How can a three-part combination lock, with each part consisting of ten possible numbers (0 - 9), be hacked?
Why Nmap?

• A useful tool for identifying security holes on your network.
• As stakeholders of the security of systems, there’s need to be familiar with the functionality and features of Nmap towards building on our defense mindset against attacks.
• Good avenue for learning about the types and nature of vulnerabilities that occur on computer systems.
• Effective tool for the bad guys: target profiling, reconnaissance.
Features of Nmap

- Port scanning
- Operating system detection
- Version detection
- Host discovery
Some Specific Uses of Nmap

• Finding and exploiting host/network vulnerabilities
• Identification of open ports and their states on a target host
• Network security audit: identification of any new hosts on the network (are there any rogue hosts?)
• Network maintenance (inventory, asset management, etc.)
• Generating traffic destined for hosts on the network
Nmap Options

- At the command prompt: “nmap”, “man nmap”
- Will show all the options and features of Nmap
- Let’s run Nmap at the prompt and view the available options and features
- Note: Nmap is available in GUI as Zenmap. You can specify targets and scan types by interacting with the graphical interface.
- To install Zenmap:
  - sudo apt-get update
  - sudo apt-get install zenmap
- Running Zenmap: sudo zenmap (root privilege required)
- You can optimize your scans (Nmap/Zenmap) and improve scan performance by applying the appropriate options (e.g., -T4, -F)
Some Sample Scans

• nmap -v -A -T4 127.0.0.1
• nmap -v -A -T4 www.ucalgary.ca
• What interesting information do you find in our scan results? Why do you find them interesting?
• We can detect whether a host is up or down by means of a ping scan as follows (localhost is our target):
  - nmap -v -sP localhost | grep up
  - nmap -v -sP localhost | grep down
• We can also scan an entire network, using the above format, to discover all the hosts that are up or down. In this case, simply replace “localhost” with the address of the entire network. (How do you specify an entire network?)
Activity – Exploring Nmap

• Run a default scan (no options) of your localhost and www.ucalgary.ca. How do these outputs differ from the ones in our preceding scans, in terms of contents and run time.
• Do a ping scan of all the guests on your host machine.
• Scan the arbitrary class C network 192.168.1.0/24. How many hosts are up? How many are down?
• What services are currently running over the open ports on your localhost?
• Applying the appropriate option (-T4) that enables fast execution, perform a service discovery scan of the first 500 ports on www.ucalgary.ca. Attempt this scan without the fast execution option. What does your observation tell you about scan performance/optimization?
Activity – Exploring Nmap. Cont’d

• Scan one of your guest machines for the port states over the following services: telnet, ftp, http, https, smtp, and ssh.
• Perform a scan that detects the OS type running on your guest machine(s)?
• Applying various options available on the man page of Nmap, examine different scans with regard to output information and scan duration. (let your target host be localhost)
• Install Zenmap on your Linux box and explore the GUI. Specifying your localhost as the target, select different scan types and observe each output.