**Security noter til uge 5**

**Godt link der det meste af øvelsen**

<https://docs.google.com/document/d/1yo5B2Vqh_v_8zx3bIbwZyZnZyaH3erRen1WEinjIbQg/edit>

**Metasploitable2**

Løsning af problem ved netværksindstillinger på host-only-adapter i metasploitable2

Fil 🡪 Håndtering af værtsnetværk 🡪 opret 🡪 dette opretter en host-only-adapter ved navn: ”vboxnet0”

Den kan nu tilføjes under netværksindstillinger.

**Kali Linux**

På Kali Linux - Set netværksindstillinger til bridge-adapter

**Login**

1. Brugernavn: kali
2. Adgangskode: kali

**For at scanne virtual Box**

1. I terminal på Kali Linux: *nmap -v -A scanme.nmap.org*
2. Her kan man bl.a. se hvilke porte der er åbne og server typen (OS)

**For at scanne PC**

1. I terminal på ens egen PC: *ipconfig getifaddr en0*
2. Tilbage i Kali Linux terminal, for at scanne PC: *nmap -v -A ”ip-adresse”*
3. Her kan man bl.a. se hvilke porte der er åbne og server typen (OS)

**For at gemme en tekstfil lokalt på Virtual Box med den detekterede scanning på den pågældende IP-adresse**

1. I Kali Linux terminal:
2. *ls*
3. *cd Documents/*
4. *nmap -v -A ”ip-adresse” -oN ”filename.text”*

Tekstfilen ligger under /Documents/localscan.txt

1. **Start Metasploitable (server) og login**
   1. Brugernavn: msfadmin
   2. Adgangskode: msfadmin
2. **For at finde eventuel og interessant sårbarhed**

**I Kali Linux Terminal (anvend netdiscover)**

* 1. **Find mask**

*sudo ifconfig*

* 1. **Find server (metasploitable)** **HAV TÅLMODIGHED**

*sudo netdiscover -r ”* *xxx.xxx.xxx.1/24” (xxx er mask IP-adresse)*

* 1. **Scan metasploitable server:**

*sudo nmap -v -A ”metasploitable IP-adresse\*”*

\**metasploitable IP-adresse* skulle gerne komme frem ved kørsel af b.

På FireFox i Kali Linux skulle man gerne kunne skrive IP-adressen på den pågældende server, som der ønskes at blive hacket. Desuden kan man forsøge med forskellige porte, som eventuelt skulle være åbne.

**For eksempel**

I URL’en skriv: ”*metasploitable IP-adresse* + *portnummer (8180*)”

* Dette viser en Tomcat apache

1. **Find sårbare tjenester**

**I Kali Linux Terminal (anvend nikto)**

1. **For at specificere port skriv -p ”portnummer” (kan undlades)**
2. *sudo nikto -host ”metasploitable IP-adresse” -p 8180*
3. For at gemme det i en fil, tilføj efter ovenstående:
4. ”filename”.txt

Hvis ja, udnyt sårbarhed. 🡪 hvordan det gøres, afhænger af sårbarheden