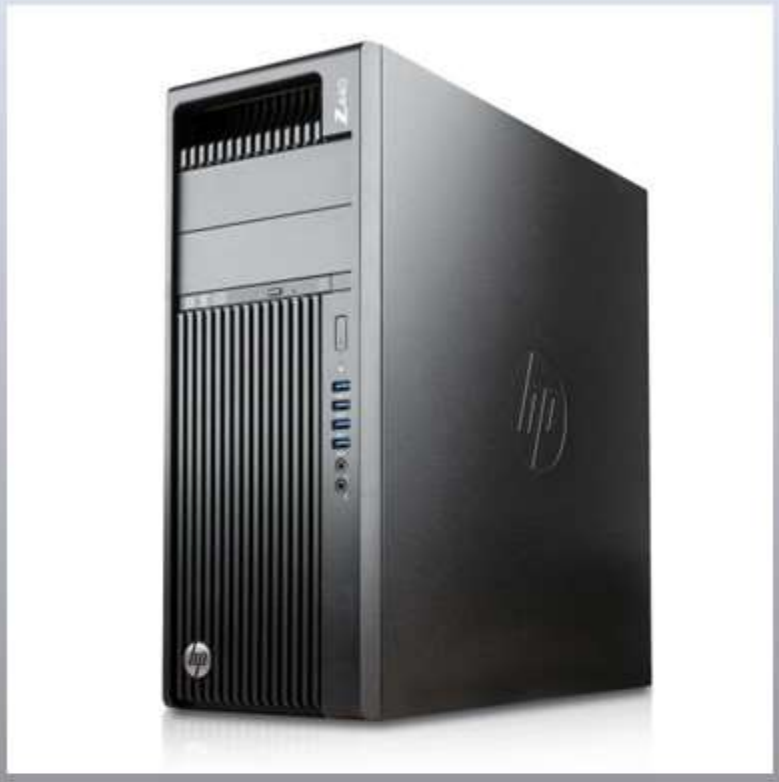
The 440 project

440



Project 440

The goal of the 440 project The goal of the 440 project is to inspire the next generation cyber security experts, IT professionals and web designers. The project is geared towards entry level individuals as to not intimidate individuals from learning a new skill.

What is project 440?

The 440 project is another example of life cycled equipment being repurposed to create a cost-effective entry-level Linux learning environment for individuals interested in learning about Cyber Security, computer hardware or just learning how to better protect yourself from cyber criminals. The 440 is an HP Z440 desktop pc repurposed as a self-contained range. It is a multipurpose unit designed to allow an individual to choose the type of project they would like to pursue. I chose Linux Mint for the base operating system for the purpose of an easy format to introduce Linux to individuals who have never had an opportunity to work with Linux. What makes this project special is VirtualBox, a hypervisor which makes it possible to load and use multiple pc's without having to spend an outrageous amount of money and space to have a physical version of each pc. At the time of composing this article the 440 machine has Twelve VMs loaded.

The basics

The Machine itself has Linux Mint installed. If you don't know much about Linux, Linux mint is a great way to get started. It is a user-friendly desktop environment with a little similarity to a Windows PC in layout. The basic menus and other operations are logical and easy to understand. Even if you don't do anything with VirtualBox, there is plenty to learn within the basic machine. Some of the processes of Linux are the same no matter which version you're using. Basic line commands is one thing that can be learned while using just the Linux Mint Operating system. All Linux systems have the ability to run functions by line commands in a terminal window. It's also an easy way to experience some of the software programs available through the software manager.

What can you do with the 440 project?

- Learn Linux
- The basics of using line commands and a terminal window
- Basic network tools
- Computer work station and server hardware essentials
- Software installation
- Work with cyber-Security tools
- Learn how to work with WordPress websites
- Learn about HTML and writing html code
- Practice working with Python script
- Working with VirtualBox
- Practice with Capture the Flag VM's

Scenario 1

The basics. If you would like to work with Linux and get a better knowledge base, the 440 Project can help by providing a basic easy to use and understand version of Linux, Linux Mint. There are more advanced versions (flavors) of Linux, but Linux mint is great for entry level since it has similarities to Windows systems.

Scenario 2

Use the system to work with other types of operating systems virtually so you don't have to have build a physical computer for each project. Some of the projects in 440 are Ubuntu server, TrueNas Server, VyOS router / Router. pfSense Router, Kali Linux, Parrot OS and Caine OS just to mention a few.

