Laporan Resmi Praktikum Keamanan Data

Network Scanning & Network Probing

Dimas Rizky H.P. – 2110141011 – 3D4 IT A

**Dasar Teori**

Pada pemrograman berbasis socket, server merupakan host yang menyediakan sebuah layanan dan client adalah host yang mengakses atau menggunakan layanan tersebut. Socket adalah gabungan dari alamat IP dan nomor port, salah satu contohnya adalah layanan mail PENS dengan socket 202.9.85.49:25. Alamat IP dari layanan tersebut adalah 202.9.85.49, dengan nomor port 25 menggunakan protokol SMTP.

Layanan tersebut dapat diserang dengan berbagai cara, karena pada dasarnya layanan spesifik semacam SMTP memiliki celah keamanan yang sangat rentan terhadap serangan. Dengan mengetahui port mana yang terbuka akan mudah bagi penyerang untuk memanfaatkan celah port sebagai serangan. Mak a dari itu sebaiknya host hanya menyediakan layanan yang diperlukan saja.

Pemindaian ini merupakan langkah awal penyerang untuk meretas layanan pada jaringan. Port scanner merupakan program yang didesan untuk menemukan layanan apa saja yang dijalankan pada host jaringan. Pemindaian ini dapat dilakukan menggunakan aplikasi Nmap (Network Mapper). Nmap merupakan tool open source untuk eksplorasi dan audit keamanan jaringan. Nmap menggunakan paket IP raw untuk mendeteksi host yang terhubung dengan jaringan. Nmap juga menyediakan informasi sistem operasi, jenis firewall/filter paket yang digunakan dan sejumlah karakteristik lainnya. Outputnya dapat berupa,

* Nomor port
* Nama layanan
* Status port : open, filtered, closed atau unfiltered
* Nama reverse DNS
* Prakiraan sistem operasi
* Jenis device dan alamat MAC

Nmap memiliki beberapa tipe pemindaian, tiap tiap tipe ini memiliki metode yang berbeda dalam melakukan scanning. Tipe-tipenya antara lain,

* ***Connect scan (-sT)***

Scan ini akan membuat koneksi penuh hingga menyelesaikan three-way handshake untuk mendeteksi port atau host yang up

* ***TCP SYN scan (-sS)***

Scan ini akan membuat koneksi namun tidak sampai menyelesaikan three-way handshake. Teknik ini dikenal sebagai half-opening scanning, dan dengan teknik ini akan dapat membedakan tiga buah state port, yaitu port, filtered ataupun closed.

* ***TCP FIN scan (-sF)***

Scanning ini bekerja dengan mengirimkan suatu paket FIN ke port sasaran. Dengan dikirimkannya paket FIN, respon yang akan dikirim adalah suatu RST untuk setiap port yang tertutup. Teknik ini hanya dapat dipakai pada stack TCP/IP

* ***TCP Xmas Tree Scan (-sX)***

Teknik scanning yang menggunakan paket FIN, URG ataupun PUSH ke port sasaran. Respon yang akan diterima adalah RST untuk semua port yang tertutup

* ***TCP Null scan (-sN)***

Teknik scanning ini membuat off semua flag, berdasarkan RFC 793, sistem sasaran akan mengirimkan suatu RST untuk semua port yang tertutup.

* ***TCP ACK scan (-sA)***

Teknik ini digunakan untuk memetakan aturan firewall dan dapat membantu untuk menentukan apakah firewall itu merupakan suatu simple packet filter atau rule yang hanya membolehkan koneksi-koneksi tertentu atau suatu firewall yang menjalankan advance packet filtering

* ***TCP Windows scan***

Teknik scanning ini mendeteksi port-port terbuka maupun terfilter/tidak terfilter pada sistem tertentu sehubungan dengan anomali dari ukuran windows TCP yang dilaporkan

