Intro to Hacking and Programming

Level 0x00: The Shell

Quick Overview

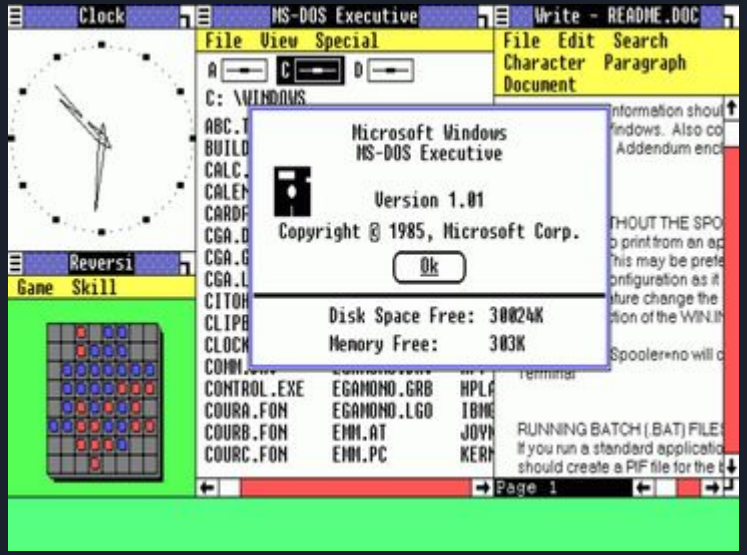
- Basic Programming
  - C (and C++)
  - Python
  - Scripting (bash)
- Operating system concepts
  - User privileges
  - Networking
  - Memory
- Software Security Concepts
  - Crypto / Hashing
  - Disassembly / Reverse Engineering
  - How are bugs in software turned into exploits

Operating Systems - UNIX-like

- Unix
  - AT&T Bell Labs in 1970s by Ken Thompson, Dennis Ritchie, Brian Kernighan
  - Examples include: BSD, HP-UX, Solaris, SGI Irix
  - Multi-tasking, multi-user, programming tools included
  - Unix philosophy: “Write programs that do one thing and do it well”
- OpenBSD / FreeBSD
  - University of California Berkeley open sources their Unix - permissive license
  - Also used by Mac OS, iOS, Playstation 3 (and newer)
- Linux
  - Created by Linus Torvalds, first posted to Usenet in 1991
  - RedHat, Suse, Debian, Ubuntu, Android

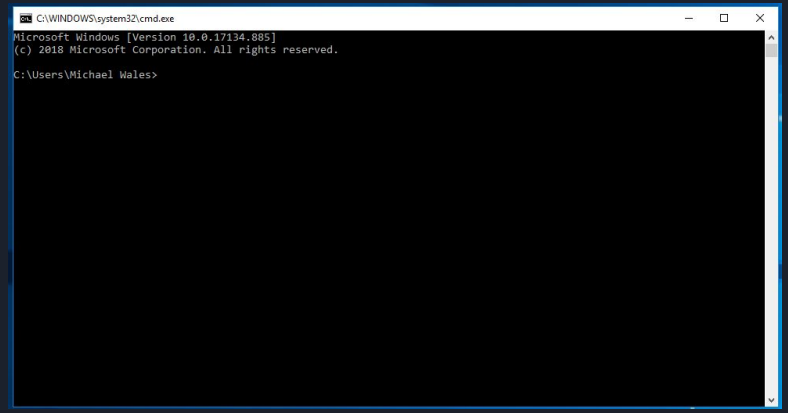
Operating Systems - Windows

- MS-DOS
  - Main PC operating system in the 80s
  - One application at a time
  - 8.3 filenames
- Windows (DOS Application)
  - Multiple applications
  - Resizable GUIs, Networking
- Windows 95/NT
  - Became core operating system
  - Long filenames
  - Start menu
  - 32-bit Only