Scenario 3

Use the basic system to learn nMAP, a network mapping tool. nMAP is used industry wide to investigate and identify your network devices. It's a great tool to identify potential vulnerabilities within both your home or work place network. You can identify which device is using which IP address and which ports the device is using. You can even possibly identify devices that don't belong on your network.

Scenario 4

The 440 Project can be used as a capture the flag training event. By starting the VM router, one of the CTF targets and one of the forensic VM desktops, you can work on your capture the flag skills.

Scenario 5

Start up the router, one of the WordPress websites and one of the desktop pc's you can learn how to manage a WordPress website, by using the admin console page and testing your work.

Scenario 6

Start the router, the TrueNAS server and one of the desktops and you can work on your server administrator skills. This allows you to gain an understanding of file sharing from a server. TrueNAS allows you practice as a system administrator and manage permission to access files and folders as well as user management.

Scenario 7

Use VirtualBox to create your own VM. By downloading an ISO of your favorite operating system and creating a new machine in VirtualBox

Scenario 8

Use the systems tools to manage hard drive space using tools such as Gparted. Use the basic tools to create and manage different types if storage systems and understanding the different RAID systems.

There are more scenarios that this project can be used for as the ones listed above are just a small sample of what can be done with this machine.

What's in it?

Hardware

HP Z440 or HP8300

- I7 Processor with 4 cores and 8 threads or Xeon with 6 cores and 12 threads
- 32gb RAM
- 1TB hard drive
- Graphics card
- 1 additional ethernet adapter (nic)

Software

Linux Mint OS

The purpose of Linux Mint is to produce a modern, elegant and comfortable operating system which is both powerful and easy to use. This is an excellent entry level introduction to Linux.

Some of the reasons for the success of Linux Mint are and why it's used in this project:

- It works out of the box, with full multimedia support and is extremely easy to use, excellent for individuals who are looking for an easy introduction into Linux.
- It's both free of cost and open source.
- It's community-driven. Users are encouraged to send feedback to the project so that their ideas can be used to improve Linux Mint.

- Based on Debian and Ubuntu, it provides about 30,000 packages and one of the best software managers.
- It's safe and reliable—thanks to conservative software updates, a unique Update Manager, and its robust Linux architecture.
- Linux Mint requires very little maintenance (no regressions, no antivirus, no anti-spyware...etc.).

VirtualBox is open-source software program for virtualizing the x86 computing architecture. Basically, it's a program that allows you to run an entire Operating system without having to install it on its own hardware. VirtualBox makes it possible to have multiple operating systems on one machine. It acts as a hypervisor, creating a VM (virtual machine) where the user can run another OS (operating system). The operating system where VirtualBox runs is called the "host" OS. The operating system running in the VM is called the "guest" OS. VirtualBox supports Windows, Linux, or macOS as its host OS.

Nmap ("Network Mapper") is a free and open-source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts.

Gparted The gparted application is the GNOME partition editor for creating, reorganizing, and deleting disk (hard drive) partitions. A disk device can be subdivided into one or more partitions. The gparted application enables you to change the partition organization on a disk device while preserving the contents of the partition.

Brave internet browser the core of Brave's best-in-class online privacy. By default, Brave blocks ads and trackers on the websites you visit. And you can easily import bookmarks and other settings from your old browser.

Fedora media writer is a tool that helps users put images / operating systems on their portable drives such as flash disks. It is able to automatically download the required image for them and write them in a dd-like fashion, using either dd itself or some other way to access the drive directly. This overwrites the drive's partition layout though so it also provides a way to restore a single-partition layout with a FAT32 partition.

K3b DVD Kreator If you have used a burning program such as Nero under Windows, K3b will feel quite familiar. Featuring a simple, yet powerful graphical interface, K3b provides various options for burning a CD, DVD, or BD (Blu-ray disc). Various types of optical projects are supported including (but not limited to) audio and data, video projects for DVD and VCD, as well as multi-session and mixed-mode discs. K3b also has the ability to erase re-writeable media and can perform more complicated tasks such as audiovisual encoding and decoding.

Midori internet browser The Midori browser has been developed, keeping in mind, your privacy and security online. The way it does this is by preventing sites from getting access to any of your data. They also prevent the allocation of ads, which means you get a browsing experience that is pure and hassle-free.

Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc.) free and open-source application which aims to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users. Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines. Scan results can be saved and viewed later. Saved scan results can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database.

