Cybersecurity Workshop 2025

1. **Teaching:**

* Go over Slides

1. **Activity:**

0. Preparation

o Set up WSL environment on computers, ensure students have admin permissions

o Connect to the network device that we set up (at least 5 can connect at a time)

§ Run through the stages of an attack, using the network connection and navigating using WSL

* Include a dummy device on the network
* Possible OS for dummy device:
  + Metasploitable
  + Windows XP or Windows 7
  + Ubuntu or Debian Linux

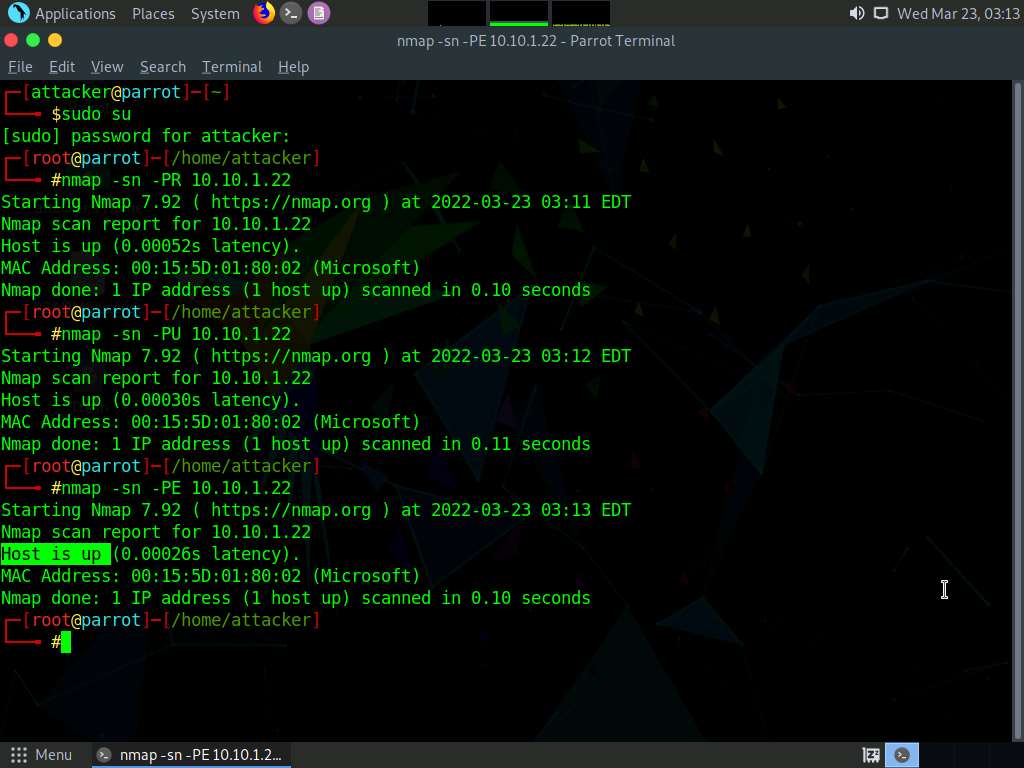
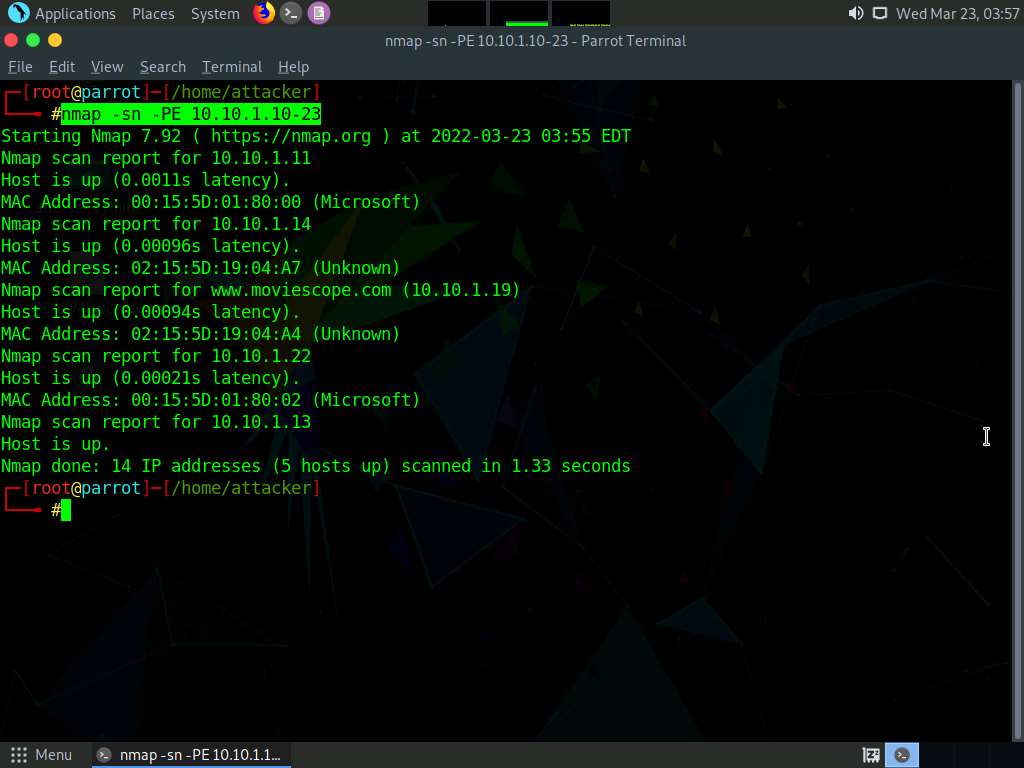
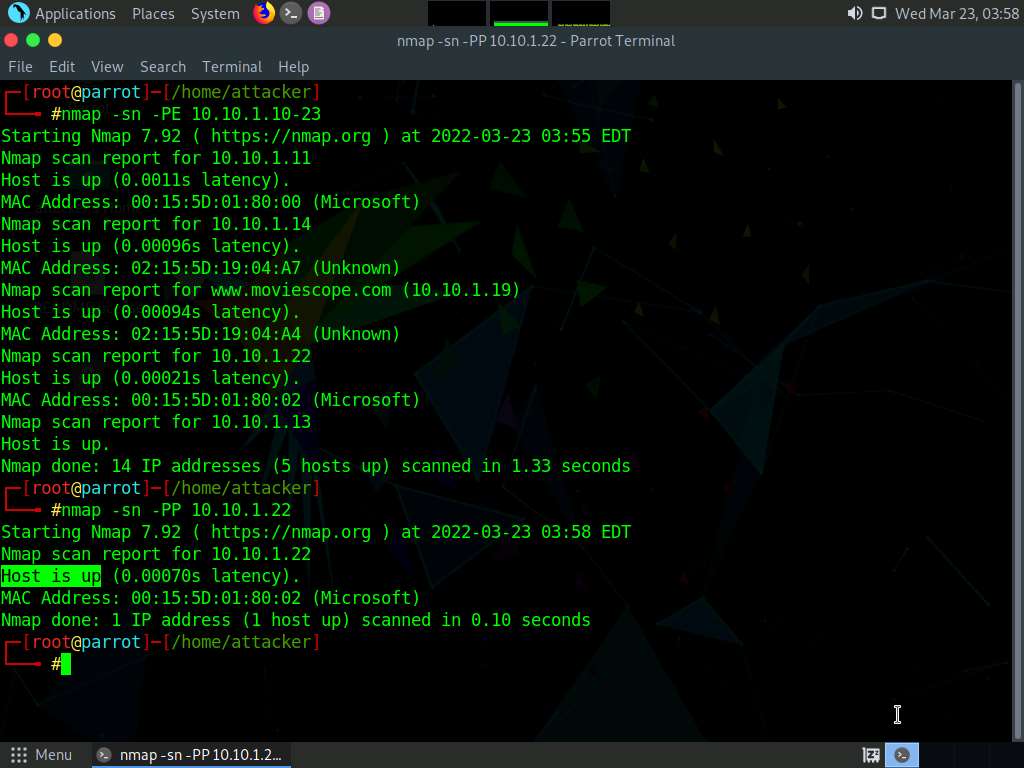
0.5 Footprinting

