the software which sits between the machine hardware or on the primary OS and provides the VMs with shared access to system resources.
  - https://www.youtube.com/watch?v=VtXNly_noWg
- While there many hypervisors I use Oracle VirtualBox due to it being open source and multi platform. The links/resources are mainly for VirtualBox (but feel free to use a different hypervisor like Vmware and search for alternative resources).
  - https://www.virtualbox.org/wiki/Downloads
- The full manual on VirtualBox is lengthy and complex, but it is an excellent resource
  - https://download.virtualbox.org/virtualbox/UserManual.pdf

OPERATING SYSTEM INSTALLATION

- Once the VM hosting environment has been setup you can begin the process of creating virtual machines.
- A **minimum basic lab setup** should consist of 2 virtual machines, a Kali attacking VM and a target Windows 10 or Windows Server VM (you may also add a second target, for example an Ubuntu VM)
  - Kali Linux (VMs also available) download: https://www.kali.org/downloads/
  - MS Windows 10 downloads: https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/
  - MS Windows Server download: https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019
  - Ubuntu download: https://www.ubuntu.com/download/desktop
- Oracle provide a very clear and easy to follow guide for OS installation
  - https://docs.oracle.com/cd/E26217_01/E26796/html/qs-create-vm.html
- **Notes:**
  - As NCI students you may also have free access to Windows Server through Microsoft Azure Education: https://ms.portal.azure.com/#blade/Microsoft_Azure_Education/EducationMenuBlade/software
  - While I go with Kali, if you are already familiar with it you may want to try a different distro. Start by reading through some comparison lists as there are plenty online, for example: https://itsfoss.com/linux-hacking-penetration-testing/
- **Tips:**
  - Allocate at least 30GB of hard disk space for Linux VMs and 50GB for Windows VMs
    - If short on storage space, you can place your VMs on an external HDD / USB drive
  - Choose dynamically allocated setting so that the VMs will only the space they need

VM NETWORKING

- Familiarise yourself with the various ways to setup VM networking?
  - https://www.thomas-krenn.com/en/wiki/Network_Configuration_in_VirtualBox
  - https://www.nakivo.com/blog/virtualbox-network-setting-guide/
  - https://www.virtualbox.org/manual/ch06.html

	VM ↔ VM	VM → Host	VM ← Host	VM → LAN	VM ← LAN
Not attached	–	–	–	–	–
NAT	–	+	Port Forward	+	Port Forward
NAT Network	+	+	Port Forward	+	Port Forward
Bridged	+	+	+	+	+
Internal Network	+	–	–	–	–
Host-only	+	+	+	–	–

VM NETWORKING SECURITY

- Which networking mode is the most secure?
- According to VirtualBox manual section 6.11:
  - The NAT attachment type is the slowest and most secure of all attachment types
  - However, there is no explanation why
- A lot of debate on NAT vs. bridged on the web
  - https://www.bleepingcomputer.com/forums/t/603217/virtualbox-how-to-run-a-vm-safely
  - https://www.wilderssecurity.com/threads/virtualbox-better-to-use-nat-or-bridged-adapter-for-a-malware-test-machine.360353/
  - NAT network
    - VM traffic goes through the host and you have little control on it (e.g., cannot filter it with firewalls).
    - However, each NAT networked VM has their own virtual router and is isolated.
    - Services running on the VM are not visible externally (without port forwarding).
  - Bridged network
    - Vulnerable VMs are connected directly to the external work/home network
    - Could potentially spread malware.
    - Malicious users on the network could potentially attack the VMs.
    - However, you can setup firewalls on the guest and host/network and filter the traffic (**but will you?**)