WireShark is a network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions.

Visual Studio is a lightweight but powerful source code editor which runs on your desktop and is available for Windows, macOS and Linux. It comes with built-in support for JavaScript, TypeScript and Node.js and has a rich ecosystem of extensions for other languages and runtimes (such as C++, C#, Java, Python, PHP, Go, .NET).

Sublime is a versatile, fun, and fast text editor for code and prose that automates repetitive tasks so you can focus on the important stuff. It is supported on macOS, Windows and Linux. Its versatility comes from a wide range of community-developed third-party packages that provide syntax highlighting, snippets, or other automation backed by Python plugins. The default distribution of Sublime Text aims to provide a basic but very functional set of features, but it can easily be turned into a full-fledged IDE, if so desired.

Atom is a free and open-source text and source code editor, available for cross platform Operating Systems – Windows, Linux and Mac OS X. It is released under MIT License, written in C++, HTML, CSS, JavaScript, Node.js and Coffee Script, Atom is based on Chromium.

BlueFish is a powerful editor targeted towards programmers and web developers, with many options to write websites, scripts and programming code. Bluefish supports many programming and markup languages.

VirtualBox VM's Below you will find a list of Virtual Machines currently installed in the 440 project.

Router / firewall

The 440 system uses a combination of a virtual router through VirtualBox and the physical ethernet connections to create IP addresses for the system. The virtual router can either be the pfSense VM or the VyOS VM, both of these routers work great as a virtual router / firewall or if you have an old PC, you can build a dedicated router. The biggest difference out of the box is that pfSense uses a graphical user interface (GUI) and VyOS is run with line commands. Both of these are great to use and each one has its own advantages and is a matter of personal preference. These are excellent tools for learning how a router or firewall works. Probably the biggest advantage to using a virtual router is that if you make a mistake and can fix your problem you can reset the VM and start over. There are 2 ethernet jacks on the pc, one that can be connected to a live internet connection, WAN (optional) and a second ethernet jack is setup to be a bridged connection creating a LAN for both the VM's inside of VirtualBox and a connection for additional PC's to be connected to system.

pfSense software is a free, open-source customized distribution of FreeBSD specifically tailored for use as a firewall and router that is entirely managed via web interface. In addition to being a powerful, flexible firewalling and routing platform, it includes a long list of related features and a package system allowing further expandability without adding bloat and potential security vulnerabilities to the base distribution.

VyOS More than a router. VyOS is not just a router: It's an open, customizable platform for network devices. VyOS is an open-source network operating system based on Debian. VyOS provides a free routing platform that competes directly with other commercially available solutions from well-known network providers. Because VyOS is run on standard amd64 systems, it can be used as a router and firewall platform for cloud deployments.

The biggest difference between these two routers is that VyOS doesn't have a web interface to manage, it strictly uses a terminal console and command line interface (CLI)

Forensics

CAINE 13.0 (Computer Aided investigative Environment) is an **Italian** GNU/Linux live distribution created as a Digital Forensics project. CAINE offers a complete forensic environment that is organized to integrate existing software tools as software modules and to provide a friendly graphical interface.

The main design objectives that CAINE aims to guarantee are the following:

- an interoperable environment that supports the digital investigator during the four phases of the digital investigation
- a user-friendly graphical interface
- user-friendly tools

Kali Linux is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. It does this by providing common tools, configurations, and automations which allows the user to focus on the task that needs to be completed, not the surrounding activity.

Parrot Security OS Parrot Security (ParrotOS, Parrot) is a Free and Open-source GNU/Linux distribution based on *Debian Stable* designed for security experts, developers and privacy aware people. It includes a full portable arsenal for IT security and digital forensics operations. It also includes everything you need to develop your own programs or protect your privacy while surfing the net.

Server VM's

Ubuntu 22.04 LTS server. In the 440 project, Ubuntu Server is labeled dotlamp, partly because this was built to broadcast the local web pages for the range as well as provide a server application.

TrueNAS Core server is the free version of TrueNAS. TrueNAS CORE (formerly known as FreeNAS) is the world's most popular storage OS because it gives you the power to build your own professional-grade storage system to use in a variety of data-intensive applications without any software costs. Simply install it onto hardware or a VM and experience the true storage freedom of open-source storage. TrueNAS also has other versions of their server software which are used throughout the industry.

