



Høyskolen
Kristiania

ETH2100 - Etisk Hacking

Eksamensform

Mappeinnlevering

EKSAMEN (14 dager, individuell, hjemmeeksamen)

- Praktisk del
- Teoretisk del

PENTEST RAPPORT (utleveres i midten av semesteret)

VALGFRI ØVING (teller ikke på karakter, må kun bestås)

- (enten) Skrive et Ducky Script (øving til leksjon 17), kan være løst i gruppe
- (eller) Mestre låsdirking på nivå 2 «yellow belt» (øving til leksjon 15)
- (eller) Demonstrere bruk av et exploit (øving til leksjon 19, 20, mfl)

Alle 3 delene av mappen må være bestått

Mappeeksamen

- På EKSAMEN vil den praktiske delen vil telle 50%, og den teoretiske delen vil telle 50% av karakter på rapporten – vil gi en samlet delkarakter fra A-F
- Pentest rapport vil karaktersettes til A-F basert på antall sårbarheter funnet, tekniske beskrivelser, og profesjonalitet – denne rapporten vil kunne endre eksamenskarakter en karakter opp eller ned
- Pentest rapport teller 30% av total karakter, men hvis pentest rapport er bedre enn eksamen får karakteren en +0.2 «bonus» (rapporten kan trekke opp mer enn den kan trekke ned...)

		14 dagers eksamen				
Pentest rapport		A	B	C	D	E
	A	A	A	B	C	D
	B	A	B	B	C	D
	C	B	B	C	C	D
	D	B	C	C	D	D
	E	B	C	D	D	E

- Matematisk: $= \text{EKSAMEN} * 70\% + \text{RAPPORT} * 30\% + \text{IF}(\text{RAPPORT} > \text{EKSAMEN}; 0.2; 0)$
- En pentest rapport som er en eller flere karakterer bedre enn eksamenskarakteren vil sette emne-karakteren opp 1 karakter fra eksamen
- En pentest rapport som er **to eller flere** karakterer dårligere enn eksamenskarakteren vil sette emne-karakteren ned 1 karakter fra eksamen

EKSAMEN: Praktisk del

- Praktisk del: 4 praktiske oppgaver (angrep) som skal utføres mot et virtuelt labmiljø
- Oppgavene vil være av varierende vanskelighetsgrad (en eller to oppgaver vil være for å skille ut A og B karakterer)
- Eksempler kan være å knekke passord, utføre SQL Injection, sette opp cookie stealer, bruke exploit kode, osv
- Vil være mot den virtuelle maskinen som blir utlevert til pentest delen av mappen ELLER en av de virtuelle maskinene vi har brukt i øvingstimene, dette betyr at det forutsettes at alle oppgaver i øvingene er fullført (hvis ikke må du sette opp labmiljøet under eksamen!)

EKSAMEN: Teoretisk del

- Teoretisk del: 3 teori (fritekst) oppgaver, 2-4 siders besvarelse per oppgave
- Krever enten grundige tekniske forklaringer, eller drøfting av problemstillinger som er relevante for faget
- For beste karakterer kreves at svarene underbygges av kilder
- Spørsmålene vil gå utover det vi har lært om i forelesninger, forutsetter at studenten setter seg inn i emnet med andre bøker, artikler og så videre (under eksamen)

1 VALGFRI ØVING – MÅ (kun) bestås, ikke karakter.

Studentene kan velge mellom en av følgende tre:

- (enten) Skrive et Ducky Script (øving til leksjon 17), kan være løst i gruppe, dokumenteres ved PDF dokument som viser scriptet og dokumenterer med skjermbilder og tekst hva som skjer når Rubber Ducky deployeres til et mål
- (eller) Mestre låsdirking på nivå 2 «yellow belt» (øving til leksjon 15), dokumenteres ved PDF dokument bilde av dirket lås, se <https://www.reddit.com/r/lockpicking/wiki/beltranking/> for detaljer og låser
- (eller) Demonstrere bruk av et exploit (øving til leksjon 19, 20, mfl), dokumenteres ved PDF dokument som viser scriptet og dokumenterer med skjermbilder og tekst hva som skjer når exploited kjøres mot en virtuell maskin

PENTEST RAPPORT

- Pentest av en utlevert webserver
- Rapport skal ha form som en profesjonell rapport for en kunde som har bestilt en test av en server
- Det aksepteres at man ikke finner ALLE sårbarheter, men rapporten må vise et metodisk og grundig arbeid
- Utleveres ?? . november, skal jobbes individuelt
- Pentesten vil i utførelse være veldig lik arbeidskravet i faget, det vil lønne seg å «lytte til» tilbakemeldinger på arbeidskravet

Eksempler på karaktersetting

- Ikke innlevert pentest rapport, ikke innlevert praktisk del, svart perfekt på teoretisk del – karakter F (alle 3 deler må bestås)
- 40/50 på praktisk del, 50/50 på teoretisk del, dårlig – men bestått pentest – karakter B (eksamen 90/100 = A, ned til B)
- 20/50 på praktisk del, 20/50 på teoretisk del, middels oppnåelse på pentest – karakter D (eksamen 40/100 = E, opp til D)
- 40/50 på praktisk del, 0 på teoretisk del, perfekt oppnåelse på pentest – karakter D (eksamen 40/100 = E, opp til D)
- 40/50 på praktisk del, 50/50 på teoretisk del, perfekt oppnåelse på pentest – karakter A (eksamen 90/100 = A, A på pentest)
- 40/50 på praktisk del, 50/50 på teoretisk del (eksamen 90/100 = A), karakter B på pentest – karakter A

		14 dagers eksamen				
Pentest rapport		A	B	C	D	E
	A	A	A	B	C	D
	B	A	B	B	C	D
	C	B	B	C	C	D
	D	B	C	C	D	D
	E	B	C	D	D	E