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 1: EKSAMEN (14 dager, individuell, hjemmeeksamen)

- Eksamenstart 5. desember
- Innleveringsfrist (hele mappen) 19. desember (se Wiseflow for tidspunkt)
- Eksamensoppgaven publiseres på Canvas under «Eksamen 2022» klokken 12.00
- Besvarelsen leveres inn som PDF fil, eksamensbesvarelsen er «hoved levering»

Oppgavesettet består av 8 sider, og inneholder totalt 7 oppgaver som skal besvares.

Vær obs på at eksamen MÅ leveres innen fristen som er satt, og må leveres via eksamensplattformen WISEFLOW. Det vil ikke være mulig å få levert oppgaven etter fristen – det betyr at du bør levere i god tid slik at du kan ta kontakt med eksamenskontoret eller brukerstøtte hvis du har tekniske problemer.

Da dette er en hjemmeeksamen er det viktig å vise helhetlig forståelse, og oppgavene har et større preg av drøfting eller teknisk problemløsing. Det forventes derfor utfyllende og forklarende svar på alle teori oppgaver, og dokumentasjon i form av skjermbilder og tilhørende forklaringer til alle praktiske oppgaver. (Bilder som er vedlegg, men ikke satt inn i besvarelsen anses ikke som en del av besvarelsen.)

Det presiseres at studenten skal besvare eksamen selvstendig og individuelt, samarbeid mellom studenter og plagiat er ikke tillatt. All bruk av tekst, bilder og illustrasjoner som er hentet fra forelesninger, lærebøker eller internett skal føres med kildehenvisning slik at det kommer tydelig frem hva som er studentens eget arbeid, APA7 eller Chicago (forfatter, år) standardene anbefales brukt for kilder. For topp score bør svarene underbygges med relevante kilder utover ordinær pensumlitteratur. Det bør selvsagt også refereres til pensumlitteratur når relevant.

OBS: Besvarelsen skal ikke være på mer enn 12 A4 sider, med font størrelse 12, normale marger og linjeavstand 1.0. I tillegg kommer de praktiske oppgavene, som bør kunne besvares med 1 side per oppgave (kanskje med unntak av oppgave 2).

Husk å oppgi kandidatnummer på din besvarelse, ikke studentnummer.

Høyskolen Kristiania

Teori oppgaver og drøftinger

Oppgave 1 – etisk hacking (15%)

For en som jobber innen informasjonssikkerhet er det viktig å forstå hva en etisk hacker er, hva en sikkerhetstest er, og hvordan rollen som etisk hacker passer inn i sikkerhetsorganisasjonen. En etisk hacker må være i stand til å forklare dette tydelig til forskjellige lag i organisasjonen, men også andre ansatte må kunne vite når og til hva man kan bruke etiske hackere, enten innleid eller i egen organisasjon.

Oppgaveformulering:

Du har nettopp startet i ny jobb i avdelingen for IT sikkerhet i et middels stort selskap. Forklar for en (tenkt) arbeidsgiver hvorfor selskapet burde gjennomføre en «penetrasjonstest» av sitt selskap. Forklar hva rollen til en etisk hacker er, og hvordan dette spiller inn i en sikkerhetsorganisasjon.

Oppgave 2 – exploit brukt i hacking (15%)

I denne oppgaven skal du vise at du kan bruke det du har lært om skadevare og informasjonssikkerhet i dette og tidligere fag, og at du er i stand til å tilegne deg ny kunnskap som har vært lite dekket av pensum, sette dette i kontekst til en angriper/hacker, og forklare dette videre med egne ord.

Oppgaveformulering:

Sett deg inn i sårbarheten EternalBlue, forklar hvordan denne sårbarheten fungerer, og hvordan denne sårbarheten har vært brukt i skadevare, og hvordan dette kan brukes av en hacker for å få tilgang til et datanettverk. Du må bruke kildehenvisninger for å underbygge besvarelsen. Merk at du skal forklare sårbarheten og skadevare med egne ord fra hva du kan lære fra flere kilder (kopiering av tekst direkte fra internett vil kunne bli oppfattet som plagiat).

Oppgave 3 – Living Off the Land (20%)

I denne oppgaven skal du vise at du klarer å fordype deg i et emne, raskt finne kilder med relevant informasjon, og har evne til å omsette dette til kunnskap du kan bruke i et praktisk oppdrag. Å bruke verktøy som allerede er installert på en maskin til noe annet enn verktøyene var ment for, og i denne konteksten; bruke de til å gjennomføre en fase i et hackerangrep, kalles for Living Off the Land. Dette er viktig for å ikke bli oppdaget av endepunktssikkerhet på maskinene du har kompromittert. Se «Videre studier» på forelesning 21 i uke 46 som inneholder en link til LOLbins som et utgangspunkt.

Oppgaveformulering:

Sett deg inn i begrepet Living Off the Land. Bruk flere tilgjengelig kilder og skriv en kort rapport som forklarer HVA Living Off the Land betyr, HVORFOR det er viktig, og HVORDAN det brukes ved å vise til et interessant utvalg av teknikker og verktøy som kan brukes i et redteam oppdrag.

