PreLab 10: Securing workstations

Or: *ACLs really need to be planned out ahead of time*

What You Will Do:

1. Create ACLs to secure workstations for 3 different types of usage
2. [Optional] To maximize your success in lab, test some of the ACLs in PT or NetLab
3. [During your lab] You will actually deploy and test the ACL you have written to protect your workstation. The specific ACL will be assigned by the lab Professor.

Things that you will need to know or learn:

1. The skill of writing extended ACLs that you developed in the previous post-lab.

What you need to submit and when:

1. **TWO PRINTED COPIES** of your ACLs, submitted in person within 5 mins of the official start time of your lab session. Clearly separate the ACLs into three different sections.

This post-lab is worth **36%** of this lab, even though the number of points may differ between the three parts.

References and Resources:

- Slide decks on ACLs
- Post-Lab 9 exercise on extended ACLs

Hints and Tips

– Some research may be required to determine specific allowed IP addresses.
– Completing the postlab 9 quiz will be of great help in composing the new ACLs.

(Continued on next page.)

Scenario

Your workplace needs to secure the workstations for three different uses. These are defined below. You need to submit the exact details of complete *named* ACLs (for Cisco devices) that will limit traffic to known applications and known destinations as defined below.

Your job is to (a) determine exactly which protocols and/or ports must be included in the set of ACEs for each ACL; then (b) compose the required ACL. Choose appropriate names!
Important: Are you designing your ACLs for traffic *inbound to* or *outbound from* the user??

1. Ordinary user (think of a grandparent) – 9 protocols/ports
   - boot-up into windows
     Hint: one protocol isn't always be particularly noticeable, but check bottom right of screen!
   - surf the internet
   - use an email client of their preference (e.g. Thunderbird). You do **not** know what kind of server they will be connecting to, so allow access for all possible setups.
   - **ALL OTHER TRAFFIC IS BLOCKED** and must be monitored by a matching ACE

The only acceptable DNS servers are Google and CloudFlare's public servers.

2. Networking Student – 5 additional protocols/ports
   - all the same applications and specifications as an ordinary user
   - NetLab
   - Run the two (most common!) network troubleshooting tools
   - FTP
   - **ALL OTHER TRAFFIC IS BLOCKED** and must be monitored by a matching ACE

3. Network device (router, switch) – 6 protocols/ports
   - Factory-fresh (completely uninitialized) systems must be able to boot up from the network
   - Prepared configs must be retrieved from a TFTP server
   - Send log messages to an external server (Ref: read ENSA section 12.3.4!)
   - Run the two (most common!) network troubleshooting tools
   - All other traffic will be permitted

The purpose of the ACL(s) is to monitor the *number of packets* of each type that *exit* ("egress") and *enter* ("ingress") to/from the device. So even though all traffic is ultimately permitted, it must nonetheless be matched by individual ACEs.

Q. Consider whether you need *two separate* ACLs or whether a single ACL can be applied to both the input and output of the interface. Does that affect the design or your ACL?