**CSCD 434**

**Lab 3**

**Introduction to NMap**

# NMap

The purpose of this assignment is to learn how to use nmap, the network mapping tool.

**Documentation**

* [https://nmap.org](https://nmap.org/)

**Part 1: Understanding Use**

* Open your VPN for EWU and connect
* SSH into cscd-linux01.eastern.ewu.edu

Explain the output for each nmap command below. From cscd-linux01:

* nmap 10.101.130.\*   
  Lists all devices with IP addresses beginning with 10.101.130.
* nmap 10.101.130.100-120   
  Lists all devices with IP addresses ranging from 10.101.130.100 to 10.101.130.120
* nmap 10.101.130.0/24
* Complete a ping scan on 10.101.130.0/24 What address ranges are active?   
  .1, .20, .50, .55, .57, .61, .77, .81
* Scan all TCP ports. What ports are open on my windows server? What commands did you use? What is the IP address?domain, http, msrpc, netbios-ssn, Microsoft-ds, vmrdp, ms-wbt-server
* Nearly every address in the 10.101.130.1-255 range is assigned to some device. Explain why you see so few.   
  They could currently be offline.
* Complete a ping scan on 10.102.134.235-255 How many hosts did the ping scan discover? Were there gaps in the host numbers? Why? What are these machines?  
  8 hosts, .235, .236, .237, .242, .243, .247, .248, .254. They are most likely lab computers.
* Complete a version scan on 10.102.134.235 What command did you use? What are the results? Be specific as possible.nmap -A 10.102.134.235. It lists the currently running services, their version, the ssl certificate, OS, and scripts.

**Part 2: OS** What’s the difference between these two commands?

* nmap 10.101.130.1
* sudo nmap -O 10.101.130.1
* Answering “The second command uses sudo and -O” is not good enough. Why!?   
  The second enables OS detection, which can also show uptime, generation, device type, and vendor.

**Part 3: Look for machines**

Look for a computer in the 10.101.130.0 – 10.101.130.255 range that has port 902 open.

* What command did you use?   
  nmap –p 902 10.101.130.\*
* What are the computer’s IP address(es)?   
  10.101.130.81
* What are the name(s)?   
  cscd-win-server.eastern.ewu.edu
* My school desktop is one of the machines. What is its name and IP address? What other ports are open?   
  No other results are named.

Look for a computer in the entire 23-bit subnet that has the “domain” port open.

* What command did you use?
* Did you find one? What are the computer’s IP address(es)? What is its name?   
  nmap -sV -p domain –open 10.101.130.0/23

Look for the computers in CEB 207/CEB 208.

* What command did you use? • What are the computer’s IP address(es) and names (list 3 or 4)?

**Part 4: Analysis**

Using all the completed scans answer the following.

* Which TCP port appeared the most?   
  http
* Are there any security vulnerabilities associated with any of the open ports? Where did you look? Google or some other search engine is not acceptable.
* How might a system administrator discover someone running nmap or a similar program to probe their network? How can someone scanning a network with a tool similar to nmap avoid detection? (I am expecting at least a couple of sentences in response to this, think about it)

Users can scan more slowly or use one of the stealth options for nmap

# Turn In

* Single PDF containing the question and your work.
* Name your pdf your last name first letter of your first name lab3.pdf (Example: steinerslab3.pdf)