



AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## UNIT 5

### Computer Basics and Virtualization





# Learning Objectives

- Participants will understand the internal components of a computer
  - Basic computer concepts and terminology
  - Common security issue types
- Participants will understand operating system purpose, types, and security
  - Purpose and use of operating systems
  - Major operating systems
- Participants will understand the basics of virtual computing
  - Provide overview of virtual machines, terminology, use, and architecture
  - Describe basic security risks for virtual computing (hypervisor, hosts, guests)
- Participants will gain a broad understanding of major networking components and concepts
  - Overview of basic network types, concepts, and terms/definitions
  - Cisco Networking Academy





AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

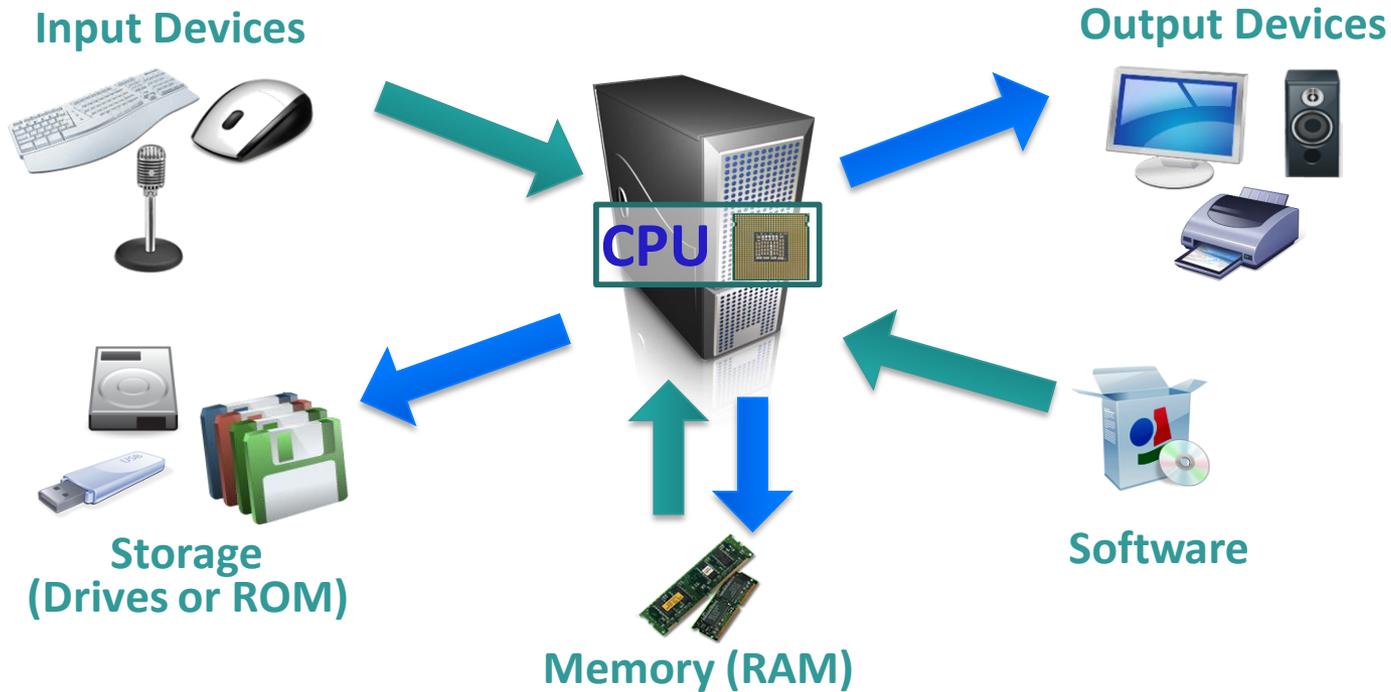
## SECTION 1

### How Computers Work





# Computer Anatomy 101



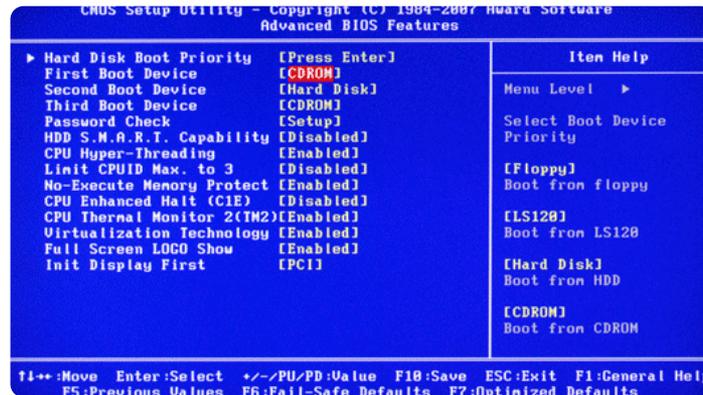
- The central processing unit (CPU) does the grunt work of the computer.
- Random access memory (RAM) saves your progress in many different software programs so that you can access that temporarily saved data later on. RAM is temporary. It is wiped when you turn off the computer.
- Storage allows use to save data more permanently. Read-only memory (ROM) is read-only and does not change often.





