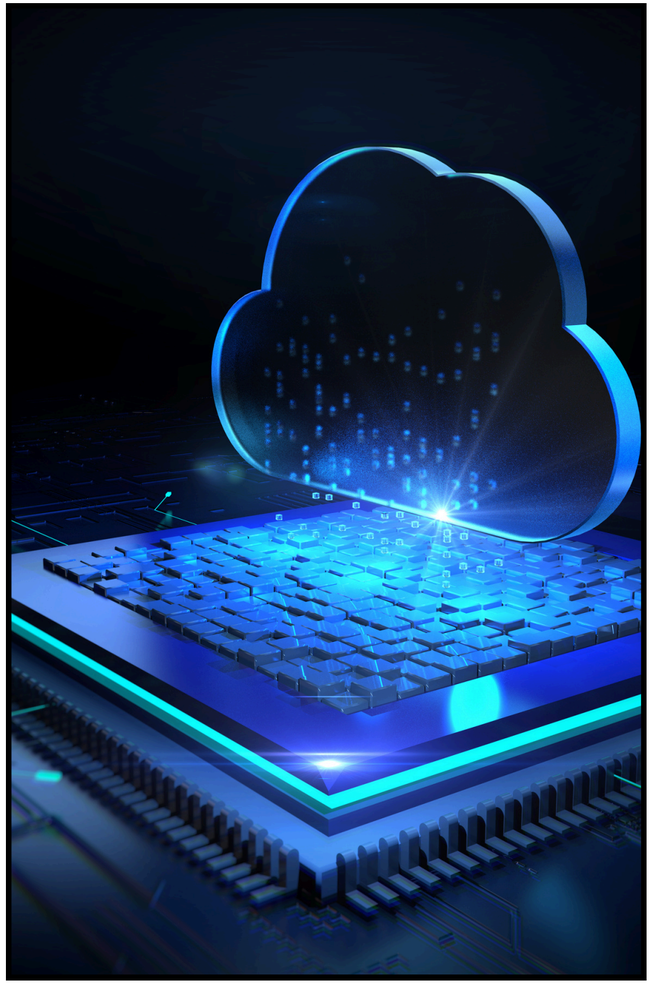
Hacktales

Virtualization, Linux & Network Services

WEEK 2

WHAT IS VIRTUALIZATION?

INTRO TO VIRTUALIZATION



DEFINITION

Virtualization is the process of creating virtual versions of computing resources, such as operating systems, servers, storage, or networks, instead of using physical hardware directly. It allows multiple virtual environments to run on a single physical machine, improving efficiency, flexibility, and resource management.

WHAT IS VIRTUALIZATION?

TYPES:

- Server Virtualization – Multiple virtual servers run on a single physical server (e.g., VMware ESXi, Microsoft Hyper-V).
- Desktop Virtualization – A full OS runs as a VM on a desktop (e.g., VirtualBox, VMware Workstation).
- Network Virtualization – Virtual networks overlay physical infrastructure (e.g., VLANs, SDN).
- Storage Virtualization – Combines multiple storage devices into a single virtual storage pool.
- Application Virtualization – Runs applications in isolated environments without installing them on the host OS (e.g., Docker, Citrix).

KALI LINUX LAB SETUP

INTRO TO KALI & UTILIZING LINUX

INTRO

Kali Linux is a Debian-based Linux distribution designed for cybersecurity professionals, ethical hackers, and penetration testers. Developed and maintained by Offensive Security, Kali comes preloaded with hundreds of tools for penetration testing, digital forensics, reverse engineering, and security research.

Its key feature is the suit of pre installed security tools.

