Høyskolen Kristiania

Emnekode:	**ETH2100**
Emnenavn:	**Etisk Hacking**
Vurderingskombinasjon:	**Mappevurdering**
Innleveringsdato:	**22. desember 2023**
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 8. desember
- Innleveringsfrist (hele mappen) 22. desember (se Wiseflow for tidspunkt)
- Eksamensoppgaven publiseres på Canvas under «Eksamen 2023» klokken 09.00
- 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. Det er ikke tillatt å presentere andres arbeid som ditt eget – dette inkluderer arbeid utført av kunstig intelligens (som tekst- eller kode-genereringsmodeller). 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 standarden skal brukes for kilder. For topp score bør svarene underbygges med relevante kilder utover ordinær pensumlitteratur. Det bør selvsagt også refereres til pensumlitteratur når relevant.

OBS: De 3 teorioppgavene (oppgave 1 – 3) skal ikke være på mer enn 12 A4 sider, med font størrelse 12, normale marger og linjeavstand 1.0. I tillegg til teorioppgavene kommer de praktiske oppgavene (de praktiske oppgavene inngår ikke i sideantallet på 12 sider, som kun gjelder for teorioppgavene samlet).

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.

Svaret må underbygges med relevante kilder. Besvarelser som ikke har korrekt oppgitt kildereferanse på APA7 format vil ikke oppnå poeng. Kildelisten skal oppgis for hver deloppgave separat.

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 – Metodologi (15%)

Når man skal gjennomføre en revisjon av sikkerheten i en applikasjon eller et selskap er det viktig å følge en test-metodologi, for en etisk hacker er det derfor essensielt å kjenne de forskjellige typene for å kunne forstå hvilke som er best egnet til forskjellige oppgaver, og for å kunne velge en metodologi for et gitt oppdrag. Dette valget må også kunne kommuniseres til en oppdragsgiver. I denne oppgaven skal du vise at du kan bruke det du har lært om test-metodologi til å vurdere og sammenligne disse.

På denne oppgaven må besvarelsen inneholde minimum en referanse til hver av pensumlitteraturene (Kali Linux 2018 og Owasp), og minimum en annen referanse.

Besvarelser som ikke har korrekt oppgitt kildereferanse på APA7 format vil ikke oppnå poeng. Kildelisten skal oppgis for hver deloppgave separat.

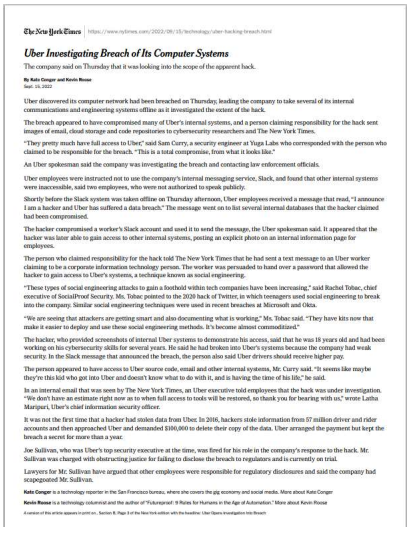
Oppgaveformulering:

Sammenlign OWASP Complete Testing Guide med å bruke test-metodologien som presentert i pensumboken i kapittel 3 «General Penetration Testing Framework» (side 92 til 108, eller 89 til 105 – avhengig av versjon av boken). Hvis en penetrasjonstester skal utføre en test av en web applikasjon, hvilke styrker og svakheter har de to modellene sett opp mot hverandre. Drøft styrken til OWASP Complete Testing Guide, og hvilke begrensninger denne eventuelt har.

Avslutt besvarelsen på denne oppgaven med ett avsnitt (maksimalt 6-7 linjer) som forklarer bruk av en av de to metodologiene brukt i testing av en web applikasjon, slik du ville formulert det i starten av en penetrasjonstestrapport.

Oppgave 3 – Analyse av hacker angrep (20%)

Som en etisk hacker vil man ofte bli bedt om en ekspertuttalelse om et hacker angrep som har fått fokus i media, du skal i denne oppgaven derfor vise at du er i stand til å tilegne deg ny kunnskap, sette dette i kontekst til en angriper/hacker, og forklare dette videre med egne ord.



