Høyskolen Kristiania

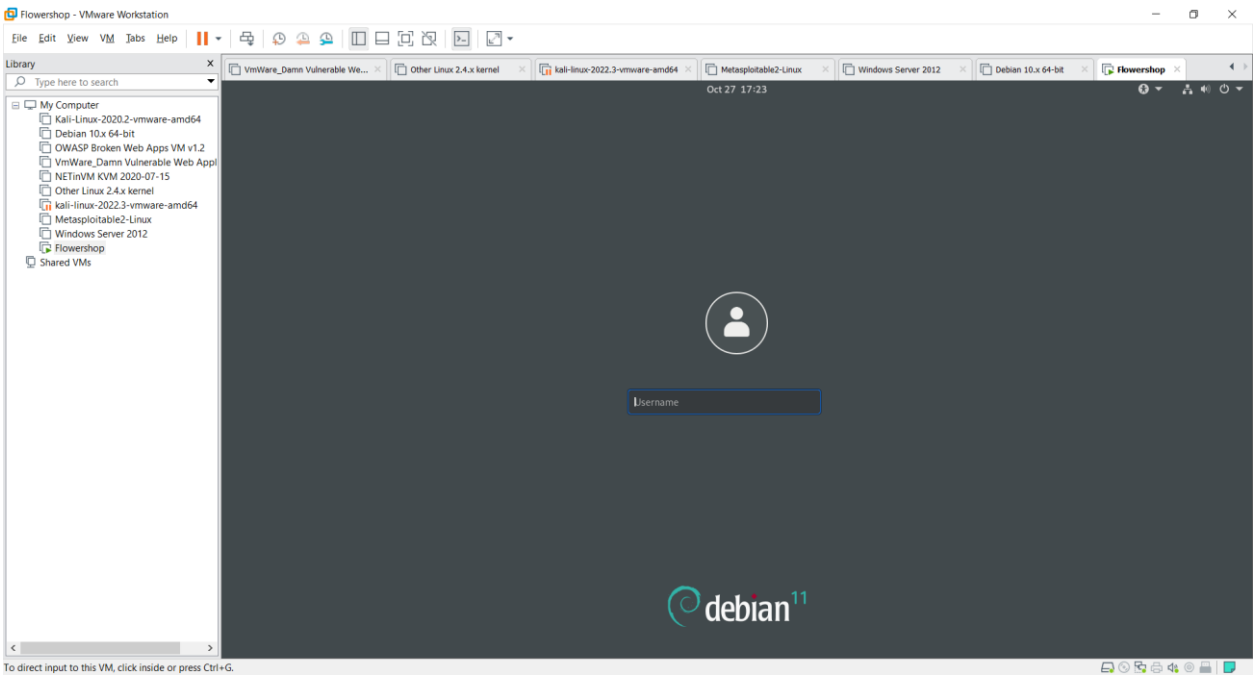
Emnekode:	**ETH2100**
Emnenavn:	**Etisk Hacking**
Vurderingskombinasjon:	**Mappevurdering**
Innleveringsdato:	**19. desember 2022**
Filformat:	**PDF m/ vedlegg**

Eksamen er en mappevurdering og består av 3 deler. Karakter blir satt basert på ALLE delene som en helhet, alle 3 delene må være bestått. Se første forelesning for detaljer om karaktersetting.

Del 2: PENTEST RAPPORT (48 dager, individuell)

- Utleveres tirsdag 1. november klokken 20.00 (etter forelesning)
- Oppgave beskrivelse publiseres på Canvas under «Eksamen 2022»
- VMware fil for testing publiseres på Canvas under «Eksamen 2022»
- Rapporten leveres inn som vedlegg til eksamensbesvarelsen

Det skal gjennomføres en «penetrasjonstest» (teknisk sårbarhetsrevisjon) av en web applikasjon. Applikasjonen kan lastes ned fra EASTWILLSECURITY.COM (filen var for stor for Canvas), og ligger i filen eksamen_ETH2100_H22_del2_vm. Filen inneholder et VmWare image dere skal starte, og som kjører en web applikasjon. Imaget er konfigurert til å kun bruke nettverksadapteret Host-Only (VmNet1).



Husk å oppgi kandidatnummer på din besvarelse, ikke studentnummer.

