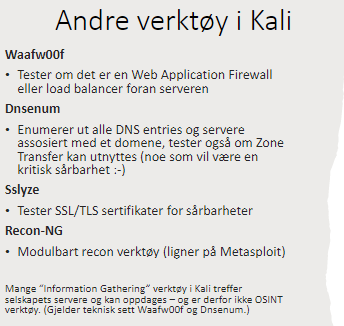
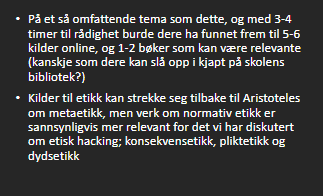
Etisk Hacking 02 My Name Is Bond:

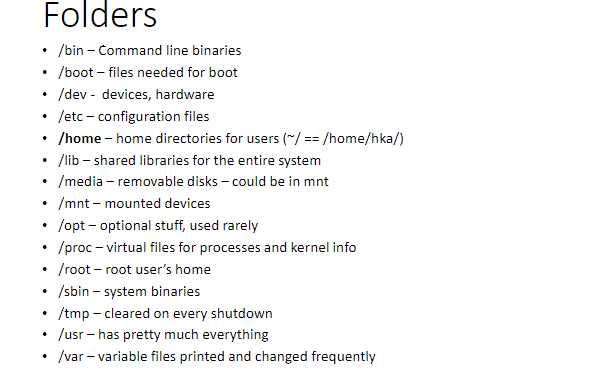
* Open-Source Intelligence (OSINT) Åpen kilde Etteretning
* Etikk , juss , lover (Burde ha henvist til kilder hvis dette var gitt på eksamen )
* Moral ( Personlig etikk) noe som er personlig -Bengt
* Forskjell på etikk og etisk hacking
* Etisk feil å angripe en nasjon , men juridisk sett nei, moralsk sett kan variere
* Etisk hacker er hacker som følger loven (juridisk) og moralsk og er innenfor et etisk rammeverk , eller en white hat hacker.
* Kan ikke straffe en varsler
* Tenke som en kriminell er viktig for å jobbe med etisk hacking (utnytte kriminelle metoder osv)
* Rekognosering , (Bengt- Trenger ikke tillatelse for å kjøre OSINT)
* Username password filetype : xlsx (man finner brukernavn og passord på nettet selv om det ikke er ment til det)
* Bruk nøkkelord for å søke etter filer osv. Bruk avansert søk
* Ansatte må legge ting på offentlige anbud som Doffin og Mercel
* Doffin er indeksert på google (site:doffin.no)
* OSINT er i utgangspunktet lovlig , men ikke mot hemmelig mål.
* Ikke lov å bruke OSINT hvis man utnytter en sårbarhet.
* Ikke mot privatpersoner
* Ikke hvis noen blir lei seg
* Henlagt sak kan dukke opp på rulleblad
* Bransjer kan kreve vandeltest eller sikkerhetsklarering.
* Pentest forberedelser må skje i forkant i arbeidet

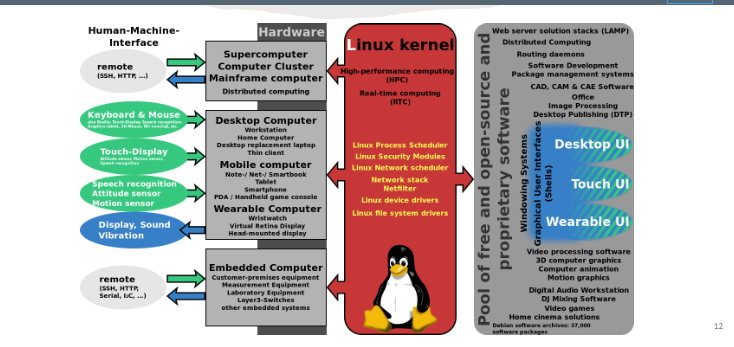


Etisk Hacking Forelesning 03 (Your Internets Belong To Us) Part 1:

Viktige roller I Operativ System :

* File Management
* Process Management
* Processing
* Self organization
* Handling hardware
* GNU har ingen kenel
* 488 av 500 supermaskiner kjører linux idag
* Klokker , microkjøleskap , atommaskiner kjører linux
* Ekstremt allsidig
* operativsystem
* Server
* Desktop
* Cluster
* Embedded
* Mye av programmene på Linux er Open Source
* Kunne terminal er viktig for å mestre kali - linux
* Alt på linux er en fil





Your Internets Belong To Us Part 2 Forelesning 04:

* **Nmap <<vg.no>> er hacking**
* Rapporten må bestå av et rammeverk:
* OWASP top 10
* OWASP ASVS
* Blackbox text (ingen tilgang fra selskapet)
* Tester må finne alt selv = tar lenger tid =realistisk test
* Graybox test = tilgang til dokumentasjon eller et selskap , be om info underveies (anbefales)
* White box test = tester har tilgang til alt , kildekode all intern dokumentasjon , mest realististe testen -Bengt
* OWASP top 10 bør ikke brukes som standard under en pen-test (dekker noen punkter men ikke alt)
* Owasp testing guide komplett rammeverk for å utføre en pen-test
* Hovedkapitler og underkapitler er en god basis for en grundig test og rapport
* PCI gjelder for selskaper med behandling av kortbehandling med unntak av nettbutikk
* Må være en del av PCI 3.2 og pen-test
* PTES – er en angrepsfasemetodikk
* Brukes for å bygge pen-test med denne metodikken
* Intelligence gathering
* Threat modeling
* Vunerability analysis
* OSSTMM er ikke egnet for web applikasjons testing for selskaper
* LPT methodology for infrastruktur testing av selskaper
* Utviklen av EC – Council
* Footprint og OSINT
* Social Engineering etc.

Faser i en pentest:

* Rekognisering
* Scanning og enumering (viktig for en tester å investere tid i denne fasen)
* Skaffe tilgang (phishing, (kartlegg ansatte , se etter brukernavnet og passordet bruke login hvis de er oppdaget)
* Fysisk tilgang for å skaffe tilgang
* Martin ingensen
* Les linux kapittel 7 boka
* Noen sårbarhetsskannere kan vise falske sårbarheter
* Fjerne falske positive når man skriver en rapport