The New York Times https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html

Uber Investigating Breach of Its Computer Systems

The company said on Thursday that it was looking into the scope of the apparent hack.

By Kate Conger and Kevin Roose
Sept. 15, 2022

Uber discovered its computer network had been breached on Thursday, leading the company to take several of its internal communications and engineering systems offline as it investigated the extent of the hack.

The breach appeared to have compromised many of Uber's internal systems, and a person claiming responsibility for the hack sent images of email, cloud storage and code repositories to cybersecurity researchers and The New York Times.

"They pretty much have full access to Uber," said Sam Curry, a security engineer at Yuga Labs who corresponded with the person who claimed to be responsible for the breach. "This is a total compromise, from what it looks like."

An Uber spokesman said the company was investigating the breach and contacting law enforcement officials.

Uber employees were instructed not to use the company's internal messaging service, Slack, and found that other internal systems were inaccessible, said two employees, who were not authorized to speak publicly.

Shortly before the Slack system was taken offline on Thursday afternoon, Uber employees received a message that read, "I announce I am a hacker and Uber has suffered a data breach." The message went on to list several internal databases that the hacker claimed had been compromised.

The hacker compromised a worker's Slack account and used it to send the message, the Uber spokesman said. It appeared that the hacker was later able to gain access to other internal systems, posting an explicit photo on an internal information page for employees.

The person who claimed responsibility for the hack told The New York Times that he had sent a text message to an Uber worker claiming to be a corporate information technology person. The worker was persuaded to hand over a password that allowed the hacker to gain access to Uber's systems, a technique known as social engineering.

"These types of social engineering attacks to gain a foothold within tech companies have been increasing," said Rachel Tobac, chief executive of SocialProof Security. Ms. Tobac pointed to the 2020 hack of Twitter, in which teenagers used social engineering to break into the company. Similar social engineering techniques were used in recent breaches at Microsoft and Okta.

"We are seeing that attackers are getting smart and also documenting what is working," Ms. Tobac said. "They have kits now that make it easier to deploy and use these social-engineering methods. It's become almost commoditized."

The hacker, who provided screenshots of internal Uber systems to demonstrate his access, said that he was 18 years old and had been working on his cybersecurity skills for several years. He said he had broken into Uber's systems because the company had weak security. In the Slack message that announced the breach, the person also said Uber drivers should receive higher pay.

The person appeared to have access to Uber source code, email and other internal systems, Mr. Curry said. "It seems like maybe they're this kid who got into Uber and doesn't know what to do with it, and is having the time of his life," he said.

In an internal email that was seen by The New York Times, an Uber executive told employees that the hack was under investigation. "We don't have an estimate right now as to when full access to tools will be restored, so thank you for bearing with us," wrote Latha Maripuri, Uber's chief information security officer.

It was not the first time that a hacker had stolen data from Uber. In 2016, hackers stole information from 57 million driver and rider accounts and then approached Uber and demanded $100,000 to delete their copy of the data. Uber arranged the payment but kept the breach a secret for more than a year.

Joe Sullivan, who was Uber's top security executive at the time, was fired for his role in the company's response to the hack. Mr. Sullivan was charged with obstructing justice for failing to disclose the breach to regulators and is currently on trial.

Lawyers for Mr. Sullivan have argued that other employees were responsible for regulatory disclosures and said the company had scapegoated Mr. Sullivan.

Kate Conger is a technology reporter in the San Francisco bureau, where she covers the gig economy and social media. More about Kate Conger

Kevin Roose is a technology columnist and the author of "Futureproof: 9 Rules for Humans in the Age of Automation." More about Kevin Roose

A version of this article appears in print on , Section B, Page 3 of the New York edition with the headline: Uber Opens Investigation Into Breach

På denne oppgaven må besvarelsen inneholde minimum en referanse til pensumlitteraturen; Kali Linux 2018 kapittel 7 «Social Engineering», og minimum to andre referanser. Besvarelser som ikke har korrekt oppgitt kildereferanse på APA7 format vil ikke oppnå poeng. Kildelisten skal oppgis for hver deloppgave separat.