Bred bruk av gode kildereferanser er viktig for å besvare denne oppgaven godt, det kan omfatte både forskningsartikler, videopptak fra større konferanser (vis i så fall til minutt inne i videoen hvor referansen er hentet fra), større artikler hentet fra internett, og relevante bøker.

Høyskolen Kristiania

Praktiske oppgaver

Oppgave 1 – Passord brute-force (10%)

I denne oppgaven skal du vise at du kan gjennomføre et brute-force angrep med OWASP ZAP eller Burp Suite. Du skal demonstrere de faktiske verktøyene du bruker og dokumentere hvordan du har gått frem for å løse oppgaven, inklusive skjermbilder og kommandoer du har kjørt.

I denne oppgaven skal du bruke maskin med Kali Linux og OWASP ZAP (eller Burp Suite) konfigurert, eller du kan bruke din host maskin hvis du har konfigurert OWASP ZAP (eller Burp Suite) på denne maskinen. Som «offer» maskin skal du bruke den virtuelle maskinen Damn Vulnerable Web Application (DVWA). DVWA VMen skal være satt opp i henhold til øvingsoppgave i uke 37 (ETH2100_U37_Øvingsoppgaver_Kali_Virtlab)*.*

Oppgaveformulering:

Du skal starte DVWA VMen. Så skal du åpne opp en vanlig nettleser som du har konfigurert til å bruke OWASP ZAP *(eller Burp Suite)* som web proxy (dette kan være i Kali Linux eller på din host maskin avhengig av hvor du har konfigurert proxy programmet). I nettleseren skal du gå til IP adressen til DVWA serveren, du vil da automatisk bli redirigert til login.php.

Du skal forsøke å logge deg inn med brukernavn admin. Du skal bruke OWASP ZAP *(eller Burp Suite)* sin «Fuzzer» til å brute-force passordet på serveren. Vis og forklar i programmet (ved hjelp av skjermbilder) hvordan du kan se at passordet du fant er korrekt. Du skal bruke en standard wordlist som du har hentet fra Kali Linux, men for denne oppgaven kan du bruke en kopi av wordlisten som inneholder de 50 første passordene (for å kunne la den fullføre).

Oppgave 2 – Kjedet angrep mot Windows (15%)

I denne oppgaven skal du vise at du kan gjennomføre et angrep i flere faser mot en Windows server. Angrepet består av flere (enkle) faser, hvor det er viktig at du utfører fasene i riktig

rekkefølge. Du skal demonstrere de faktiske verktøyene du bruker og dokumentere hvordan du har gått frem for å løse oppgaven, inklusive skjermbilder og kommandoer du har kjørt.

Hvert angrep skal ha en underoverskrift «Del A», «Del B» og så videre. Hvert angrep er fra oppgaveforfatter ment å være forholdsvis enkelt, men hvis du sitter fast på et angrep kan du skrive [IKKE UTFØRT], for så prøve neste del, det er i så fall mulig å simulere at delen du hoppet over fungerte ved å forutsette at du nå har riktig informasjon (har funnet et passord eller opprettet en bestemt fil). Merk at en besvarelse som inneholder deler som ikke virker uten at det er dokumentert godt vil få større trekk enn en oppgave som har skrevet IKKE UTFØRT på en underdel – sensor må i førstnevnte tilfelle konkludere med at det betyr at studenten ikke forstår hva som skulle vært utfallet av denne delen av oppgaven.

I denne oppgaven skal du bruke maskin med Kali Linux. Som «offer» maskin skal du bruke den virtuelle maskinen «Bengts Windows VM». Windows VMen skal være satt opp i henhold til øvingsoppgave i uke 38 (ETH2100_U38_Øvingsoppgaver_Pentest_Verktøy), slide 64 til 78*. I tillegg skal VMen ha tilleggsprogramvare og konfigurasjon som satt opp i:*

- *uke 43 (*ETH2100_U43_ØvingsoppgaverIntoTheRabbitHole_Exploits*), slide 8 til 10,*
- *uke 45 (*ETH2100_U45_ØvingsoppgaverPasswordEqualsGod*) slide 6 til 12, hvis dere av en eller annen grunn ikke fikk TightVNC til å fungere er det akseptert å heller installere en annen VNC server som beskrevet på forelesning 20 slide 7, og*
- *uke 46 (*ETH2100_U46_ØvingsoppgaverDeeperIntoTheRabbitHole*) slide 7 til 20.*

På grunn av flere underoppgaver er det naturlig at denne oppgaven bruker mer enn 1 A4 side, sørg for at skjermbildene er leselige og ikke sett inn veldig mange små skjermbilder på en side. (Sensor må kunne lese hva som står i skjermbildet.)

Oppgaveformulering:

Du skal starte opp Windows VM, og logge deg inn som Administrator.

