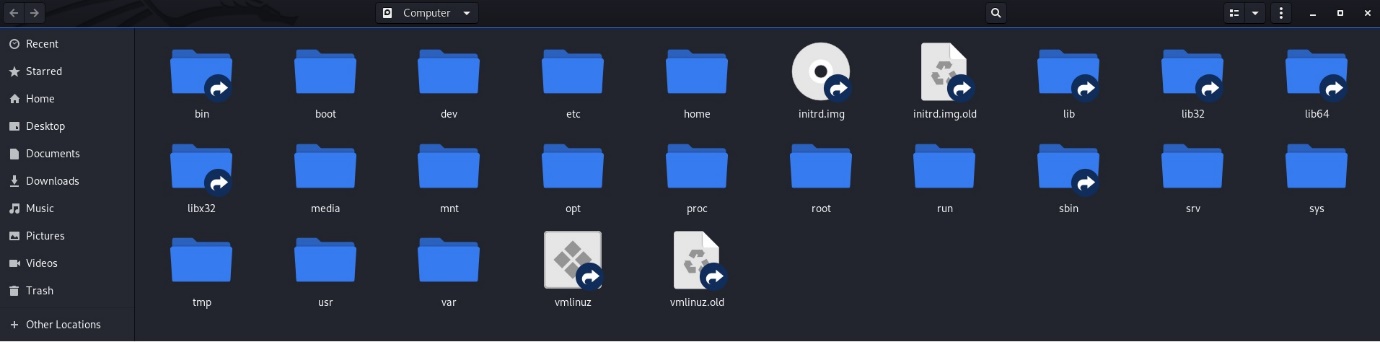
[Home](https://doretox.github.io/) » [Posts](https://doretox.github.io/posts/)

**Understanding the Linux file system**

Understanding how Linux file system is organized.

April 13, 2020 · doreox

The Linux filesystem structure is somewhat different from that of Windows. Linux has roots in UNIX so it has the backslash for directory separation and its name system is case sensitive. For example, on a Linux file system the following files: file.txt, File.txt and FIle.txt are different. The Linux system is completely file-based and this makes it different from Windows systems. Let’s see below how the file system is organized in Linux.

*Folders in Kali Linux.*

**/bin**

Bin is an abbreviation for binaries. Here is where application binaries (the equivalent of executables in Microsoft Windows) reside. For example, LS (to list directories), cat (to show the contents of a file) and other basic functions.

**/sbin**

Sbin means system binary. These are binaries that only the system administrator can use, and that a standard user would be able to use without permission.

**/boot**

This directory contains everything necessary to initialize your system. For example the Linux Kernel.

**/cdrom**

There may be differences here depending on the distribution you are using. On Ubuntu-based distributions this folder is present, it is responsible for the temporary storage of CD-ROMs inserted in the system.

**/dev**

The /dev directory contains the special device files for all the devices connected to your computer. For example, any device that is plugged into your computer (mouse, monitor and keyboard) will have a file created within this directory. This directory is commonly accessed by drivers.

**/etc**

There are a lot of discussions about the meaning of etc, but it was confirmed by Dennis Ritchie, co-creator of Linux which means etcetera. It is in this folder all the system configurations and scripts accessed by programs, for example, the APT command.

**/home**

The user’s home directory. Here is stored all your personal data, files and user-specific configuration files.

**/lib, /lib32 and /lib64**

In this folder are the libraries. Libraries are files that programs can use to execute functions stored in \ bin and \ sbin.

**/media**

Where CDs and USB devices are usually attached or mounted to the filesystem.

**/mnt**

Where other filesystems are attached or mounted to the filesystem.

**/opt**

Here applications are installed manually and are not a part of the critical functioning of the system.

**/proc**

Proc is where you will find files with information about processes and resources. Every process will have a file in this directory. It does not exist directly on your machine, they are created every time the machine is started.

**/root**

This directory works much like / home, storing files for the ROOT user.

**/run**

This folder stores various information from the period of which the machine was on, such as which user logged into the machine. Like / proc this directory is also virtual, being deleted and created again every time your computer is restarted.

**/srv**

This folder is used if you are using a server. The files that will be accessed by external users are stored here for greater security.

**/sys**

This directory is an interface to the kernel.

**/tmp**

This is the temporary files directory. Here applications store files that will be used in the current session.

**/usr**

Here they are installed as applications used by the system user.

**/var**

Here variables are stored that the system expects to increase in size over time, such as system logs.

**Conclusion**

At first the file system on Linux may seem confusing, but it’s just a matter of getting used to it. Most users grew up using a computer with Windows or Mac, so any system other than this ends up generating some discomfort. Over time you will find that the Linux file system is very well organized and intuitive.