* ***TCP RPC scan***

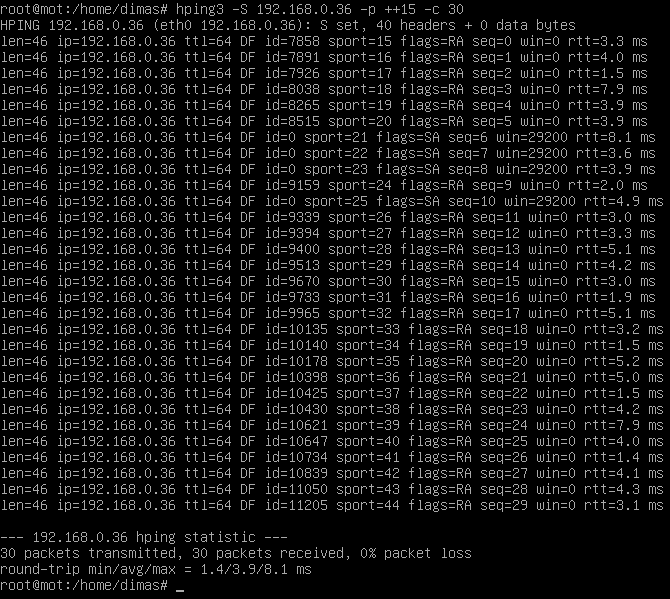
Teknik ini spesifik hanya pada system UNIX dan digunakan untuk mendeteksi dan mengidentifikasi port RPC dan program serta nomor versi yang berhubungan dengannya

**Laporan Pendahuluan**

**Percobaan**

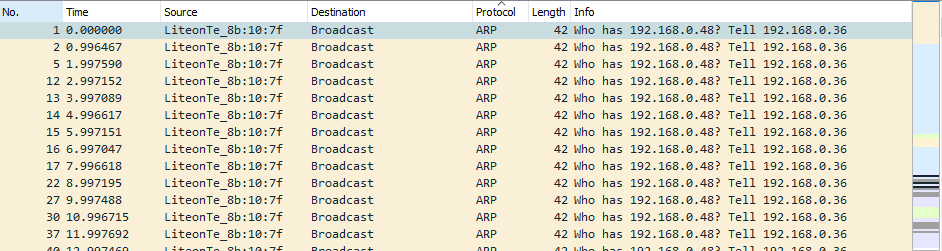
1. Jelaskan cara kerja nmap network scanning menggunakan *hping3* dan *nmap –sP/-sN* 
   1. *Hping3*

Dalam scanning menggunakan hping3 dapat menggunakan beberapa teknik dengan menggabungkan parameter yang ada pada aplikasi hping3, salah satunya adalah menggunakan XMAS scan dengan perintah *$hping3 –S <alamat IP yang ingin di scan> -p ++<port yang ingin di scan> -c <banyaknya iterasi port yang ingin di scan>.*

**

*Gambar 1.0, scan menggunakan hping3*

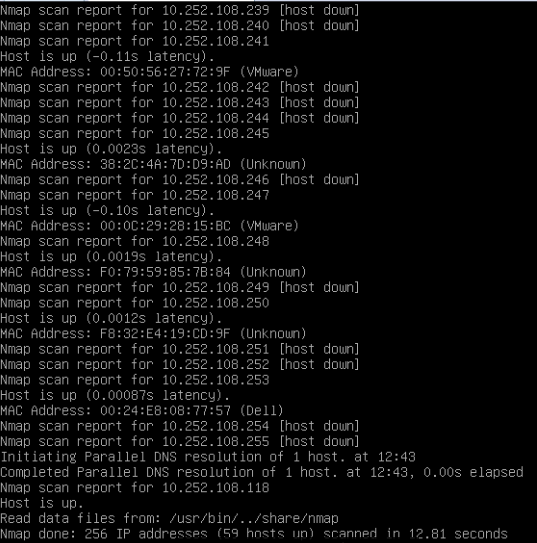
Penggunaan hping3 memanfaatkan koneksi TCP untuk melakukan scan terhadap portnya, dalam gambar 1.0, record dengan id=0 adalah port yang terbuka. Scanning juga dapat dilakukan jika tabel ARP sudah memiliki pemetaan IP di jaringan yang ada.



