Raleigh, NC ISSA Information Systems Security Association

Capture The Flag Challenge Prep Class

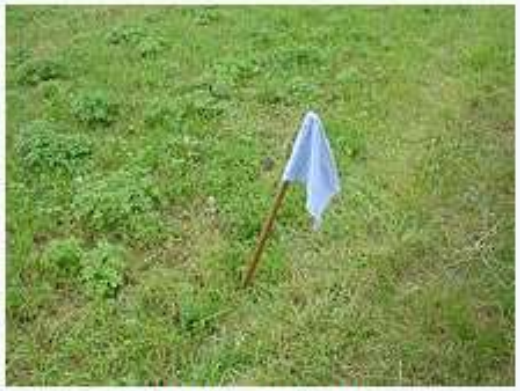
Raleigh, NC ISSA Information Systems Security Association

CTF???

- A traditional outdoor game where two teams each have a flag (or other marker) and
- The objective is to capture the other team's flag, located at the team's "base," and bring it safely back to their own base.

-- **Wikipedia**

Capture the Flag

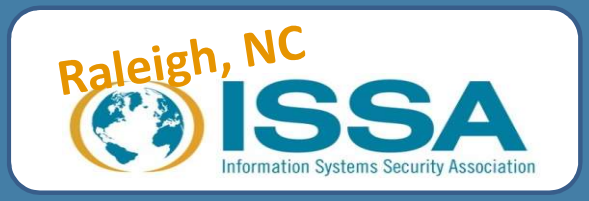


An uncaptured flag

Players	Large group, more than 6 players in a team
Skill(s) required	endurance, observation, strategy

Capture the flag in Computer Security

- Is a competition to capture as many “flags”.
- May be played between teams (blue vs. red) or by many against one.
- Typically requires participants to employ variety of skills in ethical hacking or pen-testing
  - System administration
  - Programming
  - Cryptanalysis
  - Network sniffing
  - Protocol analysis
  - Reverse-engineering, etc.
- Goal is to identify and carry out attacks against vulnerable systems to find clues that will lead them to additional vulnerabilities or clues.



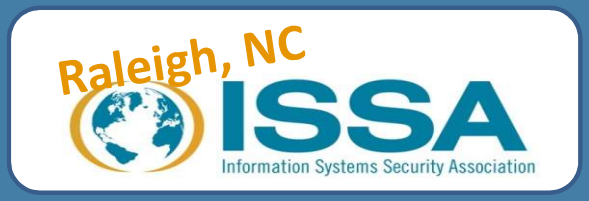
CTF Preparation Class

- Today's Goal
  - Build a small, safe environment that can be used for learning and practicing popular techniques and tools for CTF challenges.
- What we will cover
  - How to install VM software
  - How to install Kali
  - How to install vulnerable virtual machines (VM) as practice targets
  - Additional resources

Raleigh, NC ISSA Information Systems Security Association

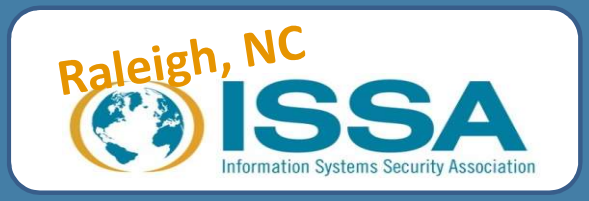
Required Items

- Laptop – preferably later models with at least 40 GB of free hard drive space
- Download the following before you come to the class
  - VirtualBox – Just because it is free and popular
    - Windows hosts download
    - OS X hosts download
    - Linux distributions
  - Kali - https://www.kali.org/downloads/
    - Kali 64 bit ISO
    - Kali 32 bit ISO
    - You need only one. And get 32-bit one if you aren't sure which one to get.
  - Practice targets
    - UltimateLAMP - https://sourceforge.net/projects/lampsecurity/
    - Metasploitable 2 - https://sourceforge.net/projects/metasploitable/
- Desire to learn and no shame



