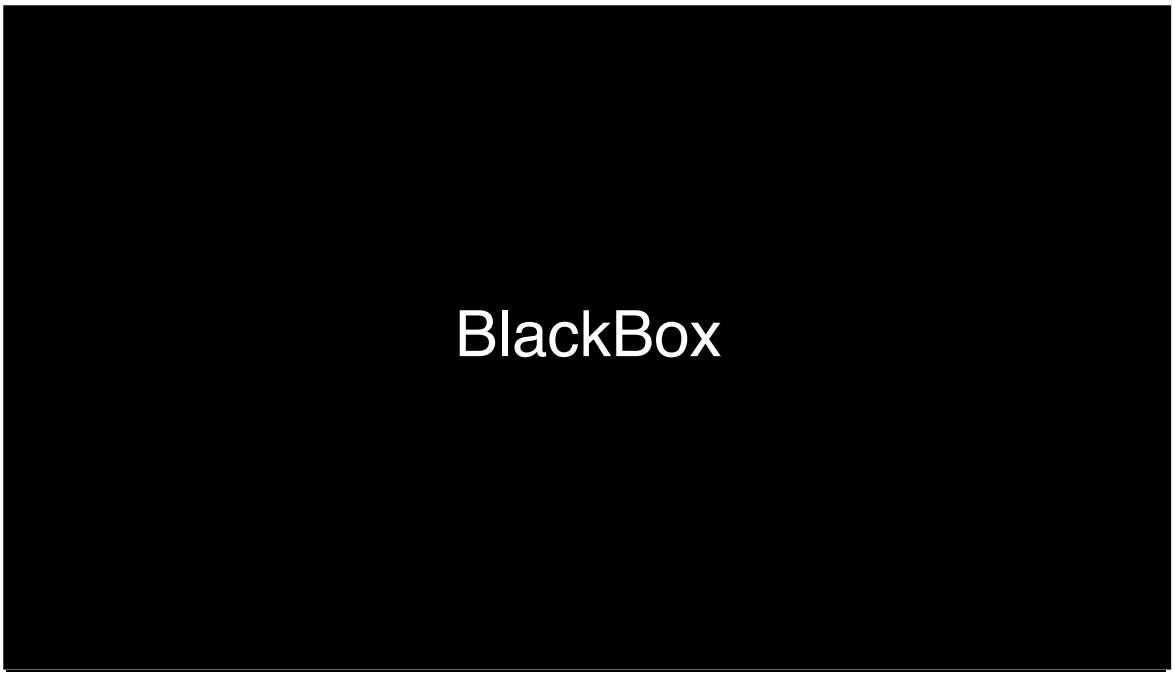
Welcome to the CybatiWorks™ Blackbox competition. The Blackbox emulates a complete ICS/IT/Internet system for you to enhance your cyber asset discovery, protocol analysis, engineering logic and vulnerability assessment capabilities. The Blackbox uses real Industrial and IT protocols along with traditional IT services and is extended with real Industrial and IT configuration logic. We hope you enjoy your time within the CybatiWorks™ Blackbox.



Task / Mission Description	Blackbox Wizard ICON
Open the **"Launch the Blackbox Wizard Console"** folder on the desktop of the CybatiWorks-1 VM. This step may have already been performed. If necessary, the host username is root with password cybati.	BLACKBOX
The following steps match the ICON names in the folder.	
Step 0. RESET. The wizard will reset the environment for game play.	BLACKBOX 0. RESET

Task / Mission Description	Blackbox Wizard ICON
Step 1. Start the Blackbox. Select the complexity level. The wizard will execute a series of scripts to build a complete IT/ICS/Internet network comprising of almost 40 active nodes. **At this time complexity level does not influence point allocation.** **MISSION 1 (5 pts.).** Identify the host IP address and default gateway.	1. Start the Blackbox
Step 2. Active Host Discovery. Use Zenmap or alternate tools to discover the Industrial network cyber assets. Close Zenmap when complete. **MISSION 2 (5 pts.).** Identify the number of hosts responding within the Industrial Network. **MISSION 3 (5 pts.).** What services are running on the host with the DNS name relay?	2. Active Host Discovery
Step 3. Passive Host Discovery. Use Wireshark within the Industrial Network to baseline active host-to-host communications. Close Wireshark when complete. **MISSION 4 (5 pts.).** Identify the active connections to the HMI.	3. Passive Host Discovery
Step 4. Initial VirtuaPlant. Enable the VirtuaPlant bottling process and HMI. Review the HMI and visual bottling process.	4. Initialize VirtuaPlant
Step 5. Review Engineering Schematic. Review the Engineering schematic for the VirtuaPlant bottling process. **MISSION 5 (5 pts.).** What point is associated with the NOZZLE?	5. Review Engineering Schematic
Step 6. Host Tap Assignment. Identify the new active communications for the Bottling facility.	6. Host Tap

Task / Mission Description	Blackbox Wizard ICON
MISSION 6 (5 pts.). Which hosts and Industrial protocol(s) are used for the process?	Assignment
Step 7. Execute Logic Attacks. Execute the Move and Fill logic attack. To stop the attack execute the script again and click the Cancel button.	7. Execute Logic Attacks
Step 7. Host Tap Assignment. **MISSION 7 (5 pts.).** What host performed the attack? **MISSION 8 (5 pts.).** What industrial protocol register was attacked?	8. Host Tap Assignment
MISSION 10 (10 pts.). What is the PLC password contained in the RSS file? **MISSION 11 (10 pts.).** What is the PLC password contained in the PLF file? **MISSION 12 (10 pts.).** What malware is contained in the DOCX file? **MISSION 13 (10 pts.).** What is the executable (.exe) file? How could it be used? **MISSION 14 (10 pts.).** Describe findings of the two VMEM files located in the /opt/CybatiWorks/Labs/volatility directory. The files are titled CybatiWorks Windows*.vmem	EXTRA and ADVANCED MISSIONS
Stop the Blackbox and submit your competition findings at blackbox@cybati.org **Additional wizards, laboratories and online lectures are available within our courseware.**	100. Stop the Blackbox