*Gambar 1.1, penggunaan ARP untuk scanning*

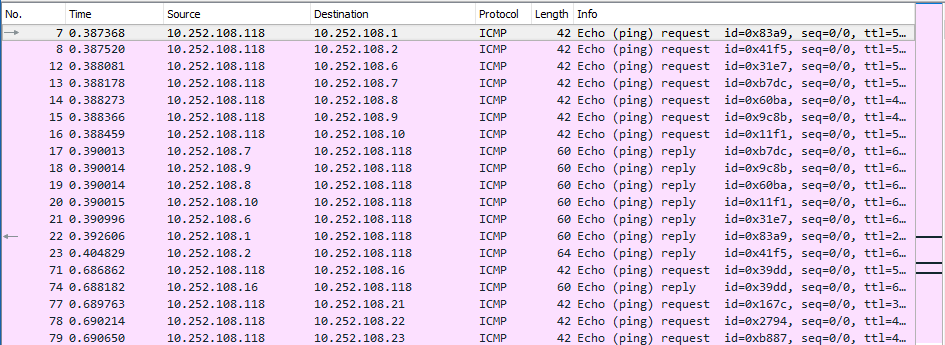
* 1. *Nmap –sP/-sN pada network 10.252.108.0/24 dan host jun*

Nmap scan menggunakan parameter –sP menghasilkan host mana saja yang up dan mana saja yang down, dengan cara mengirimkan ping pada host yang dispesifikan.



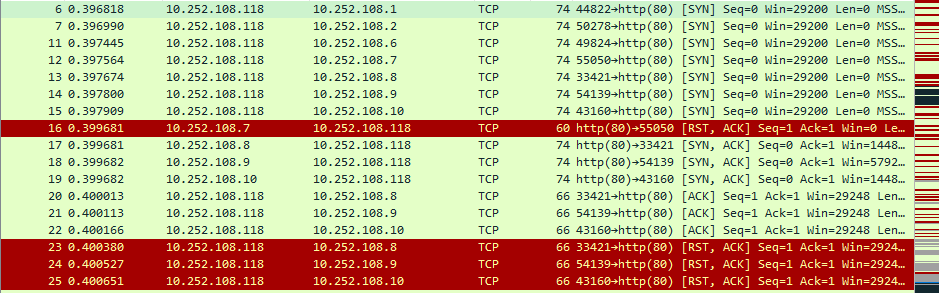
*Gambar 1.2 Scanning menggunakan nmap –sP*

Scan dengan teknik ini menggunakan ping ke masing masing host yang dispesifikan dan dianalisa jika ada reply/dapat melakukan ping ke host tersebut berarti host tersebut berstatus up



*Gambar 1.3 Scan menggunakan ICMP ping*

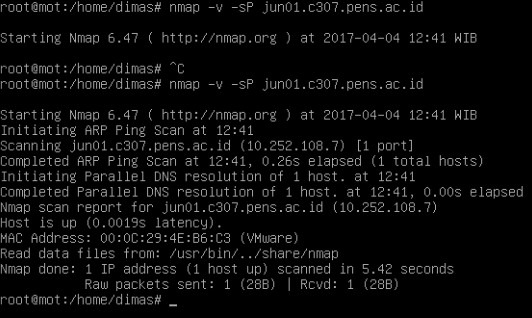
Pada scanning –sN yang dimanfaatkan adalah menggunakan packet TCP untuk scanning pada host yang sedang up.



*Gambar 1.4 scan menggunakan –sN TCP Null*

Scanning menggunakan –sN memanfaatkan pengiriman packet SYN untuk melakukan scanning terhadap host yang up.