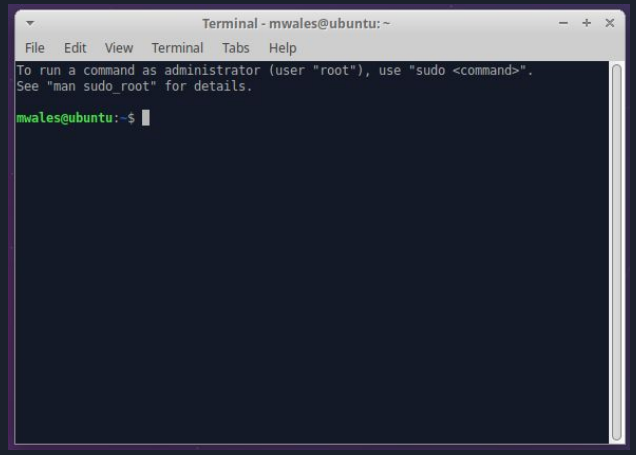
Windows Shell Basics

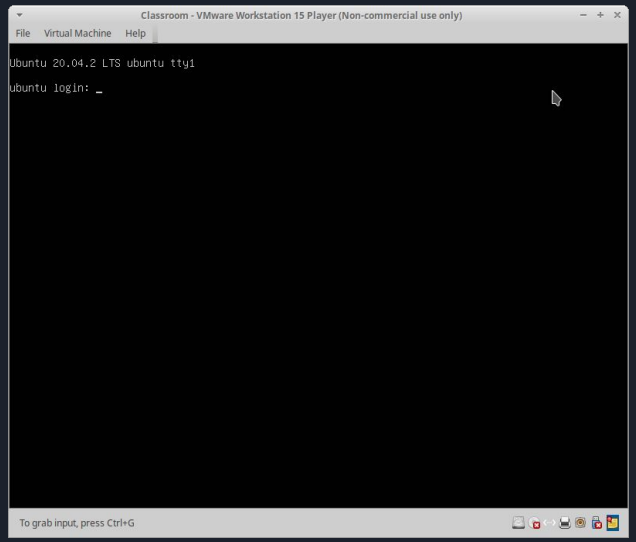
- Windows Basic Shell
  - Press Win+R to bring up Run dialog
  - Type cmd to open shell
  - Functional, but very basic
- Windows Alternative Shells
  - Powershell
  - WSL (Windows Subsystem for Linux)
  - WSL2



Linux Shell Basics

- Bourne Shell (sh): Standard old-school shell for Linux and Unix systems
- Alternative shells:
  - bash, dash: Very similar, more features
  - csh, tcsh, ksh, zsh, probably more…
- Many ways to access the shell
  - GUI Shell Program (Terminal)
  - `/dev/tty1` text console
    - CTRL+ALT+F1 (through F6 typically)
    - CTRL+ALT+F7 restores GUI
  - Serial port
  - Remotely via SSH (or Telnet)





Filesystem

- Filesystem is usually a directory of files on your SSD / hard disk
  - Windows: C: D: (drive letters)
  - *nix: / /mnt /media/cdrom
- Each directory can have thousands of files and other directories

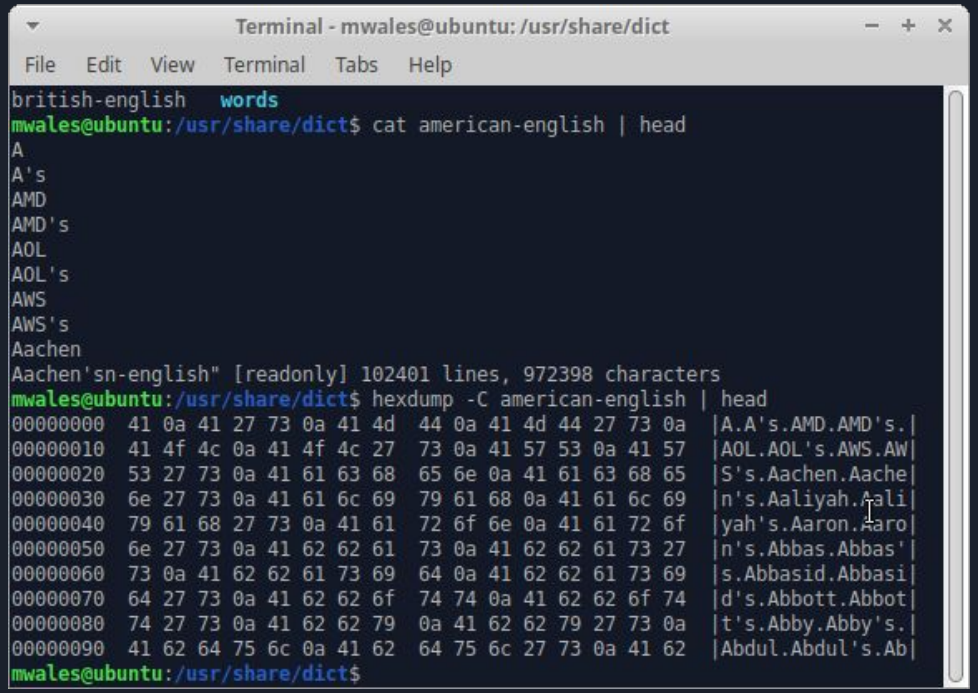
Command	Explanation
`pwd`	Present working directory
`ls`	List contents of a directory

