Øvelse 53 - Efterforskningsproces

Formålet med øvelsen

Formålet med denne øvelse er **forståelse for systematisks efterforskningsproces i tilfælde af en sikkerhedshændelse**, og samtid introducer koncepet bag *Detection in depth*. I øvelsen skal der reflekteres over identificeing, isolering, analyse og rapportering af en sikkerhedshændelse i overensstemmelse med en standardiseret proces.

Hvad er "Detection in Depth", og hvorfor er det vigtigt i en efterforskningsproces?

Når vi efterforsker en sikkerhedshændelse, ønsker vi at opdage den så tidligt som muligt. **Detection in Depth** handler om at opbygge flere lag af detektion, så et angreb kan opdages fra forskellige vinkler.

Forestil dig en bank med flere sikkerhedsforanstaltninger:

- **Kameraer ved indgangen** (overvågning af adgang)
- **Bevægelsessensorer inde i banken** (overvågning af aktivitet)
- **Alarmer på pengeskabet** (overvågning af adgang til kritiske ressourcer)

Hvis en røver slår et af disse systemer fra, er der stadig andre lag, der kan opdage ham. **Samme princip gælder for it-sikkerhed**.

Hvordan hjælper "Detection in Depth" i en efterforskning?

Når et angreb har fundet sted, kan vi bruge "Detection in Depth" til at:

1. **Forstå, hvordan angriberen bevægede sig gennem systemet**
   - Hvilke systemer blev påvirket?
   - Hvor blev der efterladt spor?
   - Hvilke sikkerhedsforanstaltninger blev omgået eller udnyttet?
2. **Sikre, at vi har pålidelige beviser**
   - Hvis en log er blevet ændret eller slettet, kan en anden kilde (f.eks. netværkslogs eller adgangskontroller) stadig indeholde spor.

- Logs fra flere steder kan bekræfte hinanden og styrke efterforskningens troværdighed.

3. **Afsløre angriberens metoder**
   - Hvis angriberen brugte stealth-teknikker (f.eks. sletning af logs), kan vi stadig opdage mistænkelig adfærd i andre systemer.
   - Fx: En angriber kan slette shell history, men hvis vi har audit logs over kommandokørsel, kan vi stadig genskabe, hvad der er sket.
4. **Opbygge bedre forsvar**
   - Ved at analysere, hvor angrebet blev opdaget (og hvor det ikke blev), kan vi forbedre vores overvågning.
   - Eksempel: Hvis vi kun fandt angrebet i systemlogs, men ikke i netværkslogs, bør vi måske forbedre netværksmonitoreringen.

Eksempel på **Detection in Depth** i en it-efterforskning:

Overvågningslag	Hvad det kan afsløre
Systemlogs	Hvem loggede ind og hvornår? Var der fejl ved login?
Audit logs	Hvilke filer blev åbnet, ændret eller slettet?
Netværkslogs	Sendte maskinen data til en mistænkelig IP-adresse?
Brugeraktivitet	Var der unormale autentificerings-tider eller shell-kommandoer?

Ved at bruge **flere lag af overvågning**, sikrer vi, at vi ikke kun afhænger af én enkelt logfil eller ét overvågningsværktøj. Hvis angriberen forsøger at slette spor, vil vi stadig kunne finde beviser i andre kilder.

Information

Efterforskning af sikkerhedshændelser kræver en struktureret tilgang for at sikre korrekt håndtering og dokumentation.
De primære faser i en efterforskningsproces er:

1. **Identificering**
   - Hvad er der sket? (Indicators of Compromise - IoC)
   - Hvem er involveret? (Hvem skal underrettes?)

- Hvilke dele af systemet er berørt?

2. **Isolering**
   - Stop hændelsen
   - Isolér berørte hosts/dele af systemet
3. **Oprettelse af kopi**
   - Kopier alle relevante logfiler
   - Opret eventuelt et image af lagringsmediet
   - Overvej en VM-klone
   - **Checksum på ALT** for at sikre integritet
4. **Sikring af integritet**
   - Lav en hash-sum af logfiler
   - Lav en hash-sum af øvrige involverede filer
5. **Analyse**
   - Gennemgå logs og relaterede data for at forstå hændelsen
   - Overvej **Detection in Depth**:
     - Hvilke tegn på angreb kan I opdage på forskellige niveauer?
     - Hvordan kan flere lag af overvågning sikre, at angrebet ikke går ubemærket hen?
6. **Rapportering**
   - Dokumentér hændelsesforløbet
   - Identificér root cause (hvorfor skete det?)

Instruktioner

1. **Scenario:**
   - En angriber har opnået **escalation of privilege**, hvilket giver dem superbrugerrettigheder på en host.
   - I skal danne og beskrive en proces for at efterforske kompromitteringen af denne host.
2. **Gennemfør efterforskningsprocessen:**
   - Brug ovenstående faser til at strukturere jeres efterforskning.
   - Dokumentér, hvilke metoder I vil bruge i hver fase.
   - Overvej, hvordan I kan **forbedre systemets sikkerhed** efter hændelsen.
3. **Tænk i scenarier:**

- Hvilken type angreb kan være sket?
- Hvilken adfærd kan være mistænkelig?
- Hvilke logfiler vil I kigge i for at finde spor efter angrebet?
- Hvordan ville en kompromitteret log se ud?

4. **Brug "Detection in Depth" til at forbedre jeres efterforskning:**
   - Identificér **flere steder**, hvor angrebet kunne opdages (fx brugeraktivitet, systemlogs, netværksforbindelser).
   - Overvej, hvordan angriberen potentielt kunne forsøge at skjule deres spor.
   - Hvordan kan **flere lag af overvågning** sikre, at I opdager og forstår angrebet bedre?
5. **Dokumentér jeres proces og diskuter i gruppen:**
   - Hvilke skridt var mest kritiske?
   - Hvordan kan lignende angreb forhindres i fremtiden?

Links

- Detection in Depth - SpecterOps
- ISO 27001 Incident Response
- Linux Audit Framework Guide

2025-04-03 05:55:59