|  |  |
| --- | --- |
| **Author:** | Sam Marge |
| **Student ID:** | \*00000001 |
| **E-Mail:** | [smarge@uco.edu](mailto:smarge@uco.edu) |
| **Course:** | CMSC 4163/5163 Secure System Administration and Certification |
| **CRN:** | 00000 Fall 2021 |
| **Assignment:** | A4 |
|  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Exercise** | **Maximum** | **Earned** | **Explanation** |
| **1** | **10** |  |  |
| **2** | **10** |  |  |
| **3** | **10** |  |  |
| **4** | **10** |  |  |
| **5** | **10** |  |  |
| **Total** | **50** |  |  |

**Submission format**

**A4\_firstname\_lastname.zip**

Inside this archive file

A4\_firstname\_lastname folder/

A4\_firstname\_lastname.docx (this file modified)

Q1.ps1

Q2.ps1

Q3.ps1

-5 points for any wrong format

PowerShell Programming

**Q1. PDF finder (Q1.ps1)**

Find all PDF files in the system and store them in “ALL\_PDF.txt”.

Sort these files by their sizes and store them in “SIZE\_PDF.txt”.

Group these files by their access time and store them in the following format in “Date\_PDF.txt”

<empty line>

\* YYYY/MM (latest)

<empty line>

List of files

<empty line>

…

<empty line>

\* YYYY/MM (oldest)

<empty line>

List of files

<empty line>

**Q2. Large files finder (Q2.ps1)**

Find the top 100 largest files in the system.

Print the following information in the “LARGEST.CSV” file. Note this is a CSV file.

This file has the following columns.

Column 1: File name

Column 2: Directory

Column 3: File size

Column 4: Last modified time

Column 5: File hash MD5 format (use Get-FileHash cmdlet)

Column 6: File hash SHA1 format (use Get-FileHash cmdlet)

Column 7: File hash SHA512 format (use Get-FileHash cmdlet)

The files are sorted by their sizes from the largest file to the least size file.

Run this script in your computer and find executable files

Get their MD5 hashes.

Go to the virustotal website and enter their hashes.

<https://www.virustotal.com/gui/home/search>

Make a summary of the output.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Order | File name | Directory | | Size | Last modified time | MD5 Hash | Summary of file info from Virustotal |
| 1 | cf74cbdb-0275-41eb-8232-291be8baf1cd1633299063366-0.tmp.exe | C:\Users\saman\AppData\Local\Temp\cf74cbdb-0275-41eb-8232-291be8baf1cd1633299063366-0.tmp.exe | 552151440 | | 10/3/2021 17:19 | D8925C43785BA0F2E0897D460290C298 | Creation Time 2104-08-11 12:54:27  First Seen In The Wild 2021-09-30 15:27:44  First Submission 2021-09-30 16:31:37  Last Submission 2021-10-25 11:08:06  Name: Docker installer  File type: [Win32 EXE](https://www.virustotal.com/gui/search/tag%253Apeexe)  **NOT MALICIOUS**  Signed file valid signature |
| 2 | MRT.exe | C:\Windows\System32\MRT.exe | | 141529560 | 11/12/2021 23:06 | 6FBB07CC9579A0899A967CC90637D16F | Creation Time 1974-04-04 21:44:14  First Seen In The Wild 2020-11-08 21:35:29  First Submission 2021-11-08 21:12:19  Last Submission 2021-11-08 21:12:19  Name: Microsoft Microsoft Windows Malicious Software Removal Too  FileType: Win32 EXE  NOT MALICIOUS  Signed file valid signature |
| 3 | setup\_redlauncher.exe | C:\Steam\steamapps\common\Cyberpunk 2077\setup\_redlauncher.exe | | 138945928 | 8/19/2021 19:29 | 8AE4965C272E31675F3FA3B835843A23 | Creation Time 2020-11-15 09:48:30  First Seen In The Wild 2020-12-09 20:17:55  First Submission 2021-08-19 23:29:28  Last Submission 2021-08-19 23:29:28  Name: Red Launcher  FileType: Win32 EXE  NOT MALICIOUS  Signed file valid signature |
| 4 | lghub.exe | C:\ProgramData\LGHUB\depots\104662\core\lghub.exe | | 136443968 | 11/19/2021 21:00 | 219F713B3002A6741F40FD2D7B82B793 | Creation Time  2021-06-22 18:10:35  First Seen In The Wild  2021-11-16 09:15:06  First Submission  2021-11-16 19:07:49  Last Submission  2021-11-16 19:07:49  Name: LGHUB  FileType: Win32 EXE  NOT MALICIOUS  Signed file valid signature |
| 5 | GeForce\_Experience\_Update\_v3.23.0.74\_Official\_026B48.exe | C:\ProgramData\NVIDIA Corporation\Downloader\60f2d0e7dee93517db08a8f8a2f371dd\GeForce\_Experience\_Update\_v3.23.0.74\_Official\_026B48.exe | | 129592168 | 6/22/2021 23:47 | 4E345EDFB3DDA7910CD1DC36CA889DB2 | Creation Time  2019-04-02 05:08:01  First Seen In The Wild  2021-06-07 20:36:51  First Submission  2021-08-04 23:04:43  Last Submission  2021-08-04 23:04:43  Name: NVIDIA Package Launcher  FileType: Win32 EXE  NOT MALICIOUS  Signed file valid signature |