# Software: The BIOS

## Basic Input-Output System



Source: itprostuff.com

- Allows the **operating system** (OS) to connect with input, output, and storage devices
- Embedded on the motherboard by the manufacturers and is a permanent piece of the computer
- Connects the CPU with the OS so the computer can boot up
- Manages basic system settings like date and time and power management

Source: [www.Computer.HowStuffWorks.com](http://www.Computer.HowStuffWorks.com)





# Common Hardware/BIOS Vulnerabilities

- Backdoors – Can be built into hardware and later get exploited by attackers.
- Environmental Concerns – All hardware is susceptible to flooding, fires, and dust, which can lead to loss of capability or data if not properly stored or physically secured.
- BIOS – Can be attacked through malware that can crash the BIOS. Also can be accidentally harmed by users using unauthenticated files to update the files that have unintended consequences.
- RAM – Some malware can install itself on RAM rather than the hard drive, making them much more difficult to detect and eliminate.





# Software: Operating System

- **Examples:** Microsoft Windows, Linux, Mac OS X
- Coordinates system resources so it performs and responds predictably for the user
- Allows users to configure the computer's resources without making permanent changes to them
- Uses graphical user interface to make it easier for non-technical users to use navigate the system
- Manages the hardware/software resources so they are used efficiently by **applications**



Source: [getintopc.com](http://getintopc.com)



Source: [distrowatch.com](http://distrowatch.com)



Source: [theguardian.com](http://theguardian.com)

Source: [www.Computer.HowStuffWorks.com](http://www.Computer.HowStuffWorks.com)





# Major Operating System Families

- Microsoft Windows
  - Most commonly used operating system
  - User-friendly and used in offices and homes
  - Examples: Windows 8, Windows 10
- Linux
  - Often open-source, meaning that anyone can use or modify Linux operating systems or software
  - Many different “flavors” or significantly varied operating systems
  - Examples: Ubuntu, Debian, Mint, Fedora
- Mac
  - Distantly related to Linux operating systems
  - Generally more secure than Windows because malware is less likely to target non-Windows systems
  - Examples: OS X Lion, OS X Yosemite





# Common Operating System Vulnerabilities and Issues

- Passwords – Computers with weak or no passwords can be broken through brute force or dictionary attacks.
- File Access – Insecure permissions can give individuals more access to important files than necessary.
- Stop Error (BSOD or Blue Screen of Death) – Windows error screen caused by malware, hardware issues, or software processes that the operating system can't handle. Users are forced to restart their machine after receiving a BSOD.
- Unpatched Systems – Outdated operating systems have many known, easily exploited vulnerabilities.

```
A problem has been detected and Windows has been shut down to prevent damage to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

Technical information:
*** STOP: 0x00000001 (0x0000000000000010,0x0000000000000002,0x0000000000000000,0
x0000000000000000)

*** NDIS.sys - Address FFFFFA0FC80B5578 base at FFFFFA0FC80AD000, DateStamp
45d699f1

Beginning dump of physical memory

Physical memory dump complete.
Contact your system administrator or technical support group for further
assistance.
```

Stop Error







AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

## SECTION 2

### Virtual Machines





# What is a VM?

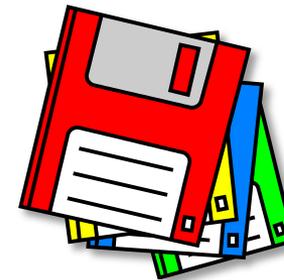
- A virtual machine (VM) is an environment, such as a program or operating system that does not physically exist, but is created within another environment
- Does not have hardware, a power supply, or other resources that would allow it to run on its own
- Essentially allows you to run a computer within your computer





# VM Terminology

- **Host [operating system]:** The OS on the physical computer on which the VM is installed
- **Guest [operating system]:** The OS the VM runs
- The Host OS and Guest OS do not need to be the same
- **Image:** Another term for VM
- **Hypervisor:** software that can create and run virtual machines (example: VMware Workstation Player)





# VM Advantages

- **Flexibility**
  - Run multiple OSES on one physical machine
- **Scalability**
  - Run multiple VMs on the same computer
- **Portability**
  - Easily transfer VMs to different computers
- **Cost**
  - Save time testing new programs or configurations on a VM rather than disrupting the host
  - Run multiple systems on the same computer (save hardware costs and floorspace)