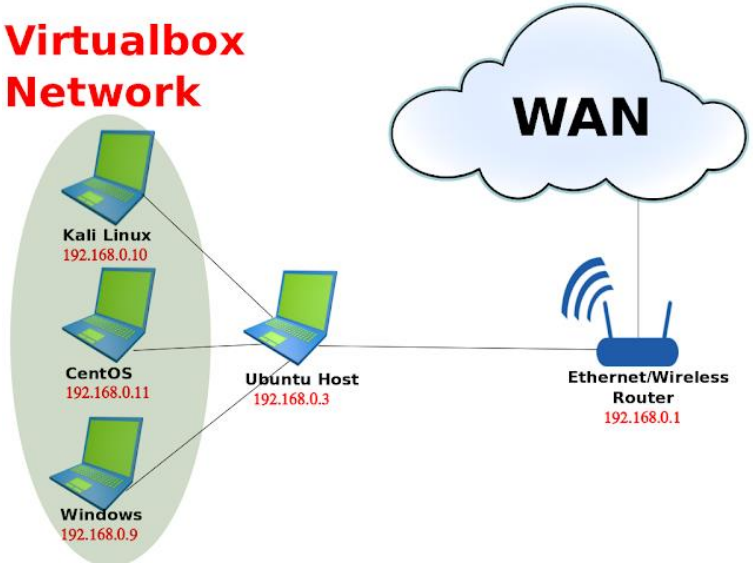
OPERATIONAL SECURITY

- Some best practice tips
  - Familiarise yourself with your VMs before interacting with an external network.
  - Suspend the VMs when not in use
  - Use the right connection for the task you have to perform.
  - Set-up two network adapters for each VM (e.g., NAT + internal/host-only)
  - When you don't need Internet access, disable the NAT adapter and use only the internal adapter.
- If using bridged network, ensure that
  - All local network shares are free of sensitive data
  - Network attacking tools or port scanners are not automatically operating
  - Bridged or accessible VMs are adequately secured with strong access credentials
  - Firewalls are properly configured
- In VirtualBox disable
  - Shared Folders
  - Drag and Drop
  - Shared Clipboard

BASIC LAB SETUP WITH 2/3 VMS

Steps

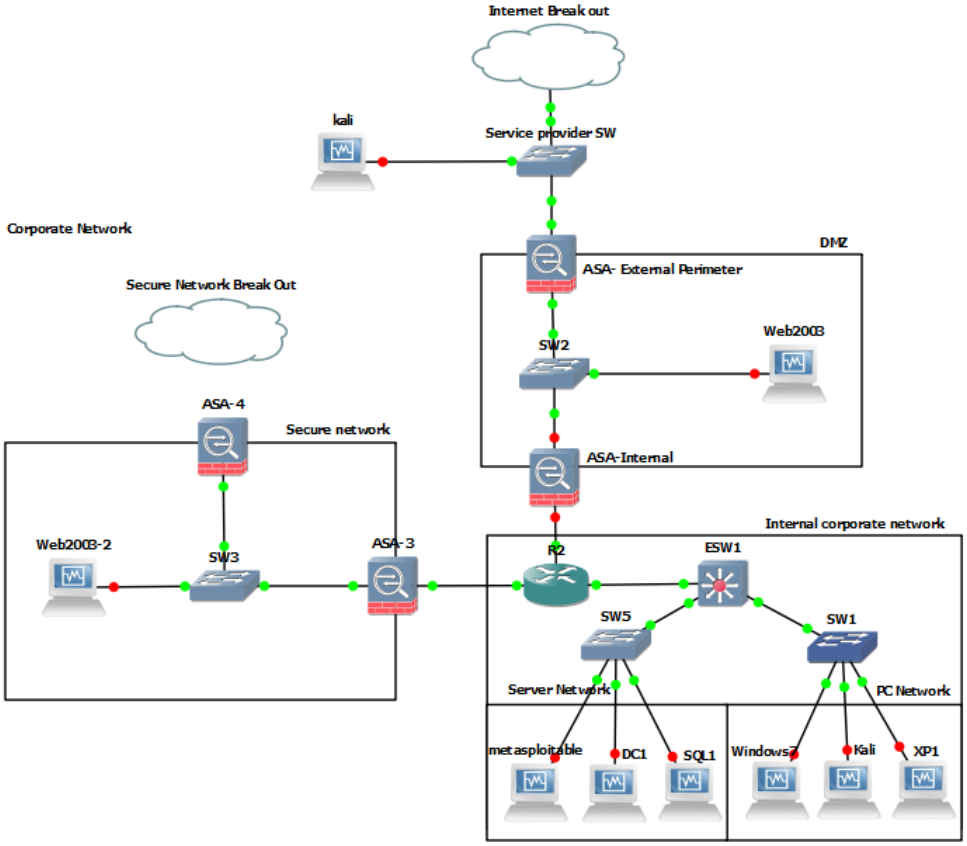
1. Install VirtualBox (personal preference but you can use VMware, Parallels, etc.)
2. Install Kali Linux as attacking machine. Download the pre-made VM **or** follow an installation tutorial:
   https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/
   https://www.youtube.com/watch?v=irGTD6jmYhc
3. Install a Windows 10 / Server target machine.
4. Optionally also install a Linux target machine (e.g., Ubuntu).
5. Install VirtualBox Guest Additions (not needed if using the pre-made Kali VM):
   https://www.kali.org/docs/virtualization/install-virtualbox-guest-additions/
6. Configure your network (see previous slides for resources and security tips)