**Q3. ~~Rock Paper Scissors~~ UCO, OU, OSU, OCU game (Q3.ps1)**

Note: Do not copy the source code on the internet. They will be compared!

* Replace “Rock” with “OU”
  + OU > OCU, OU < OSU
* Replace “Paper” with “OSU”
  + OSU > OU, OSU < OCU
* Replace “Scissors” with “OCU”
  + OCU < OU, OCU > OSU
* Add “UCO”
  + UCO > OU, UCO > OSU, UCO > OCU

Once your script starts, it starts an infinite loop getting one of five words: OU, OSU, OCU, UCO, q

Once q is inserted, the script finishes.

An opponent is simulated using a random number (use Get-Random)

In each turn, show

* Either “You won” or “CPU won”
* CPU’s play and your play
* The total number of plays so far
* The total number of wins so far.
* Please use some colors to make messages interesting

**Q4. Please find the summarize University Central Oklahoma’s policies (https://www.uco.edu/technology/forms-policy/)**

|  |  |  |
| --- | --- | --- |
|  | Summary | URL link |
| Code of Ethics | The code of ethics for UCO has three main values. Civility, Character, and Community. These values are what the code of ethics was based upon. There are some standards that UCO imposes upon any office of information and technology who is granted privileges .  There are 9 standards. 1. Abiding by policies regarding tech. 2. Preventing unauthorized users any access to sensitive info  3. Staying confidential 4. Only altering systems or info when instructed to do so by bosses. 5. Making sure you don’t unauthorized software at work e.g. games  6. Tech needed for job will be provided by UCO  7. Honestly don’t understand this one. Talks about action requests. Meaning corrective action taken against you but wants you to pass it to another employee. The wording is strange. 8. Ask boss when in doubt. 9. Report others if they break rules.  Basically, these rules apply to all OIT members and if these rules are violated UCO says it takes these violations very seriously. Violations can result in losing your job, or being expelled.  I WILL PUT LINK IN THIS BOX AND ONLY IN THIS BOX FOR THE FOLLOWING BOXES. THIS IS BECAUSE FORMATTING IS STRANGE AND IF I PUT THE URL LINK IN THE URL LINK BOX IT MESSES UP THE FORMATTING.  <https://uco.teamdynamix.com/TDClient/1843/Portal/Shared/FileOpen?AttachmentID=994fec3b-e02b-4b2a-9ebb-211d42ab6b43&ItemID=39846&ItemComponent=26&IsInline=0> |  |
| Information security Policy | There are many sub policies in the Information Security Policy. 1. UCO must give students and staff access to the resources they need with an obvious direction. 2. The policy must show intent of UCO and promote IT. 3. Some policies may be from previous policies. 4. Some more can be created on the fly. 5. Director of Information Security will take care of the information security program. 6. Organizations within UCO must have a liaison with the Director of Information security. The university must have policies that support the UCO framework. 8. The university will make sure all responsibilities are known. 9. The university will provided a minimum security requirement. These are just some of the policy details.  There are also responsibilities for certain positions e.g. Director for Information security must administer any security programs. They must also deal with training and reporting of security practices. Directors are responsible for reviewing and updating programs, as well as providing reports on how well the program is doing.  Divisions, colleges, and department leadership must also adhere to certain policies. They must review and implement policies, update standard operations to follow policies, identify who needs training and make sure they do said training, protect sensitive information, and report any information that may have been unintentionally or intentionally disclosed.  <https://uco.teamdynamix.com/TDClient/1843/Portal/Shared/FileOpen?AttachmentID=aead795b-384f-476f-849d-c029dd0b72fb&ItemID=39941&ItemComponent=26&IsInline=0> |  |