Lab Practice, Setup & Linux Tutorial

Refer to the Practice lab manual

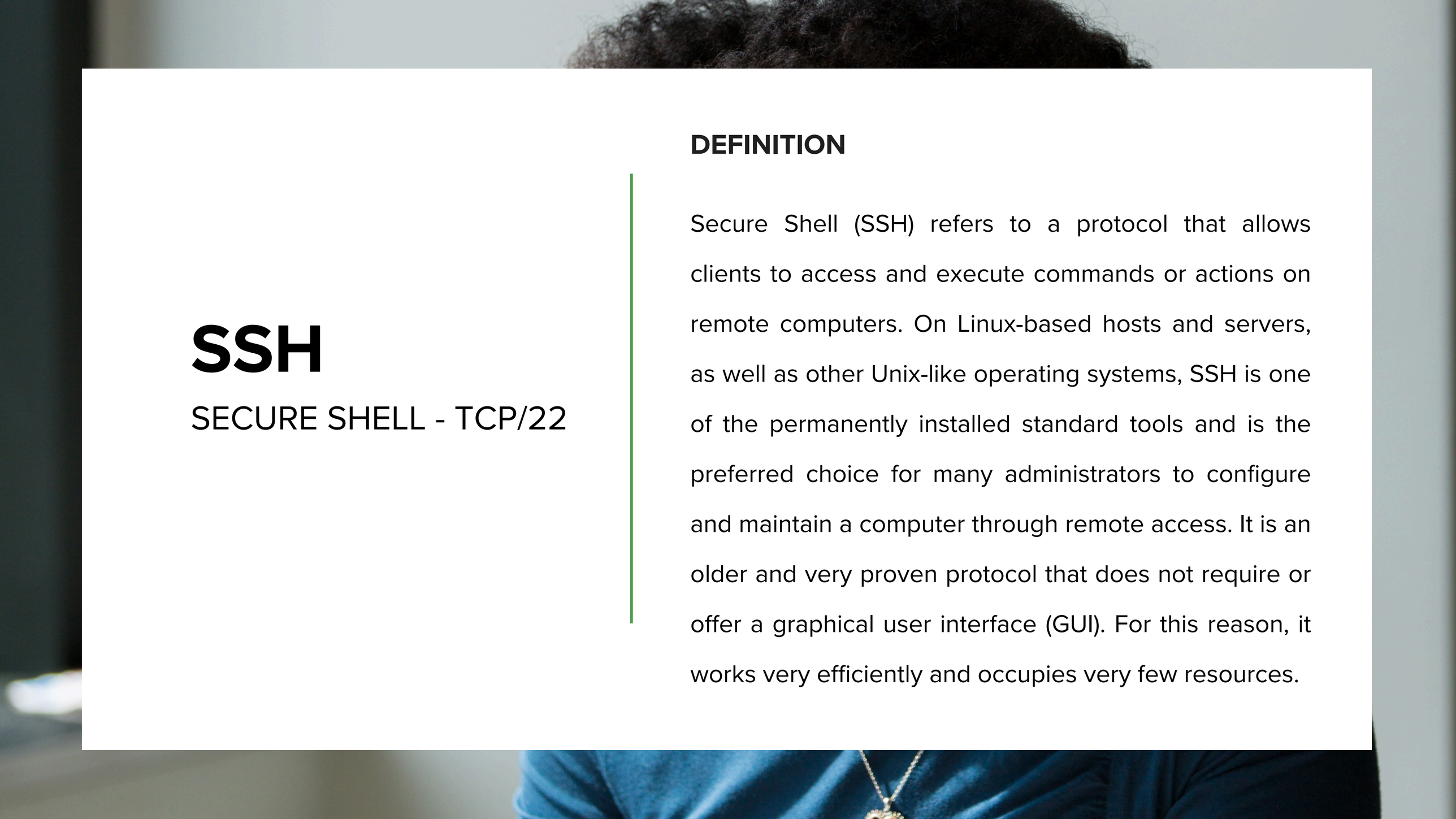
SERVERS & NETWORK SERVICES

SERVERS

A server is a computer or software that provides services, resources, or data to other computers (clients) over a network. Servers are designed to handle requests and manage resources efficiently, making them essential for web hosting, file storage, databases, and cloud computing.

NETWORK SERVICES

Network services are applications or processes that enable communication, resource sharing, and data exchange between devices over a network. These services allow users and systems to interact efficiently, whether on a local network (LAN) or the internet.



SSH

SECURE SHELL - TCP/22

DEFINITION

Secure Shell (SSH) refers to a protocol that allows clients to access and execute commands or actions on remote computers. On Linux-based hosts and servers, as well as other Unix-like operating systems, SSH is one of the permanently installed standard tools and is the preferred choice for many administrators to configure and maintain a computer through remote access. It is an older and very proven protocol that does not require or offer a graphical user interface (GUI). For this reason, it works very efficiently and occupies very few resources.

FTP

FILE TRANSFER PROTOCOL - TCP/20,21

DEFINITION

The File Transfer Protocol (FTP) is one of the oldest protocols on the Internet. The FTP runs within the application layer of the TCP/IP protocol stack. Thus, it is on the same layer as HTTP or POP. These protocols also work with the support of browsers or email clients to perform their services. There are also special FTP programs for the File Transfer Protocol. In an FTP connection, two channels are opened. First, the client and server establish a control channel through TCP port 21. The client sends commands to the server, and the server returns status codes. Then both communication participants can establish the data channel via TCP port 20. This channel is used exclusively for data transmission, and the protocol watches for errors during this process.

One of the most used FTP servers on Linux-based distributions is vsFTPd. The default configuration of vsFTPd can be found in /etc/vsftpd.conf, and some settings are already predefined by default. There are many different alternatives to it, which also bring, among other things, many more functions and configuration options with them. Some configurations are dangerous and can be exploited by an attacker to gain access to sensitive files served on the File Server.

DANGEROUS CONFIGS

Some dangerous configs include the following:
anonymous_enable=YES anon_upload_enable=YES
anon_mkdir_write_enable=YES
no_anon_password=YES
anon_root=/home/username/ftp write_enable=YES

SMB

SERVER MESSAGE BLOCK - TCP/445

OVERVIEW

SMB is a client-server protocol that regulates access to files, directories, and other network resources such as printers, routers or interfaces for the network. Main application area was on Windows and newer Microsoft OS can easily communicate with devices that have older OS (Downwards compatible). A free software iteration of SMB is Samba on Linux and can also be known as Common Internet File System (CIFS). An SMB server can provide arbitrary parts of its local file system as shares, Access rights are defined by ACL. ACL right are defined based on the shares and do not correspond to the local rights on the server. NetBIOS service usually runs along side it connects over 137,138,139/TCP but CIFS uses soly 445/TCP.

DANGEROUS CONFIGS

The following are dangerous configurations on an SMB server that could be leveraged by an attacker to compromise an SMB sever:

- browseable = yes
- read only = no
- writable = yes
- guest ok = yes
- enable privileges = yes
- logon script = script.sh
- magic script = script.sh


Q
&
A

ASSIGNMENT

Complete this Nmap room on TryHackMe that provides a comprehensive guide to how the tool works
https://tryhackme.com/room/furthernmap