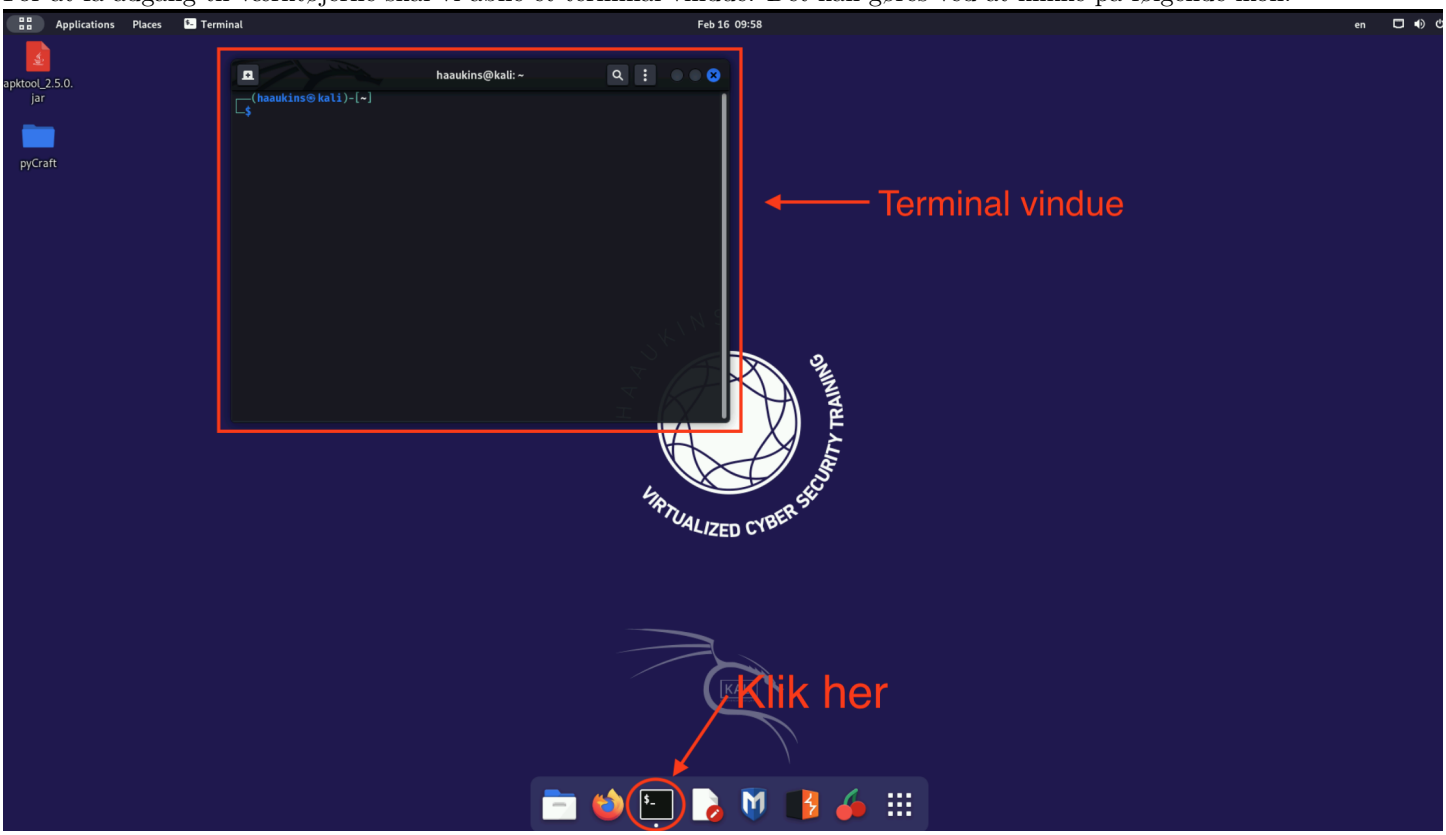
Værktøjskassen

Dette er en værktøjskasse, med et par gængse værktøjer, som du vil få brug for til nogle opgaver inde på Haaukins platformen. Alle værktøjer som skal bruges til opgaverne er allerede installeret på den virtuelle linux maskine. For at bruge nogle af værktøjerne skal vi benytte os af et terminal vindue. Husk at alle værktøjer beskrevet herunder kan rigtig mange ting og derfor vil det altid være en god ide bruge lidt tid med at søge lidt på internettet eller lignende inden man bruger de forskellige værktøjer.

Terminal

For at få adgang til værktøjerne skal vi åbne et terminal vindue. Det kan gøres ved at klikke på følgende ikon:



For at navigere mellem mapper i terminal vinduet kan vi bruge følgende kommandoer:

```
$ ls # Vis hvilke filer vi kan se i den mappe som vi er i.
$ cd # Bruges til at gå over til en anden mappe.
# ------------ EKSEMPEL -------------------
$ cd Downloads # Gå til Downloads
$ ls # Vis filer der ligger i Downloads
$ cd # Gå tilbage til start
$ cd .. # Gå en mappe op i mappe hierakiet.
```

Prøv at taste ovenstående ind i dit eget terminal vindue.

