TUGAS KEAMANAN JARINGAN KOMPUTER

TAHAP SCANNING

DISUSUN OLEH:

NAMA : Fahrul Rozi

NIM : 09011181320022

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

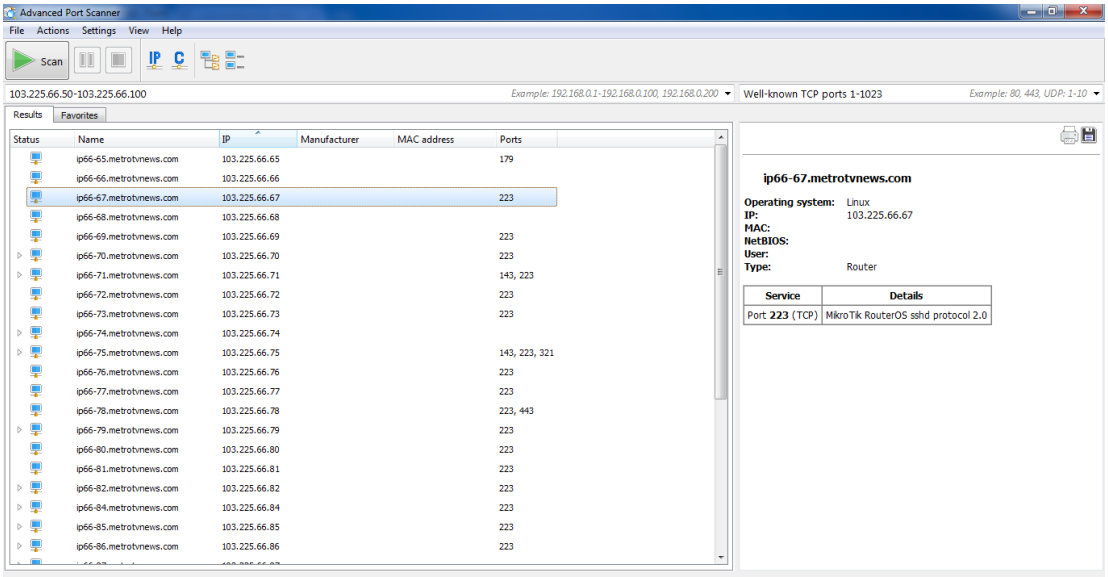
Tahap scanning

Sebelumnya telah dilakukan tahap reconnaissance yaitu mendapatkan / mengumpulkan data informasi sebanyak-banyaknya dari target . target pada tahap ini sama seperti tahap sebelumnya yaitu MetroTV. Pada tahap ini penulis melakukan scanning pada target yang bertujuan untuk mencari apakah ada kelemahan pada sistemnya.

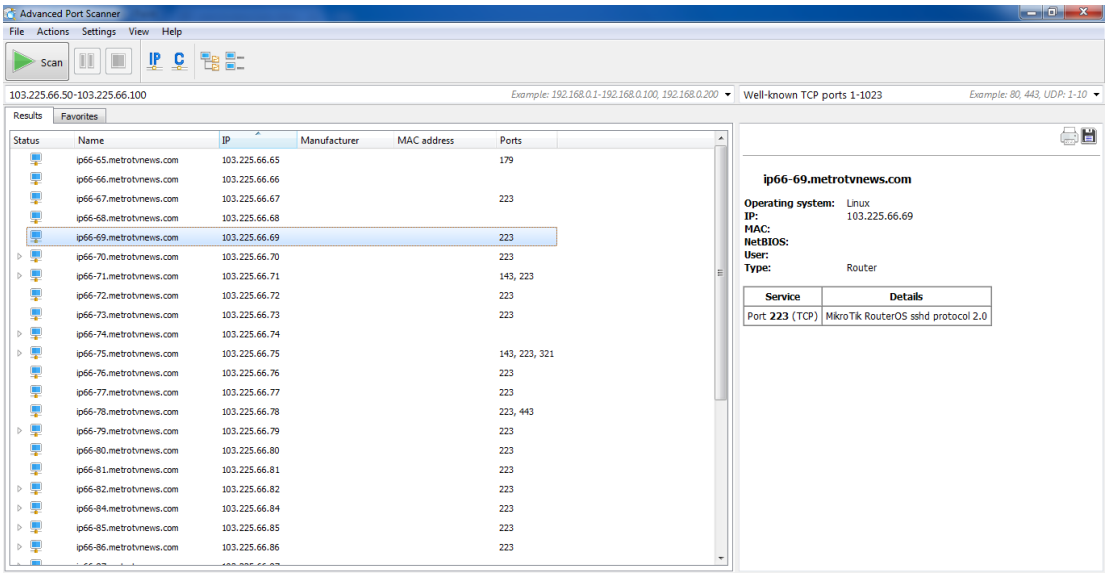
Scanning dapat dilakukan dengan menggunakan tools scanner , kemudian dari hasil scanning maka akan didapat CVE (Common Vulnerabilities and Exposure). Selain menggunakan tool NMAP dapat juga digunakan tools sebagai berikut:

1. Advanced port scanner

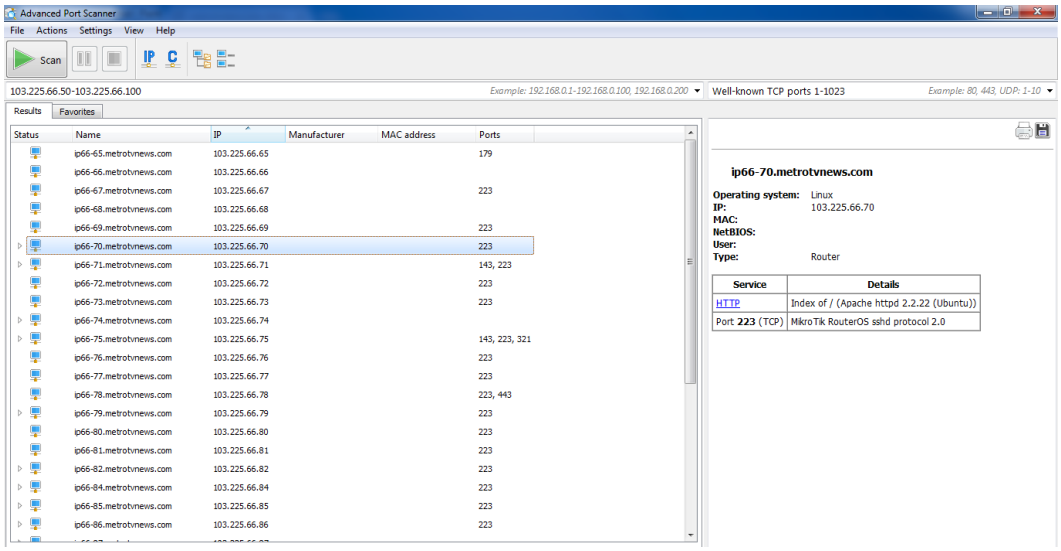
   Sebelumnya telah diketahui ip target metroTV yaitu 103.225.66.90. Pada tools ini melakukan scanning port dengan memasukan ip dengan range tertentu , disini penulis memasukan range ip 103.225.66.50 - ip 103.225.66.100. maka dapat diketahui ip yang aktif , port ,os, dan service yang digunakan.