En oppdragsgiver sender deg følgende artikkel fra New York Times, forfattet av Kate Conger og Kevin Roose 15. september 2022 (artikkelen er også lagt ved eksamensoppgaven på Canvas, du trenger ikke kjøpe abonnement av NYT for å få lest artikkelen):

https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html

Oppgaveformulering:

Sett deg inn i hacker angrepet som rammet Uber i 2022, som det vises til i artikkelen over. Du som teknikker må også søke flere mer tekniske kilder på egenhånd og skrive en fyldig beskrivelse av angrepet. Din beskrivelse bør inneholde informasjon om HVORDAN angrepet ble gjennomført, HVEM som stod bak angrepet, og HVA som ble skadefølgene av angrepet.

Du skal videre forklare for den tenkte oppdragsgiveren minimum 3 tiltak for å sikre at oppdragsgiver ikke (enkelt) blir offer for et tilsvarende angrep.

Praktiske oppgaver

Oppgave 4 – Passord brute-force (10%)

I denne oppgaven skal du vise at du kan gjennomføre et SQL Injection angrep for å hente ut passord hasher, for så å knekke disse passordene med John the Ripper. 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. 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 35 (ETH2100_U35_Øvingsoppgaver_Kali_Virtlab)*.*

Oppgaveformulering:

Denne oppgaven består av 2 steg. I det første steget skal du utføre et SQL Injection angrep mot DVWA VMen for å hente ut passord hasher fra serveren. Du bestemmer selv fremgangsmåten, men angrepet må utføres manuelt (og ikke for eksempel med sqlmap).

I det neste steget skal du bruke verktøyet John the Ripper i Kali Linux for å knekke passordene med en standard wordlist som du har hentet fra Kali Linux.

Oppgave 5 – EternalBlue (15%)

I denne oppgaven skal du vise at du kan gjennomføre et praktisk angrep mot en Windows server. Angrepet utnytter en sårbarhet i SMB protokollen.

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 37 (ETH2100_U37_Øvingsoppgaver_Pentest_Verktøy), slide 64 til 78*. I tillegg skal VMen ha tilleggsprogramvare og konfigurasjon som satt opp i:*

- *uke 44 (*ETH2100_U44_Øvingsoppgaver_IntoTheRabbitHole_Exploits*), slide 8 til 10,*
- *uke 46 (*ETH2100_U46_Øvingsoppgaver_PasswordEqualsGod*) slide 6 til 12, og*
- *uke 47 (*ETH2100_U47_Øvingsoppgaver_DeeperIntoTheRabbitHole*) slide 7 til 25.*

Oppgaveformulering:

Du skal starte opp Windows VM, og logge deg inn som Administrator. Denne oppgaven består av 3 steg.

Det første steget er at du skal kjøre NMAP mot VM for å sjekke om serveren er sårbar ovenfor EternalBlue sårbarheten (hint: et script i nmap kan gjøre dette).

Fra Kali Linux skal du som steg to starte verktøyet Metasploit, du skal gjennom Metasploit utnytte EternalBlue sårbarhet på Windows VMen. Du skal utnytte sårbarheten til å sette opp et reverse shell mot serveren.

Som steg tre skal du gjennom reverse shell opprette en fil på Windows VM som heter **havebeenpwned.txt**. Innholdet i filen skal være kandidatnummeret ditt på denne eksamen. I besvarelsen skal du vise skjermbilde av reverse shell i Kali 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 som viser Notepad når du har åpnet filen).

Oppgave 6 – XSS angrep med BeeF (15%)

I denne oppgaven skal du vise at du kan gjennomføre et standard angrep med Browser Exploitation Framework (github.com/beefproject/). I en enkel pentest er det normalt å kun bevise at XSS angrep fungerer ved å kjøre et enkelt Javascript (for eksempel en alert), men i en mer omfattende Red Team øvelse er det ofte nødvendig å faktisk hente ut informasjon fra offerets maskin, eller plante en bakdør eller en trojaner. BeeF er et rammeverk som kan være et mulig valg for å få mer ut av en XSS sårbarhet.

