**Exercises - Penetration Testing**

**Basic nmap**

1. First, open this [link in a browser](http://scanme.nmap.org/) and read what you are allowed to do.
2. Open a terminal:
3. Scan the website scanme.nmap.org: nmap -v -A scanme.nmap.org

Et billede, der indeholder sidder, foto, sort, bord

Automatisk genereret beskrivelse

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

1. Scan your own IP-address: nmap -v -A salandt.dk

Et billede, der indeholder tekst

Automatisk genereret beskrivelse

1. Scan your own computer and store the result in a text file:

nmap -v -A 192.168.0.13 localScan.txt

Make sure that Network settings is set on ”Bridged Adapter” (the very top menu → Devices → Network → Network Settings).

Et billede, der indeholder tekst

Automatisk genereret beskrivelse

**Reflection) For all the three scans above, reflect over the results. Was it possible to detect the OS, were there any unexpected open ports etc.)**

Ved scanning af scanme.nmap.org

* OS = Ubuntu Linux
* Serverheader = Apache
* Der er 4 åbne porte

Ved scanning af dropletten (salandt.dk)

* OS = Ubuntu Linux samt Tomcat Server
* Serverheader = NginX
* Der er en firewall på, som kun har 3 åbne porte. Det er også kun de 3 der kommer frem, når dropletten scannes.
  + HTTPS 443
  + SSH 22
  + MySql 3306

Ved scanning af computeren (Amalies computer)

* Der angives ikke en OS
* Der er 3 åbne porte, 2 af dem er uventede.
  + MySql 3306
  + TCP 49152 og 49400

**Nmap for Penetration Testing/Information Gathering**

1. Network Settings er sat til **Host-only Adapter**
2. Start **Metasploitable 2**
3. Åben en terminal enten lokalt eller I Kali VM.
4. Find Metasploitable der skal hackes:

sudo netdiscover -r xxx.xxx.xxx.1/24

(xxx is the first part of IP-address, 24 er submask)

Ved at bruge netdiscover kan man finde relevante IP-adresser på netværket, som man vil undersøge nærmere.

1. Scan Metasploitable og gem resultatet i en fil:

nmap -v -p 0-65535 -A IP\_OF\_metasploitable -oN meta1.txt

Ved at bruge nmap på den interessante IP-adresse, kan man finde frem til f.eks. hvilke porte der er åbne, og eventuelt udnytte denne port.

1. **Hint:** Nedenstående kommando er en hurtig løsning:

nmap -v IP\_OF\_metasploitable

**Discovering Vulnerabilities/hacking discovered Services**

1. Undersøg manuelt i en browser, den fundne IP-adresse. I dette her tilfælde er det Metasploitable.

* IP\_FOR\_Metasploitable (to test the default web-services running on port 80)
* IP\_FOR\_Metasploitable**:8180**

1. Find svagheder og gem resultatet i en fil:

nikto -host IP\_FOR\_Metasploitable -p 8180 > nikto.txt

1. Hvad er nikto?

man nikto

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

3) Attacking the Juice Shop SPA-application

Solve the first problem: *Find the carefully hidden ‘ScoreBoard’ Page*

Now solve as many as you can of the challenges given on the ScoreBoard.

You can probably find many challenges, which you can use to demo topics covered throughout the semester

Brug Google Developer Tools 🡪 source 🡪 fil = “main/es2015.js” 🡪 søg efter “score-board”) for at få en liste med paths. Sæt denne op i URL.

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

Et billede, der indeholder skærmbillede

Automatisk genereret beskrivelse

**VI KUNNE IKKE FÅ METASPLOITABLE TIL AT VIRKE!**

**1)** Attacking the Tomcat Manager Application

As the Kali-users already know, since nikto discovered that the Tomcat Version used, included a default account (which obviously should have been deleted before production)

1. Try to login to the manager application  with (username, password) → (tomcat, tomcat)
2. What “damage” could a hacker do in here?

**Hint:** Try to upload the war-file from [here](https://github.com/SecurityDatFall2018/Week14) and see what you get (rename it to ROOT.war, if you like ;-)

|  |
| --- |
| **Challenge:**   This vulnerability is actually much more serious than what you did above (if being able to delete all your web-apps is not serious enough). Via Google, you can find information for (with this combination of OS and Tomcat):   * how to actually get a Linux-shell as the Tomcat-user * If you Google even more: how to elevate this user to a user with higher privileges   Expect to spend several hours if you go for both :-) |

2) Attacking the Mutillidae Web Application

*Most of you will probably spend your time better on the "Exam Preparation" part*

Enter this address in your browser (Firefox for Kali-users): http://IP\_FOR\_Metasploitable/mutillidae/

**Important:** See the hints-section at the end of this document to fix the database-problem

Play around with this, as much as you have time for. You can probably find many examples here, which you can use to demo topics covered throughout the semester

**Hints:**

*Login to Metasploitable2 (msfadmin, msfadmin) and navigate into the folder /var/www/mutillidae (if you have a problem with the ‘/’ character, just cd into the mutillidae folder, step by step.*

*In this folder, open config.inc with nano:*

***sudo nano config.inc*** *and change the value of dbname into* ***owasp10*** *(*[*ref*](https://za1d.com/2017/01/31/fix-table-metasploit-accounts-doesnt-exis-in-metasploitable-2/)*)*

