Keamanan Jaringan Komputer

Scanning dan CVE

Disusun Oleh

Nama: Orlando Dacosta

NIM: 09121001029

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

INDRALAYA

TAHUN AJARAN 2016/2017

Scanning dan CVE

Target: www.kemenperin.go.id

IP Address: 202.47.80.118

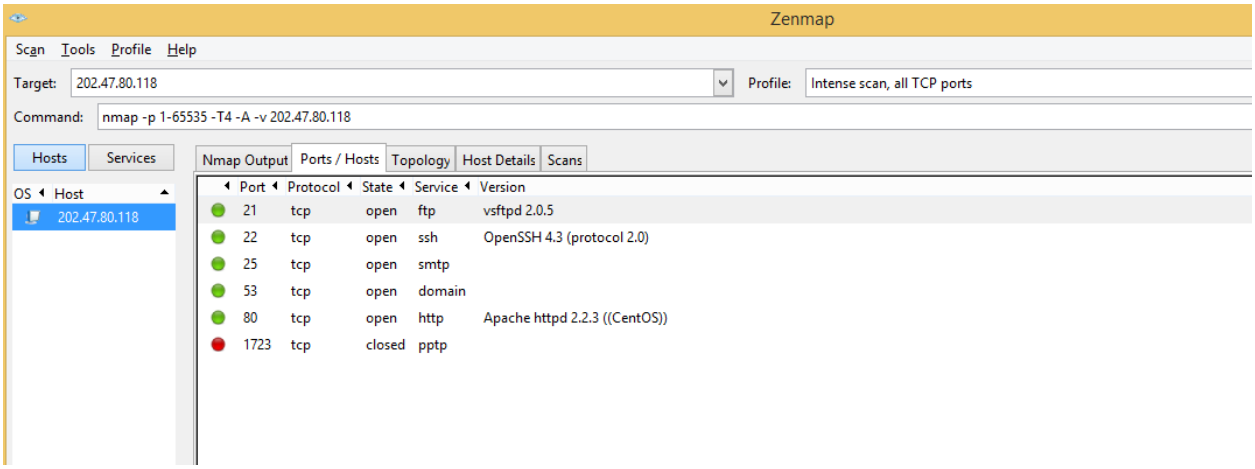
Tools yang digunakan: 1. Zenmap

2. Nessus

3. Nmapsi4

1. Scanning pada Zenmap

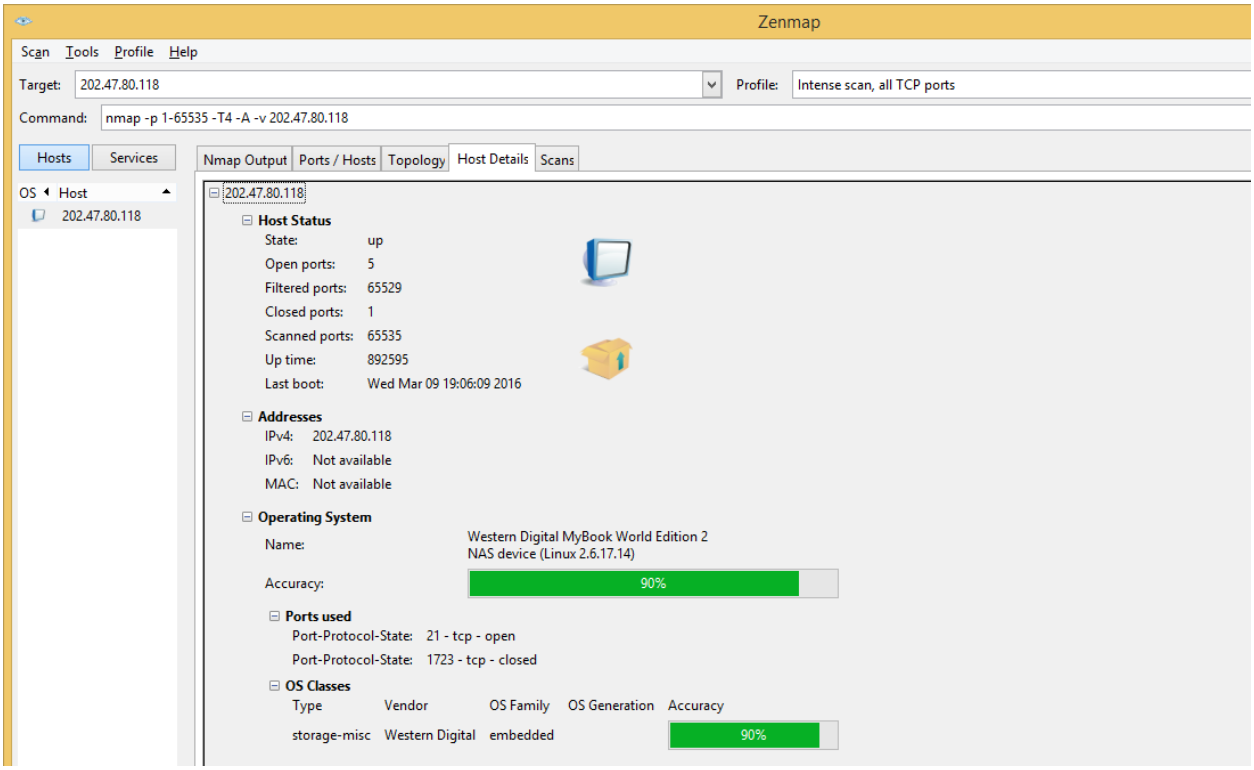
Scanning Ports



Analisa:

Scanning menggunakan zenmap dengan target ip 202.47.80.118 ada 6 port yang didapatkan yaitu 5 port open dan 1 port