Week-05 Security+Penetration-Testing, Tools + how to practice

- **Explain briefly about the concept of Security Testing, and more thoroughly about Penetration Testing**

Security testing er en type af software test som gerne skulle kunne afsløre usikkerheder, trusler, og risici i en software applikation. Håbet er at kunne identificere alle loopholes og svagheder systemet har som kunne resulterer i negative konsekvenser for firmaet og dets medarbejdere.

En penetration test (pen test) er et simuleret angreb mod et software system for at kontrollere for sårbarheder som kan udnyttes. Pen testing er del op i 5 faser:

- Opklaring (Reconnaissance): Opsamling af vigtigt information om systemet, for at kunne lave et bedre angreb på sagt system. Checke headers fra en request til serveren om info ville for eksempel være en mulighed, da det giver et overblik om nogle specs og software der kunne ligge på serveren.
- Scanning: Involverer typisk et teknisk værktøj til at give yderligere information om systemet. For eksempel kan NMAP bruges til at scanne for åbne porte.
- Få adgang (Gaining access): gøre brug af den indsamlede data til at angribe systemet. Denne proces kan også gøres ved et værktøj som automatiserer angreb på kendte svagheder.
- Vedligeholde adgang (Maintaining access): For at have vedvarende adgang kræves gøres der brug af de ovenstående faser gentagende gange, for at konstant at udnytte systemet / udtrække data.
- Dække fodspor (Cover tracks): målet med denne fase er at dække sit angreb fra systemet, for at forblive anonym.

- **Explain the pros & cons related to Penetration Testing**

  Pros:
  - Kan identificerer en række af sårbarheder i et system.
  - Kan forudsige at mange små sårbarheder kan skabe en stor svaghed i systemet

  Cons:
  - Tests der ikke er lavet korrekt kan ende med at blotte data, gøre data korrupt, crashe servere og mm.
  - Man giver pen testeren fuld adgang, så det handler også om tiltro til personen der laver testen.

- **Explain a few (one or two) of the tools meant for Penetration Testing**

Kali Linux er en "Linux Distribution", en form for virtuel maskine, som indeholder en lang række af sikkerheds værktøjer.

- **Explain the purpose of NMap and what can be discovered with the tool, using one or more prepared samples**

NMAP er et værktøj der følger med i Kali Linux, som kan bruges til at monitorere diverse dele af et netværk. NMAP kan for eksempel bruges til:

- Host Discovery: identificere hosts på et netværk.
- Port Scanning: Gennemgåelse og opremsning af åbne porte på en specifik host.
- OS Detection: Fastlægge OS (Operating System) og hardware karakteristikker på netværks apparater (devices).

- **Explain “ways” to legally practice Penetration Tester Skills**

Det som der gør det uetisk at udøve pen testing på andres applikation og services, kan sammenlignes med at ruske i andres dørhåndtag for at se om døren er åben (analogi fra undervisningen). Så længe at ejeren er indforstået og er gået med til at der bliver foretaget en pen test på deres app eller service, er det i orden. Derudover er der lavet apps som man selv kan hoste og er designet til at blive pen testet og øvet på - blandt andet OWASP Juice Shop. Juice Shop er en webapp lavet, med vilje, fyldt med sikkerhedsfejl som kan udnyttes for at få adgang til dummy data der medfølger. Det er lavet for at simulere en webapp med dårlig sikkerhed.

- **Explain the concepts (where do they fit in) Kali Linux, Metasploitable 2 (and 3) OWASP Juice Shop.**

Metasploitable er en virtual machine, hvorimod Juice Shop er en webapp. De er begge designet med sårbar sikkerhed så man kan øve sig på pentesting. Metasploitable er dog lavet til at simulere en server. Kali Linux er et værktøj som man bruge til at lave disse pen tests med, både på Juice Box og på Metasploitable.

- **Explain a possible test-setup using Kali Linux and Metasploitable x (or similar) and why testing/practising in this way “makes sense”**

Med Kali Linux medfølger der en funktion NMAP der gør det muligt at se hosts services fra en host. Her kan vi lave et setup hvor vi bruger nmap gennem kali linux på din metasploitable VM, og kigge på om der eventuelt er nogle service versions som der har nogle kendte sårbarheder.

Eksempel ville være at der på port 80 ligger en apache service som har en version, som kan google for sårbarheder.

https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-77221/Apache-Http-Server-2.2.8.html <- den specifikke versions kendte sårbarheder.

Nmap funktionen er som følgende:

```
sudo nmap -sV [metasploitable IP]
```

sv er service versions, som er det vi kigger efter I denne test.