* [Linux](https://doretox.github.io/tags/linux/)



* [Learn](https://tryhackme.com/r/hacktivities)
* Zeek



Zeek

Introduction to hands-on network monitoring and threat detection with Zeek (formerly Bro).

medium

120 min

Share your achievementHelpSave Room

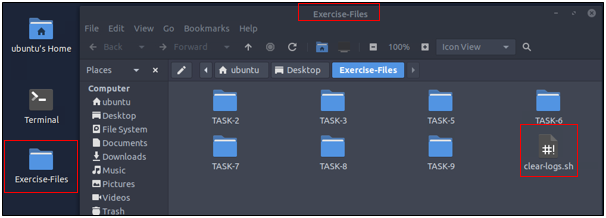
628

Options

**Room completed ( 100% )**

Task 1Introduction

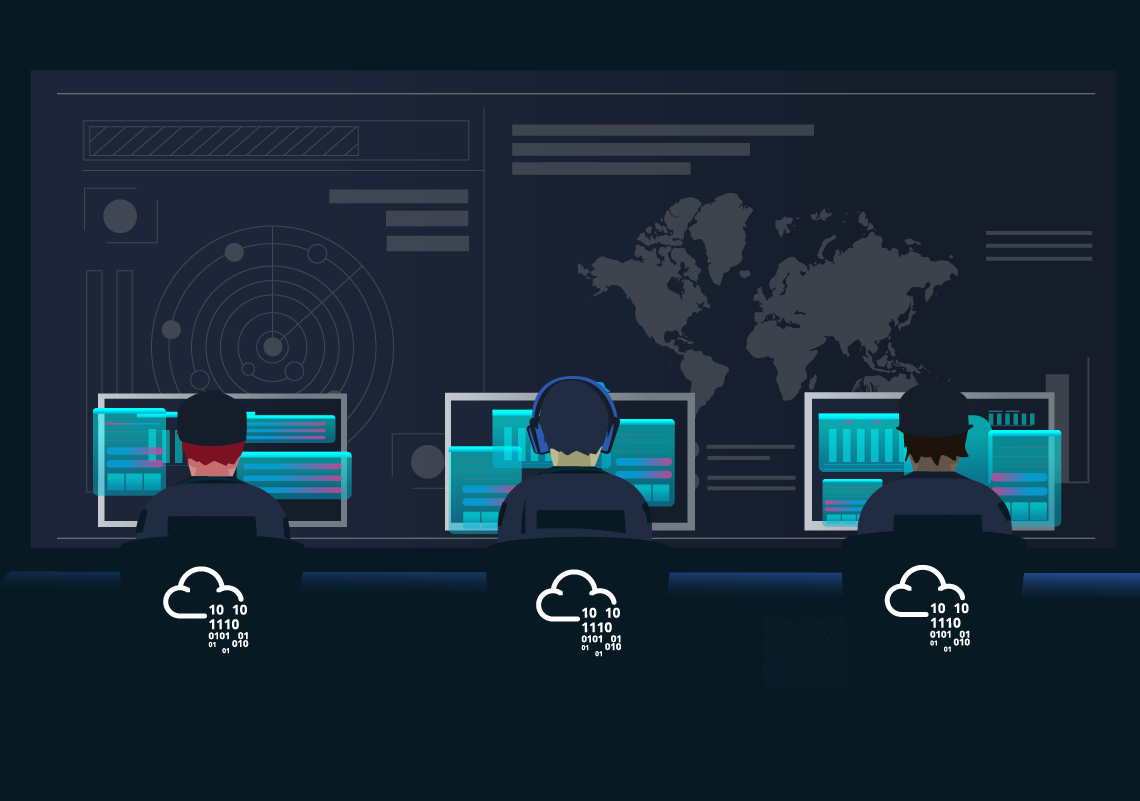




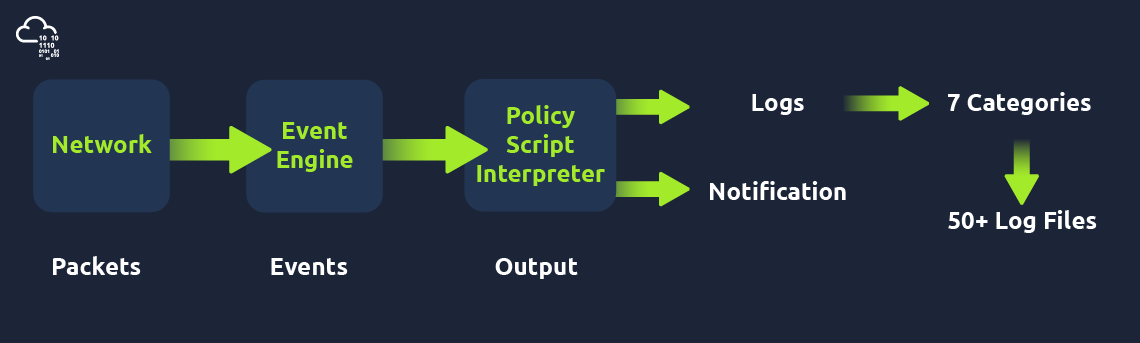
Top of Form

Bottom of Form

Task 2Network Security Monitoring and Zeek



|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

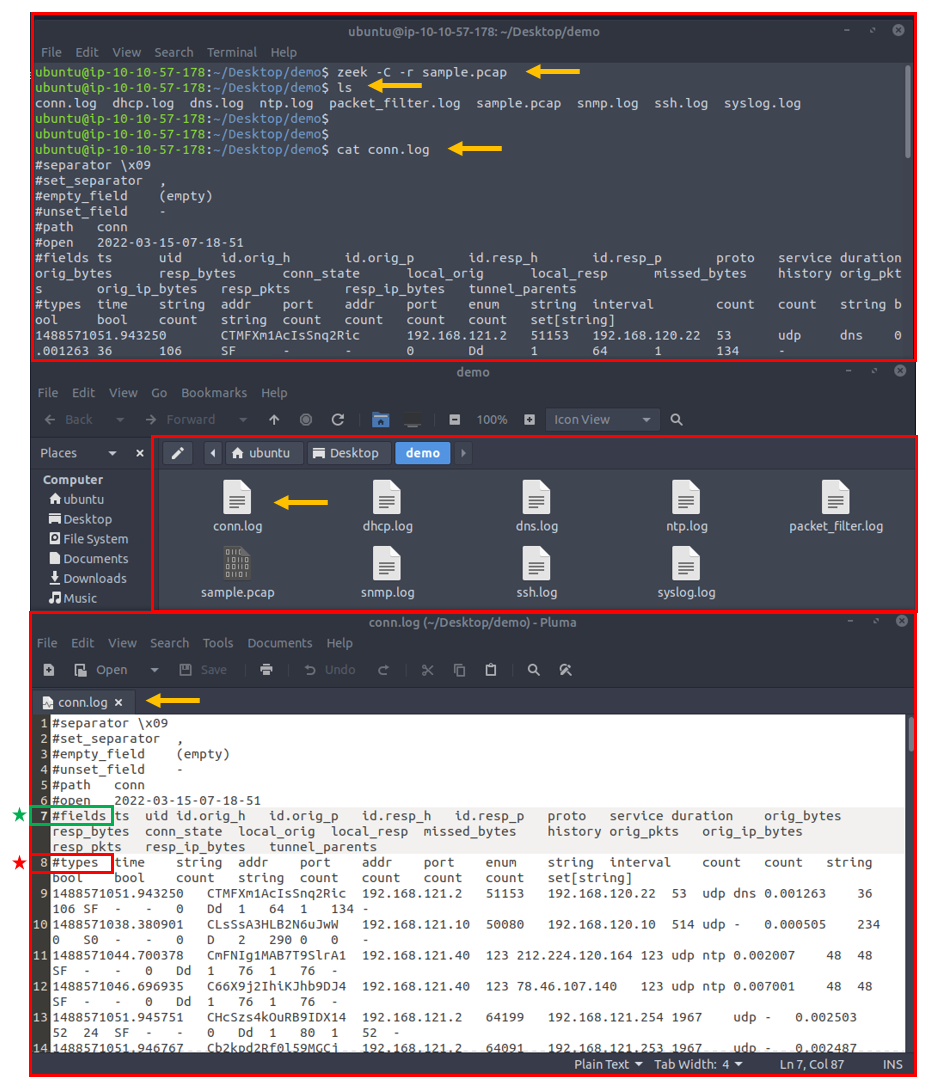
Task 3Zeek Logs



|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |



|  |  |
| --- | --- |
|  |  |
|  |  |

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Task 4CLI Kung-Fu Recall: Processing Zeek Logs



|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |
| --- | --- |
|  |  |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Top of Form

Bottom of Form

Task 5Zeek Signatures



|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

|  |
| --- |
|  |
|  |

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

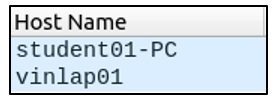
Top of Form

Bottom of Form

Task 6Zeek Scripts | Fundamentals



|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |



|  |
| --- |
|  |
|  |

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Task 7Zeek Scripts | Scripts and Signatures



Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Task 8Zeek Scripts | Frameworks



Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Task 9Zeek Scripts | Packages



|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Top of Form

Bottom of Form

Task 10Conclusion

**Congratulations!**You just finished the Zeek room. In this room, we covered Zeek, what it is, how it operates, and how to use it to investigate threats.

Now, we invite you to complete the Zeek Exercise room: **[ZeekExercises](https://tryhackme.com/room/zeekbroexercises" \t "_blank)**