closed. Port open terdiri dari port 21 dengan service ftp versi vsftpd 2.0.5, port 22 dengan service ssh versi OpenSSH 4.3(protocol 2.0), port 25 dengan service smtp, port 53 dengan service domain, dan port 80 dengan service http versi Apache httpd 2.2.3 ((CentOS)). Sedangkan port closed adalah port 1723 dengan service pptp.

Daemon

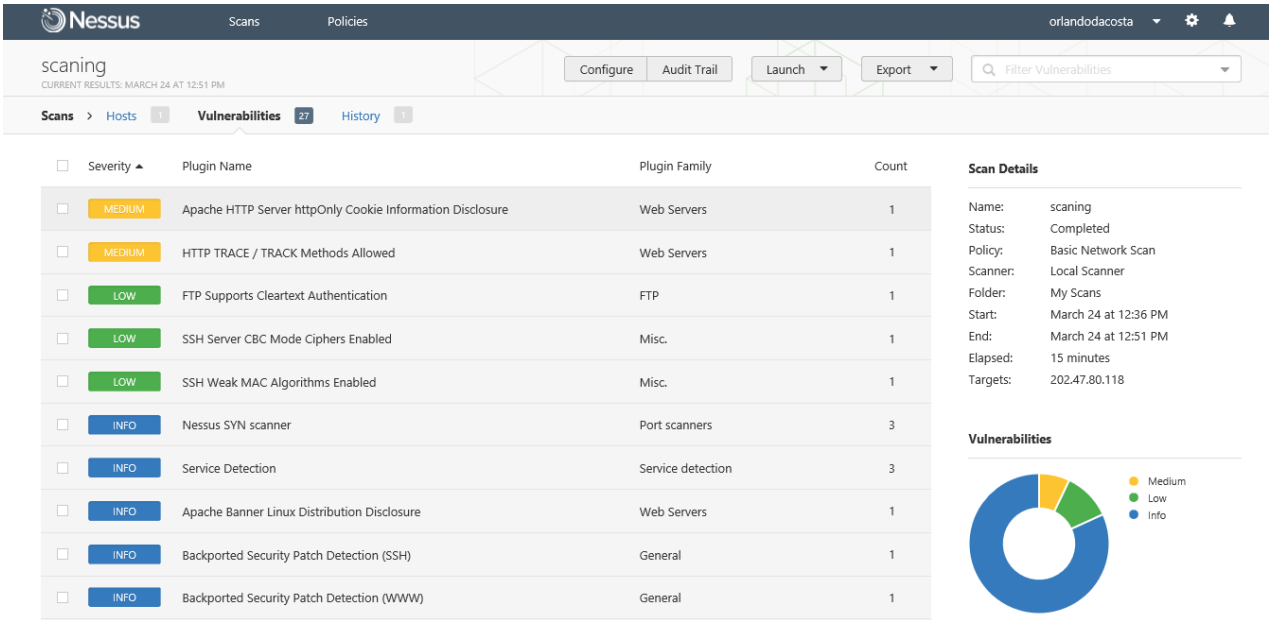


Analisa:

Dari informasi yang di dapatkan oleh Zenmap bahwa target menggunakan OS Western Digital MyBook World Edition 2 NAS device (Linux 2.6.17.14). Type Storage yang digunakan adalah Western Digital.