Del A

Fra Kali VMen skal du åpne Metasploit og starte **scanner/vnc/vnc_login**, bruk denne for å finne riktig passord til VNC på serveren. I besvarelsen skal du vise oppstart og kjøring av Metasploit, inklusive vise med skjermbilde at den finner riktig passord.

Del B

Fra Kali VMen skal du åpne verktøyet **vncviewer** (hvis du ikke har det allerede må du installere det med **sudo apt install xtightvncviewer**). Har du installert vncviewer på host maskinen kan du eventuelt koble deg til derfra. Koble deg til VNC serveren på Windows VMen (med passordet du fant i forrige del). I besvarelsen skal du vise oppstart og kjøring av vncviewer, inklusive vise med skjermbilde at klarer å koble seg til serveren.

Del C

Gjennom **vncviewer** skal du installere/starte et reverse shell på Windows serveren. Dette kan være **ncat** (fra nmap pakken), denne har oppgaveforfatter lastet opp til følgende URL hvor dere kan laste den ned fra, eller dere kan sette opp deres eget system for å hente den: www.eastwillsecurity.com/eth2100/tools/ncat.exe
I besvarelsen skal du vise skjermbilde av vncviewer hvor du laster ned ncat til offeret.

Del D

Gjennom **vncviewer** skal du opprette en regel for Windows Firewall ved å bruke **netsh advfirewall** verktøyet, regelen skal tillate trafikk over TCP porten du har satt opp til reverse shell (porten ncat lytter på). I besvarelsen skal du vise skjermbilde av vncviewer hvor du setter opp regelen på offeret.

Del E

Åpne **nc** fra Kali VM og koble deg til reverse shell på Windows VM. Gjennom nc skal du opprette en fil på Windows VM som heter **havebeenpwned.txt**. I besvarelsen skal du vise skjermbilde av nc hvor du oppretter filen, og så logge deg inn på Windows VM og vise at du klarte å opprette filen et sted på serveren (dokumenteres med et nytt skjermbilde fra VMen).

Oppgave 3 – Responder (15%)

I denne oppgaven skal du vise at du kan gjennomføre et standard angrep med Responder, for så å bruke et program for passord cracking til å knekke et passord. Du skal demonstrere

de faktiske verktøyene du bruker, og du skal dokumentere hvordan du har gått frem for å løse oppgaven, inklusive skjermbilder og kommandoer du har kjørt.

I denne oppgaven skal du bruke maskin med Kali Linux, og du kan bruke en Windows VM som «offer», eller du kan velge å bruke din egen fysiske host maskin som «offer».

Oppgaveformulering:

Du skal sette opp Responder på din Kali maskin til å lytte på og svare på trafikk som kan være relevant for denne oppgaven. Fra «offer» maskinen skal du starte Windows Explorer, og så aksessere et nettverksshare på en server som ikke finnes. Når du blir spurt om brukernavn og passord skal du oppgi brukernavn Bengt og passord 987654321.

Du skal ta hashen du finner i Responder for brukeren 'Bengt' og knekke denne med John The Ripper. Du skal bruke en standard wordlist som følger med Kali Linux.

I besvarelsen skal du vise oppstart og kjøring av Responder, du skal dokumentere at du blir bedt om brukernavn og passord på Windows maskinen (med skjermbilde), og du skal vise bruk av John The Ripper – inklusive vise med skjermbilde at den finner riktig passord.

Oppgave 4 – PostgreSQL; pwn 2 root (10%)

I denne oppgaven skal du vise at du kan gjennomføre et angrep med Metasploit og Meterpreter, og utnytte et reverse shell for å oppnå root privilegier på en Linux server.

Du vil i denne oppgaven bli utfordret på å bruke Metasploit mot en tjeneste vi ikke har testet i øvingsoppgaver eller undervisningen, samt å bruke verktøyet Meterpreter, og med det tester oppgaven studentenes evne til å benytte erfaringen fra emnet til å tilegne seg ny kunnskap og nye ferdigheter.

I denne oppgaven skal du bruke maskin med Kali Linux, og som «offer» maskin skal du bruke den virtuelle maskinen Metasploitable. Metasploitable VMen skal være satt opp i henhold til øvingsoppgave i uke 38 (ETH2100_U38_Øvingsoppgaver_Pentest_Verktøy).

Oppgaveformulering:

Du skal starte opp Metasploitable VM, og logge deg inn som brukeren msfadmin. Kjør først et portscan av maskinen, dokumenter at du har testet ALLE åpne porter med et skjermbilde eller annen logg fra nmap. Hvilken port kjører PostgreSQL?

Start metasploit i Kali, finn exploit som heter «postgres_payload», du skal laste og kjøre dette exploitet. Finn et «privilege escalation» exploit som kan kjøres i denne konteksten.

For å demonstrere at du nå har oppnådd rettigheter på serveren som «root» skal du skrive ut innholdet av filen /etc/shadow (til skjerm).

I besvarelsen skal du vise kjøring og resultat av både angrepet mot PostgreSQL og priv-esc exploitet, inklusive vise med skjermbilde at du får frem innholdet av shadow filen.

-

Slutt på oppgavesettet