Flow

- Overview of test environment
- Creation of test lab
  - Installation of virtualization software
  - Installation of Kali
  - Installation of targets
- Get to know the environment
  - Using Kali
  - Practice with UltimateLAMP
- Additional resources



Test/Lab Environment

- Host
  - Windows or Linux system with virtualization software
- Targets
  - Systems or applications that hide “flags”
  - Systems running applications or processes with vulnerability
- Attack system
  - Kali VM
- Test network
  - Private, isolated network
  - Block traffic to and from outside networks, especially to and from the vulnerable targets
  - But allows the attack system and target nodes to communicate
  - Created using virtualization software

Install VMware / VirtualBox

- Oracle VirtualBox
  - Installation Details: https://www.virtualbox.org/manual/ch02.html
  - Intro: https://www.virtualbox.org/manual/ch01.html#intro-installing
- VMware Player
  - Downloading and installing
  - https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2053973

Networking Modes - VirtualBox

- Network Address Translation (NAT)
  - If all you want is to browse the Web, download files and view e-mail inside the guest, then this default mode should be sufficient for you, and you can safely skip the rest of this section. Please note that there are certain limitations when using Windows file sharing (see Section 6.3.3, “NAT limitations” for details).
- NAT Network
  - The NAT network is a new NAT flavour introduced in VirtualBox 4.3. See 6.4 for details.
- Bridged networking
  - This is for more advanced networking needs such as network simulations and running servers in a guest. When enabled, VirtualBox connects to one of your installed network cards and exchanges network packets directly, circumventing your host operating system's network stack.
- Internal networking
  - This can be used to create a different kind of software-based network which is visible to selected virtual machines, but not to applications running on the host or to the outside world.
- Host-only networking
  - This can be used to create a network containing the host and a set of virtual machines, without the need for the host's physical network interface. Instead, a virtual network interface (similar to a loopback interface) is created on the host, providing connectivity among virtual machines and the host.

Raleigh, NC ISSA Information Systems Security Association

Networking Modes – VirtualBox

	VM ↔ Host	VM1 ↔ VM2	VM → Internet	VM ← Internet
Internal	–	+	–	–
Host-only	+	+	–	–
NAT	–	–	+	Port forwarding
NAT Network	–	+	+	Port forwarding
Bridged	+	+	+	+

Networking Types - VMware

- **Host-only networking**
  - Used in isolated test environments where virtual machines do not need to communicate with other environments.
  - Connects virtual machines to a private LAN shared only by their host machine and any other virtual machines also using host-only networking.
  - Other host machines on the host LAN cannot communicate with the virtual machines.
  - The default network adapter interface is vmnet1.

Networking Types - VMware

- **Network Address Translation (NAT) networking**
  - Used in environments where virtual machines do not provide services but still need to access a network.
  - Connects virtual machines to an external network using the host machines IP address for external communication.
  - Connects virtual machines to the Internet through their host machines dial-up connection, Ethernet adapter or wireless Ethernet adapter.
  - Connects virtual machines to a non-Ethernet network, such as Token Ring or ATM.
  - Establishes a private LAN shared only by your host machine and any other virtual machines also using NAT networking.
  - Other host machines on the host LAN communicate with the virtual machines, however external host machines cannot initiate communication with virtual machines unless NAT port forwarding is also in use. NAT port forwarding causes network traffic destined for a port on a host machine to be forwarded to a specific port on a virtual machine.
  - The default network adapter interface is vmnet8.
- **Bridged networking**
  - Used in environments where virtual machines provide services or participate in a real network.
  - Connects virtual machines to the Local Area Network (LAN) of their host machine, whether wired or wireless, and allows them to connect to any other host or virtual machines (if they are also bridged) on the network.
  - Connects the virtual network adapter in a virtual machine to the physical Ethernet adapter in its host machine.
  - You can establish additional virtual bridges to use in custom configurations that require connections to more than one physical Ethernet adapter on the host computer.
  - The default network adapter interface is vmnet0.

