



Educate  
Engage  
Inspire

# Module 4

Student workbook

Module 4

## Computer basics and virtualisation

### Learning objectives

Students will understand:

- Internal components of a computer
- Operating system purpose, types, and security
- Basics of virtual computing
- Major networking components and concepts



Presented by



**NORTHROP  
GRUMMAN**

In partnership with



## Common hardware / BIOS vulnerabilities

Define the following terms and the role that each has in modern computing. Include the full name for any acronyms or initialisms:

**Operating system**

**BIOS**

**Motherboard**

**RAM**

**GUI**

Find a real-world example of the following vulnerabilities being used to exploit a system:

**Backdoors**

**Environmental concerns**

**BIOS malware**

**RAM malware**

## Operating systems

Identify the operating system that you use on your current computer or device:

For each of the following, what actions do you or the operating system, take to reduce vulnerabilities?

### **Passwords**

### **File access/permissions**

### **System patch**

## Software applications

Taking stock of the software applications you use.

**How many can you identify?**

**Are they all up to date?**

**Are there any that you do not use anymore that you could uninstall?**

**Research if there are any that you could install to improve your system:**

# Virtual Machine

Define the following terms as they relate to Virtual Machines:

**Guest**

**Host**

**Image**

**Hypervisor**

Complete an advantages and disadvantages table for Virtual Machines.

Include security benefits (advantages) and concerns (disadvantages).

Advantages of Virtual Machines	Disadvantages of Virtual Machines

## Networking

Describe the roles of each of the following components in a network:

**Server**

**Switch**

**Router**

**Firewall**

Identify a potential vulnerability below and the steps to take to defend against exploits:

**Wireless Access Points**

**User access**

**Emails**

**Incorrectly configured Firewalls**

**Information moving through a network (network traffic)**

## Case study — Wannacry ransomware

In May 2017, a worldwide cyber-attack occurred affecting more than 200 000 computers in 150 countries with damages ranging from hundreds of millions to billions of dollars.

**What Operating system did this ransomware affect?**

**What vulnerability did it exploit?**

**Microsoft had already released a patch for exploit. Why did the attack work despite this patch?**

**Wannacry was a ransomware crypto worm. Describe how this kind of malware works?**

**How can you ensure that your business is protected against this type of exploit in the future?**

## Learning reflections

### Computer components and common vulnerabilities

My understanding of computer hardware and BIOS and their common vulnerabilities.

**Needs more work**

**Completely confident**



### Operating systems

My understanding of my operating system's purpose, type, and security levels.

**Needs more work**

**Completely confident**



### Virtual computing

My ability to use VMWare and a virtual computing images.

**Needs more work**

**Completely confident**



### Networking

My understanding of fundamental networking components and the vulnerabilities of each.

**Needs more work**

**Completely confident**

