Introduction to Network security

**Module Description:** This module introduces network security. In the first micro module, students will be given an overview of networks, and then move to network attacks, such as Denial-of-service attacks. The second micro module discusses network encryption and some network protocols, such as IPV6, SSH, SSL/TLS, HTTPS, IPSec. Network defense techniques are introduced in the third micro module. This micro module focuses on techniques such as firewalls, intrusion detection and prevention systems, honeypot.

**Prerequisite Knowledge:**  Students are expected to understand the introduction to cybersecurity concepts module and know network basics.

**Length of Completion:** This module includes 3 micro modules. The total length of the module is around 7 hours.

**Level of Instruction:** This module intended for upper division undergraduate students majoring in computer science or computer engineering.

**Learning Setting:** This module is suitable for many forms of delivery: online/in-class/hybrid.

**Lab Environment:** None

**Activity/Lab Tasks:** There will be in-class discussion and an out-of-class written assignment.

**Lab Files that are Needed:** None

# learning outcomes

MODULE learning oUTCOMES

* Students will be able to understand network basics.
* Students will be able to describe Denial-of-Service attacks.
* Students will be able to explain Distributed DoS attacks.
* Students will be able to define Zombies and Botnets.
* Students will be able to understand some of the network protocols which have security features built in (such as SSH, SSL/TLS, HTTPS, IPSec).
* Students will be able to describe network data encryption.
* Students will be able to understand different types of firewalls and what are the advantages of each type.
* Students will be able to understand intrusion detection and prevention systems.
* Students will be able to describe honeypot and what is the purpose of setting up a honeypot.

# module Details

**Instructional Files and Online Resources that are Needed:**

Slides:

Lesson 1: Network basics and threats (CSP-M6-L1.pptx)

Lesson 2: Network encryption and protocols (CSP-M6-L2.pptx)

Lesson 3: Network defense technologies (CSP-M6-L3.pptx)

**Assessment:**

Written homework questions (CSP-HW6.docx)

# lessons

**Overview of Lessons:**

Lesson 1: Network basics and threats

Lesson 2: Network encryption and protocols

Lesson 3: Network defense technologies

**Lesson 1 Learning Outcomes:**

Upon completion of this lesson:

* Students will be able to understand network basics.
* Students will be able to describe Denial-of-Service attacks.
* Students will be able to explain Distributed DoS attacks.
* Students will be able to define Zombies and Botnets.

**Lesson 1 Details:**

**Warm Up:** Refresh students with an overview of network basics.

**Lesson:**

Topics to be covered in this lesson include:

* Basics of network (OSI model, DoD TCP/IP model)
* Network attacks
* Denial-of-Service attacks
* Distributed Denial-of-Service attacks
* Zombies and Botnets

**Active Learning Activity:**

In-class discussion:

What problems can Denial-of-Service attacks bring? How to avoid being attacked?

**Lesson 2 Learning Outcomes:**

Upon completion of this lesson:

* Students will be able to understand some of the network protocols which have security features built in (such as SSH, SSL/TLS, HTTPS, IPSec).
* Students will be able to describe network data encryption.

**Lesson 2 Details:**

**Warm Up:**

Ask students how data transfers from software/application, over the network, to the user at the other end.

**Lesson:**

Topics to be covered in this lesson include:

* Network encryption concepts and tools
* Network protocols (IPv4, IPv6, SSH, SSL/TLS, IPSec, HTTPS)

**Active Learning Activity:**

In-class discussion:

Ask students how encryption can be used to protect data being transferred over networks.

**Lesson 3 Learning Outcomes:**

Upon completion of this lesson:

* Students will be able to understand different types of firewalls and what are the advantages of each type.
* Students will be able to understand intrusion detection and prevention systems.
* Students will be able to describe honeypots and what is the purpose of setting up a honeypot.

**Lesson 3 Details:**

**Warm Up:**

Ask students: Do they have firewall installed on their computers? What are the purpose of having a firewall?

**Lesson:**

Topics to be covered in this lesson include:

* Different types of firewalls and what are the advantages of each one.
* Intrusion detection systems
* Intrusion prevention systems
* Honeypot

**Active Learning Activity:**

Discussion:

What are the advantage and disadvantage of using intrusion detection systems? Do you want to use sensitive alert or not? What are the pros and cons of having sensitive alert?

Please attribute Dr. Jim Alves-Foss and Dr. Jia Song, University of Idaho  
  
  
  
Except where otherwise noted, this work is licensed under <https://creativecommons.org/licenses/by-nc-sa/4.0/>  
  
Notwithstanding the non-commercial license terms, non-profit educational institutions are granted a non-exclusive, royalty-free license to adapt and use this material, with attribution.  
  
Creative Commons and the double C in a circle are registered trademarks of Creative commons in the United States and other countries. Third party marks and brands are the property of their respective holders.

Project sponsored by the National Security Agency under grant Number H98230-17-1-0199. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation herein.