Directory Commands

Command	Explanation
`mkdir DIRECTORY`	Makes a new directory
`cd DIRECTORY`	Changes to a subdirectory
`cd ..`	Changes to the parent directory
`rmdir DIRECTORY`	Removes a directory (must be empty)
`tree`	Lists all files / subdirectories

Files

- Common contents of a file
  - Text
  - Executable Programs
  - Databases (SQL)
  - Compressed Archive
  - Images
  - Word document
    - Compressed Archive
    - Text
    - Images

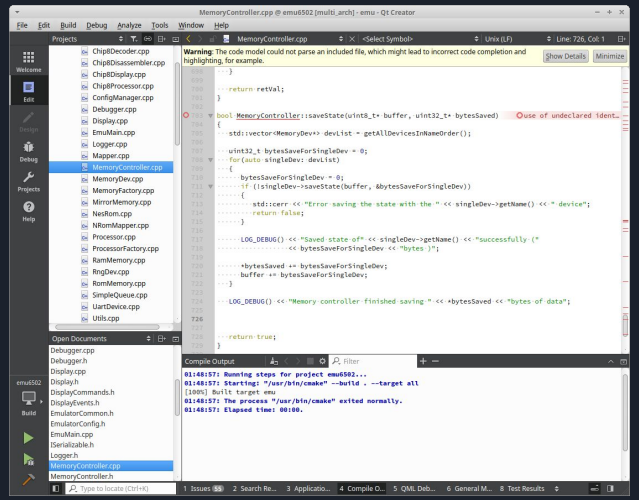


File Commands

Command	Explanation
`touch FILE`	Creates a blank file
`cat FILE`	Displays contents of a file
`head FILE`	Displays beginning of a file
`tail FILE`	Displays ending of a file
`hexdump FILE`	Displays contents of a binary
`file FILE`	Tells you what type of a file

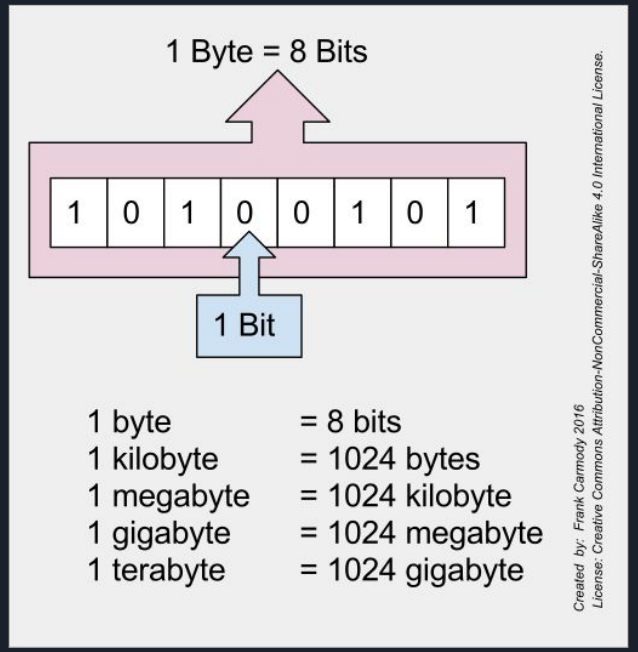
Editors

- GUI
  - Simple: write text, save to a file
    - Gedit, Mousepad, Notepad
  - Coding: automatic coloring, auto-complete
    - Geany
    - Sublime ($)
    - Atom
  - IDE: integrated development environment
    - Qt Creator
    - Visual Studio
    - CLion
- Command Line
  - vi / vim, emacs
  - nano, pico