Pada scanning dengan host, yaitu jun01.c307.pens.ac.id juga dilakukan scanning menggunakan parameter –sP



*Gambar 1.5 scan jun01 menggunakan –sP*

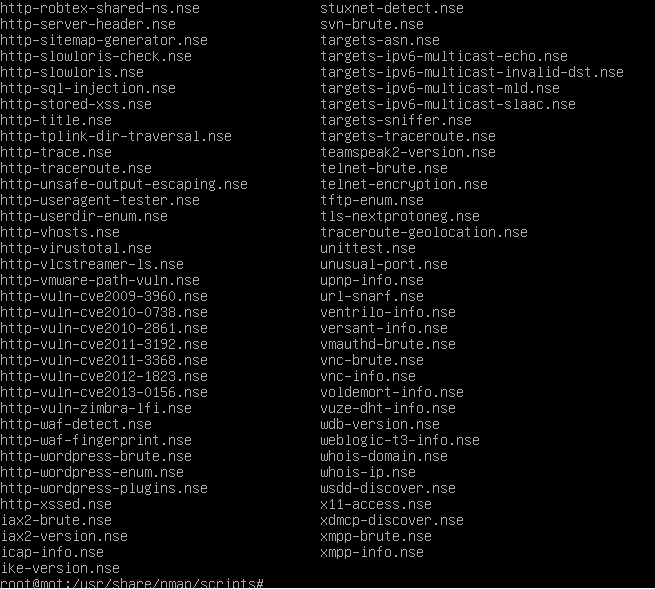
Pada scanning dengan host yang memiliki resolve name, akan dilakukan scan berupa –sP menggunakan ping. Jika host tersebut berada pada jaringan local, maka ARP scan akan digunakan.



*Gambar 1.6 scan jun01 menggunakan –sN*

1. Jelaskan penggunaan nmap script!
   1. Dimanakah letak nmap script

Letak nmap script adalah berada di */usr/share/nmap/scripts*



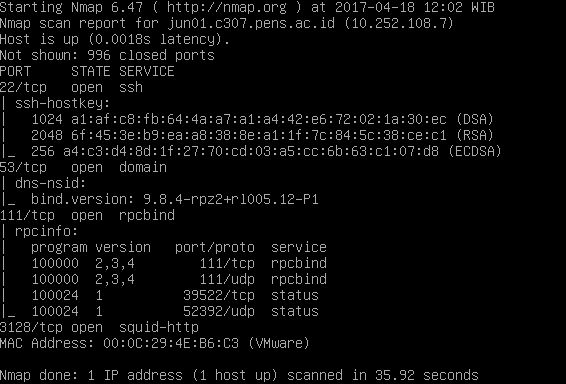
*Gambar 2.0 nmap script*

* 1. Ada berapa kategori yang ada pada nmap script

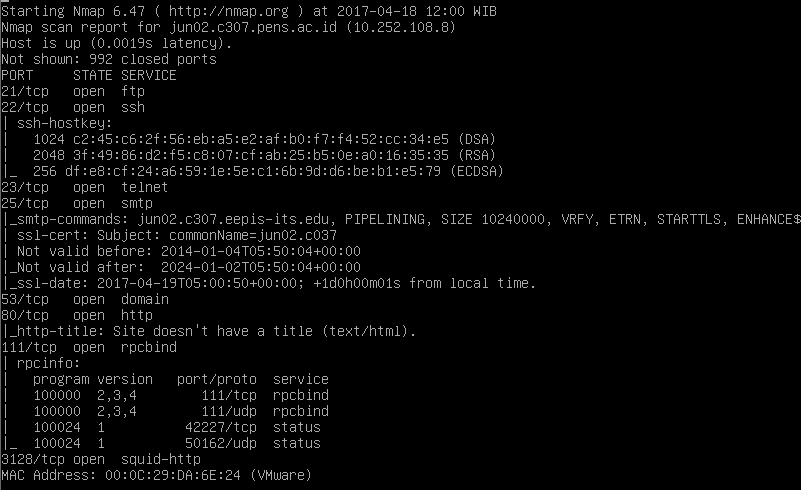
Terdapat 14 kategori script nmap, antara lain adalah

