network defense

**Module Description:** The intent of this Knowledge Unit is to provide students with an understanding of network threats and defensive techniques.

**Prerequisite Knowledge:**  Students are expected to have a basic understanding of data representations, networking and cyber security principles.

**Length of Completion**: 8 lecture/meeting/active learning hours, 8 hours outside of lecture reading/preparation, homework.

**Level of Instruction:** This module intended for advanced 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:** A Linux machine (or VM) with iptables and wireshark available for students use. Lab experiments will be provided in through labtainers.

**Activity/Lab Tasks:** Learning activities involves group discussion and working some sample cryptography problems. More advanced task could include writing code that uses crypto libraries.

**Lab Files that are Needed:** None.

# learning outcomes

MODULE learning oUTCOMES

* Students will be able to describe and discuss network threats and attacks.
* Students will be able to list characteristics of a firewall
* Students will be able to explain the types of firewalls
* Students will be able to describe firewall locations and configurations
* Students will be able to use iptables to define restricted access to communication between hosts.
* Students will be able to use a network monitoring tool to view functionality of the firewall rules.
* Students will be able to describe the basic concepts of intrusion detection
* Students will be able to explain the different types of intruders
* Students will be able to explain the differences between statistical anomaly detection (both threshold and profile based) and rule-based detection.

# module Details

**Interconnection:** This module assumes prior knowledge from internetworking, cryptography modules, and cyber security principles.

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

* Lesson 1: Lesson\_1\_Network\_Defense.pptx
* Lesson 2: Lesson\_2\_Firewalls.pptx
* Lesson 3: Lesson\_3\_Netfilter.pptx
* Lesson 4: Lesson\_4\_Intrusions.pptx
* Optional Lesson: Lesson\_SlammerWorm.pptx

**Assessment:** This provides a reference of what is included in the assessment guide and a mapping of how the assessment items cover all module and lesson learning outcomes.

# lessons

**Overview of Lessons**

* Lesson 1: Lesson\_1\_Network\_Defense.pptx
* Lesson 2: Lesson\_2\_Firewalls.pptx
* Lesson 3: Lesson\_3\_Netfilter.pptx
* Lesson 4: Lesson\_4\_Intrusions.pptx
* Optional Lesson: Lesson\_SlammerWorm.pptx

**Lesson 1: Network Defense**

Have students read the paper about Mitnick before class: <https://www.giac.org/paper/gsec/1929/kevin-mitnick-hacking/100826>

Lesson 1 Learning Outcomes:

Upon completion of this lesson:

* Students will be able to describe and discuss network threats and attacks.

Lesson 1 Details:

**Warm Up:** Ask the students to discuss network threats. (Hint: We want to differentiate between attacks against single machines on the network, attacks against network applications such as web servers, attacks against network services and attacks against network protocols.)

**Active Learning Activity:** In small groups, discuss the attributes of the Mitnick attack

* What security measures could have been put in place to stop this attack
  + Discuss external devices/monitors
  + Discuss changes to protocols

**Lesson 2: Firewalls**

Lesson 2 Learning Outcomes:

Upon completion of this lesson:

* Students will be able to list characteristics of a firewall
* Students will be able to explain the types of firewalls
* Students will be able to describe firewall locations and configurations

Lesson 2 Details:

**Warm Up:** This lesson should take a 1-2 lectures. Start with a recall of the previous lesson. Ask the student some questions about the previous material. Lead up to the idea of a single device that acts as a defender and a guard of your network.

**Lesson:** The lesson here is based on the PowerPoint slides and is a standard lecture. Allow time for questions and discussion during the lecture.

**Active Learning Activity:** The active learning is tied into the next lesson, Netfilter.

**Lesson 3: Netfilter**

Lesson 3 Learning Outcomes:

Upon completion of this lesson:

* Students will be able to use iptables to define restricted access to communication between hosts.
* Students will be able to use a network monitoring tool to view functionality of the firewall rules.

Lesson 3 Details:

**Warm Up:** This lesson should take a couple of lectures. Discuss the lesson on firewalls, and talk about configuring a firewall – what needs to happen?

**Lesson:** The lesson here is based on the PowerPoint slides, but these could be provided as a resource to the students and not actually given as a lecture. Instead, students can use them as a guide with hands on use of Netfiler (through iptables) in Linux.

**Active Learning Activity:** Try each of the commands in the slide deck with iptables on the Linux machine. Then progress to the lab assignments.

**Lesson 4: Intrusions**

Lesson 4 Learning Outcomes:

Upon completion of this lesson:

* Students will be able to describe the basic concepts of intrusion detection
* Students will be able to explain the different types of intruders
* Students will be able to explain the differences between statistical anomaly detection (both threshold and profile based) and rule-based detection.

Lesson 4 Details:

**Warm Up:** This lesson should take a couple of lectures. Ask the students about the types of intruders found on a network.

**Lesson:** The lesson here is based on the PowerPoint slides and is a standard lecture. Allow time for questions and discussion during the lecture.

**Active Learning Activity:** Snort – is Snort an IDS?

**Optional Lesson: Slammer Worm**

Optional Lesson Learning Outcomes:

Upon completion of this lesson:

* Students will be able to describe the basic attack concepts of the slammer worm.

Optional Lesson Details:

**Warm Up:** This lesson should take 1 lecture. Ask student what they know about internet worms.

**Lesson:** The lesson here is based on the PowerPoint slides and is a standard lecture. Allow time for questions and discussion during the lecture.

**Active Learning Activity**: Ask students to write down 2 different firewall rules to prevent the slammer worm. Have them hand them in. Then list them on the board. Discuss how to implement them. Will they break normal functionality? How could the attacker get around them? How hard is this to do for all similar network services? Can it be automated –if so how?

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.