Du skal demonstrere at du mestrer oppsett, konfigurasjon og deployering av BeeF verktøyet, 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 skal bruke webserveren Damn Vulnerable Web Application (og undersiden "XSS Reflected"*, med security satt til* Low*), og som «offer» kan du velge å bruke din egen fysiske host maskin (eller en annen VM hvis du foretrekker det). DVWA VMen skal være satt opp i henhold til øvingsoppgave i uke 35* (ETH2100_U35_Øvingsoppgaver_Kali_VirtLab.pptx).

Oppgaveformulering:

Du skal sette opp BeeF på din Kali maskin (hvis du ikke allerede har det), og sette opp et Reflected XSS angrep mot webserveren. Fra «offer» maskinen skal du starte starte en nettleser og gå til den XSS-sårbare webserveren.

Du skal redigere config.yaml filen til BeeF og endre navnet på hook_file til å være ditt kandidatnummer på denne eksamen – etterfulgt av filendingen ".js", slik (eksempel for kandidat nummer 10042):

```
# Hook
hook_file: "/10042.js"
hook_session_name: "BEEFHOOK"
```

I besvarelsen skal du vise oppstart og kjøring av BeeF, du skal dokumentere hvordan du utfører XSS angrepet, og du skal vise både skjermbilde av BeeF som kjører på Kali, og du skal vise at du kobler deg på administrasjonsgrensesnittet til BeeF og klarer å se at «offer» maskinen har blitt hacket. I BeeF skal du vise at du får opp browseren din som et offer, og du skal ta en skjermbilde av Details fanen som viser verdiene browser.window.cookies og browser.window.hostname. Hva er offerets PHPSESSIONID?

Oppgave 7 – pwn 2 root; Shellshock (10%)

I denne oppgaven skal du vise at du kan gjennomføre et avansert angrep med Shellshock sårbarheten mot den sårbare maskinen PwnOS.

Spesifikt er PwnOS sårbar ovenfor CVE-2014-6271, du skal bruke den sårbarheten til å legge til «vmware» brukeren til sudoers listen (`echo "vmware ALL=(ALL) ALL" >> /etc/sudoers`*), slik at du kan oppnå root på maskinen.*
https://en.wikipedia.org/wiki/Shellshock_%28software_bug%29

Du vil i denne oppgaven bli utfordret på å kombinere flere forskjellige teknikker for å oppnå shell tilgang med root privilegier på en server. Du står ganske fritt til å velge fremgangsmåte, men en del av angrepet ditt må være at du utnytter Shellshock (CVE-2014-6271) for å legge til vmware til sudoers listen. Resten av fremgangsmåten bestemmer du selv, du må dokumentere fremgangsmåten med skjermbilder av de involverte maskinene og verktøy du bruker, og forklare hvordan du kom frem til denne fremgangsmetoden.

I denne oppgaven skal du bruke maskin med Kali Linux, og som «offer» maskin skal du bruke den virtuelle maskinen PwnOS. PwnOS VMen skal være satt opp i henhold til øvingsoppgave i uke 47 (ETH2100_U47_Øvingsoppgaver_DeeperIntoTheRabbitHole.pptx, *og ytterligere forklaringer fra forelesning den uken*).

Oppgaveformulering:

Du skal starte opp PwnOS VM. Kjør først et portscan av maskinen, dokumenter at du har testet ALLE åpne porter med et skjermbilde eller annen logg fra nmap. Hvilken porter er åpne?

Du skal så opprette en CGI fil inne på serveren, du kan selv velge hvilken sårbarhet du skal bruke for å få opprettet filen lokalt på serveren (men må ikke kreve root), og så skal du trigge Shellshock sårbarheten, med Shellshock skal du legge til vmware som sudoer (se over).

For å demonstrere at du nå har oppnådd rettigheter på serveren som «root» skal du nå koble deg til SSH med brukernavn vmware (passordet for denne brukeren er h4ckm3, du skal slippe å bruke tid på å knekke dette passordet). Ved å bruke sudo su skal du elevere brukeren til root – og så skal du skrive ut innholdet av filen /etc/shadow (til skjerm).

I besvarelsen skal du vise kjøring og resultat av utnyttelse av Shellshock sårbarheten, og vise med skjermbilde at du får frem innholdet av shadow filen.

-

Slutt på oppgavesettet