* + - Auth, script yang berjalan pada lingkup autentikasi
    - Broadcast, script yang menemukan host yang aktif dengan melakukan broadcast pada local network
    - Brute, script yang melakukan brute force pada credential di remote service
    - Default, script yang secara otomatis akan menjalankan nmap dengan opsi –sC atau -A
    - Discovery, script yang berfungsi untuk mencoba mendapatkan informasi terhadap network target
    - Dos, script yang memungkinkan aplikasi target crash sehingga menyebabkan denial of service terhapda service tersebut
    - Exploit, script yang melakukan eksploit pada system target
    - External, script yang mengirimkan data ke program ppihak ketiga lewat jaringan target
    - Fuzzer
    - Intrusive, script yang mengirim random data yang invalid untuk menemukan bugs pada sistem target
    - Malware, script yang melakukan test apakah target terinfeksi malware maupun backdoor
    - Safe, script yang dapa dijalankan secara ‘aman’ sehingga tidak akan menyebabkan crash pada aserver
    - Version, script yang digunakan untuk mengetahui versi dari aplikasi yang berjalan pada target
    - Vuln, script yang dapat melakukan cek apakah target rentan terhadap serangan
  1. Lakukan scanning menggunakan nmap –script

Pada scanning host *jun01.c307.pens.ac.id* menggunakan script terlihat apa saja port yang terbuka dan service apa saja yang terbuka pada host tersebut

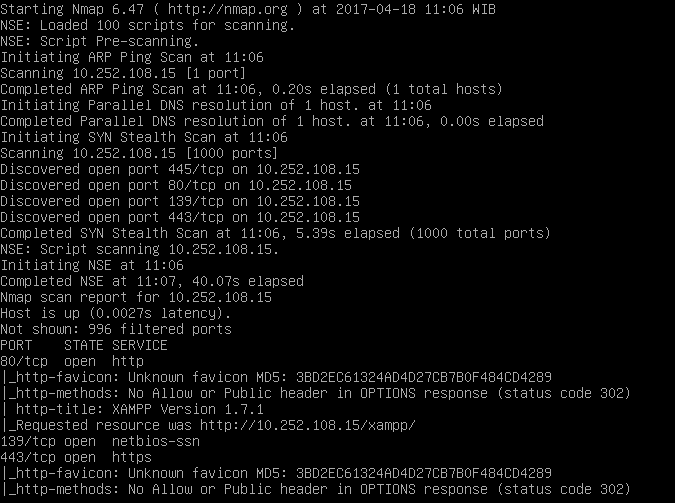


*Gambar 2.1 scan menggunakan nmap script pada jun01.c307.pens.ac.id*

**

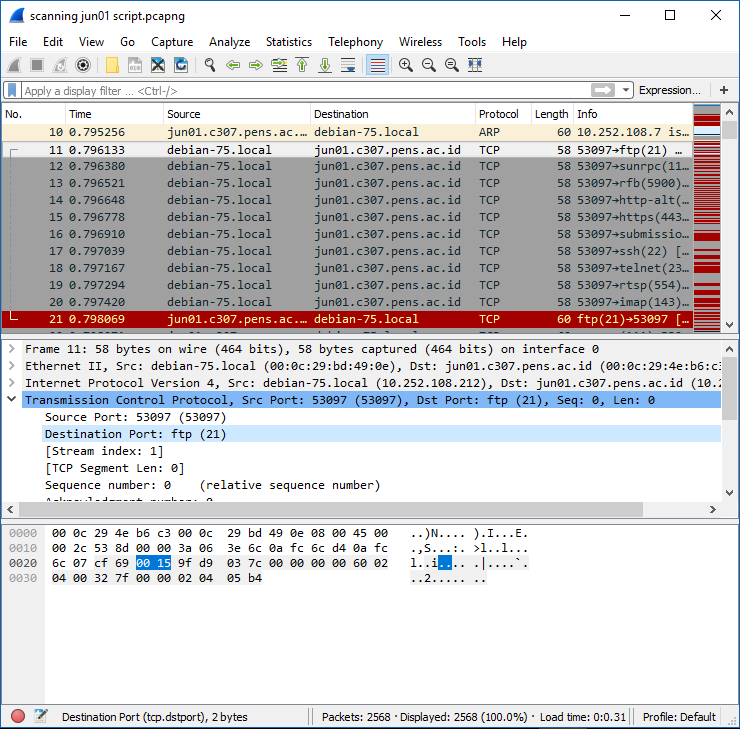
*Gambar 2.2 scan menggunakan nmap script pada jun02.c307.pens.ac.id*