Bits / Bytes

- Bit: Either 0 or 1 (binary)
- Bytes: 8 bits (uint8_t)
  - 00000000 = 0
  - 11111111 = 255 = 0xff
  - 2 possible states for 8 bits = 2^8
- Bigger Numbers via more bits.
  - 2^{16} = uint16_t = 65,536
  - 2^{32} = uint32_t = 4,294,967295
- Negative numbers (Signed Integers) int8_t
  - Highest bit is a sign bit
  - 2's complement
- Floating Point (32-bit and 64-bit)



ASCII Encoding

- ASCII encoding: Mapping of number 0 - 127 to characters
  - 1-byte for each character
  - 1st bit of ASCII always 0 (less than 128)
- Some of the 128 are non-printable
  - 10 = newline “\n”
  - 7 = bell
  - 127 = delete
- Other encoding
  - UTF-8, UTF-16, UTF-32
  - Emoji

Dec	Chr	Dec	Chr	Dec	Chr	Dec	Chr	Dec	Chr
0	NUL	26	SUB	52	4	78	N	104	h
1	SOH	27	ESC	53	5	79	O	105	i
2	STX	28	FS	54	6	80	P	106	j
3	ETX	29	GS	55	7	81	Q	107	k
4	EOT	30	RS	56	8	82	R	108	l
5	ENQ	31	US	57	9	83	S	109	m
6	ACK	32		58	:	84	T	110	n
7	BEL	33	!	59	;	85	U	111	o
8	BS	34	"	60	<	86	V	112	p
9	HT	35	#	61	=	87	W	113	q
10	LF	36	$	62	>	88	X	114	r
11	VT	37	%	63	?	89	Y	115	s
12	FF	38	&	64	@	90	Z	116	t
13	CR	39	'	65	A	91	[	117	u
14	SO	40	(	66	B	92	\	118	v
15	SI	41	)	67	C	93	]	119	w
16	DLE	42	*	68	D	94	^	120	x
17	DC1	43	+	69	E	95	_	121	y
18	DC2	44	,	70	F	96	`	122	z
19	DC3	45	-	71	G	97	a	123	{
20	DC4	46	.	72	H	98	b	124	|
21	NAK	47	/	73	I	99	c	125	}
22	SYN	48	0	74	J	100	d	126	~
23	ETB	49	1	75	K	101	e	127	DEL
24	CAN	50	2	76	L	102	f		
25	EM	51	3	77	M	103	g		

File Commands

Command	Explanation
`strings FILE`	Prints out printable strings of a binary file
`sort [FILE]`	Prints lines in alphabetical order
`uniq [FILE]`	Removes redundant lines out output
`wc [FILE]`	Counts number of words in a file
`dos2unix / unix2dos [FILE]`	Converts file line endings
`more / less [FILE]`	Shows output 1 page at a time
`grep needle [FILEs]`	Searches for a string

Standard Input / Output

- 3 file descriptors open by CLI application
  - 0 = stdin (standard input)
  - 1 = stdout (standard output)
  - 2 = stderr (standard error)
- Pipes (|) can be used to connect output from one application to input of another application

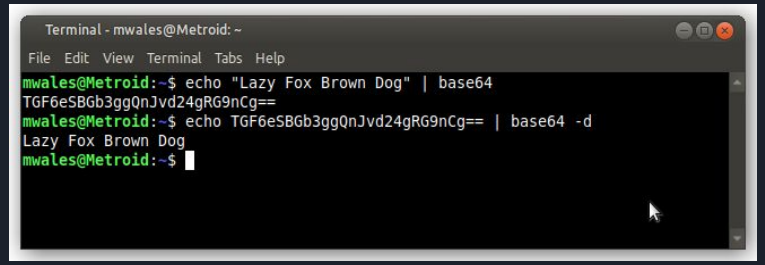
```
strings somefile | grep -i password

cat logfile | sort | unique
```

