IN1020 uke 9

GRUPPE 10

Plan for dagen

- Repitisjon av hacking
- Eksamensoppgaver
- Lab

Angrepsvektor og skadevare

Begreper:

- Digital sårbarhet
  - En feil i et IKT-system grunnet svakhet, feildesign eller feilimplementering.
- Nulldags-sårbarhet
  - En sårbarhet som er ukjent for eller uadressert av leverandør.
- Angrepsvektor
  - Den konkrete metoden en angriper velger for å utføre et angrep på en datamaskin, et nettverk eller et system.

Digital sårbarhet

To kategorier sårbarheter:

1. Kjente og aksepterte
2. Ukjente eller feilvurderte, og dermed heller ikke håndterte



Skadelig programvare, *skadevare*

Skadevare:

- er en samlebetegnelse på ulik programvare som har som oppgave å gjøre skade.
- utnytter sårbarheter i et datasystem.
- kan være et enkeltstående program, eller en del av et *vertsprogram*.
- kan ha den egenskapen at den formere seg og infiserer andre systemer.

Skadevares oppbygning

1. Stridshode: Beskriver hvordan skadevaren skal infisere et datasystem.
2. Spredning: Beskriver hvordan skadevaren skal spre seg videre.
3. Nyttelast: Beskriver oppgaven skadevaren er satt til å gjøre.

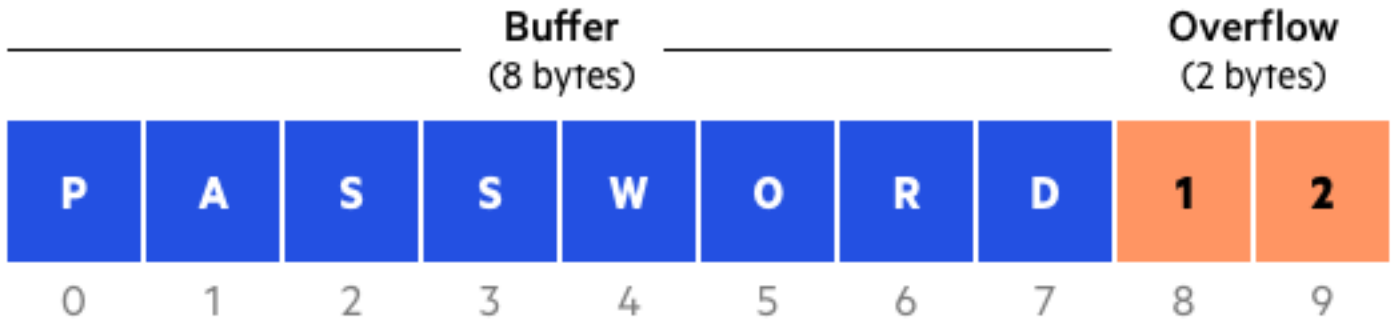
Et utvalg av typer skadevare:

Gruppene er til dels overlappende, og ikke alltid presist definert.

 Virus	Kjennetegnes ved at det sprer seg hver gang en fil med virus blir åpnet av bruker eller systemet.
 Dataorm	Skadevare som på egenhånd er i stand til å spre seg og finne nye ofre.
 Trojaner	Skadevare som utgir seg for å være et nyttig program.
Bakdør	En ubeskyttet og ukjent åpning inn i et datasystem, laget av en angriper.
 Spionvare	Programvare for å spionere på en bruker i håp om å få tak i f.eks. informasjon, passord, kontoinformasjon.
 Tastelogger (Keylogger)	En enhet eller programvare som er koblet til tastatur eller maskin og som lagrer eller videresender alle tastetrykk. En variant av spionvare.
Rootkit	Skadevare som endrer eller erstatter funksjoner i OS eller applikasjoner, med mål å ta kontroll over en maskin eller et system.
Exploit	Et program, en sekvens med data, eller en oppskrift på hvordan en sårbarhet kan utnyttes.

Buffer overflow

- Et buffer er en sammenhengende seksjon i minnet i datamaskinen, avsatt til å inneholde data.
- En feil i et dataprogram, som gjør at programmet når det kjøres kan overskride bufferets grenser i minnet, kalles bufferoverskridelse
- Brukes til å krasje program, føre til korrupt data og hente data fra minnet osv.
- Generelt sett så brukes det av hackerer til å kontrollere hvordan programmet ditt skal oppføre seg
- forklaring på buffer overflow



SQL injisering

Eksempel: Tabellen «Bruker»:

BrukerId	Brukernavn	Passord	Fornavn	Etternavn	Kredittkort #
1001	anneh	ewtgfst45yh	Anne	Hansen	1609983275417533
1002	pederaa	67efg3ndfa	Peder	Aas	4586890148239766

Eksempel på brukerdialog:

Oppgi brukernavn: anneh Oppgi passord: xyxyxy OR 1=1

Dette kan resultere i følgende gyldige SQL-setning:

```
SELECT * FROM Bruker
WHERE Brukernavn = anneh and Passord = xyxyxy  OR 1=1;
```

Løsning: filtrer all input

Cross Site Scripting (XSS)



1. Angriper plasserer ondsinnede kode på en webside, kamuflert som innhold fra en bruker. Lagres på web-tjeneren.



2. Intetanende bruker besøker websiden, og ondsinnet kode sendes tilbake til brukeren med innholdet.



3. Angriperen tar kontroll over brukerens maskin og/eller data via den injiserte koden.

Sosial manipulasjon

- Sosial manipulasjon handler om å utnytte menneskers tillit og svakhet
- Spoofing: Forfalske avsender i e-post eller SMS
- Phishing: Lure offeret med falske nettsider og e-post for å få informasjon
  - Masse-phising: Bredt utsendt e-post eller sms – ofte mindre troverdig
  - Spyd-phising – målrettet angrep, samler opplysninger i forkant for å gjøre henvendelser mer troverdig
  - Direktørsvinel – går etter «de store fiskene», målrettet angrep mot de med makt og myndighet
- Løsning: Bevissthet og opplæring
  - Stopp. Tenk. Klikk
  - Virker noe for godt til å være sant
  - Sjekk avsender på alle e-post
  - Vær forsiktig med å følge linker i e-post
  - Hold OS, drivere, programvare oppdatert med siste versjon
  - Tillit – Ikke stol blindt på noen før de viser seg troverdig

Eksamensoppgaver

- La oss se hvor mye vi kan hittil
- Ser på eksamen IN1020 høsten 2019

Lab

- Midtveisevaluering
- Jobbe videre med oblig eller ukesoppgaver
- Send meg mail eller teamsmelding hvis dere lurer på noe eller trenger hjelp til oblig
- myhd@uio.no