# VM Disadvantages

- Performance depends on host machine's hardware
- Single point of failure
  - If the host fails, progress on VM is lost
- Running VMs pulls hardware resources from host machines





# VM Security

- Security Benefits
  - Unknown software can be tested on virtual machines to ensure it is secure without the risk of damage to the host machine
  - Virtual machines can be isolated enough from host that malware may only be able to infect one OS
  - Snapshots can be used to roll back VMs that have become infected
- Security Concerns
  - Hypervisors are software that can be targeted by attackers if not up-to-date
  - Software within virtual machines and the virtual machine itself must also be kept up-to-date
  - Communications between virtual machines need to be monitored as much as physical machines





# VMware Workstation Player

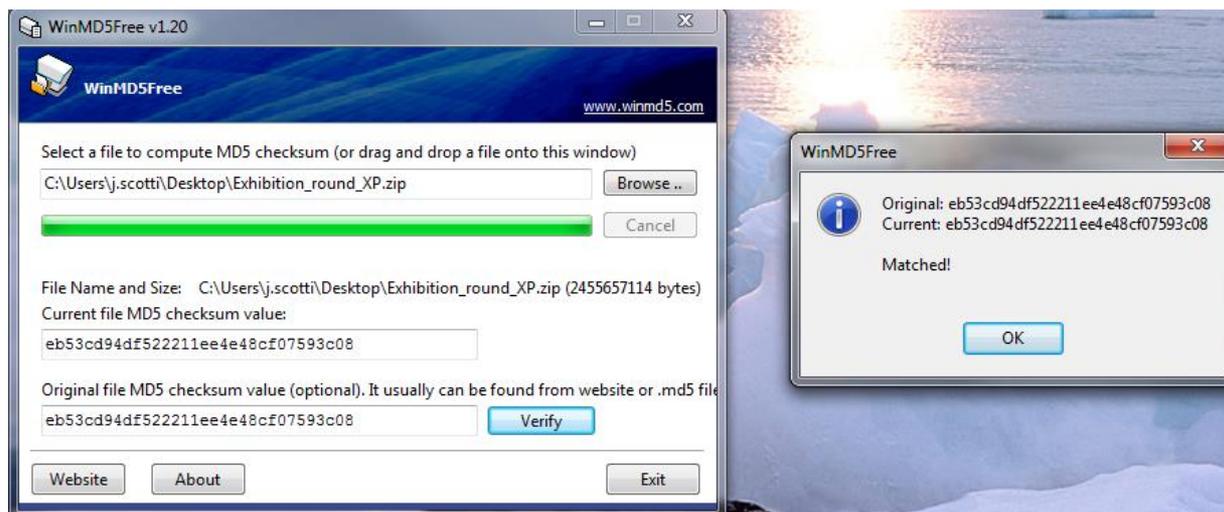
- A software program used to create and run VMs
- Used to run CyberPatriot competition images
- VMware images contain several files **that should not be modified**:
  - **\*.vmdk**: virtual disk files
    - Simulate the hard drive for your virtual system
  - **\*.vmx**: configuration files
    - Contain details such as the type of hardware to simulate for the virtual system and the amount of memory to allow the VM to use
  - **\*.nvram**: VM's BIOS files





# Checksums

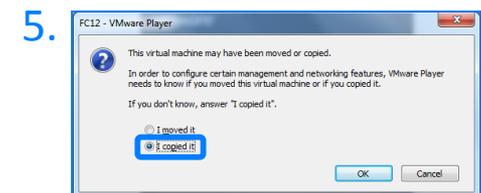
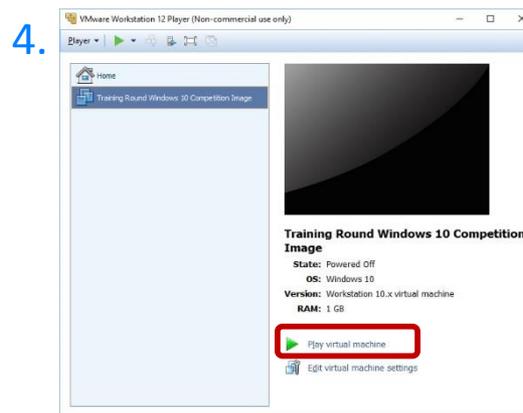
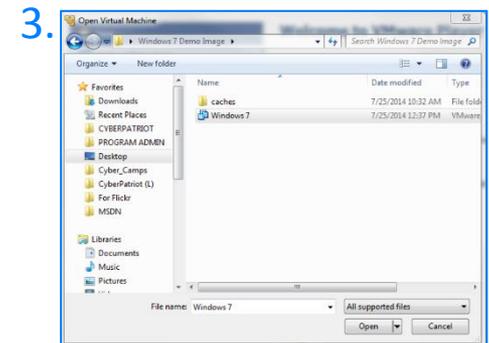
- A mathematical calculation based on the data contained in a file
- Comparing the checksum of a program you downloaded to the checksum it is supposed to have will allow you to determine if the file has been corrupted or modified
- Before each round, CyberPatriot teams must verify the checksums of the competition images to make sure the images downloaded correctly