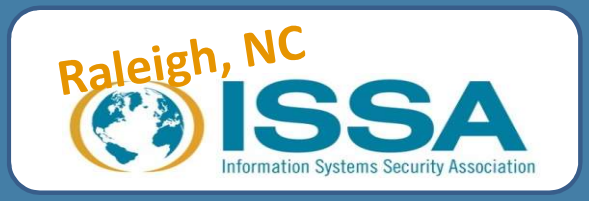
Raleigh, NC ISSA Information Systems Security Association

Kali Overview

- The new generation of the industry-leading BackTrack Linux penetration testing and security auditing Linux distribution.
- Kali is a Linux distribution specifically geared towards professional penetration testing and security auditing.
- You do not have to install Kali to use the tools. – Run it in Live mode
- You can customize Kali and run it from USB keys.
- You can install Kali on Chromebook, Raspberry Pi and other ARM devices.
- Kali Linux Tutorial - https://www.kali.org/category/tutorials/

Install Kali on Oracle VirtualBox

- **Kali Linux Installation Requirements**
- https://docs.kali.org/installation/kali-linux-hard-disk-install



Install UltimateLAMP

- Uncompress the ctf8.zip file.
- Create a virtual machine called CTF8.
  - Oracle VirtualBox
    - File -> New
    - Name: CTF8
    - Type: Linux
    - Version: Other Linux
    - Memory Size: 768 MB
    - Hard drive: Use an existing virtual hard drive file – ctf8.vmdk
    - Once the virtual machine is created, ensure the MAC address reads “0800275EA506”.
    - Check the network adapter is attached to “Internal” or “Host-only Adapter”.
  - VMware Play
    - Open and navigate to the ctf8.vmdk image, then click the “Play the virtual machine” button.
    - If prompted, choose “I moved it”.

Install Metasploitable on Oracle VirtualBox

- Metasploitable – VM created to test Metasploit
- https://information.rapid7.com/metasploitable-download.html
- **Setting Up a Vulnerable Target**
- https://help.rapid7.com/metasploit/Content/getting-started/setting-up-test-env.html

- https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide

CFT Challenge Resources

- Vulnerable VMs by design - https://www.vulnhub.com/
- Root-me.org - https://www.root-me.org/en/Challenges/
- GhostSec's pentest labs
- Hackthissite.org
- Hacking-lab
- CTF365.com - https://blog.ctf365.com/
  - Free for 30 days

VMware Tools in a Kali Guest

- https://docs.kali.org/general-use/install-vmware-tools-kali-guest

Update Kali

- Change Kali's network type to NAT or Bridged mode
- Run following commands from command line interface or Terminal
  - apt-get update
  - apt-get upgrade –y
  - apt-get dist-upgrade -y

Installing VirtualBox Guest Addition in Kali VM

- **Installing on Kali with rolling updates**
  - **echo "deb http://http.kali.org/kali kali-rolling main contrib non-free" >> /etc/apt/sources.list**
  - (*)apt-get purge virtualbox-guest-x11
  - (*)apt-get autoremove --purge
  - (*)reboot
  - apt-get update
  - apt-get dist-upgrade
  - reboot
  - apt-get update
  - apt-get install -y virtualbox-guest-x11
  - reboot
  - * Only if you previously attempted to install vitualbox guest-addition

- **Installing VirtualBox Guest Additions in Older Kali Versions**
  - apt-get update && apt-get install -y linux-headers-$(uname -r)
  - Attach the "Guest Additions" CD-ROM image.
  - cp /media/cd-rom/VBoxLinuxAdditions.run /root/
  - chmod 755 /root/VBoxLinuxAdditions.run
  - cd /root
  - ./VBoxLinuxAdditions.run
  - reboot