IT-ADVENTURES
MAKING IT FUN

Module 1 Activity 2 Answer Key

Confidentiality: Preventing unauthorized users from reading or accessing information. (passwords, credit card numbers, etc.)

Integrity: Ensuring that an unauthorized user has not altered information.

Availability: Making sure that information can be accessed when needed by authorized users.

Vulnerability: A weakness in some aspect of a computer system that can be used to compromise a system during an attack.

Exploit: The action of taking advantage of a vulnerability within a system.

Risk: The likelihood of something being attacked by considering several factors like threat, vulnerability, and impact.

Threat (computer security): A pending danger in a system, facilitated by a vulnerability. That if left unpatched can result in negative consequenses.

Impact: The measure of potential damage if a system or data is compromised by a security breach.

Risk Assessment: The process of determining and evaluating how much resources need to be devoted to its protection.

Script Kiddies: Attackers that have little programming knowledge but use software on the Internet to attack other computers. A novice hacker.

CRC Press, 2012. Jacobson & Idiorek, Computer Security Literacy: Staying Safe in a Digital World, 9781439856185

Virtual Machine: In essence, a VM is a computer emulation running within a computer. In later modules you will use your computer to create, manage and defend virtual machines found in the “cloud”.

ISERink: The virtual arena that you will be using throughout the entirety of the IT-Adventures program. It is hard to understand merely from words so here is a quick map of the ISERink layout.

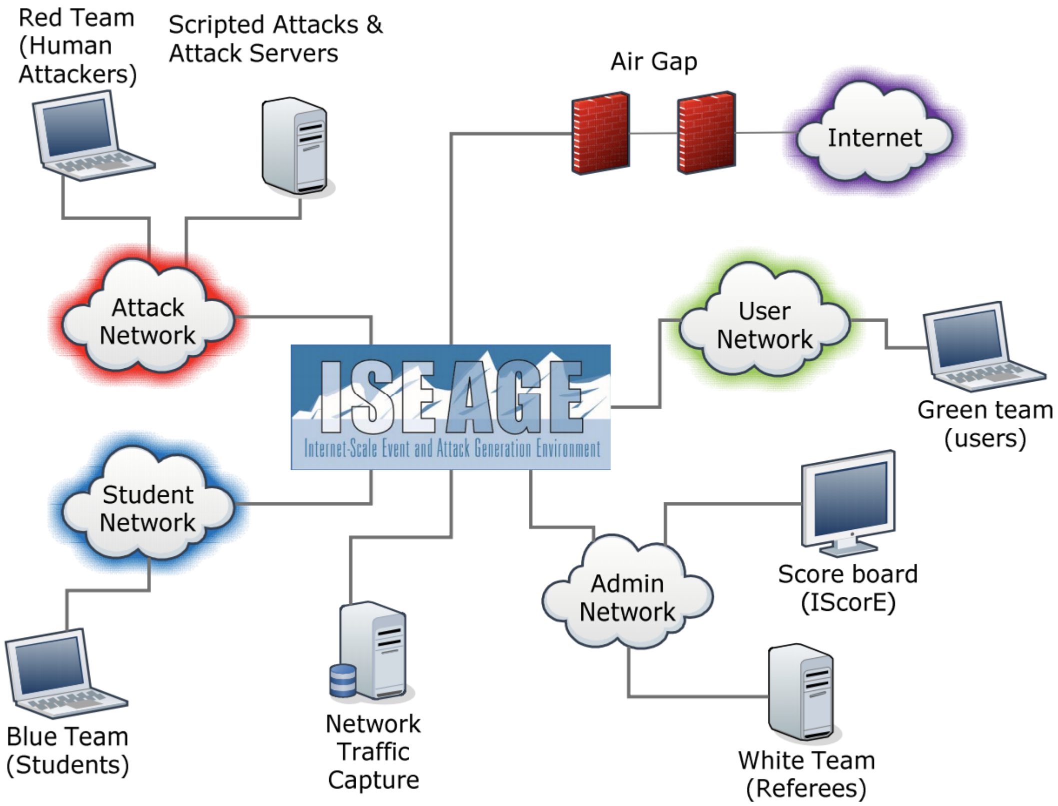


Figure 1 ISERink playground

CRC Press, 2012. Jacobson & Idiorek, Computer Security Literacy: Staying Safe in a Digital World, 9781439856185

Within a Cyber Defense Competition there are a lot of different color teams.