I/O Redirection

- Using "`> file.txt`" after a command causes output from stdout to be redirected into a file
  - You won't be able to see it on screen
  - stderr will still be displayed
- Using "`2> file.txt`" after a command causes stderr to be redirected into file
- Using "`> file.txt 2>&1`" causes both to be redirected
  - Order matters!
- `tee` will write standard output to a file and also write it to the screen
  - Ex: `./myprogram arg1 arg2 | tee logfile.txt`
- >> will append to existing file, > overwrites it

base64



- A byte represents 0 - 255.
- Printable ASCII is 32 - 127 (94 characters)
- `base64` uses 64 characters (6 bits)
  - A-Z a-z
  - 0-9
  - + /
  - = (padding, it's always at the end)
- You can use base64 to encode binary data into printable text (3 binary bytes -> 4 `base64` characters)
- Uses
  - Email attachments
  - Dumping a binary file out via serial shell
  - Simple obfuscation
- `base64 -d` decodes base64 back into binary/ASCII

Shell scripts

- A series of commands in a text file
  - Linux
    - Can start text file with #! (shebang) and make executable
    - Can call interpreter directly
  - Windows
    - .bat (batch) files
    - Windows Power Shell
- Can take arguments ($1, $2)
- Number of arguments ($#)
- Command Substitution (not just for scripts)
  - `echo “There are `ls *.txt | wc -l` files in this directory”`
  - `echo “There are $(ls *.txt | wc -l) files in this directory”`

Basic Networking

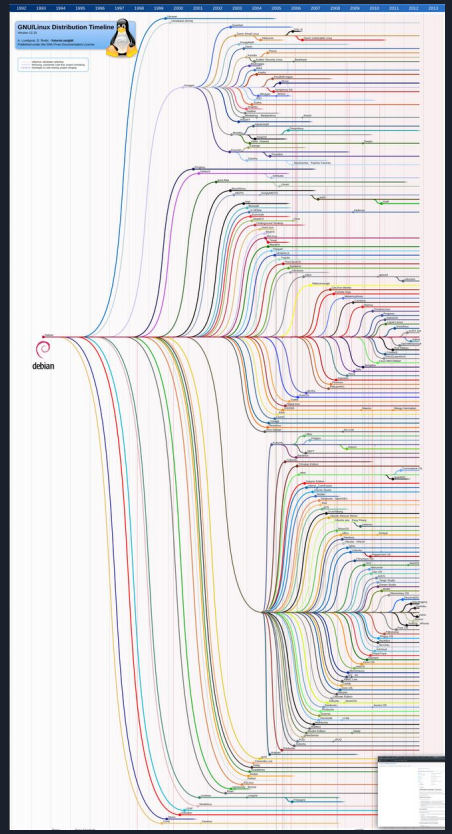
- IP4 Address
  - 32-bit number
  - 4 octects 0-255, example: 192.168.1.101
- Port Number
  - 0 - 65535
  - Ports 0-1023 are special, require root to listen on
- Secure Shell (SSH)
  - Usually listens on port 22
  - Allows remote shell access via name/pass, or name/encryption-key

Netcat / Socat

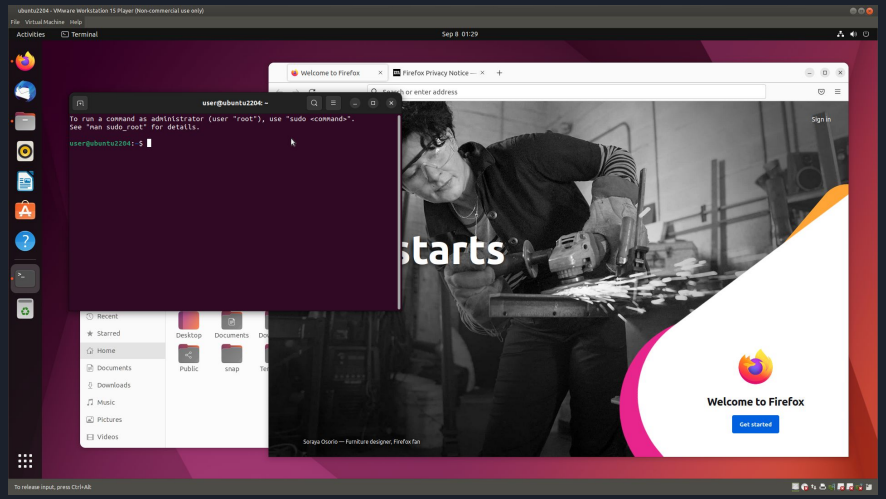
- Utilities to listen/connect to TCP/UDP sockets
  - Netcat (nc): old / many implementations
  - socat: newer, can do encryption, files
- Netcat chat
  - Server
    - `nc -l -u 1337`
    - Listens for UDP
  - Client
    - `nc -u remote_ip 1337`
    - Connects to UDP server
- Create a remotely accessible shell
  - `socat tcp4-listen:1337 exec:/bin/sh`

