



IA Initiative at Hampton University

How and Why We Do the Things We Do.

**Robert A. Willis Jr.
Department of Computer Science
Hampton University**

Topics



- **Goal**
- **Collaborations**
- **Mapping**
- **Hardware and Software Configurations**
- **Lab Usage**
- **Teaching “hacking”?**
 - Resolutions
- **Conclusion**

Laboratory Configurations



- Hardware is easy, configuration is not.
- Questions:
 - What are we going to use the lab for?
 - Will we teach some of the “dangerous” topics.
 - What will the University allow?
 - Do we have the expertise to maintain the configuration?

Hardware Configuration



- An installation of Linux as a host OS was performed on one machine as a test bed with the final list of modifications performed on each machine (and tool(s) used) was as follows:
 - repartition of hdd (gparted)
 - 3 partitions created
 - 15g OS partition, 50g VM partition, 83g OS image partition
 - creation of backup image of OS partition in 83g partition (CloneZilla)
 - building of XP virtual machine image and copying into VM partition (VMWare)
 - copying 7 Linux virtual machine images to VM partition (OS copy tools)
 - backup of all virtual machine images and base XP OS image to network server and portable USB drive (OS copy tools)
- In addition, instructions to perform a backup and restore of the host OS were created.

Software Configuration: Virtuality



- An XP VMWare virtual machine was created and a clean install of Windows XP was performed in VMWare to provide a Windows guest OS. This image was copied into the 50 gig partition on each of the IA lab machines.
- Seven pre-built Linux virtual machine images were provided by the RIT team. These included CentOS5, CentOS6, Knoppix (ISO image), RedHat 8, RedHat 9, and others. These VM images were also copied to the 50 gig partition of each of the seven IA lab machines.
- With these VMs in place, regardless of host OS, both Linux and windows VMs can be running independently or simultaneously, and any or all of the features available in VMWare can be used to provide environments in isolation, or not, as appropriate.

Software Configuration: Virtuality



- Finally, a copy of AVG Free AntiVirus was installed and current updates to the virus definition files were applied to the host XP OS prior to imaging it to the 83gig partition.
- All of the VM images, as well as the host OS (XP) CloneZilla image, were backed up to the room file server AND to a portable USB drive. Restoration of the host OS on any machine is possible in approximately 10 minutes, and the guest VMs can be restored in as long as it takes to copy the VMs from either the USB drive or from the network server.

Laboratory Usage



- Used only for IA purposes.
- Used to teach any IA subject that requires “safe” computers.
- Configuration:
 - One server
 - Seven computers
 - One 24 port 10/100 smart switch
 - One printer and standalone computer.
- All but one internet connections are disabled.
 - Why?

Controversy



- Do we want to teach “destructive” topics?
 - After some discussion, we reluctantly decided that teaching “hacking” techniques with strong and continuous ethical discussions was feasible.
- This decision led to a protracted negotiation with the University’s Center for Information Technology.

Proposed Agreement



- A separate network will be created for this lab. For example, it will be configured as a subnet with a statically assigned IP address,
- The CIT will develop an ACL (access control list) on its network router allowing access to only ports 80 and 443,
- The Department of Computer Science will develop a **CONFIDENTIALITY AND NONDISCLOSURE AGREEMENT** that every student (using the lab) must sign in order to protect the University resources.
- Only students enrolled in these classes will be allowed in the room and will be closely monitored.

Proposed Agreement

A decorative graphic in the top right corner consisting of several overlapping, glowing blue rings or loops, resembling a stylized sphere or a complex network structure.

- No media allowed in classroom unless issued by professor during class.
- The PC's that will be used in this class must have Deep Freeze and/or VMWare installed; because the hacking websites all carry malware, viruses, and Trojans that may be problematic in the network;
- VMWare and Deep Freeze will reboot to a clean state after each session.
- All servers must be a part of the subnet .
- DNS entries will be from an outside DNS server (i.e.: Cox, Verizon, Yahoo)
- Local logins to will be used, since no access to any HU servers will be allowed.
- The use of only local printers is allowed.

Future Plans



- Construct a Remote Laboratory Emulation System (RLES) with assistance from RIT.
- “RLES has been used as a platform for the manipulation of virtual servers, to deploy special purpose applications, to create a secure environment for computer forensic analysis, for the investigation of viruses and malware, and for MS level graduate projects.” (Border)
- RLES is a more robust and practical solution than our present configuration.

Future Plans

- **Construct a computer forensics cluster.**



Questions

