# Cybersecurity

## Project 1.2.5: It’s a Trap

Copy and paste screenshots and/or answer questions from the activity.

#8 **Plan of Action**

1. Firewall Rules: *How will you disable Windows file sharing? Are there other services/ports you need to disable?*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 137 | TCP | netbios-ns | nbname | NETBIOS Name Service |
| 137 | UDP | netbios-ns | nbname | NETBIOS Name Service |
| 138 | UDP | netbios-dgm | nbdatagram | NETBIOS Datagram Service |
| 139 | TCP | netbios-ssn | nbsession | NETBIOS Session Service |



1. Suspicious files: *How can you identify suspicious files?*

* Check file extensions
* Obvious file name

1. Downloaded files: *How will you know where to look for files downloaded from the internet?*

* Downloads folder

1. Lost/deleted user files: *Where will you find your friend’s “deleted” files?*

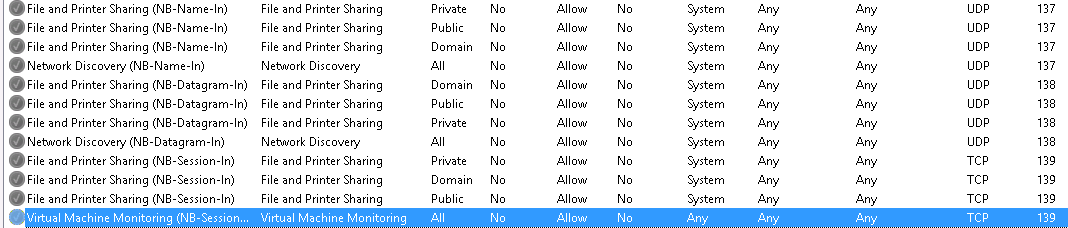
* Trash can

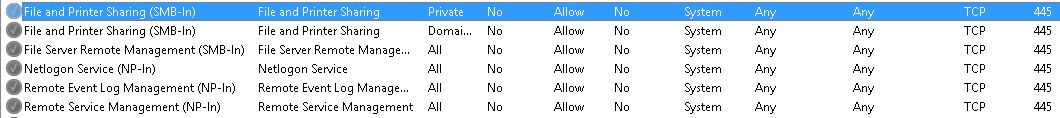
1. Suspicious processes:*How will you determine suspicious processes and what will you do with them?*

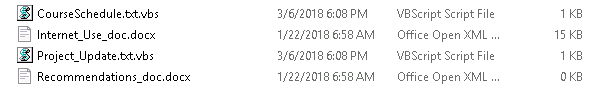
* Task manager

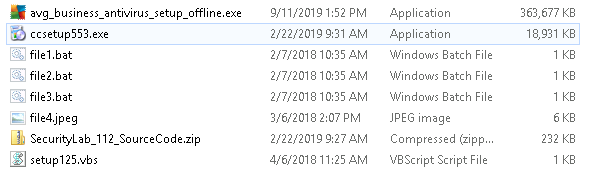
#11 **Implement Your Plan of Action**

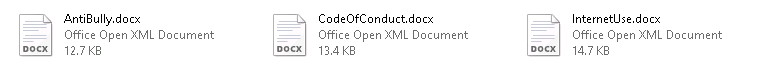
* Thoroughly document how you found and how you fixed each problem. Take screenshots for each of the step of your action plan (a through e) to help you explain what you did. Another team should be able to read your notes and perform the same tasks you did to secure the computer. **(BETTER TO HAVE TOO MUCH THAN TOO LITTLE)**

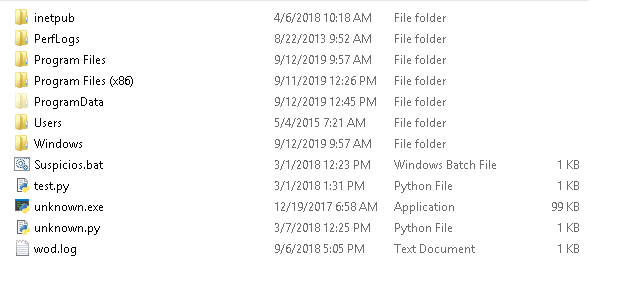


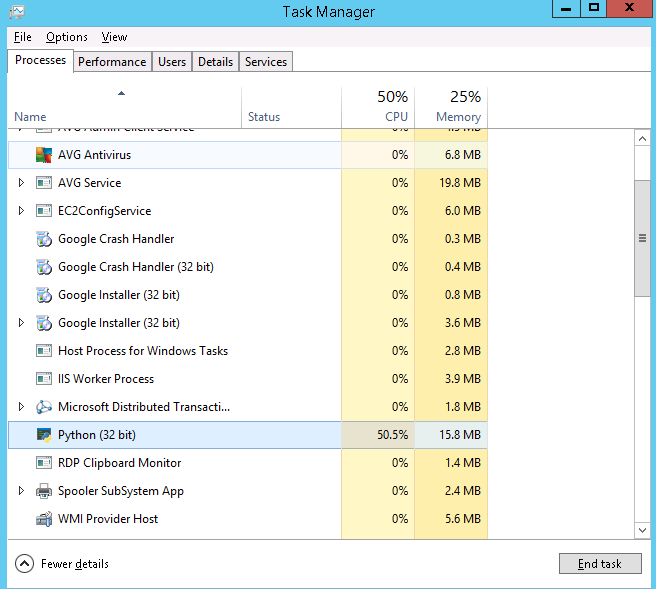


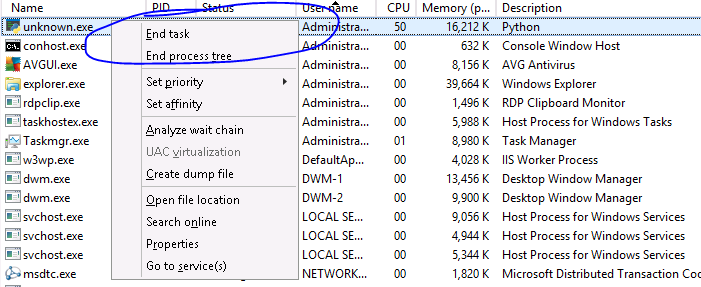












* Next to each “fix” that you documented, note which Cybersecurity Lifecycle activity you performed. Some fixes or tasks may fall into more than one category.
* Show hidden files & file extensions (.exe, .bat, .vb)
* Look at processes and check if it has a verified owner
* Check recycle bin
* Disable inbound packets in the firewall

“Ignore 13 & 16” – Mr. Eaton, 2:12:56 pm September 2, 2021