Cybersikkerhed – kan du løse escape roomet?

Introduktion

> Hver dag bliver der smadret mod Danmarks digitale forsvarsværk, men der uddannes ikke nok 'good guy'-hackere til at forsvare os. Det skal du prøve! Skolens system er blevet ramt af et angreb. Alt er låst ned, og tiden løber. I skal arbejde som et team af etiske hackere, finde ud af hvem der står bag, og knække koden, før nedtællingen når nul. Nogle spor ligger på skærmen – andre ligger på selve skolen…

Sikkerhed

VIGTIGT – læs dette sikkerhedsafsnit, inden du går i gang!

Opmærksomhed

Alt du foretager dig i denne aktivitet er med fokus på etisk hacking, for at forstå hvordan du kan beskytte dig selv og andre.

- Alle navne, IP-adresser, servere og mails i aktiviteten er fiktive eller ligger i et lukket øvemiljø.
- Det er ulovligt at skaffe sig adgang til andres computere, konti eller servere uden tilladelse (straffelovens § 263). Du må kun arbejde i det miljø, læreren har åbnet for.
- Indtast aldrig dine egne rigtige brugernavne eller adgangskoder i øvelsen.

Forholdsregler

- Hold jer til de systemer og den adresse, læreren har givet jer. Prøv ikke at scanne eller afprøve andre sider eller netværk.
- Ingen må tage skolens ting væk eller åbne lokaler, der ikke er en del af øvelsen. Alle fysiske spor ligger frit synlige på de aftalte steder.
- Ret ikke i andres filer eller indstillinger på øveserveren.
- Skriv aldrig rigtige personoplysninger ned i opgaverne.

Førstehjælp

- Hvis du er kommet til at indtaste rigtige oplysninger et sted, så sig det straks til læreren. Skift adgangskoden med det samme, og fortæl en voksen.
- Bliver det for stressende, så sig stop. Tidspresset er en del af spillet, men ingen skal have det dårligt over det. Der er altid hints og en nødudgang.
- Hvis noget går i stykker på øveserveren, siger du det til læreren. Det kan nulstilles, og der er ingens skyld.

Oprydning

- Luk alle faner og log ud af øvesystemerne.
- Læg alle fysiske spor, post-its, USB-nøgler og udskrifter tilbage hos læreren, så de kan bruges igen.
- Slet ikke noget på servere, og gem ikke koder eller oplysninger til senere.

□□ Materialer

I skal bruge følgende:

- En computer eller tablet pr. gruppe (3-4 elever)
- Link til escape roomet: skolelabs.dk/cyberescape
- Printede opgaveark: mailens afsendeoplysninger, kort over serverplacering, kodeark
- Papir, blyant og et kodeark til Cæsar-chiffer
- Kombinationslås eller låst boks (efter lærerens ønske)
- QR-koder placeret rundt på skolen

- Ur eller storskærm med nedtælling
- Hint-kort (3 pr. gruppe)

□ Vejledning

Følg vejledningen trin for trin:

Intro: Alarm og lockdown

- Klassen får en mail fra “skolen”, og læreren åbner den.
- Mailen leder til en loginside, og så starter lockdown med nedtælling.
- Gruppernes mål er at finde en slutkode, der låser systemet op.
- Hver mission giver et kodefragment. Skriv dem alle på kodearket.

Mission 1: Hvem sendte mailen? (analog)

- Læs det printede mail-header-ark.
- Find mindst tre røde flag, fx et afsenderdomæne med stavefejl, en Reply-To-adresse et andet sted hen eller et haster-sprog.
- Antallet af røde flag eller et bogstav i domænet giver dit første kodefragment.

Mission 2: IP-adressen (analog)

- Brug øveværktøjet til at slå den fiktive IP-adresse op.
- Find udbyder, land og by.
- Diskuter: Hvad kan man se, og hvad kan man ikke se?

Mission 3: Serverens placering (analog)

- Brug kortet og rapporten på papir.
- Find ud af, hvilket land serveren står i, og skriv hvorfor det betyder noget.
- Landekoden eller en dato giver dit næste kodefragment.

Mission 4: Adgang til serveren (digital)

- Brug de hints, I får, til at udlede et svagt kodeord.
- Log ind på øveserveren, og find en fil med et kodefragment.
- Tænk over: Hvad gjorde kodeordet nemt at gætte?