CTF

Insanity A web hosting provider has asked you to test their security. Can you find the vulnerabilities on their server and gain root access?

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application. It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bWAPP prepares one to conduct successful penetration testing and ethical hacking projects.

Rickdiculously Easy is a fedora server vm, created with VirtualBox. It is a very simple Rick and Morty themed boot to root. It's designed to be a beginner CTF for entry level individuals.

More exercises are available both through WICTRA and the internet. This is just a sample and a beginners setup.

Websites

WordPress websites

WordPress is an open-source content management system (CMS). It's a popular tool for individuals without any coding experience who want to build websites and blogs. The software doesn't cost anything. Anyone can install, use, and modify it for free. more than online use WordPress.

This machine has a couple of Virtual websites created using WordPress. These VM's allow the user to experiment with how these websites are managed and also provide a way for individuals who would like to learn how to create web pages as a webpage designer.

Desktops The Desktop operating systems below are just a small sample of the options in Linux operating systems. The ones used in the setup are easy to understand for entry level individuals. These systems make

for an easy learning curve for individuals that currently only know Windows as an operating system. These versions are capable of doing just about anything in Linux, but provide a Graphic User Interface (GUI) or known as point and click.

Linux Mint The purpose of Linux Mint is to produce a modern, elegant and comfortable operating system which is both powerful and easy to use. This is an excellent entry level introduction to Linux. To read more about Linux Mint, refer to description listed above or go to the Linux Mint website. A virtual version is installed in this machine for those who would like to test their skills with managing software and other applications.

KDE Neon is another desktop operating system. It has similarities to Linux Mint in that it's a desktop system. Because it's designed on a different platform it offers a different experience on how Linux operates. More info can be found on the KDE Neon website.

Ubuntu is another desktop operating system. Ubuntu also has a server distribution which is also on this machine under servers. Ubuntu is one of the main systems used. There is more information than we room to write about. Visit the Ubuntu website for more information.

Back / restore process / system recovery

The system has a compete duplicate backup hard drive, which means that ii the event of a system crash, system becomes corrupt and needs to be reset, the system hard drive can be removed and replace with the duplicate. And the system will be back to a fresh start. Duplicate hard drives can be made using a disk duplicator.

Definitions

VM Virtual Machine

GUI What's a GUI? If you're reading this, chances are you're looking at one! GUI stands for graphical user interface. A GUI, which some folks pronounce as 'gooey', is exactly what it sounds like... a graphical way to do stuff. Simply put, a **graphical user interface** is a way to communicate what you want to a computer application (or computer operating system) using graphical symbols rather than typing the instructions in.

CTF Capture The Flag

CLI is a command line program that accepts text input to execute operating system functions.

RAID (redundant array of independent disks) is a way of storing the same data in different places on multiple hard disks or solid-state drives (SSDs) to protect data in the case of a drive failure. There are different RAID levels, however, and not all have the goal of providing redundancy.

Terminal A terminal is a text-based interface or window that allows you to interact with the operating system via a shell.

ISO An ISO file (often called an ISO image), is an archive file that contains an identical copy (or image) of data found on an optical disc, like a CD or DVD. They are often used for backing up optical discs, or for distributing large file sets that are intended to burned to an optical disc

Repository In Linux, a repository (or "repo" for short) is a central location where software packages are stored and maintained for distribution.

Root On Linux, root refers to two things: the root directory and the root user. The root directory is the parent directory that contains every file and folder on your system. You can use the wildcard "**/**" (forward slash) to denote the root directory in your commands.

Hypervisor A hypervisor is a software that you can use to run multiple virtual machines on a single physical machine. Every virtual machine has its own operating system and applications. The hypervisor allocates the underlying physical computing resources such as CPU and memory to individual virtual machines as required. Thus, it supports the optimal use of physical IT infrastructure.

Links

Code.visualstudio.com

www.sublimetext.com

itsfoss.com

www.virtualbox.org

www.pfsense.org

vyos.io

www.truenas.com

securityonionsolutions.com

kali.org

www.w3schools.com

nmap.org

linuxmint.com

ubuntu.com

distrowatch.com

caine-live.net

parrotsec.org

bitnami.com

wordpress.com

bluefish.openoffice.nl

atom-editor.cc

fedoraproject.org/en/workstation/download/

wireshark.org

www.freecodecamp.org/news/the-linux-commands-handbook/

questions or technical support contact WICTRA

at

info@wictra.org