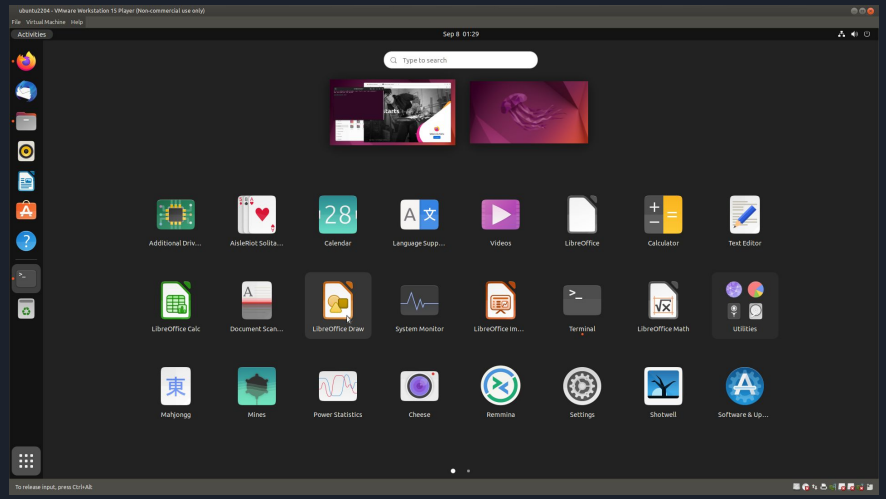
Ubuntu

- Child / Fork of Debian Linux
- Ubuntu provides:
  - Software repository with > 20,000 packages (apps, libraries)
  - Apt package manager
    - Installs new packages
    - Updates packages
    - Removes packages
- Ubuntu has many flavors
  - Which desktop manager used by default
  - Which applications used by default
  - Custom theming
- Releases every 6 months
  - LTS every 2 years. 22.04 is current LTS

