I første oppgave tester vi sslyze skriver sslyze h-ck.me:

Et bilde som inneholder tekst, skjermbilde, skjerm

Automatisk generert beskrivelse

Kjører en nmap scan av min egen ip bruker cmd i windows ipconfig

Et bilde som inneholder tekst

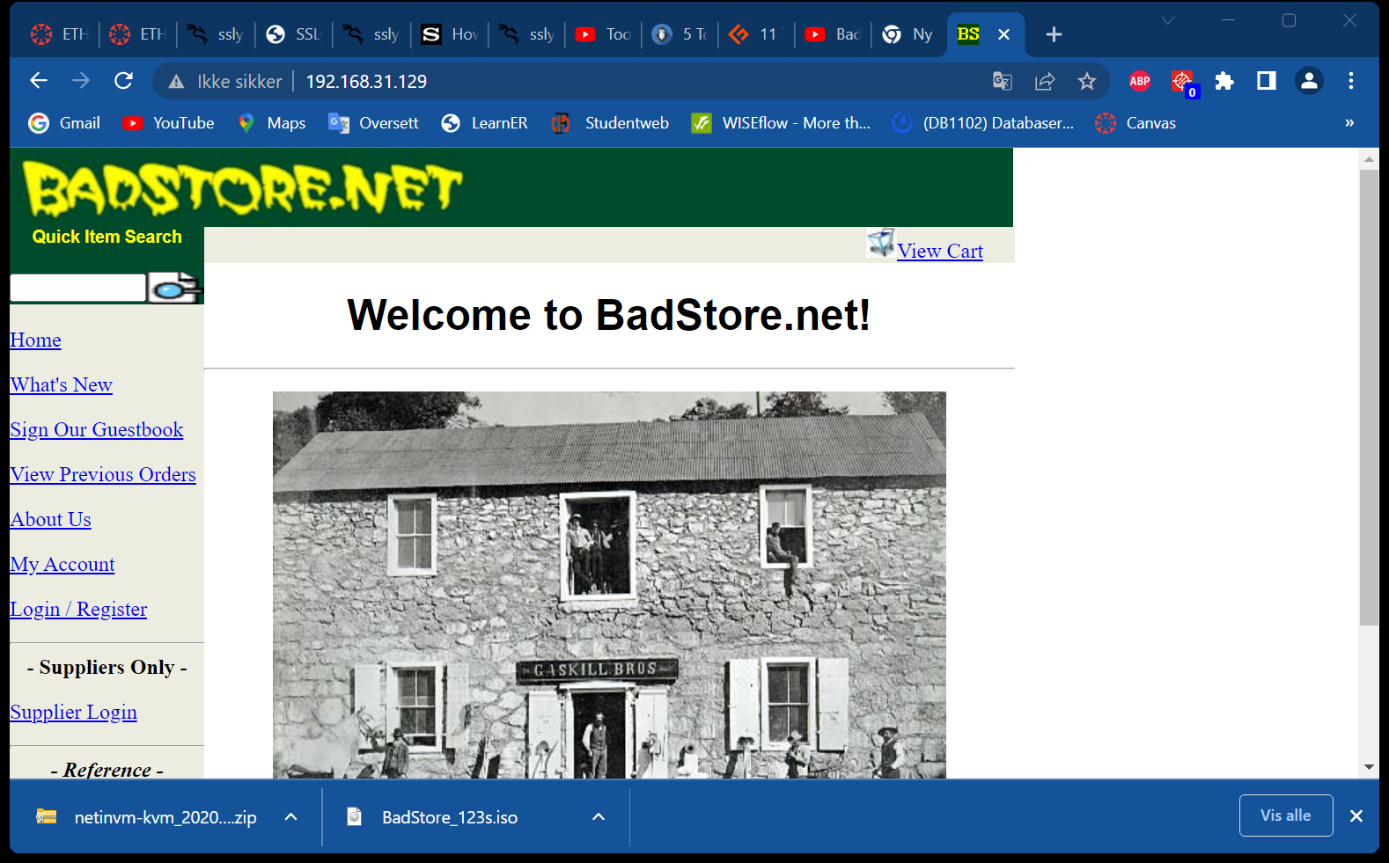
Automatisk generert beskrivelse

Kjører en full scan med nmap bruker samme ip adresse fra ovenfor

Et bilde som inneholder tekst

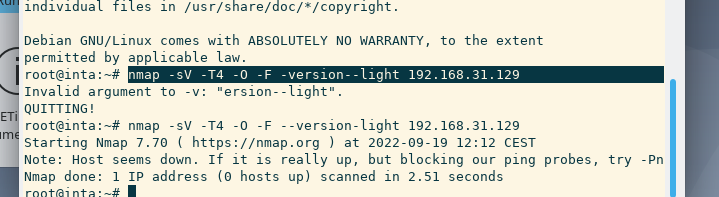
Automatisk generert beskrivelse

Skriver ipadressen : <http://192.168.31.129/>



Åpner netinvm

Og skriver root pass: You can change me. Og bruker badstore ip addressen



Et bilde som inneholder tekst

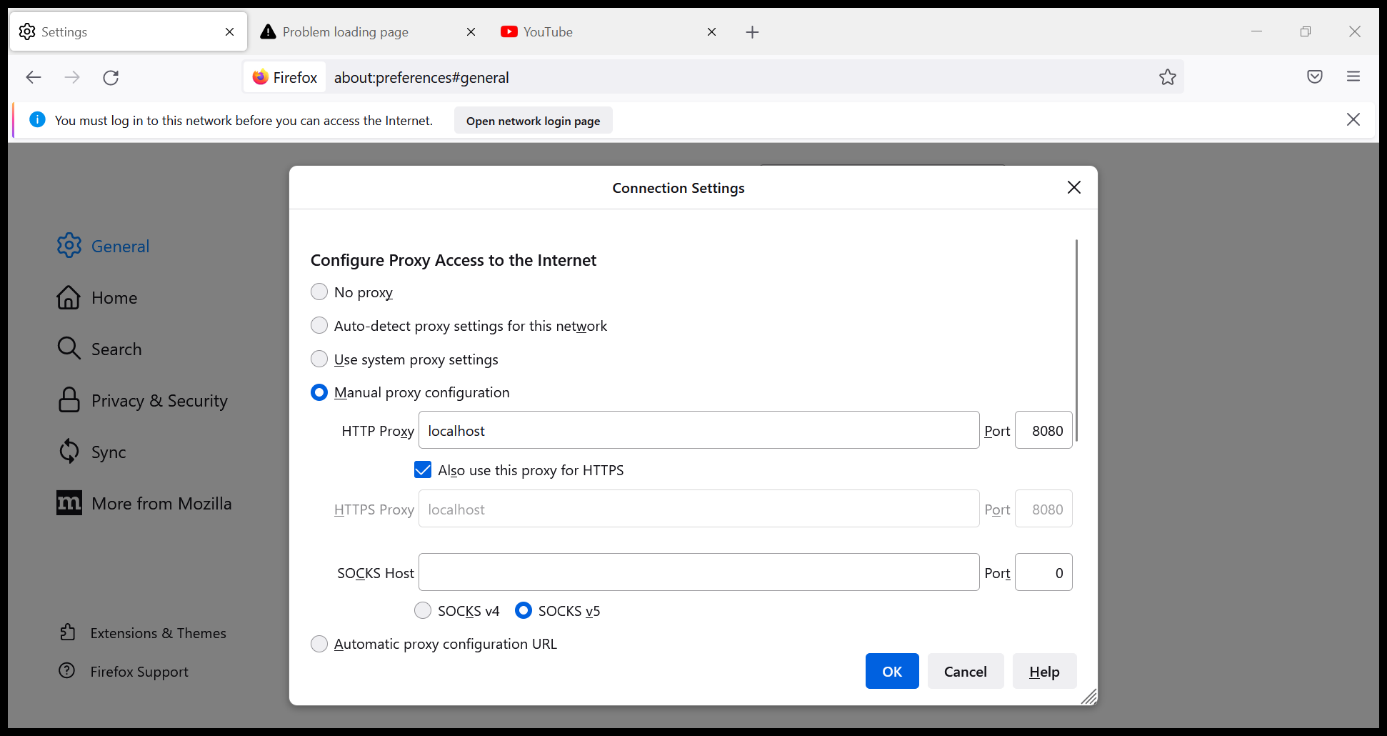