* Explain scenario where this could happen
* At a McDonald's or Restaurant
* Public Network that your laptop gives a warning may be unsafe. (people may be able to see your information over this network)

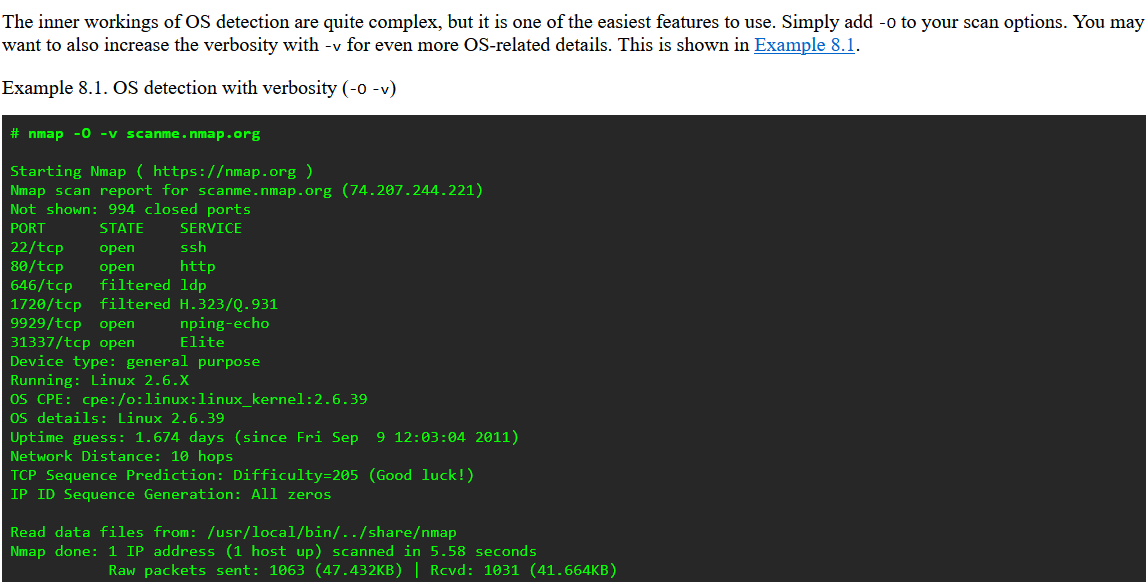
1. Scan the network

· TCP Ping scan

Make sure they have Linux commands on their machine through Ubuntu.

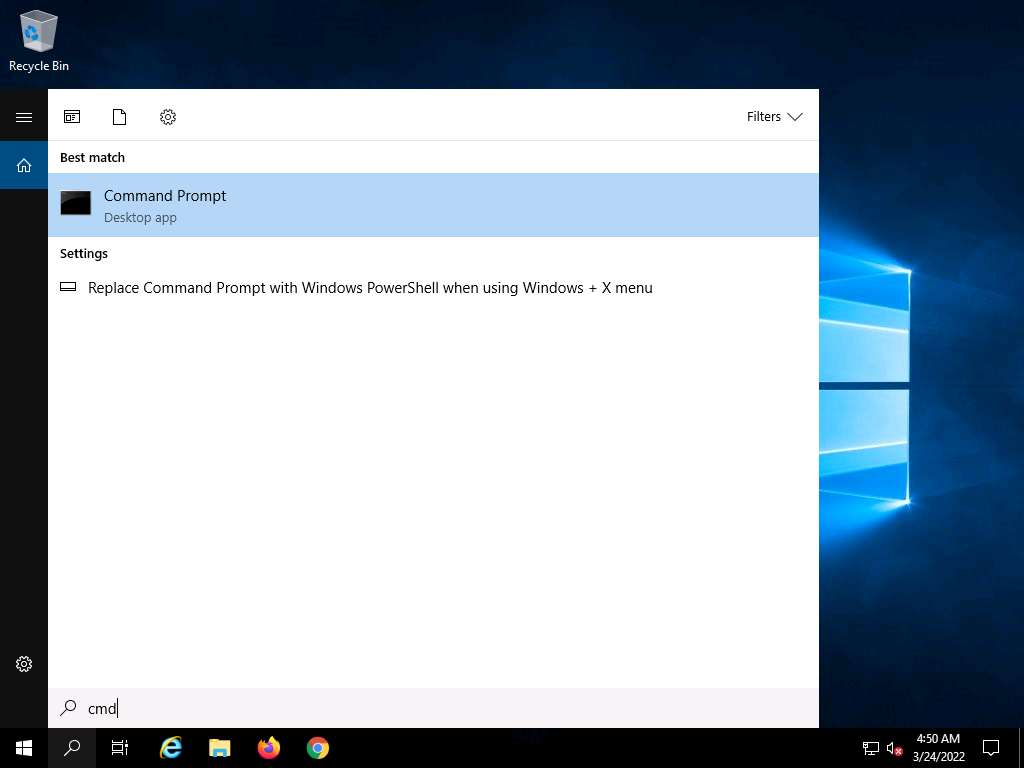
* Log in to the machine.
* Open a **Terminal** window.
* A **Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
* In the **[sudo] password for attacker** field, type **your password** as a password and press **Enter**.  
    