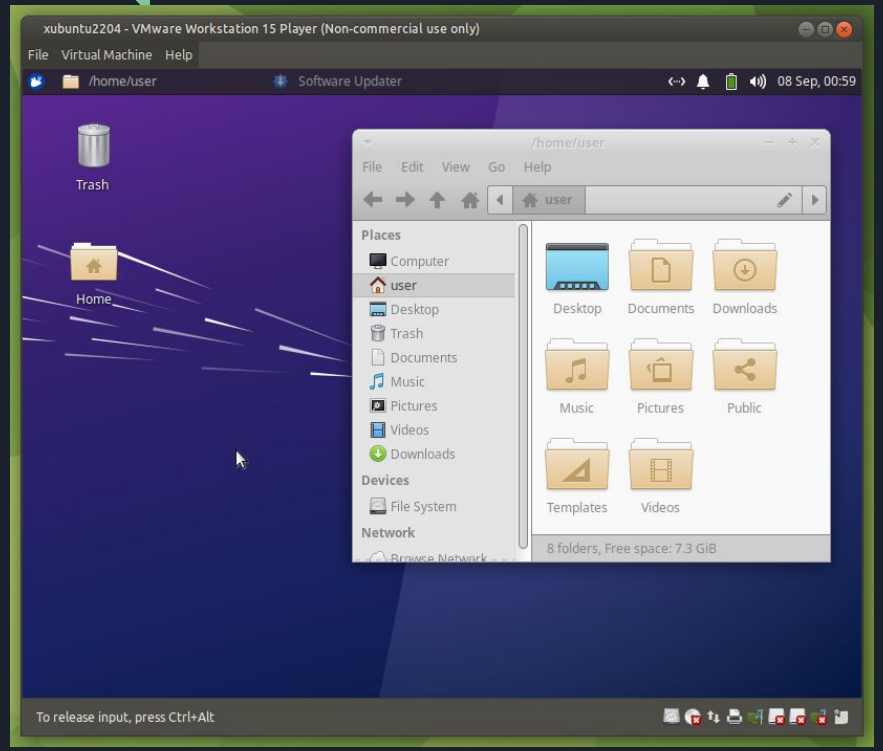


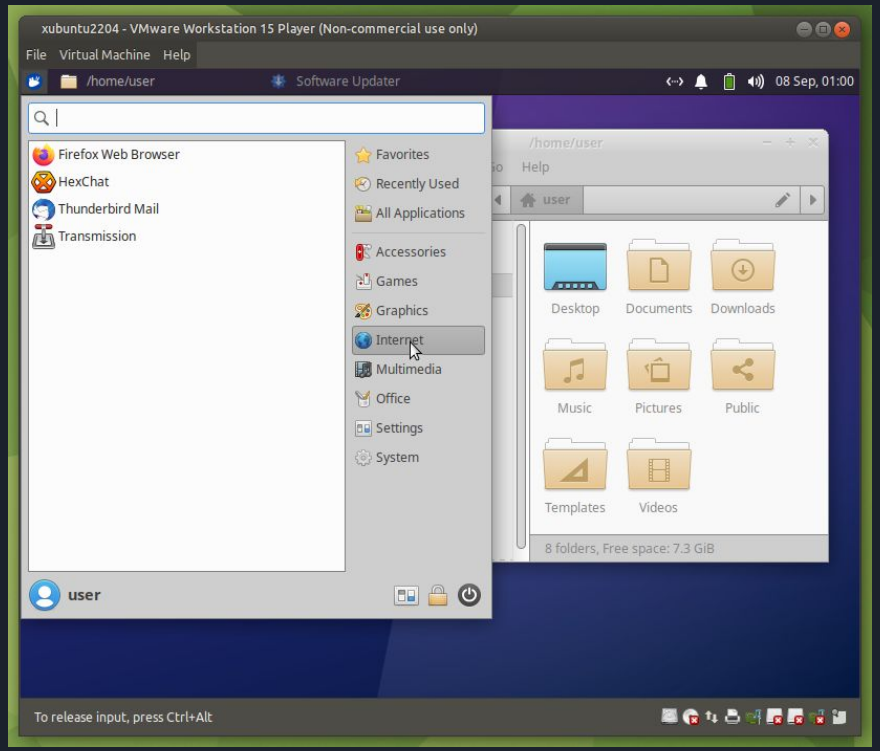
“Vanilla” Ubuntu



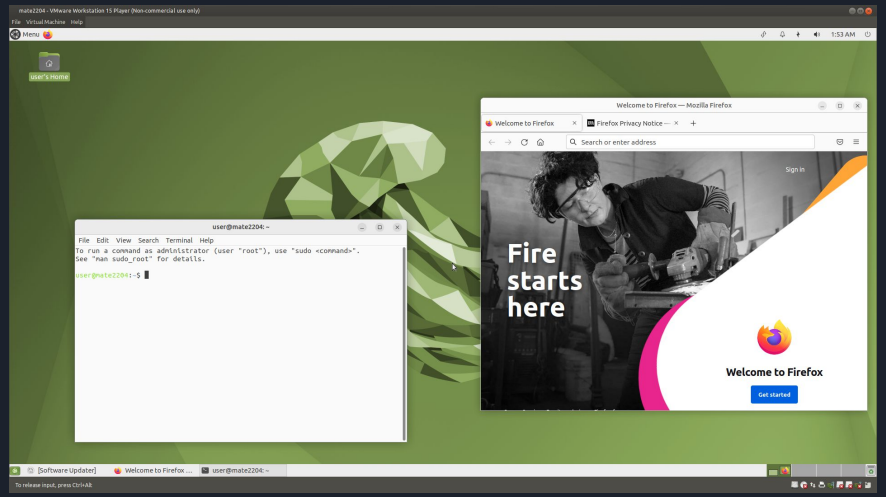


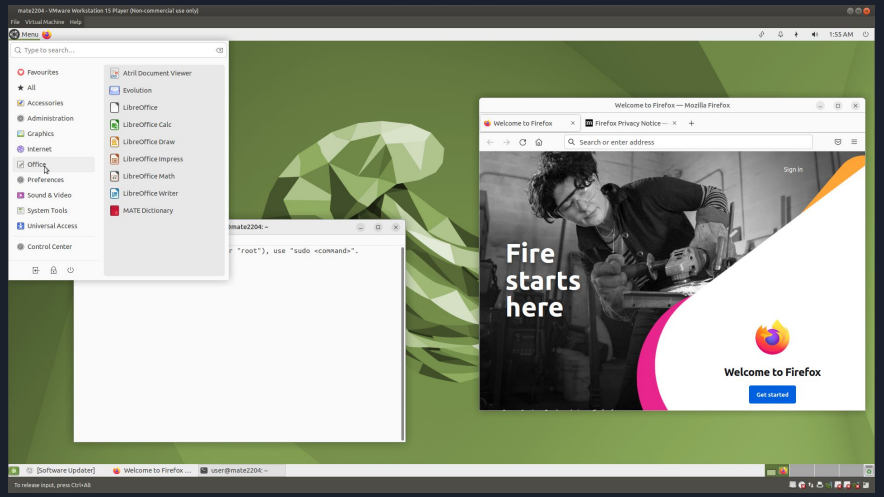
Xubuntu


xubuntu2204 - VMware Workstation 15 Player (Non-commercial use only)
File Virtual Machine Help
/home/user
Software Updater
08 Sep, 00:59
Trash
Home
/home/user
File Edit View Go Help
user
Places
Computer
user
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
8 folders, Free space: 7.3 GiB
To release input, press Ctrl+Alt


xubuntu2204 - VMware Workstation 15 Player (Non-commercial use only)
File Virtual Machine Help
/home/user
Software Updater
08 Sep, 01:00
Firefox Web Browser
HexChat
Thunderbird Mail
Transmission
Favorites
Recently Used
All Applications
Accessories
Games
Graphics
Internet
Multimedia
Office
Settings
System
user
/home/user
Help
user
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
8 folders, Free space: 7.3 GiB
To release input, press Ctrl+Alt

Ubuntu MATE


mate2204 - VMware Workstation 15 Player (Non-commercial use only)
File Virtual Machine Help
Menu
1:53 AM
user's Home
Welcome to Firefox — Mozilla Firefox
Welcome to Firefox
Firefox Privacy Notice —
Search or enter address
Sign in
Fire starts here