Automatisk generert beskrivelse

Leser guiden:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Går på options i owasp trykker på tools også ssl certificate og lagrer i datamaskinen deretter legger først inn detaljene:

****

Søker certificate i innstillinger i firefox

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Importerer filen og åpner owasp igjen

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Ser slik ut!

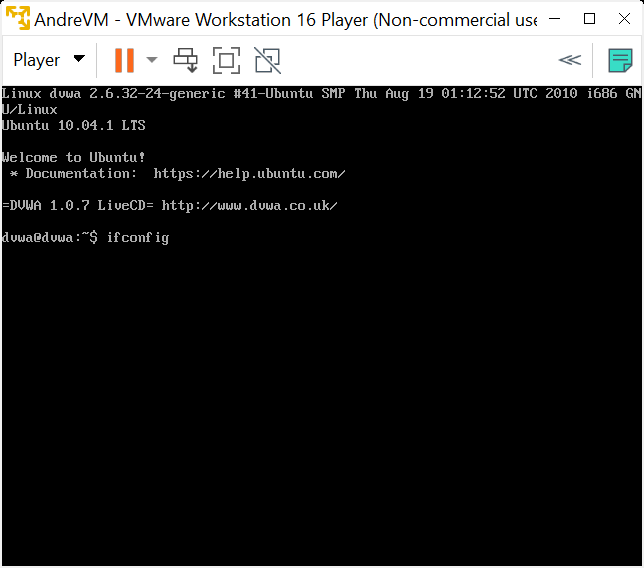
Et bilde som inneholder tekst

Automatisk generert beskrivelse

Ser slik ut etter at jeg gikk inn på h-ck.me og får opp Test i plain text.

Åpner DVWA i vmware

Skriver : ifconfig: trykker enter

’

Bruker ip adressen obs : slår av proxy i firefox (no proxy)

Og slår den på igjen

Høyre klikker på ip adressen Trykker på Attack -> active scan og får opp sårbarhetene under

Et bilde som inneholder bord

Automatisk generert beskrivelse

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Eks på Absence of Anti CSRF Tokens

Et bilde som inneholder tekst

Automatisk generert beskrivelse

NMAP:

**Bruk de forskjellige NMAP scannene du lærte om på mandag mot alle de 3**

**VMene i testsettet vårt (DVWA, BadStore og Metasploitable)**

Åpner DVWA skriver ipconfig og skriver nmap kommandoen på linux og sjekker de åpne portene:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Tilsvarende for Badstore:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