# Opening an Image

1. Open VMware Workstation Player 
2. Click “Open a Virtual Machine”
3. Browse for and open the [.vmx](#) file in the image folder you downloaded
4. Click “Play virtual machine”
5. Select “I copied it”
6. Click “OK” on Removable Devices pop-up
7. Log into the user account specified in the StartEx email if not automatically logged in





AIR FORCE ASSOCIATION'S

# CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

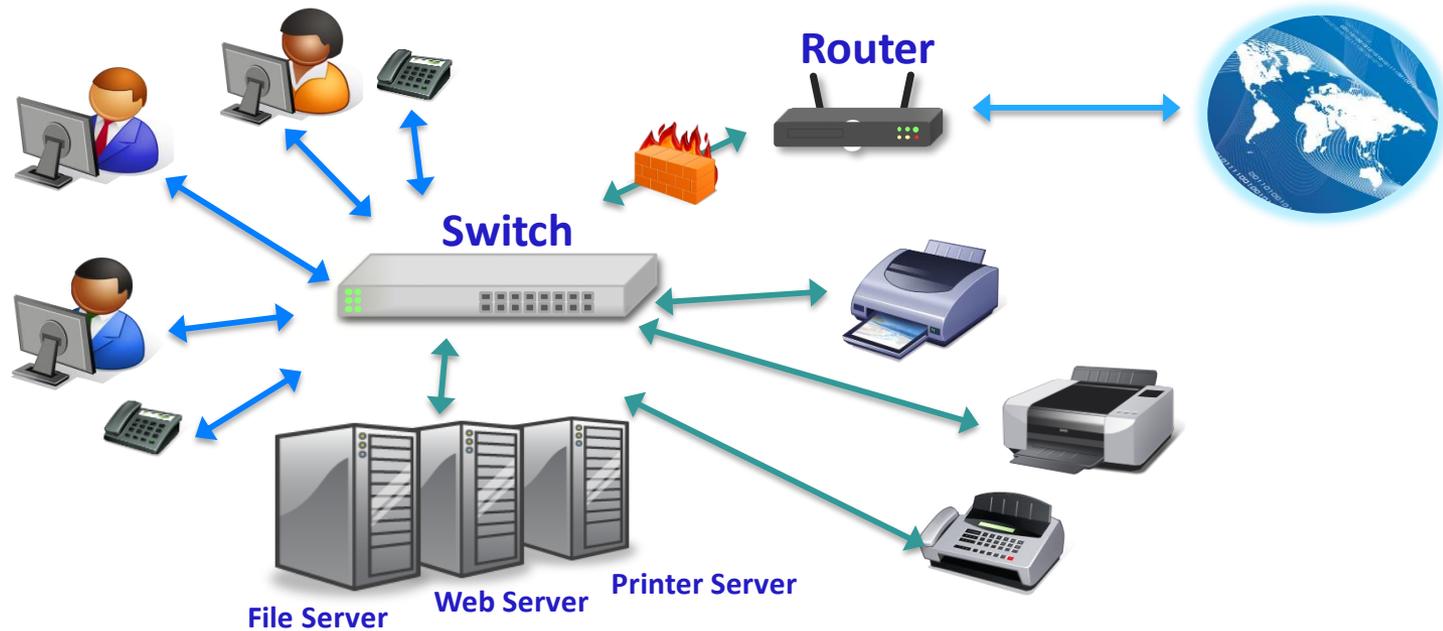
## SECTION 3

### Networking Basics





# Networking Basics



- **Servers:** Computers dedicated to managing shared resources
- **Switch:** Controls traffic within a network
- **Router:** Controls traffic between networks
- **Firewall:** Screen incoming and outgoing traffic for anomalies and potential threats

Source: [https://www.cisco.com/cisco/web/solutions/small\\_business/resource\\_center/articles/connect\\_employees\\_and\\_offices/networking\\_basics/index.html](https://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/networking_basics/index.html)





# Common Network Cybersecurity Issues

- Wireless Access Points – Often have outdated security protocols or no passwords
- Access – Users given access to more data or devices on a network than necessary can inadvertently or purposefully cause security issues
- Email – Social engineering attempts can unleash malware on a network or trick individuals into giving up personal information
- Firewalls – May be improperly configured, giving individuals too much access to a system or network
- Communications – Network traffic containing confidential information that is transported without using Secure Socket Layer (SSL) technology can be easily intercepted