Welcome to Firefox
Get started
user@mate2204: ~
File Edit View Search Terminal Help
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
user@mate2204:~$
[Software Updater]
Welcome to Firefox ...
user@mate2204: ~
To release input, press Ctrl+Alt


mate2204 - VMware Workstation 15 Player (Non-commercial use only)
File Virtual Machine Help
Menu
1:55 AM
Type to search...
Favourites
All
Accessories
Administration
Graphics
Internet
Office
Preferences
Sound & Video
System Tools
Universal Access
Control Center
Atril Document Viewer
Evolution
LibreOffice
LibreOffice Calc
LibreOffice Draw
LibreOffice Impress
LibreOffice Math
LibreOffice Writer
MATE Dictionary
Welcome to Firefox — Mozilla Firefox
Welcome to Firefox
Firefox Privacy Notice —
Search or enter address
Sign in
Fire starts here
Welcome to Firefox
Get started
[Software Updater]
Welcome to Firefox ...
user@mate2204: ~
To release input, press Ctrl+Alt

Attributions

- Ken Thompson and Dennis Ritchie: from Wikipedia, public domain
- Linus Torvalds: Wikimedia Creative Commons Attribution-Share Alike 3.0
- Windows screenshot: https://en.wikipedia.org/wiki/File:Windows1.0.png
- Bits/Bytes: Frank Carmody
- Debian Family Tree: Andreas Lundqvist, Donjan Rodic from wikimedia.org