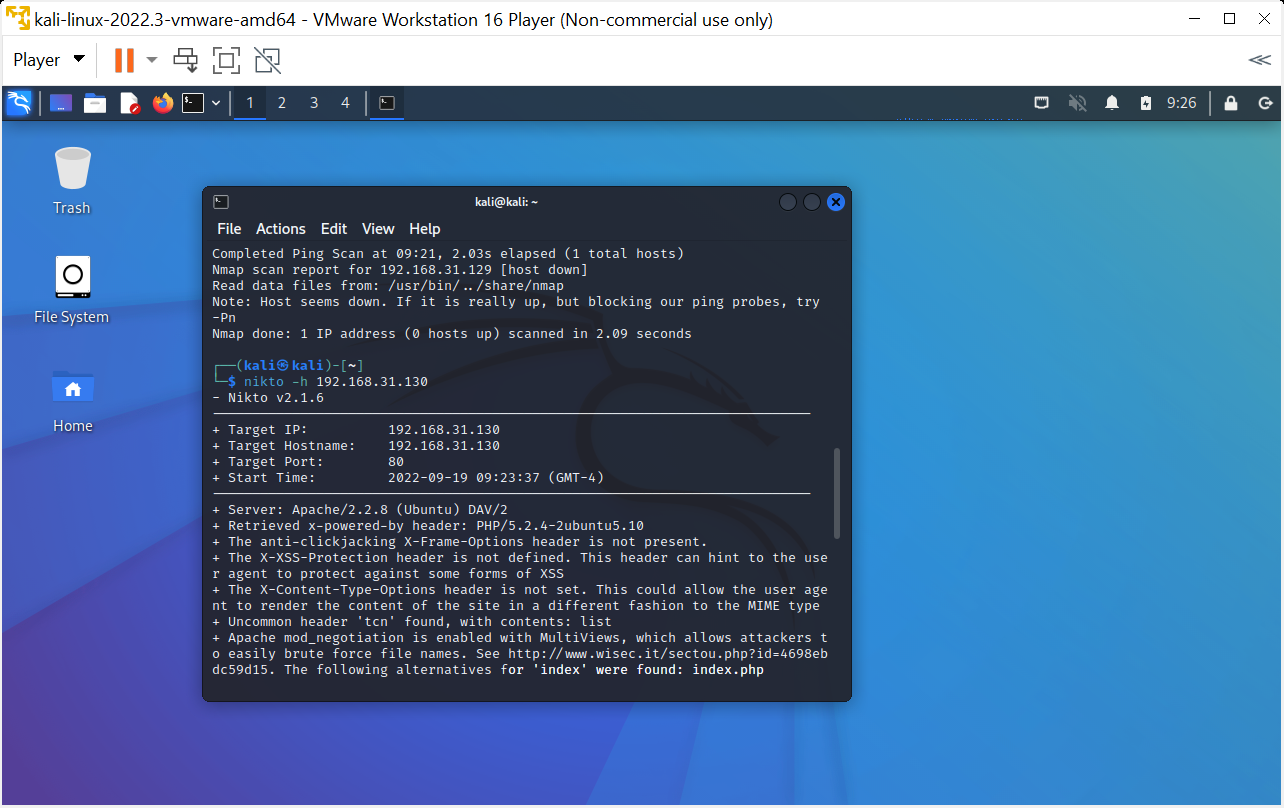
Og metasploit 2: kode msfadmin og passord er det samme i metasploitable 2:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

NIKTO:

Nikto : nikto – h (ip adresse kjør ifconfig) metasploitable 2 en sårbarhetsscanner



Badstore : nikto -h 192.168.31.129

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Finner noen sårbarheter her og

DWVA (Andre VM)

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Skriver dette etter ip

Og deretter:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

For å få en side med sårbarheter på firefox.

Ssh- audit skriver dette i linux: git clone <https://github.com/arthepsy/ssh-audit>

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Metasploitable har en eksponert SSH port, kjør SSH scan mot denne

• Diskuter resultatene i grupper

• Hva av output er faktiske sårbarheter?

Metasploitable har en eksponert SSH port, kjør SSH scan mot denne

• Diskuter resultatene i grupper

• Hva av output er faktiske sårbarheter?

Kjører metasploit login:msfadmin passord og

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Skriver kommandoen og får en liste med sårbarheter

* Aes-128-cbc (lar angriperen dekryptere kryptert data)
* 3des er en krypterings algoritme som skal beskytte mot brute force angrep
* Diffie hellmann-group-exchange-sha1 er sårbar mot Man in The middle attack angrep, men den krever autentisering for å sikre serveren mot å få tilgang til hemmelig data - men regnes som en liten sårbarhet med tanke på at angriperen fortsatt kan få tilgang til serveren
* Ssh-dss beskytter systemet mot uatorisert tilgang

Laster ned wireshark i kali linux:

Et bilde som inneholder tekst

Automatisk generert beskrivelse

Et bilde som inneholder tekst

Automatisk generert beskrivelse