Mission 5: Spor på skolen (analog)

- Find QR-koder, post-its og andre spor på de aftalte steder.
- Hvad afslører menneskelige vaner, fx et kodeord under et tastatur?
- Alle spor giver et ciffer til slutkoden.

Mission 6: Den krypterede besked (analog + digital)

- Brug kodearket til at afkode en besked, fx med Cæsar-chiffer.
- Tast resultatet ind på siden for at få det sidste fragment.

Outro: Slutkoden

- Saml alle fragmenter i den rigtige rækkefølge.
- Tast slutkoden ind, før tiden løber ud.

□ Opsamling

Prøv at svare på følgende spørgsmål:

- Hvilke tegn afslørede, at mailen var phishing?
- Hvad kunne I og kunne I ikke finde ud af ud fra en IP-adresse?
- Hvad gjorde kodeordet på serveren svagt, og hvordan laver man et stærkt?
- Hvilke spor i skolen afslørede menneskelige fejl, og hvorfor er det farligt?
- Hvad er forskellen på en etisk hacker og en kriminel?
- Hvad ville I gøre, hvis I fik en lignende mail i virkeligheden?

Faglig forklaring+

Phishing er forsøg på at narre dig til at give oplysninger eller klikke på et link ved at udgive sig for at være en betroet afsender. Typiske tegn er forkerte domæner, hastesprog og uventede vedhæftninger.

IP-adresse er en enhed på internettet, ligesom en adresse. Den afslører typisk udbyder og omtrentlig placering, ikke den præcise adresse. En VPN eller proxy kan skjule den.

Domæner og subdomæner: Det rigtige domæne står lige før endelsen. I edbit.login-sikkerhed.skolelabs.dk er domænet skolelabs.dk.

Adgangskoder: Lange, unikke koder og tofaktorlogin beskytter bedre end korte og genbrugte. En password manager gør det nemt.

Social engineering er at udnytte mennesker frem for teknik, fx ved at finde kodeord på post-its eller en tabt USB-nøgle.

Kryptering gør data ulæselige uden en nøgle. Cæsar-chiffer er en simpel og gammel form, men princippet er det samme i moderne kryptering.

Etisk hacking betyder at teste sikkerhed med tilladelse for at forbedre den.

Lærervejledning+

Tid: 2 x 45 minutter inklusiv tid til opstart og opsamling.

Forberedelse:

- Aftal forløbet med skoleleder og IT-ansvarlig, så skolens systemer ikke reagerer på phishing-siden.
- Brug kun fiktive data: IP-adresser fra de reserverede testområder (fx 203.0.113.x) og et fiktivt skolenavn.
- Phishing-siden skal have en dummy-login, hvor du selv taster opdigtede oplysninger. Ingen oplysninger må gemmes.
- Placer de fysiske spor og QR-koder før timen, og tjek at de virker.
- Test øveserveren med mange samtidige brugere, og sørg for en hurtig nulstilling.
- Print opgavearkene og hint-kortene.

Organisering: Grupper på 3-4. Lad grupperne starte med forskellige missioner, så ikke alle sidder ved skærm samtidig. Fordel roller: en læser, en skriver, en løber til de fysiske spor, en kodevogter.

Balance: Missionerne 1, 4 og 5 er analoge. Missionerne 2 og 5 er digitale.

Mission 6 kræver begge dele. Hold øje med at grupperne skifter mellem skærm og rum.

Hints: Hver gruppe har 3 hint-kort. Brug af et hint koster fx 2 minutter på uret.

Nødudgang: Hvis tiden løber ud, giver du den sidste kode som en fælles sejr. Opsamlingen er vigtigere end at have "vundet".

Differentiering: Hurtige grupper kan få bonusmissioner, fx en dybere analyse af mail-headeren. Grupper, der har brug for hjælp, får ekstra hints eller en kodeark med en del af løsningen.

Fagmål (teknologiforståelse): Digital myndiggørelse, kritisk vurdering af digitale kilder, forståelse for netværk og kryptering samt etisk refleksion.

Kildehenvisning+

- Center for Cybersikkerhed: cfcs.dk
- Sikker Digital (Digitaliseringsstyrelsen): sikkerdigital.dk
- Datatilsynet: datatilsynet.dk
- Straffeloven § 263 (uberettiget adgang til data): retsinformation.dk