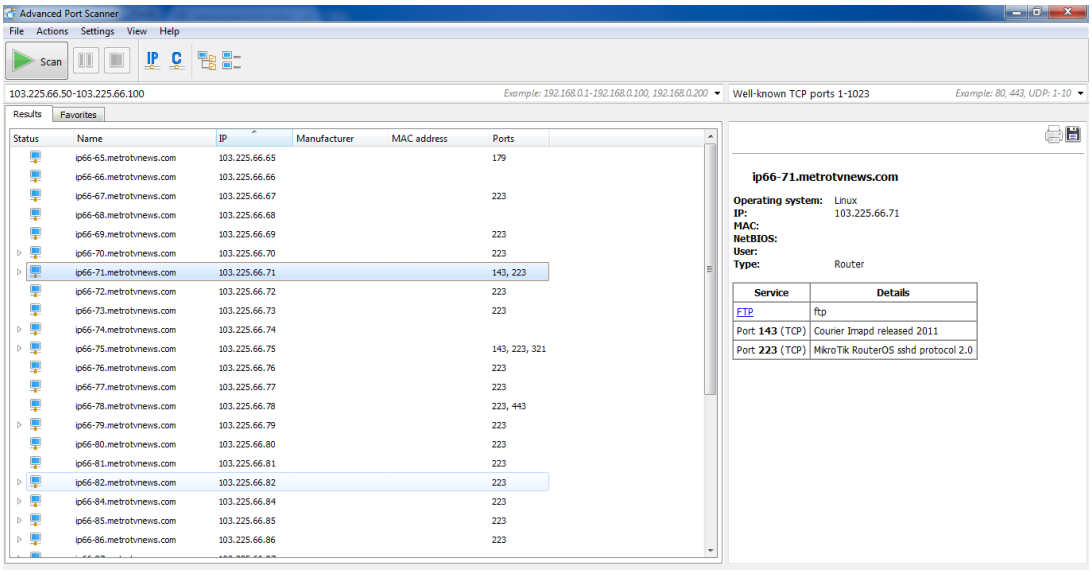
Gambar 1.1



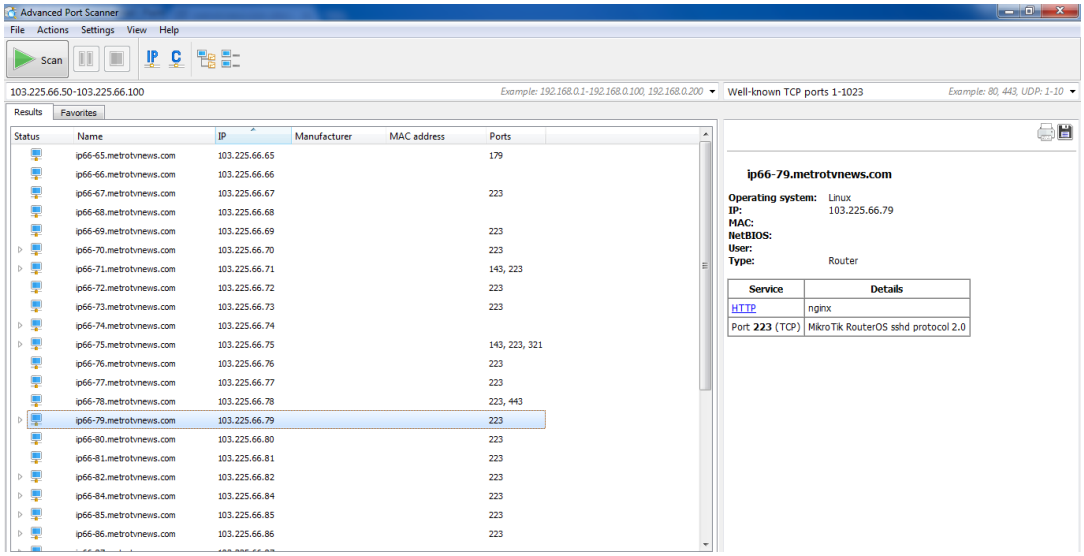
Gambar 1.2



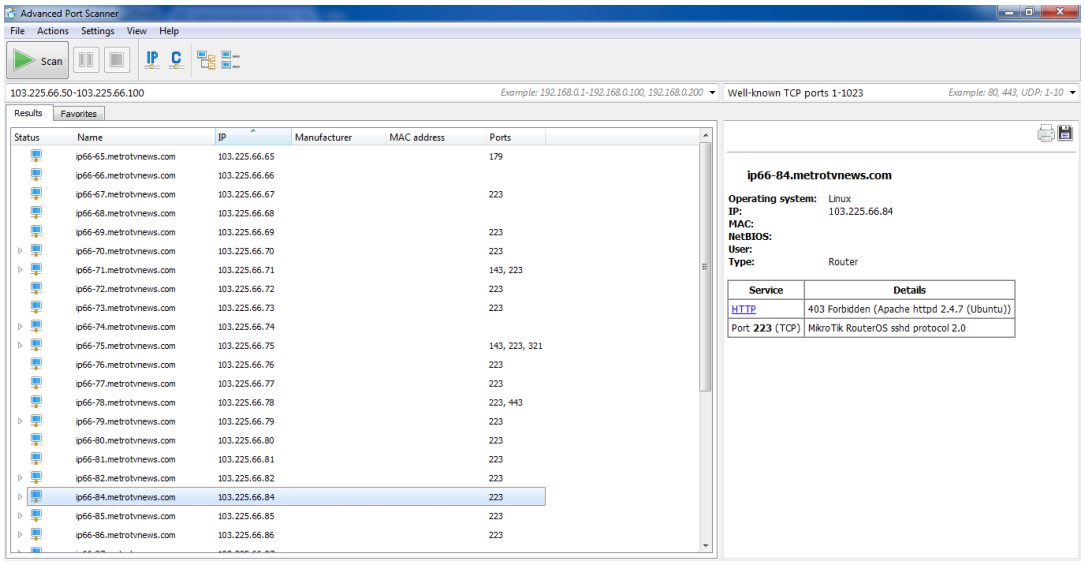
Gambar 1.3



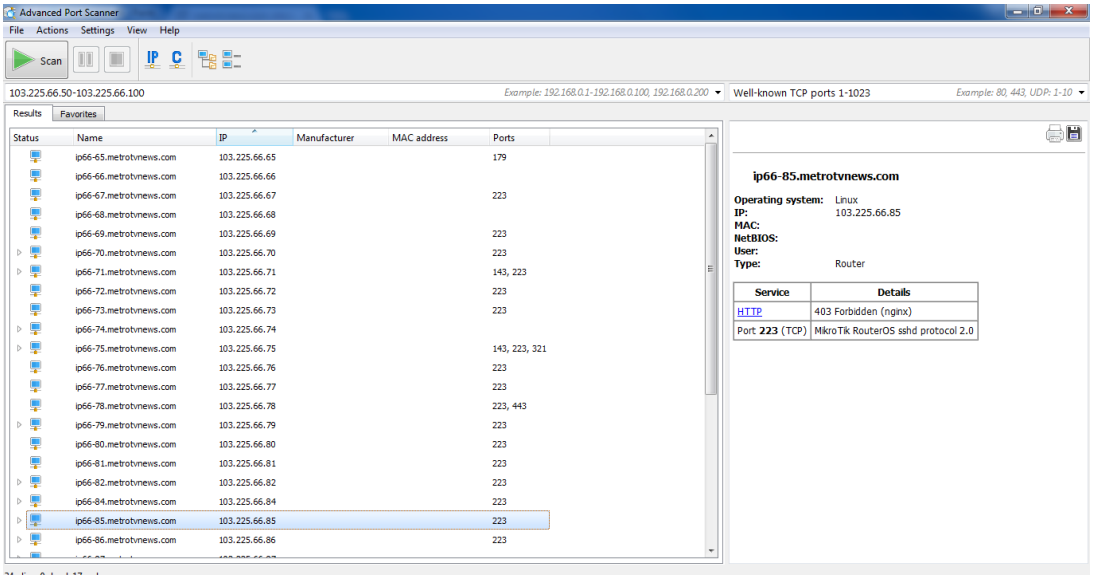
Gambar 1.4



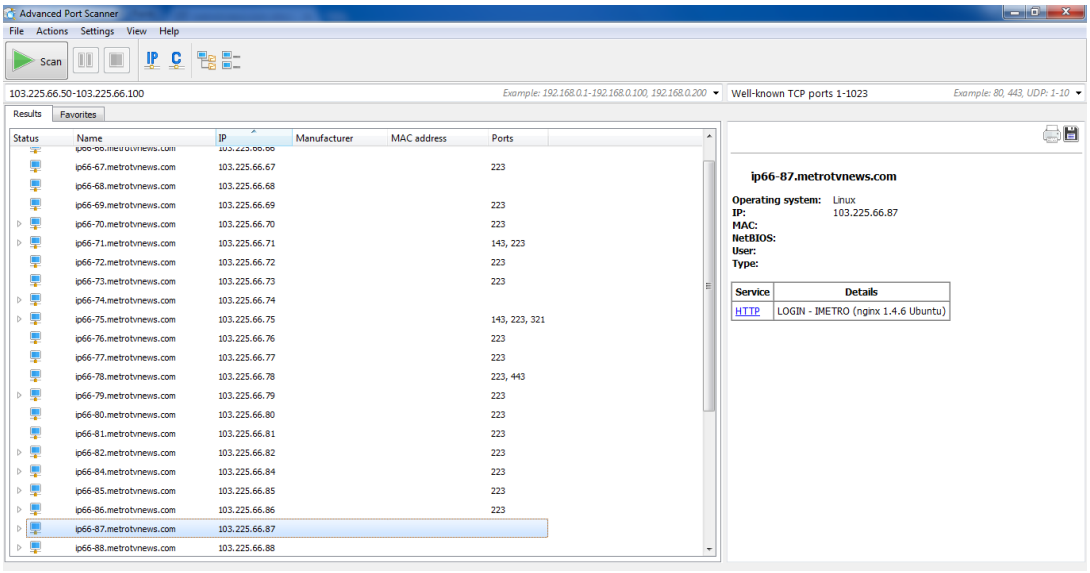
Gambar 1.5



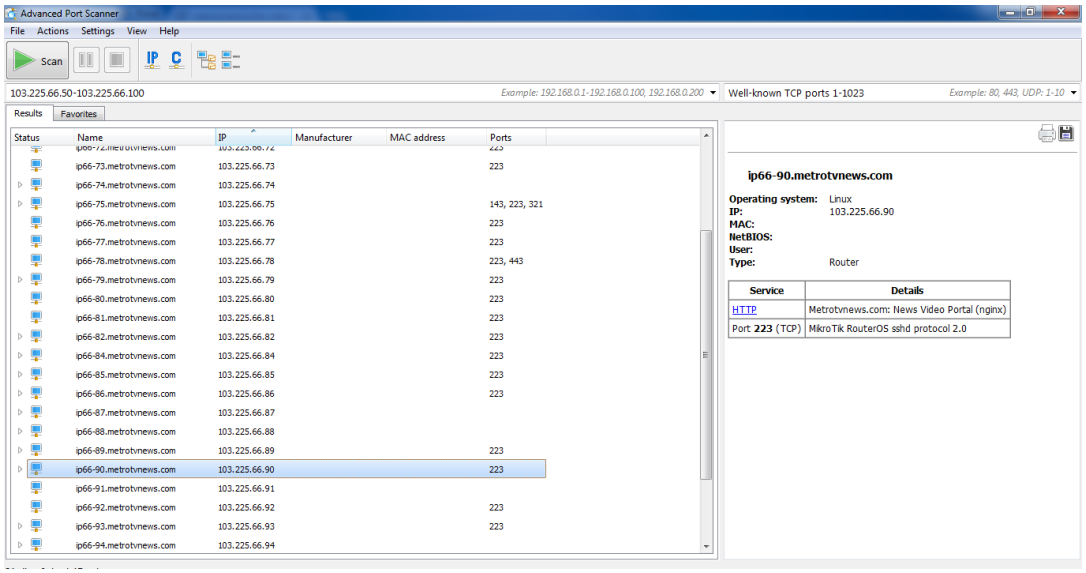
Gambar 1.6



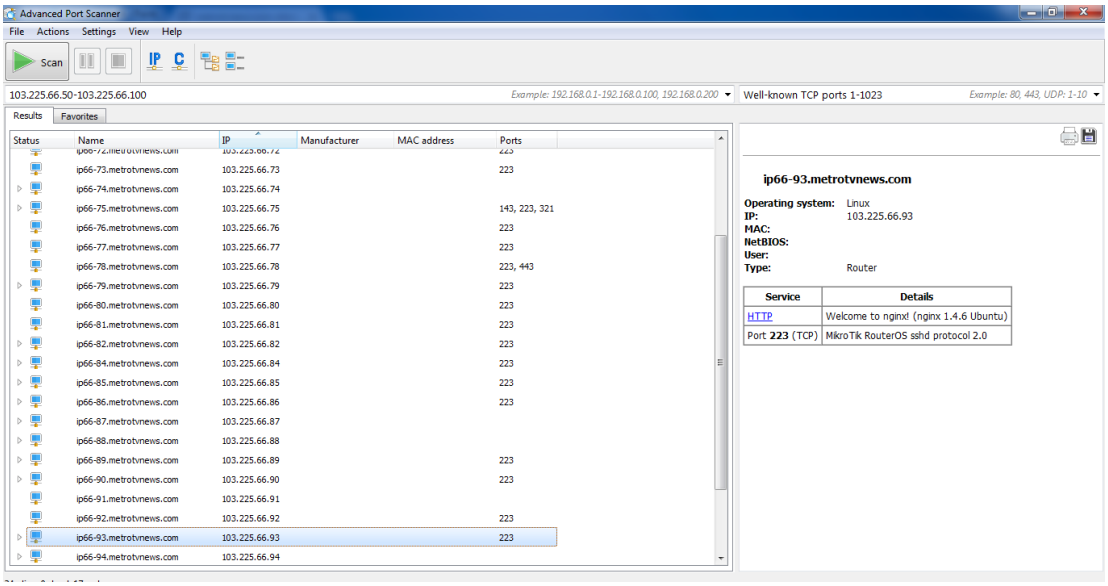
Gambar 1.7



Gambar 1.8



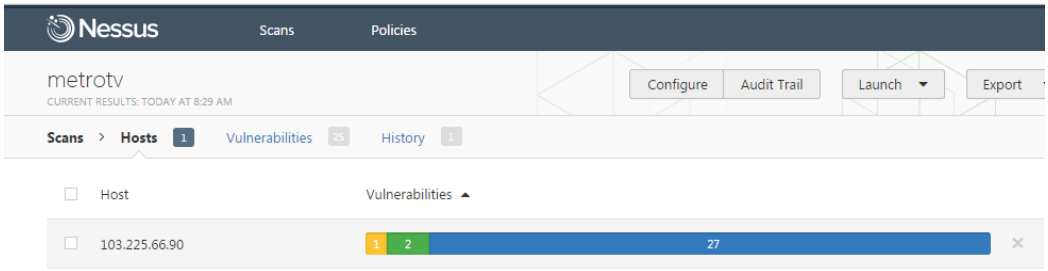
Gambar 1.9

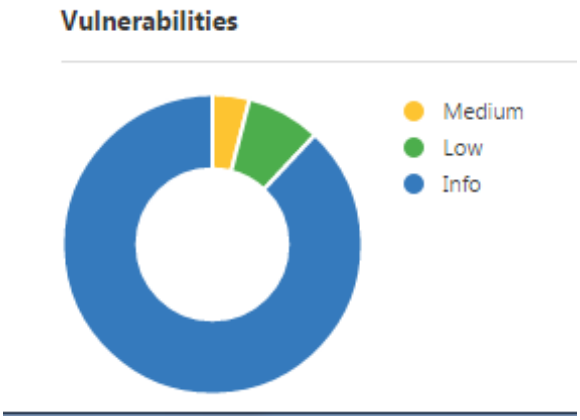


Gambar 1.10

2. Nessus

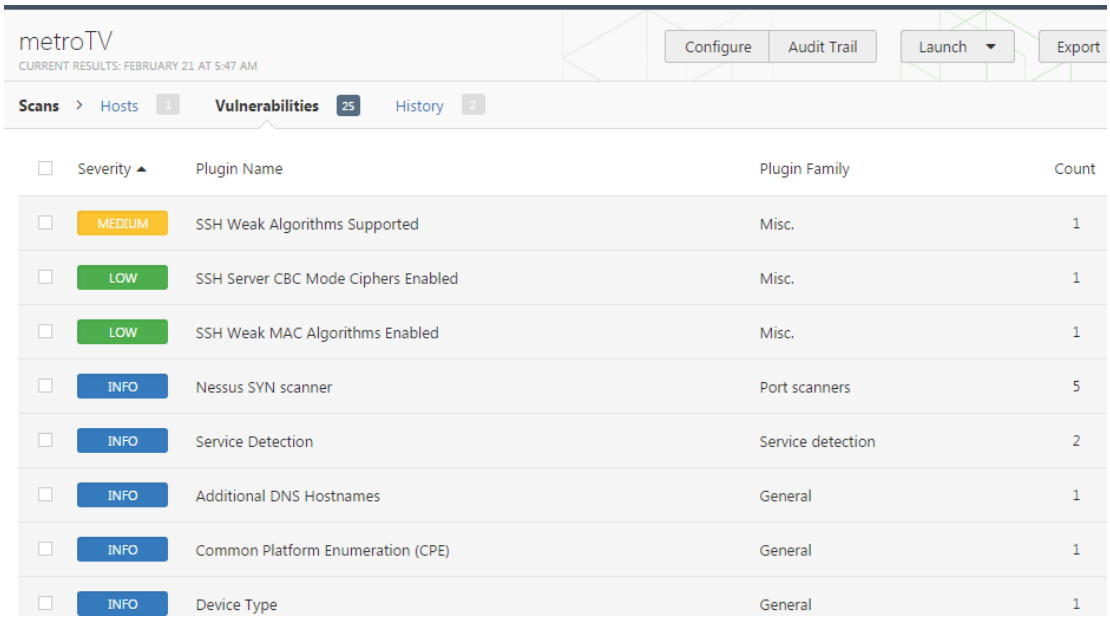