    
   The password that you type will not be visible.  
    
    
   **-PE**: performs the ICMP ECHO ping scan.  
    
    
    
   The ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the target host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if the ICMP is passing through a firewall.  
    
    
   
* Now, we will perform an ICMP ECHO ping sweep to discover live hosts from a range of target IP addresses. In the terminal window, type **Nmap -sn -PE [Target Range of IP Addresses]** (here, the target range of IP addresses is **10.10.1.10 - 23 giving them a range to start until they find the right device**) and press **Enter**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.  
    
    
   The ICMP ECHO ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply.  
    
    
   
* In the terminal window, type **Nmap -sn -PP [Target IP Address]**, (here, the target IP address is a **dummy device IP**) and press **Enter**. The scan results appear, indicating the target **Host is up**, as shown in the screenshot.  
    
   **-PP**: performs the ICMP timestamp ping scan.  
    
   ICMP timestamp ping is an optional and additional type of ICMP ping whereby the attackers query a timestamp message to acquire the information related to the current time from the target host machine.  
    
     
  
* Apart from the network above scanning techniques, you can also use the following scanning techniques to perform a host discovery on a target network.  
    
  + **ICMP Address Mask Ping Scan**: This technique is an alternative to the traditional ICMP ECHO ping scan, which determines whether the target host is live specifically when administrators block the ICMP ECHO pings.  
      
     **# nmap -sn -PM [target IP address]**
  + **TCP SYN Ping Scan**: This technique sends empty TCP SYN packets to the target host, ACK response means that the host is active.  
      
     **# nmap -sn -PS [target IP address]**
  + **TCP ACK Ping Scan**: This technique sends empty TCP ACK packets to the target host; an RST response means the host is active.  
      
     **# nmap -sn -PA [target IP address]**
  + **IP Protocol Ping Scan**: This technique sends different probe packets of different IP protocols to the target host, any response from any probe indicates that a host is active.  
      
     **# nmap -sn -PO [target IP address]**
* This concludes the demonstration of discovering the target host(s) in the target network using various host discovery techniques.
* Close all open windows and document all the acquired information.

