**Lesson 3 – Network Security**

**PROJECT 3.1.4 – FIND THE SECRETS**

**LINUX BASED COMMANDS**

|  |  |
| --- | --- |
| **COMMAND** | **DESCRIPTION** |
| ls | List the contents of a directory. With:  No argument list the current working directory.  -l return a long listing showing permissions and other information.  -a a list all files, specifically hidden files beginning with a . (dot).  -R show the entire directory structure, recursively listing all contents. |
| cd | Change directory.  cd [filename] changes to a subdirectory.  cd .. changes to the parent directory.  A . (dot) indicates the current directory. |
| pwd | Print the working directory. |
| cat | Display the contents of a file. (From concatenate.) |
| mkdir | Create (make) a directory. |
| mv | Move a file/directory to a new name and/or location. The general syntax for the move command is mv [source] [destination]. |
| touch | Create a file and/or change the file timestamp to the current time. |
| cp | Copy a file/directory to a new name and/or location. Syntax is cp [source] [destination]. |
| rm | Delete (remove) a file. |
| rmdir | Delete (remove) an empty directory. |
| File | Show a file’s type, as determined by the operating system. |
| Gpg | Encrypt/decrypt a file. With:  -c Create an encrypted version of a file.  -d Decrypt the encrypted version of a file. |
| ps | Show processes running in the system. With:  -ef Show everyone's processes, including other users, in a formatted output.  --sort=uid Group all users’ processes together. |
| more | more Display the contents of a file similar to the cat command, but you control the output. |
| bg/fg | Send process to the background or bring them to the foreground. |
| Grep | Search for strings in a file or when piped, search output of a command (as in ps -ef | grep alpha)  -e Search for separate, multiple strings. |
| Su | Change your user id to root, the account with the most privileges. |
| kill | Terminate a process. To terminate important processes, such as a shell, use the -9 or -KILL flag. |

***Sample Plan of Action:***

* **Identify unauthorized users on the system.**
  + Use the ps command to find all users running processes on the system.
  + Know the authorized users described in Activity 3.1.3.  These are root, daemon, www-data, 101, statd, 103, mysql.
  + From the project description, know that delta and gamma are also authorized users.
* **Find any processes being run by unauthorized users; they are malicious!**
  + Use ps -ef --sort=uid to organize processes by user ID. Look for processes being run by unauthorized users.
  + Also, use ps -ef |grep -e [username] to see processes owned by specific users.
  + Trace process through the process tree to find the process(es) that launched the suspicious processes.
* **Stop the malicious process(es) and ensure they do not start again**
  + Use the su and kill commands, referencing the PIDs from the previous step to kill suspicious process.
  + Take are when killing processes.
* **Find the files that started the process(es) and remove them.**
  + Escalate privileges when necessary with the su command.
  + Find the path to the scripts and the path to the executable files from the output of ps -ef.
* **Remove all files and directories associated with the malicious users.**
  + Escalate privileges when necessary with the su command.
  + Use the rm command to remove suspicious files, removing all files found that are launching suspicious processes.
  + Ensure processes did not start again, if they did, kill them, taking care with the kill command.

**Genera hints:**

* Files and directories may be hidden.
* Unauthorized users may be logged in and running malicious processes.
* Killed processes may automatically restart.
* Use either the delta or the gamma user account to perform your security tasks.
* Reference your Linux commands table to recall how to manage files, directories, and processes.

**SECURITY UPDATE REPORT**

**Identify unauthorized users on the system.**

|  |
| --- |
|  |

**Find any processes being run by unauthorized users; they are malicious!**

Unauthorized Users

|  |
| --- |
|  |

We Used

|  |
| --- |
|  |

We traced processes (2 Items)

|  |
| --- |
|  |

**Stop the malicious process(es) and ensure they do not start again (5 Items)**

|  |
| --- |
|  |

**Find the files that started the process(es) and remove them (3 Items)**

|  |
| --- |
|  |

**Remove all files and directories associated with the malicious users. (2 Items)**

|  |
| --- |
|  |

**CONCLUSION**

Compare the differences and similarities of securing processes, files, and directories in Windows and in Linux. Create a computational artifact, such as a table, Venn diagram, or mind map.

|  |
| --- |
|  |