| Service Level Agreement | A list of services provided   * Academic Tech * Accounts and access * Application Support * Communications and Collaboration * End-User computing * Help and training * Infrastructure * Security and Privacy * Tech acquisition and implementation * Web and mobile   Provider responsibility   * Make sure client has software and equipment needed * Make sure support requests are dealt with in a timely manner * Escalate issues that need resolved or resolve issues in a timely manner * Make sure communication between you and client is good * Make sure UCOs data is protected   Client responsibility   * Give provider all info and access to any equipment or software that the provider needs to maintain or update systems * Good communication between you and provider   Service availability   * The uptime target level is 99.5% dependent on priority levels. SO some things will get taken care of faster than others.   Service hour   * Monday – Friday, 8:00am to 5:00pm CST/CDT,   Service continuity (recovery or resolution time)   |  |  |  | | --- | --- | --- | | **1** | 10 minutes | Classroom, High   Profile Events, Emergencies | | **2** | 1 hour | Mission Critical   Services | | **3** | 1 business day | Non-Mission Critical   Services | | **4** | 3 business days | Requests |   Contact information  UCO Service Desk  Max Chambers Library, 1st Floor  University of Central Oklahoma  100 N. University Drive  Edmond, OK 73034  405-974-2255  Office of Information Technology  Lillard Administration Building, Suite 102  University of Central Oklahoma  100 N. University Drive  Edmond, OK 73034  405-974-2607  <https://uco.teamdynamix.com/TDClient/1843/Portal/KB/ArticleDet?ID=39579> |  |
| Acceptable Network Usage | Using the network as a means to harass others is not allowed. Any lewd, threatening, harassing content will not be allowed. Depriving others of network resources is not allowed. Try avoiding transmitting lots of data during peak hours. Do not providing false info or identification to access UCO networks. Must not be anonymous when using UCO networks. E-data should always be confidential on UCO systems. Any systems that UCO connects to is also subjected to the same policies. |  |
| Responsible Software Usage | Games that are not approved by UCO are not allowed. This also goes for software in general. Using the software to intimidate or harass or promote any lewd content is also not allowed. Accessing privileged programs, files, or data without authorization is against the rules. UCO accounts should not be used for anything NON-UCO related. |  |
| Any interesting policy that you found | UCO apparently has a policy of training people during cybersecurity awareness month, however this is not enough. In my opinion there should be more training done for everyone. Going through this major, I’ve seen how vulnerable many peoples accounts are. Something as simple as signing out of your Gmail on school computers is overlooked. |  |

**Q5. Imagine you created a company with an IT infrastructure.**

Please make policies for your company.

|  |  |
| --- | --- |
|  | Summary |
| Your Company Name | Big Fat Company |
| Your Company’s Business | ?? |
| Code of Ethics | At least 3 paragraphs |
| Information security Policy | At least 3 paragraphs |
| Service Level Agreement | A list of services provided  Provider responsibility  Client responsibility  Service availability  Service hour  Service continuity (recovery or resolution time)  Contact information |
| Acceptable Network Usage | At least 3 paragraphs |
| Responsible Software Usage | At least 3 paragraphs |
| Any interesting policies of your preference | At least 3 paragraphs |