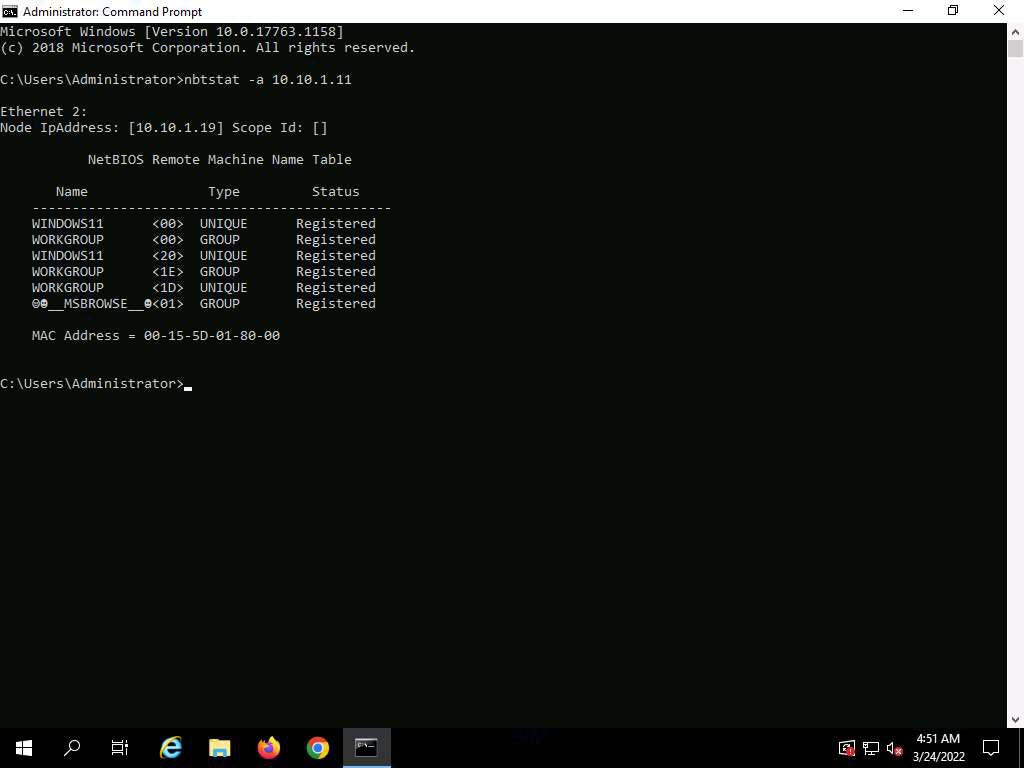
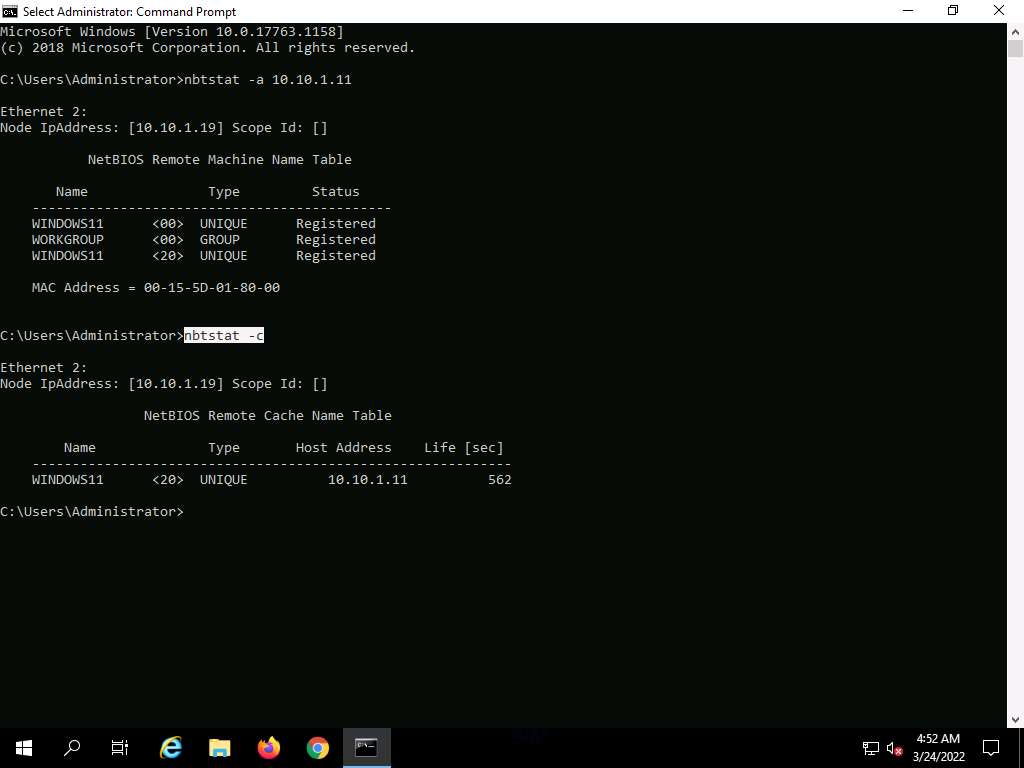
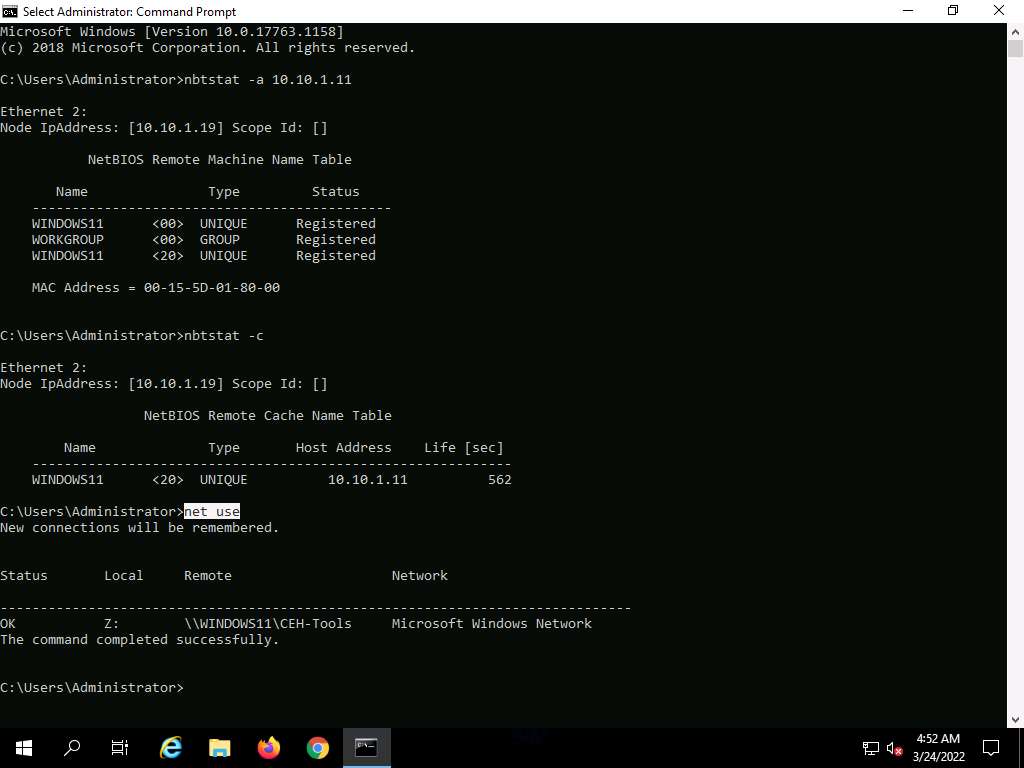
· TTL & TCP to identify OS



