Øvelse 44 – Statisk analyse af tekststrenge i binære filer

Formål

I denne øvelse skal du anvende statisk analyse til at undersøge, hvilke tekststrenge der findes i en binær fil. Det er en enkel men effektiv metode, der kan anvendes til at identificere mulige indikatorer for malware – fx mistænkelige URL'er, IP-adresser eller systemkommandoer. Du får erfaring med værktøjet `strings` og lærer at reflektere over, hvad tekstindhold i binære filer kan afsløre.

Baggrund

Ved statisk analyse undersøger man en fil uden at eksekvere den. Et simpelt men nyttigt værktøj til dette er `strings`, som scanner binære filer og trækker læsbare tekststrenge ud. Disse strenge kan afsløre mistænkelige domæner, kommandoer, navne på API-kald eller fejlmeddelelser – alt sammen spor, der kan indikere, at filen opfører sig skadeligt.

Dette er især nyttigt, hvis malware ikke er kendt endnu, og derfor ikke fanges af signaturbaserede værktøjer som ClamAV eller Maldet.

> Statisk analyse med `strings` er et af de første skridt i manuelle undersøgelser.
> I større miljøer kan lignende teknikker automatiseres og integreres i fx **SIEM/EDR-systemer** (som Wazuh eller Velociraptor) til at analysere ukendte filer, fange mistænkelige artefakter og generere indikatorer, der kan korreleres med logs.

Trin-for-trin

1. Installer nødvendigt værktøj

Installer pakken `binutils`, som indeholder `strings`:

```
sudo apt install binutils
```

---

2. Forbered testmiljø

1. Opret et testdirectory – fx:

```
sudo mkdir /maltest
cd /maltest
```

2. Hent en testfil (EICAR malware-simuleringsfil i zip-format):

```
sudo wget https://secure.eicar.org/eicarcom2.zip
```

---

3. Udfør statisk analyse

Kør `strings` på filen:

```
strings eicarcom2.zip
```

Læs output og se, om du kan identificere hvad den statisk analyse har lavet udtrak af?

Nyttige links

- strings – Linux man page

Refleksionsspørgsmål

- Hvilke typer information kan man udlede ved brug af `strings`?
- Hvordan kan denne teknik være nyttig i forhold til ny eller ukendt malware?
- Hvilke falsk positive risici er der ved at stole udelukkende på tekststrenge?
- Hvordan kunne du automatisere denne analyse som en del af et sikkerhedstjek?
- Hvordan kunne du bruge output fra `strings` til at oprette en indikator for kompromittering (IOC)?

CIS Controls – Kobling

CIS Control	Titel	Relevans

CIS Control	Titel	Relevans
10 – Malware Defenses	Statisk analyse	Du anvender `strings` til at finde potentielle indikatorer for malware
17 – Incident Response Management	Indsamling af artefakter	Teknikken kan bruges til at analysere mistænkelige filer i en hændelse
16 – Application Software Security	Forstå skadelig funktionalitet	Identifikation af kommandoer eller netværksadfærd uden at afvikle filen

2025-04-29 07:28:03