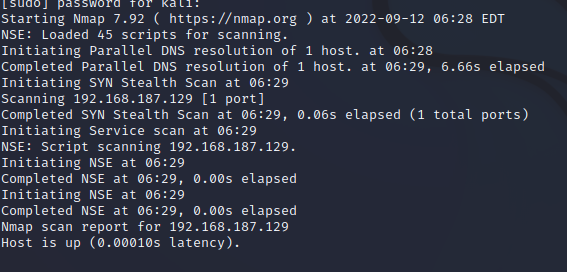
NMAP del:

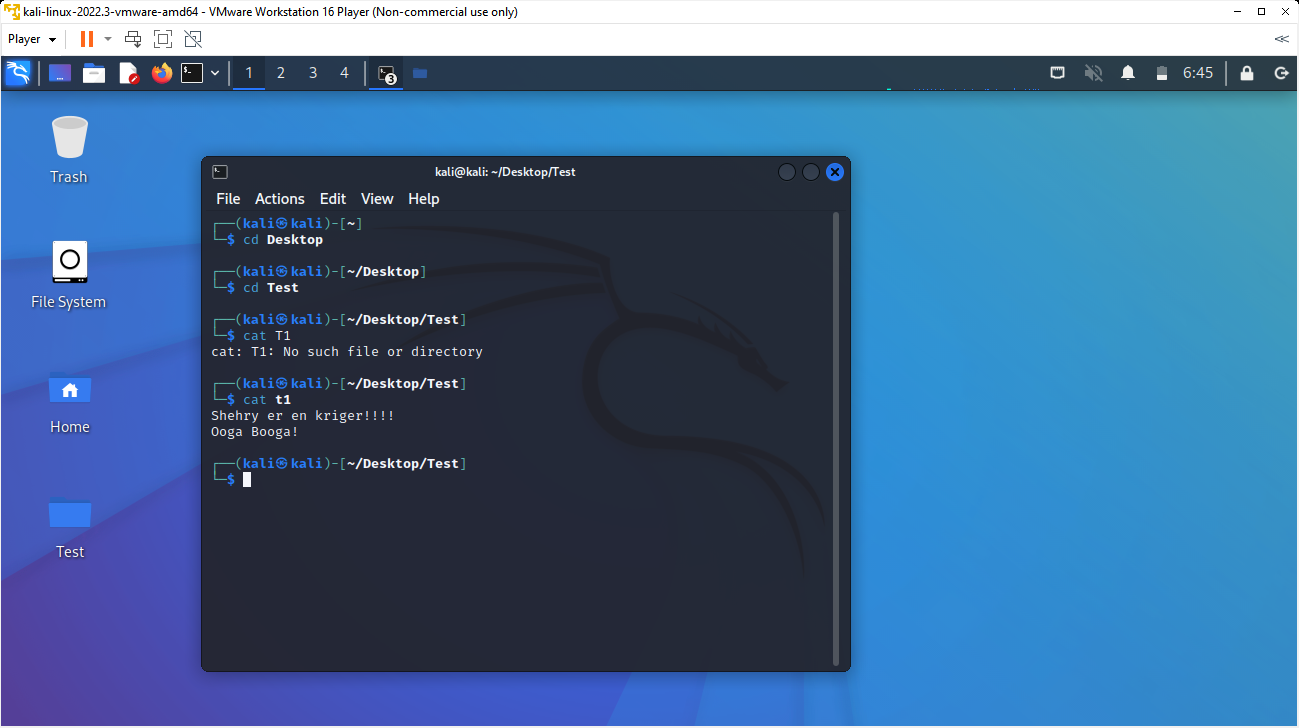
Laster ned Virtual machine work station og

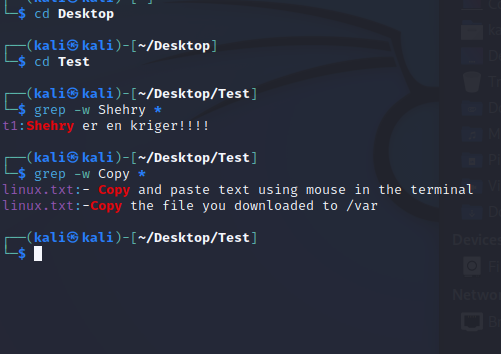
Linux lab :