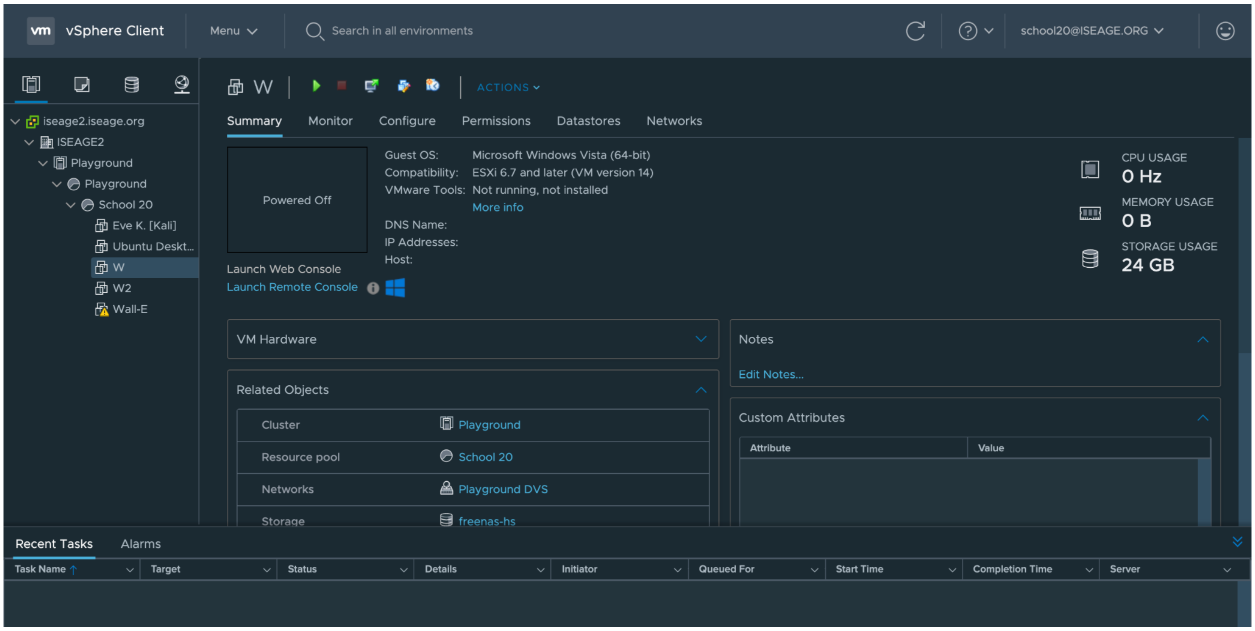
Blue Team: The people securing and keeping a close eye on their machines. You will be part of this team throughout the competition.

Red Team: The “bad guys” trying to break into your machines. Usually security professionals that are experienced and know almost every trick in the book.

Green Team: The “Neutral” team. This team is composed of normal users of the services that run on your computers.

White Team: Security experts that have undergone training as both defenders and attackers.

ISELab:



Guest OS: Microsoft Windows Vista (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Not running, not installed
DNS Name:
IP Addresses:
Host:

CPU USAGE 0 Hz
MEMORY USAGE 0 B
STORAGE USAGE 24 GB

Cluster	Playground
Resource pool	School 20
Networks	Playground DVS
Storage	freenas-hs

CRC Press, 2012. Jacobson & Idiorek, Computer Security Literacy: Staying Safe in a Digital World, 9781439856185