Pada scan menggunakan default script nmap pada IP 10.252.108.15 juga dilakukan dengan hasil port yang terbuka adalah 80, 139, 443, dan 445. Script akan mencoba melakukan scan terhadap informasi per port yang up dan melaporkannya ke penyerang



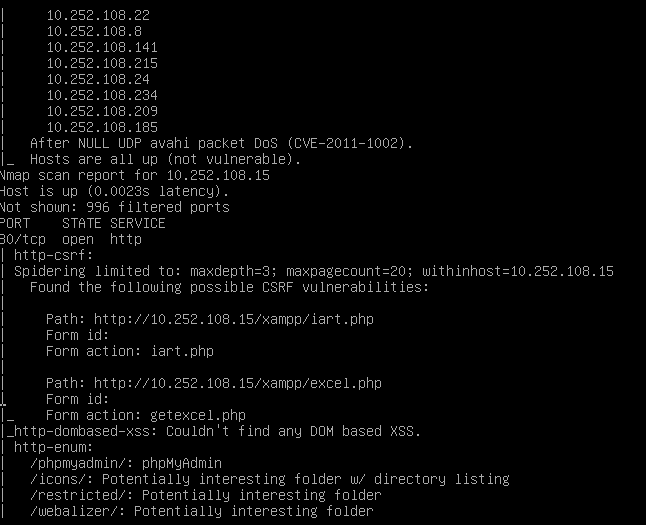
*Gambar 2.3 scan menggunakan script nmap*

Cara kerja scan dengan script nmap ini adalah degan memanfaatkan script yang sebelumnya memang sudah disediakan pada nmap. Script bekerja sejara batch dan menggunakan protocol TCP untuk mendapatkan informasi masing-masing port yang ada