<https://nmap.org/book/osdetect-usage.html>

## 2. Enumeration

Open a **Command Prompt** window.  
  
 

1. Type **nbtstat -a [IP address of the remote machine]** (in this example, the target IP address is a **dummy device ip**) and press **Enter**.  
     
     
    In this command, **-a** displays the NetBIOS name table of a remote computer.
2. The result appears, displaying the NetBIOS name table of a remote computer (in this case, the **WINDOWS11** machine), as shown in the screenshot.  
     
    
3. In the same **Command Prompt** window, type **nbtstat -c** and press **Enter**.  
     
     
    In this command, **-c** lists the contents of the NetBIOS name cache of the remote computer.
4. The result appears, displaying the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.  
     
     
    It is possible to extract this information without creating a **null session** (an unauthenticated session).  
     
     
    
5. Now, type **net use** and press **Enter**. The output displays information about the target such as connection status, shared folder/drive, and network information, as shown in the screenshot.  
     
    
6. Using this information, the attackers can read or write to a remote computer system, depending on the availability of shares, or even launch a DoS attack.

3. Look up [CVEs](https://www.cve.org/) & [NVD](https://nvd.nist.gov/)

CVE® is a publicly available and free-to-use list or dictionary of standardized identifiers for common software vulnerabilities and exposures. The use of CVE Identifiers, or “CVE IDs,” which are assigned by CVE Numbering Authorities (CNAs) from around the world, ensures confidence among parties when discussing or sharing information about a unique software or firmware

§ Abstract overview of metasploit

4. Threat Delivery

Go over the packaging of attacks

* Emails
* Links
* Downlaods

Protection:

* Virus Total
* Awareness/Training