Dengan menggunakan tools ini maka akan mendapatkan informasi adanya kelemahan (vulnerabilities) yang terdapat pada sistem target.





Gambar 2.1 : nilai vulnerabilities

Pada gambar 2.1 dengan menggunakan tool Nessus dapat mengetahui nilai vulnerabilities yaitu terdapat 1 (3.4%) medium, 2 (6.6%) low ,dan 27 (90%) info. Pada vulnerabilities terdapat bagian medium dan low yang menunjukan tingkat resiko information kemungkinan menjadi celah untuk penyerangan. Dapat dilihat pada gambar 2.2.



Gambar 2.2 :vulnerabilities

Dari gambar diatas maka dilihat dan dijelaskan bagian-bagian dari vulenerabilities tersebut:

1. Medium (ssh weak algorithms supported)

Di bagian tingkat medium terdapat pada server ssh yang lemah . nessus telah mendateksi bahwa server SSH remote di konfigurasi untuk menggunakan arcfour stream chipper atau tidak chipper sama sekali . RFC 4253 menyarankan untuk tidak menggunakan arcfour karena terdapat masalah pada lemahnya kunci. Adapun solusi yang dapat diberikan yaitu Hubungi vendor atau berkonsultasi dokumentasi produk untuk menghapus cipher yang lemah.

Output

```
The following weak server-to-client encryption algorithms are supported :
  none
The following weak client-to-server encryption algorithms are supported :