Source: http://www.thegeeky.space/2015/06/how-to-set-and-run-bridge-virtual-network-on-CentOS-Kali-Linux-Windows-in-Virtualbox-with-practical-example.html

MORE ADVANCED LAB SETUP

- You can add complexity to your lab by using network simulators / emulators
- A list of open source simulators:
  - http://www.brianlinkletter.com/open-source-network-simulators/
- Cisco Modeling Labs
  - https://developer.cisco.com/modeling-labs/
- Pentesting in GNS3
  - https://linuxtiwary.com/2020/02/24/network-security-and-penetration-testing-complete-lab-setup-using-gns3/
- Kali Linux on Eve-NG
  - https://bsnetworking.wordpress.com/2017/02/06/kali-linux-on-eve-ng/



https://www.adamcouch.co.uk/labs-projects/penetration-testing-in-gns3/

INTO THE CLOUD

- Once you have a firm grasp of virtualisation, operating system configuration and virtual networking you can look into creating a pentesting lab hosted in the cloud (IaaS / PaaS services from AWS, Azure, Google Cloud, etc.)
- Pros
  - Plenty of virtualised HW resources to setup more complex testing environments, can be accessed remotely
  - Some cloud provider offer nested virtualisation solutions, see:
    - https://www.cloudshare.com/virtual-it-labs-glossary/what-is-nested-virtualization/
    - https://blogs.oracle.com/ravello/kali-linux-security-pen-test-on-aws
    - https://www.cloudshare.com/question/what-is-an-alternative-to-oracle-ravello/
- Cons
  - Cost (pay per usage), need to carefully read their T&Cs to and understand what you are allowed to (not to) do, need for segregated virtual network between VMs not to compromise other users
  - There may be restrictions in place and may require you to get authorisation from the cloud provider, see:
    - https://aws.amazon.com/security/penetration-testing/
- **Note:** You should not use the cloud until you conquered the challenge of setting up your own environment (required for the labs practice), and you should not do penetration testing in the cloud without proper research, setup and permission.

RESOURCES / TUTORIALS

- G. Weidman 2014, *Penetration Testing: A Hands-On Introduction to Hacking*, No Starch Press
  - "Chapter 1: Setting Up Your Virtual Lab"
- Plenty of online resources/tutorials
  - https://systemoverlord.com/2017/10/24/building-a-home-lab-for-offensive-security-basics.html
  - https://resources.infosecinstitute.com/how-to-make-your-own-penetration-testing-lab/#gref
  - From HackerSploit: https://www.youtube.com/watch?v=eHwRH549qUc
  - PentestBox suite for Windows: https://pentestbox.org/
- You should search for recent resources (as older ones may not work)