2. Scanning menggunakan Nessus

Gambar 2.1 Hasil Scanning menggunakan Nessus



INFO	Backported Security Patch Detection (WWW)	General	1
INFO	Common Platform Enumeration (CPE)	General	1
INFO	Device Type	General	1
INFO	FTP Server Detection	Service detection	1
INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO	HTTP Server Type and Version	Web Servers	1
INFO	HyperText Transfer Protocol (HTTP) Information	Web Servers	1
INFO	Inconsistent Hostname and IP Address	Settings	1
INFO	Nessus Scan Information	Settings	1
INFO	OS Identification	General	1
INFO	Patch Report	General	1
INFO	Reverse NAT/Intercepting Proxy Detection	Firewalls	1
INFO	SSH Algorithms and Languages Supported	Misc.	1
INFO	SSH Protocol Versions Supported	General	1
INFO	SSH Server Type and Version Information	Service detection	1
INFO	TCP/IP Timestamps Supported	General	1
INFO	Traceroute Information	General	1
INFO	vsftpd Detection	FTP	1

Gambar 2.2 Vulnerabilities

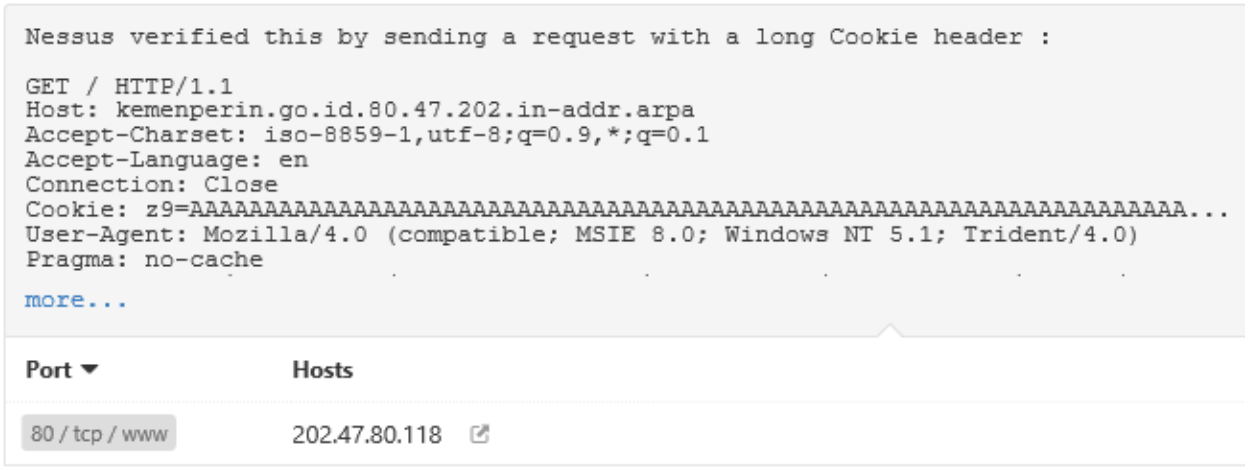
Dilihat pada gambar 2.1 hasil scanning Nessus pada target mendapatkan vulnerabilities sebanyak 2 (6,5%) medium, 3 (9,7%) low dan 26 (83,9%) info. Dari vulnerabilities yang di dapat masing-masing mempunyai risk information dan solusi. Pada bagian low dan medium sendiri menunjukan tingkat risk information yang kemungkinan dapat menjadi celah serangan. Bagian tersebut adalah web server,ftp dan misc. Adapun Risk information tersebut:

1. MEDIUM (Apache HTTP Server httpOnly Cookie Information Disclosure)

   Deskripsi: Versi Apache HTTP Server yang running pada host remote dipengaruhi oleh kerentanan keterbukaan informasi. Mengirimkan request dengan header HTTP cukup lama untuk melebihi batas Server menyebabkan web server merespon HTTP 400. Secara default, mengganggu HTTP header dan nilai yang ditampilkan adalah 400 error page. Ketika digunakan bersama dengan serangan lainnya (misalnya, cross-site scripting), ini bisa membahayakan dari HttpOnly cookie.