Skriver inn : ifconfig og får opp ip adressen og deretter sudo nmap -sS -sV -p 21 -T4 -v 192.168.187.129 ber om passordet skriver : kali

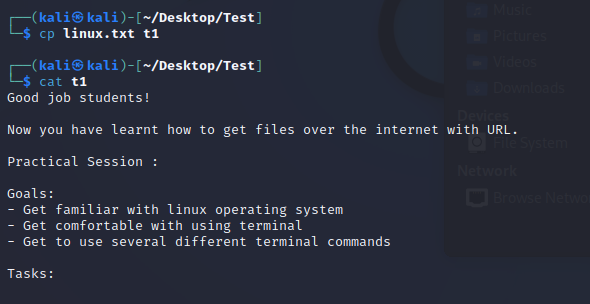


cd og cat kommandoene i terminal: cat viser innholdet i filen



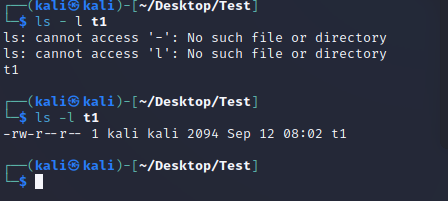


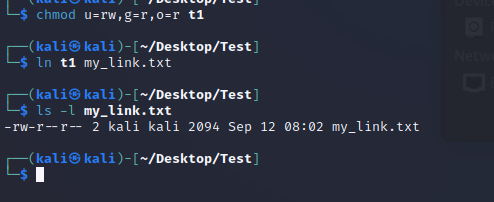
Søke i filer ovenfor:



Kopierer innhold fra en fil til en annen:

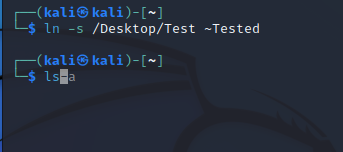
Sjekker permisjonene i filen:





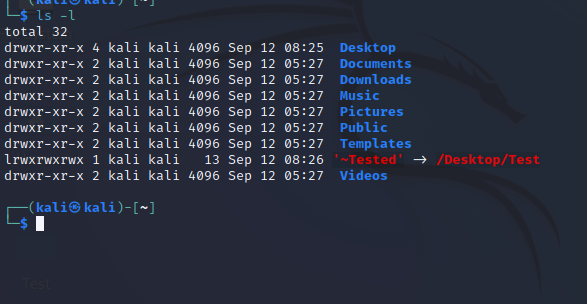
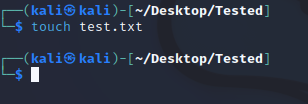
Symbolsk link til filen t1 med navnet my\_link.txt og sjekker med ls – l symlinket var laget.

Lage symlink med to mapper eller:

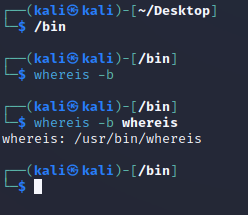


Ser at de er linket

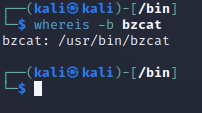
Bruk touch for å lage filer:



**Ls -l gir en oversikt over alle mappene inklusivt linkede**



bin oppgaver ovenfor



Lag deg en punktliste over de test punktene du mener vil være

viktigst for å gjennomføre en test av en web applikasjon: (Selvstudie) s.47 i pdf

* Utviklere bør sikre koden sin v/ å kryptere
* Bruke viktige verktøy for testing er viktig
* Lage en pen-test analyse (rapport hvis mulig)
* Sjekk etter sårbarheter
* Komponenter som tester : Folk , prosess og teknologi
* Ta i bruk teknikker som trussel modellering får å få en oversikt over mulig angrep mot web applikasjonen eller systemet
* Bruk en webapplikasjoner skanner får å se etter sårbarheter
* Passiv(forstå systemet og prøve å tolke det sett deg inn i web applikasjonen du skal analysere benytte verktøy for å finne info om et system) og aktiv testing (utnytter metoder for å gjennomføre en test av en webapplikasjon)
* Informasjonsinnhenting
* Testing av konfigurasjon og distribusjonsadministrasjon
* Identitetsstyringstesting
* Autentiseringstesting
* Autorisasjonstesting
* Session Management Testing
* Inndatavalideringstesting
* Feilhåndtering
* Kryptografi
* Forretningslogikktesting
* Testing på klientsiden
* API-testing