**Network & Vulnerabilities Scanning**

10 Module

# **Module Objectives:**

# Familiarize yourself with Network Scanning

# Know what the components of network scanning are

1. Understand how and why network scanning can be used by hackers and businesses
2. Learn about network/host scanning, port scanning, and vulnerability scanning
3. Put yourself through a network scanning
4. Exploit system vulnerabilities

# **Module Lesson**

| **Component** | **Title** | **Purpose** |
| --- | --- | --- |
| 1. [Slideshow](https://www.cyio.iastate.edu/cyber-defense/)  (10 minutes) | Network & Vulnerability Scanning | Learn how hackers can potentially attack a network |
| 2. [Activity 1](https://www.cyio.iastate.edu/cyber-defense/)  (30 minutes) | Network Scanning Tools | Experiment with common scanning tools |
| 3. [Activity 2](https://www.cyio.iastate.edu/cyber-defense/)  (20 minutes) | Exploiting Vulnerabilities | Red Team Tools |

Total Duration: 55 minutes

Note: All activities designed for this module are hands-on. The speed at which the activities can be completed will vary. Each module should approximately take one club or class time to complete.

# **Additional Resources:**

* [Nmap: the Network Mapper - Free Security Scanner](https://nmap.org/)
* [Networks SCAN | Types of Network Scans| Types of Network Scan |Network Scan Examples | nmap |Infosec](https://youtu.be/OYUpsJZUHV0)
* Google!
* [VMware Glossary](https://www.vmware.com/topics/glossary/)