Høyskolen Kristiania

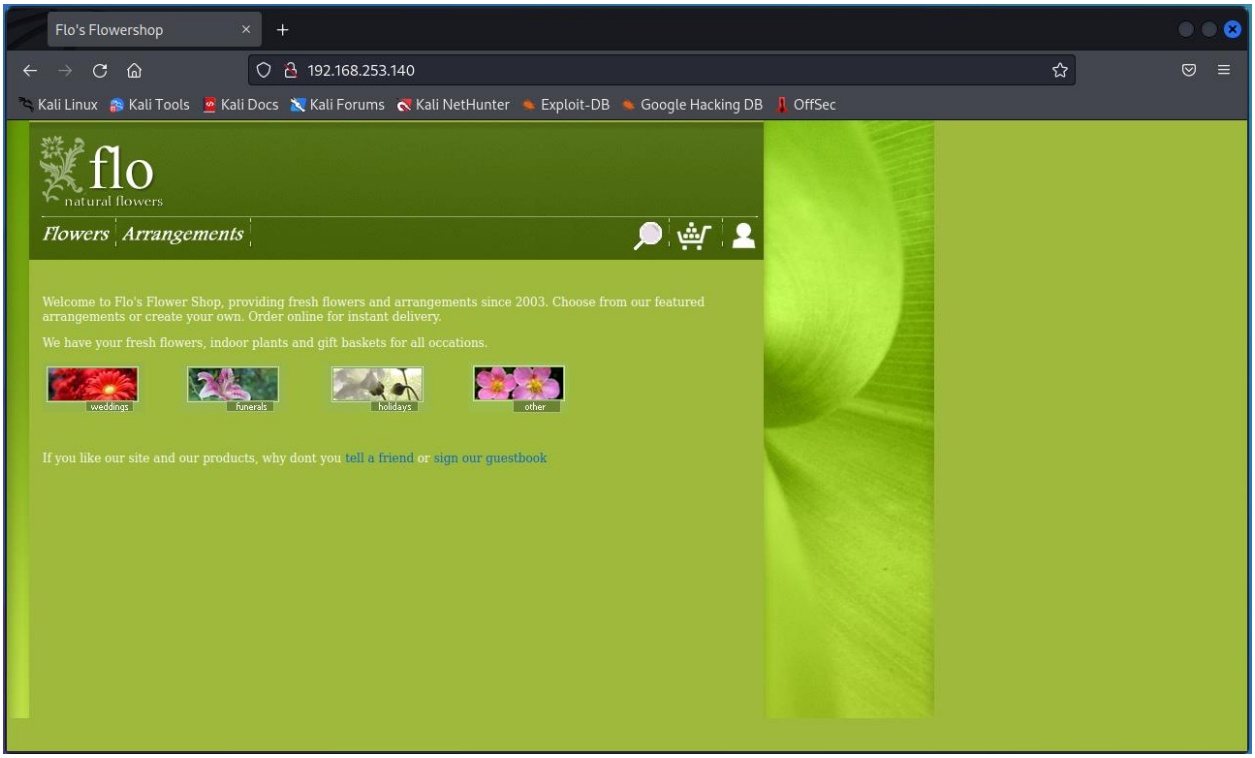
Relevante filer kan lastes ned fra følgende URL, merk at URL er case sensitive:

www.eastwillsecurity.com/eth2100/eksamen_ETH2100_H22_del2_vm.zip
www.eastwillsecurity.com/eth2100/eksamen_ETH2100_H22_del2_source.zip

Kunden er Flo blomsterbutikk AS, og har fått utviklet en nettbutikk som nå er i beta versjon. Dere har tidligere jobbet på prosjektet og kjenner koden fra tidligere. Kunden ønsker å gjennomføre en Web Application «penetrasjonstest» av applikasjonen. Testen kan gjennomføres som en whitebox test, og dere kan gjennomføre statisk kodeanalyse hvis ønskelig, kildekode er lagt ved i filen eksamen_ETH2100_H22_del2_source.zip som dere kan både finne under EKSAMEN på Canvas, eller på overnevnte URL.

Kunden har ikke oppgitt noen brukere eller passord til systemet. (Det er innenfor scope å knekke passord for innlogging, og hvis det er mulig å finne passordet skal det i så fall rapporteres som en sårbarhet.)

Dere må først finne IP adressen til serveren. Serveren bruker dynamisk IP adresse gjennom DHCP som den vil motta fra deres VmWare, men da dere ikke får innloggingspassord til serveren må dere selv finne IP adressen som blir tildelt.



Husk å oppgi kandidatnummer på din besvarelse, ikke studentnummer.

Webserveren Abyss WS starter automatisk i bakgrunnen når dere starter den virtuelle maskinen (dere trenger ikke starte noe manuelt, og trenger ikke logge inn). Installasjonen bruker HTTP, og med IPen som vist over kan den aksesseres med http://192.168.253.140/ fra en annen maskin (Kali VM eller host maskinen). Merk at da IP er dynamisk tildelt vil IP adressen være forskjellig på deres systemer.
Dere skal ikke trenge å logge inn på serveren, Abyss starter i bakgrunnen uten innlogget bruker.

Da nettbutikken er i en beta fase kan det være noe funksjonalitet som ikke virker etter hensikten.

Kunden ønsker at dere tester alt på serveren, ikke bare webserveren på port 80.

Viktig:
Da dette ikke er et reelt firma, men et fiktivt oppdrag til eksamen er «Open Source Intelligence» og «Social Enginneering» out-of-scope og **skal ikke utføres**, innlevert oppgave kan derfor hoppe over disse stegene i både metodikk og rapportering.

Det presiseres at det skal leveres en skriftlig rapport fra denne delen av mappevurderingen, og denne rapporten skal leveres inn i Wiseflow sammen med Del 1, innen fristen 19. desember.

Dere får utlevert oppgavetekst til Del 1 5. desember klokken 12.00, oppgaveteksten publiseres på Canvas under «Eksamen 2022» på emnesidene for ETH2100.