  none
```

Port	Hosts
223 / tcp / ssh	103.225.66.90

2. Low (ssh server CBC mode ciphers enabled)

Pada tingkat low terdapat server ssh , server ini di konfigurasi untuk mendukung enkripsi chipher block chaining (cbc). Hal ini memungkinkan seorang penyearang (attacker) untuk memperoleh pesan plaintext dari chipertext. Adapun solusinya yaitu hubungi vendor atau konsul produk dokumentasi untuk menonaktifkan CBC mode cipher enkripsi, dan aktifkan CTR atau GCM cipher mode enkripsi.

Output

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
```

Port	Hosts
223 / tcp / ssh	103.225.66.90

3. Low (ssh weak mac algorithm enabled)

Server SSH remote dikonfigurasi untuk memungkinkan baik MD5 atau 96-bit MAC algoritma, yang keduanya dianggap lemah. Perhatikan bahwa plugin ini hanya memeriksa opsi dari server SSH, dan tidak memeriksa versi software rentan. Dan solusi dari masalah ini yaitu Hubungi vendor atau berkonsultasi dokumentasi produk untuk menonaktifkan MD5 dan 96-bit MAC algoritma..

Output

```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5

The following server-to-client Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
```

Port	Hosts
223 / tcp / ssh	103.225.66.90