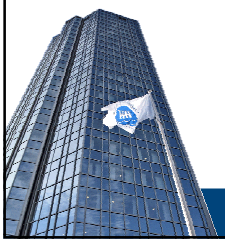
Analys av hackerverktyg



Översikt

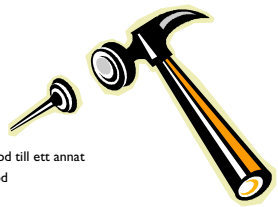
- Förhindra framtida attacker
- Gradera en viss fiende (kunskap/hot)
- Analysera hotets omfattning
- Analysera vilken skada som kan göras
- Analysera antal och typ av intrång
- Förbered för vidare utredning
- Förstå fiendens syfte och mål

- (386)

Kompilering av kod

- Körbar kod
  - maskinkod
  - binär kod
  - exekverbar kod
  - objektkod
- Kompilator
  - Översätter från ett ”språk” eller kod till ett annat
  - Koden som ska översättas = källkod

  - (386)

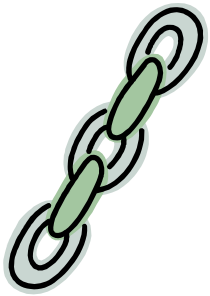


T-diagram

Länkning

- Statiskt länkade program
  - ”self contained”
- Dynamiskt länkade program
  - använder delade bibliotek
- Program med debuginformation
- Strippade program

- (387-389)



UPX

- Packar körbara filer
- Lägger till en automatisk uppackare
- Packade program körs precis som vanligt
- Packade program döljer innehållet och får ny checksumma !

- Finns många andra verktyg.
  - UPX licens är lite ”skum”

- (391-393)

Statisk analys

- Skaffa information om filen du analyserar
- Extrahera stränginnehåll och analysera detta
- Gör en kontroll med omvärlden om det är ett känt program
- Har du källkoden kan du göra en källkodsanalys

- (394)

Filtyp

- Olika typer av körbara filer för olika system (Windows, Linux…)

- file (unix)
- exetype (windows)

- (394)

Strängutvinning

- strings –a

- ASCII/Unicode

- Data att finna
  - information om källkoden, filens namn före kompilering …
  - vilken kompilator som använts
  - ”hjälp”-texten
  - felmeddelanden
  - värdet på statiska variabler

- (395-396)

Omvärldssökning

- Hittar du en kandidat?
  - Ladda hem källkoden
  - Kompilera med samma kompilator som målfilen
  - Jämför objektfilernas egenskaper, tex. storlek.
- (397-398)

Dynamisk analys

- Vilka filer påverkas?
- Vilka systemanrop görs?
- Gör nätverksanalys
- Undersök hur registryn påverkas
- Sandbox
  - VMWare
  - Ickepersistenta diskar
- Examensarbetet ”Säkerheten, hoten och spåren av U3-minnen”
- (399)

Systemanrop i Unix

- strace –o LOGGFIL MASKINKOD
- Leta efter nyckelord
  - open
  - close
  - execve
  - brk
  - mmap
  - getpid
  - setsock
  - listen
  - accept
- (401-406)

Dynamisk analys i Windows

- regmon
- filemon
- listDLLs
- Fport
- PsList

- Med debugger kan du göra maskinkodsanalys

- (409-413)