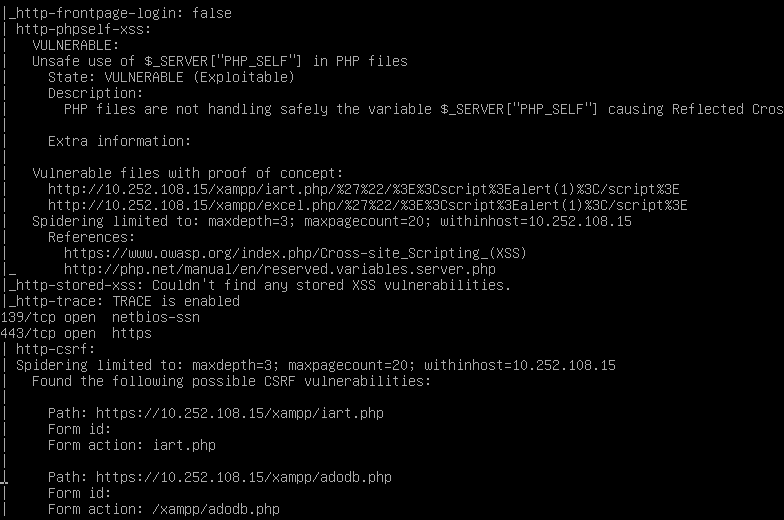


*Gambar 2.4 salah satu koneksi tcp untuk melakukan scan terahadap port 21 (ftp)*

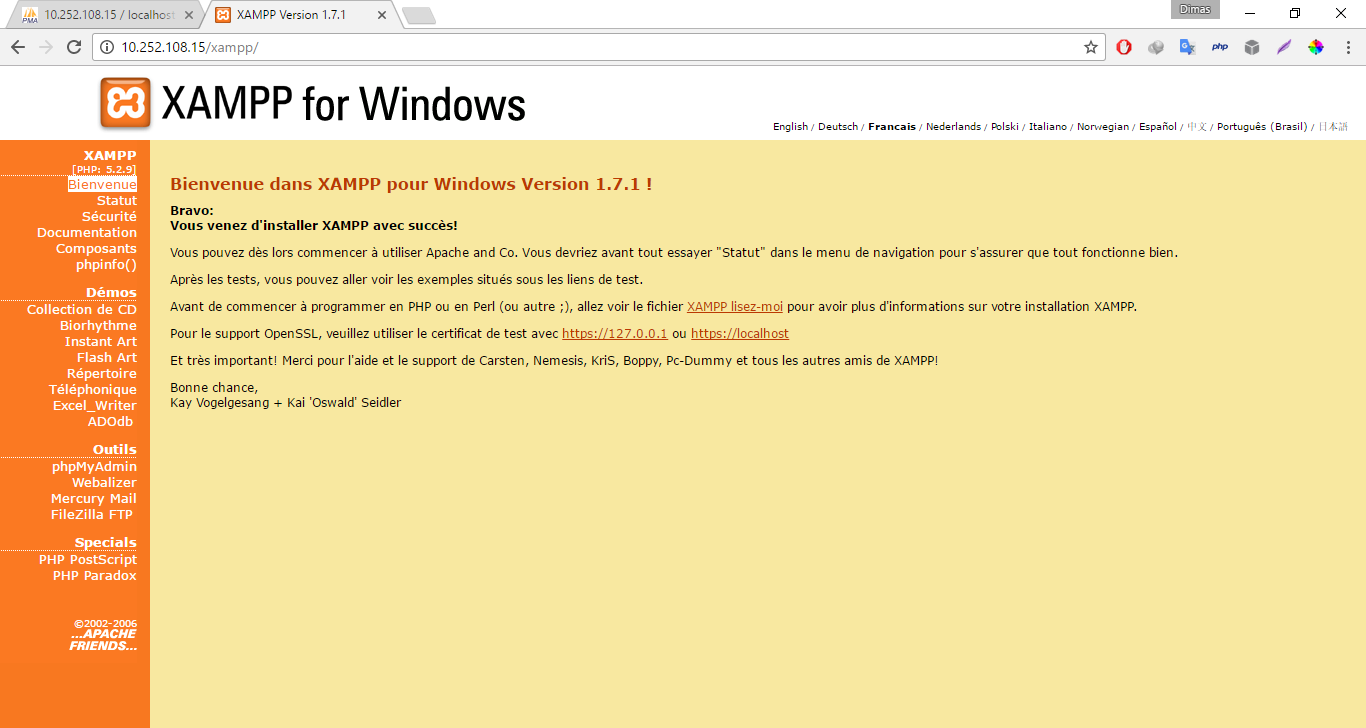
Selain melakukan scan menggunakan script, jug dapat dilakukan scan vulnerable pad aport yang terbuka pada host yang di scan menggunakan vulnerability scan pada nmap. Scan ini akan menghasilkan vulnerability terhadap port yang terbuka berdasarkan versi dan referensi ke daftar vulnerability yang ada

