**LAB12 ZENMAP WIN or LINUX**

**Class Name Student ID**

1. **Design Zenmap scanning pen-test scenario**

|  |  |  |
| --- | --- | --- |
|  | scanner | target |
| OS | Windows  Ubuntu | Windows, Linux |
| IP address | Test - bed host IP | **Don’t scan other systems(including google.com), instead use test-bed IP**  Localhost:  CTU IP: 123.30.143.225  CICT IP: 123.30.143.202  Neighboring PC IP:  VM IP(Ubuntu, Centos): |
| scanning program | Zenmap Windows  Zenmap Ubuntu |
| scanning types | scanin profile field  scan in command field  scan inmenu bar |

1. Install Zenmap on Window or on Ubuntu (select one)

**2. in profile field, scan and explain the result**

1. Intense Scan Command: nmap -T4 -A -v *<target>*
2. Intense Scan, all TCP Ports Command: nmap -p 1-65535 -T4 -A -v <target>
3. Intense Scan, no ping Command: nmap -T4 -A -v -Pn <target>

**3. Scan in command field, scan and explain the result**

1. Ping Scan Command: nmap -sn <target>
2. Quick Scan Command: nmap -T4 -F <target>
3. Quick Trace Route Command: nmap -sn --traceroute <target>

**4. Scan in menu bar explain the result**

1. Press Hosts button & explain
2. Press Services button & explain
3. Press Ports / Hosts button & explain
4. Press Topology button & explain
5. Press Host details button & explain

<https://linuxhint.com/zenmap_ubuntu_nmap/>