PENTESTING LABS AS A SERVICE

PENTESTING LABS AS A SERVICE

- A number of providers offer remote access to pentesting labs
  - Offensive Security https://www.offensive-security.com/
  - Virtual Hacking Labs https://www.virtualhackinglabs.com/
  - PentesterLab https://pentesterlab.com/
  - eLearnSecurity https://www.elearnsecurity.com/
  - Practical Pentest Labs https://practicalpentestlabs.com/
  - Hacker Dojo https://hackerdojo.com/
- Pros
  - Comprehensive setups, training materials, many challenges, certifications, etc.
- Cons
  - Can be expensive, usually tired subscription based (some offer free but limited access, others offer discounted student rates)
  - You miss out on key learning opportunities
  - Some are not suitable for network pentesting (e.g., platforms that focus only on web pentesting, CTF platforms where you do small tasks to collect points, etc.)

National College of Ireland

PENTESTING LABS AS A SERVICE

- Some free/affordable alternatives
  - CTF365 https://ctf365.com/
  - Hack The Box https://www.hackthebox.eu/
  - Root Me https://www.root-me.org/
  - Pentestit https://lab.pentestit.ru/
  - TryHackMe https://tryhackme.com/
  - Hacking-Lab https://www.hacking-lab.com
  - Ghost Lab http://www.gh0st.net/
- Other
  - VulnHub (many downloadable VMs) https://www.vulnhub.com/
  - Immersive Labs (browser based) https://immersivelabs.co.uk/
  - HackThisSite (challenges, CTFs) https://www.hackthissite.org/
  - OverTheWire (fun-filled games) http://overthewire.org/wargames/
  - AwsomeCTF (curated list) https://github.com/apsdehal/awesome-ctf#wargames
  - WeChall (list of CTF platforms and rankings) https://www.wechall.net/active_sites
  - Another list: https://wheresmykeyboard.com/2016/07/hacking-sites-ctfs-wargames-practice-hacking-skills/

National College of Ireland

TASKS - LAAS

- Visit the websites listed on the previous two slides, and check info on
  - Price plans
  - Technical details / architectures of the labs
  - If they offer training materials
  - If they offer competitions, challenges
  - If they offer certifications
  - Etc.
- Form groups and discuss how you could use these services to complement your learning and improve your skills.

TASKS - LAB SETUP

- Start to setup a basic virtual lab environment on your laptop
- **By next week**, you must have a functional lab with at least 2 VMs
  - A Kali Linux attacking VM
  - A Windows 10 / Windows Server target VM
- It will take the average student a few hours to work out how to use VirtualBox and get this environment functioning correctly with networked VMs and services.
- Working in groups and sharing prior expertise is highly encouraged.

ADDITIONAL TASKS

- After setting up a basic pen testing lab practice various basic operations.
- Practice with Linux commands. A good starting point tutorial:
  - https://diyhacking.com/linux-commands-for-beginners/
- Explore Kali Linux
  - Navigate through the list of applications
- Practice Basic Networking commands
  - Find the IP address of your host and VM machines
  - Check that you can ping and traceroute between machines and the Internet (8.8.8.8)
  - Adapt the ping command to only send 5 pings and then stop
  - Use the route command to look up your routing table.
    - What network class are you in?
  - Check the network connections using netstat command
    - See http://www.binarytides.com/linux-netstat-command-examples/
    - What services are listening on your machine (if any)?
  - Look up your ARP table using the arp command

National College of Ireland

NEXT STEPS: SPINNING UP SOME SERVICES

- Configure one of your VMs (e.g., the Windows 10 / Windows Server target VM) to act as a server running different services
  - E.g., HTTP(s) server hosting a website, Telnet server, SSH server, FTP server, remote desktop or VNC, Active Directory
  - **Do not install vulnerable apps on your host / production machine!**
- Configure one VM as your client machine, equipped with client applications
  - E.g., Internet browser, Telnet client, SSH client, FTP client, AD client
  - Note that you can also use the Kali VM (which comes with a lot of client applications) or your host OS if you do not have a separate client VM
- Practice accessing the services, HTTP, Telnet, SSH logins, accessing FTP shares.