Universitetet i Oslo
IN2120 Cybersikkerhet
Høst 2026
Teoretiske oppgaver

Teori del 5: Pentesting og angrepsmetodikk

Oppgave 1: Juridiske og etiske rammer for pentesting

a. Hva skiller en pentester (white hat) fra en ondsinnet hacker (black hat), sett i lys av motivasjon?

b. Hvorfor er skriftlig tillatelse på forhånd avgjørende for en lovlig pentest? Hva kalles denne tillatelsen i dagligtale, og hvilken lovbestemmelse gjør uautorisert datainnbrudd straffbart?

c. Forklar legalitetsprinsippet slik det gjelder for en privatperson kontra en ansatt i forvaltningen, og hvorfor dette er relevant når en offentlig virksomhet skal pentestes.

Oppgave 2: Hvit-, grå- og svartbokstesting

a. Forklar forskjellen mellom hvitboks-, gråboks- og svartbokstesting.

b. Diskuter minst to fordeler og to ulemper ved hvitbokstesting sammenlignet med svartbokstesting.

c. Du er sikkerhetsansvarlig i en bedrift med begrenset budsjett og stramme tidsfrister. Hvilken testtype vil du anbefale, og hvorfor?

Oppgave 3: Stadiene i en pentest

a. List opp og forklar kort stadiene i en pentest, fra planlegging til rapport.

b. Hva er OSINT, og gi tre eksempler på kilder en pentester kan bruke i rekognoseringsfasen.

c. Forklar hvorfor en pentester ofte utfører mesteparten av testen med vanlig brukertilgang, fremfor å bruke lang tid på å skaffe seg mer tilgang selv.

Oppgave 4: Passordangrep

a. Forklar forskjellen mellom passordspraying og et vanlig bruteforce-angrep mot én bruker. Hvorfor er passordspraying ofte tryggere for en pentester å utføre, med tanke på kontosperring?

b. Hva menes med «pass the hash», og hvorfor er dette et argument mot å gjenbruke (gode) passord?

c. Et passord består kun av 8 små engelske bokstaver (26 tegn). Regn ut hvor lang tid et uttømmende søk i snitt vil ta ved 14 milliarder forsøk per sekund. Hvorfor er reelle passord i praksis mye raskere å knekke enn den teoretiske kompleksiteten skulle tilsi?

Oppgave 5: Fra sårbarhet til gevinst

a. Forklar forskjellen mellom å kartlegge sårbarheter (f.eks. med OpenVAS) og å utnytte dem (f.eks. med Metasploit).

b. Hva er «lateral movement», og hvorfor foretrekker en pentester ofte dette fremfor å kjøre nye exploits på hver enkelt maskin?

c. Hva er fuzzing, og hvorfor beskrives det som den eneste praktiske måten å finne feil som buffer overflow?

Oppgave 6: Verktøy i pentesting

a. I foilsettet nevnes blant annet nmap, Wireshark/tcpdump, Hydra og Metasploit. Forklar kort hva hvert av disse verktøyene brukes til i en pentest, og i hvilken fase (rekognosering, initial tilgang, utnyttelse osv.) de typisk brukes.

b. Hva er forskjellen mellom John the Ripper og Hashcat til passordknekking, og når vil du velge det ene fremfor det andre?

c. Verktøy som Mimikatz og Impacket/psexec brukes til henholdsvis passorddumping og «pass the hash». Hvorfor krever slike verktøy typisk administrator- eller debug-rettigheter, og hvorfor er dette en risiko dersom en angriper får slike rettigheter ett sted i nettverket?