**

*Gambar 2.5 Vulnerability scan menggunakan nmap pada 10.252.108.15 (1)*

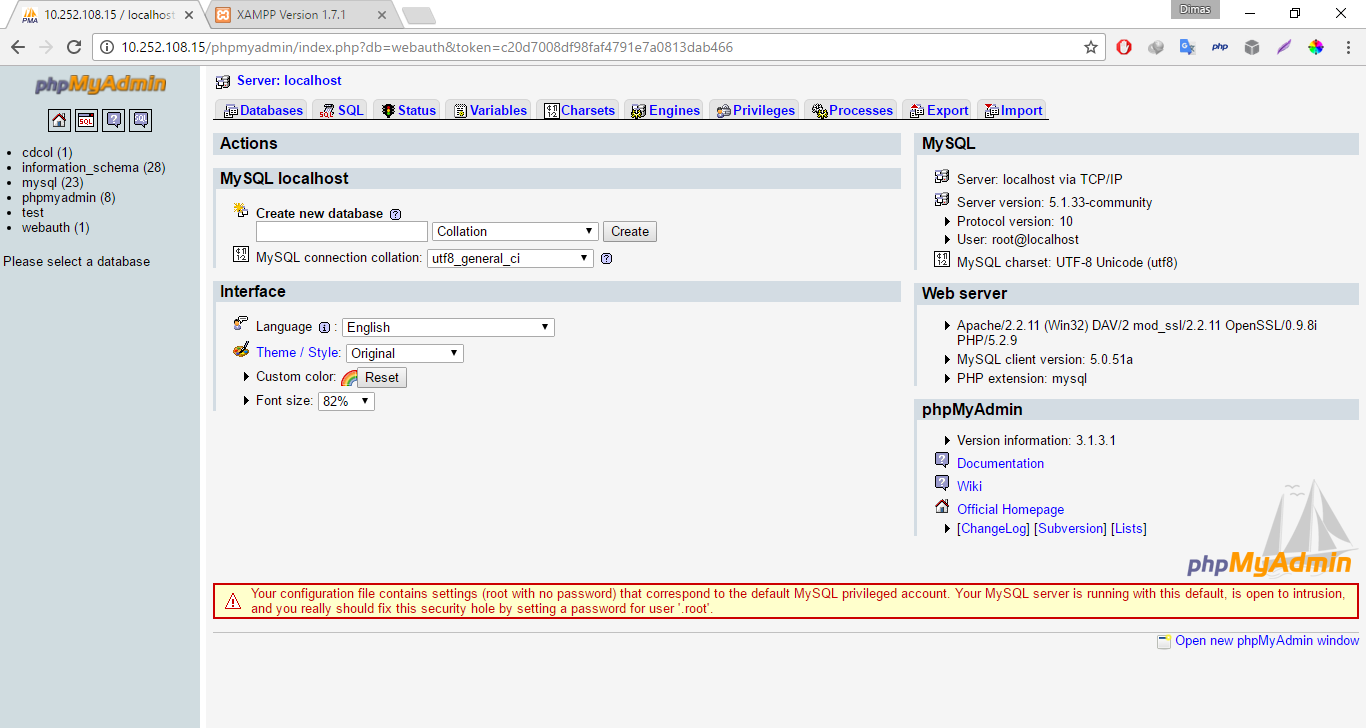
*Gambar 2.6 Vulnerability scan pada 10.252.108.15 (2)*

Vulnerability scan mengekspos seluruh celah keamanan pada semua port yang terbuka pada host yang di scan. Dalam hal ini komputer 10.252.108.15 memiliki celah keamanan pada port 80, 139 dan 443 serta samba 445. Dengan informasi ini, penyerang dapat melakukan serangan, contohnya adalah dengan mengakses web server XAMPP yang portnya terbuka,



*Gambar 2.7 halaman web server pada 10.252.108.15 dapat dibuka*

Celah keamanan lainnya adalah dapat diaksesnya halaman phpmyadmin yang merupakan panel yang mengatur database mysql pada webserver XAMPP

**

*Gambar 2.8 phpmyadmin dapat diakses tanpa menggunakan password*

**Analisa**

* *Selain digunakan untuk melakukan scanning port pada jaringan, aplikasi nmap juga dapat dilakukan untuk melakukan langkah langkah eksploitasi jaringan lainnya seperti briteforce, dos, exploit dan mencari celah keamanan pada sebuah protocol*
* *Tipe scanning nmap bermacam-macam dengan tujuan yang berbeda-beda untuk masing masing tipe scanningnya.*
* *Untuk melakukan scanning port nmap memanfaatkan ICMP ping, ARP, dan TCP connection.*
* *Melakukan port scanning ke jaringan publik dapat dikatakan ilegal, karena informasi yang didapat dirasa dapat merusak sistem yang di target.*
* *Referensi yang dihasilkan dari vulnerability scan berasal dari komunitas yang secara berkala mencari celah celah keamanan terhadap port yang terbuka*
* *Karena resiko keamanan yang sangat tinggi, disarankan kepada pengguna untuk tidak terlalu banyak menggunakan/membuka port suatu layanan.*
* *Nmap memiliki 14 kategori script dengan total pre-defined script berjumlah 437 script.*