Binwalk

Binwalk er et værktøj som kan søge i en given fil efter indlejrede filer. Det kan være brugbart i situationer hvor man gerne vil finde ud af om der er ekstra filer med i f.eks. et billede. Binwalk er et terminal program. Dvs. at for at bruge værktøjet skal man åbne terminalen, navigere til den mappe som filen, man gerne vil undersøge ligger i og derefter skrive `binwalk` efterfulgt af navnet på den fil man gerne vil undersøge. For eksempel:

```
$ cd Downloads          # Gå til downloads
$ ls                    # Vis filnavnene på filer i downloads.
$ binwalk billede.jpg   # Brug binwalk til at undersøge en fil.
```

For at læse mere om `binwalk`'s mange funktionaliter kan man google det.

Exiftool

EXIF er et værktøj som kan vise exif data, som ligger indlejret i billeder. For at bruge exif tool på et billede, kan man gøre følgende i terminalen.

```
$ cd Downloads          # Gå til downloads
$ ls                    # Vis filnavnene på filer i downloads.
$ exiftool billede.jpg  # Brug exiftool til at undersøge en fil
```

For at læse mere om `exiftool` kan man google det.

John the ripper

John the ripper(`john`) er et meget fleksibelt værktøj som kan bryde koder. Værktøjet understøtter både brug af ordlister men også brute-force angreb. Da det er et meget fleksibelt værktøj betyder det også at man skal være lidt opmærksom på at man får konverteret filen, som man gerne vil bruge `john` på, til det rigtige format. For at bruge værktøjet skal man åbne terminalen og navigere til den mappe som filen man gerne vil arbejde ligger i. F.eks.

```
$ cd Downloads          # Gå til downloads
$ ls                    # Vis filnavnene på filer i mappen.
$ john filnavn          # Brug john til at bryde en kode.
```

John skal have den fil som man gerne vil bryde koden til i et bestemt format. Men det kan du læse om på google.

Hydra

Hydra er et værktøj som er lavet til at bryde passwords til servere som f.eks `FTP` servere, som også lever i dit terminal vindue. Det er også et rigtig multifunktionelt værktøj, som du kan læse mere om hvordan man bruger på google.

NMAP:

Vi går flux videre til et andet cool værktøj som hedder NMAP, som kan bruges til at skanne det netværk man sidder på eller andre services på nettet. Herunder er et eksempel på hvordan man kan bruge nmap til at skanne sit netværk og se hvilke enheder der er online på det subnet vi skanner:

```
$ ifconfig              # Bruges til at finde din egen IP.
$ nmap 192.162.3.14     # Scan af en enkelt host.
$ nmap 192.162.3.14/24  # Scan af et helt subnet.
$ nmap -O 192.162.3.14  # Scan af en enkelt host med fingerprint.
```

Da `nmap` har rigtig mange funktionaliteter er det altid en god ide at læse lidt op på værktøjet på nettet f.eks: https://cybertraining.dk/network_scanning/#/ eller søg på google.

Wireshark

Wireshark er et værktøj som kan bruges til at lytte med på det lokale netwærk. Herunder vil der blive præsenteret en masse kommandoer som kan bruges i wiresharks søgefelt til at filtrere den internettraffik som man har opsamlet:

Filtre

Usage	Filter syntax
Filter by IP	ip.addr == 10.10.150.1
Filter by destination IP	ip.dest == 10.10.150.1
Filter by source IP	ip.src == 10.10.150.1
Filter by port	tcp.port == 25
Filter by destination port	tcp.dstport == 23
Filter by domain name	http.host == “domain.hkn”

For at lave mere avancerede filtre kan man bruge både **Logical operators** samt **Filter operators**:

Logical operators

Operator	Description	Example
and / &&	Logical AND	All the conditions should match
or / ||	Logical OR	Either all or one of the conditions should match
xor / ^^	Logical XOR	Only one of the two conditions should match
not / !	Logical NOT	Not equal to

Filter operators

Operator	Description	Example
eq / ==	Queal	ip.dest == 192.168.1.1
ne / !=	Not equal	ip.dest != 192.168.1.1
gt / >	Greater than	frame.len > 10
lt / <	Less than	frame.len < 10
ge / >=	Greater than or equal	frame.len >= 10
le / <=	Less than or equal	frame.len <= 10

Man kan læse mere om wireshark på google eller https://cybertraining.dk/network_monitoring/#/ eller søg på google.

Kali linux terminal commands

Nu er du efter at have læst ovenstående måske blevet lidt mere fortroelig med din terminal. Herunder finder du en mere udtømmelig liste med kommandoer du kan prøve kræfter med i dit terminal vindue.

System navigation

Description	Command
Ssh to host	ssh <user>@<network_domain_name>
Switching user	su <username>
List files and directories	ls
List files and directories (including hidden)	ls -a
Changing directory	cd <directory_name>
Filter by domain name	http.host == “domain.hkn”
FTP to host	ftp hostname
Download file from FTP host	get <filename>
Read text file from FTP host	more <filename>

Interacting with files

Description	Command
Creating new file	touch <filename>
Creating new directory	mkdir <directory name>
Moving file/directory	mv <file or directory name> <Destination path>
Copying file/directory	cp <file or directory name> <Destination path>
Reading contents of file	cat <filename>
Search for a specific text string in file	grep “string_to_search_for” <filename>
Writing to a file	myCommand > filetowriteto.txt

Permissions and complex commands

Description	Command
Find a file in directory tree	find <root_of_search> -name “filename”
Reading network information	ifconfig
Chaining commands	<command 1>
Changing permissions of file	chmod <permissions> filename.txt
Reading contents of file	cat <filename>
Executing files	./<filename>

Hvis du er nysgærrig på mere er følgende link et godt sted at starte: https://cybertraining.dk/metasploit_0/#/ eller søg på google.