   Solusi: Upgrade ke Apache versi 2.0.65 / 2.2.22 atau yang lebih baru.

   Output:

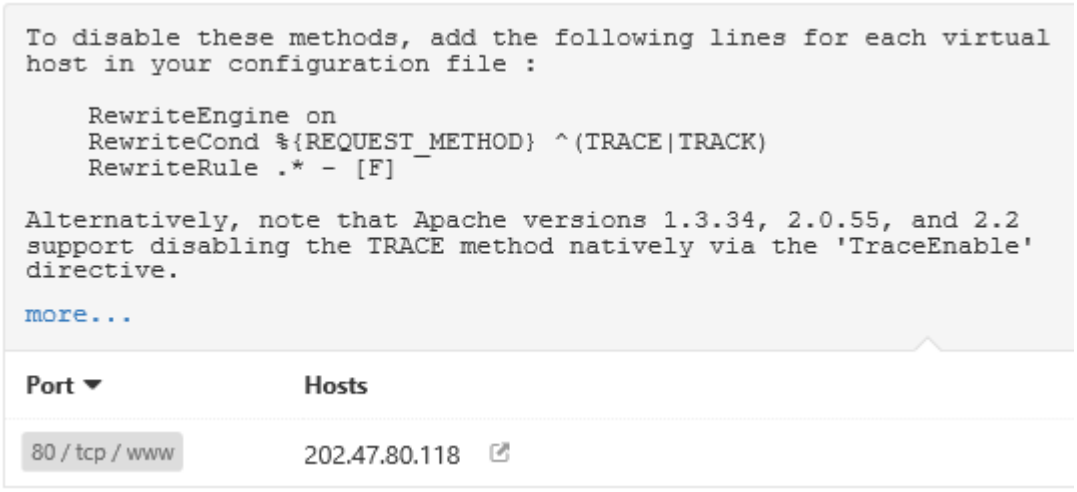


2. MEDIUM (HTTP TRACE / TRACK Methods Allowed**)**

   Deskripsi: Remote web server mendukung metode TRACE dan TRACK. TRACE dan TRACK adalah metode HTTP digunakan men debug koneksi web server.

   Solusi: Menon-aktifkan metode ini. Lihat plugin output untuk informasi lebih lanjut

Output:

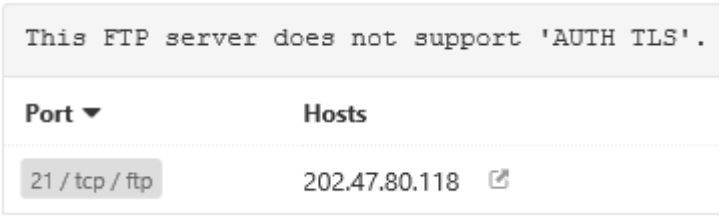


3. LOW (FTP Supports Cleartext Authentication)

   Deskripsi: Remote FTP server mengizinkan nama pengguna dan kata sandi untuk ditransmisikan dalam cleartext, yang dapat disadap oleh pelacak jaringan atau serangan man-in-the-middle.

   Solusi: Pindah ke SFTP (bagian dari SSH suite) atau FTPS (FTP over SSL / TLS). Dalam kasus terakhir, mengkonfigurasi server sehingga koneksi kontrol dienkripsi.

   Output:



4. LOW (SSH Server CBC Mode Ciphers Enabled)

   Deskripsi: Server SSH dikonfigurasi untuk mendukung Cipher Block Chaining (CBC) enkripsi. Hal ini dapat memungkinkan seorang penyerang untuk memulihkan pesan plaintext dari ciphertext. Perhatikan bahwa plugin ini hanya memeriksa opsi dari server SSH dan tidak memeriksa untuk kerentanan versi software.

   Solusi: 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
  cast128-cbc
  rijndael-cbc@lysator.liu.se
more...
```

Port	Hosts
22 / tcp / ssh	202.47.80.118

5. LOW (SSH Weak MAC Algorithms Enabled**)**

   Deskripsi: Server SSH dikonfigurasi allow MD5 atau algoritma 96-bit MAC, yang keduanya dianggap lemah. Perhatikan bahwa plugin ini hanya memeriksa opsi dari server SSH dan tidak memeriksa kerentanan versi software.

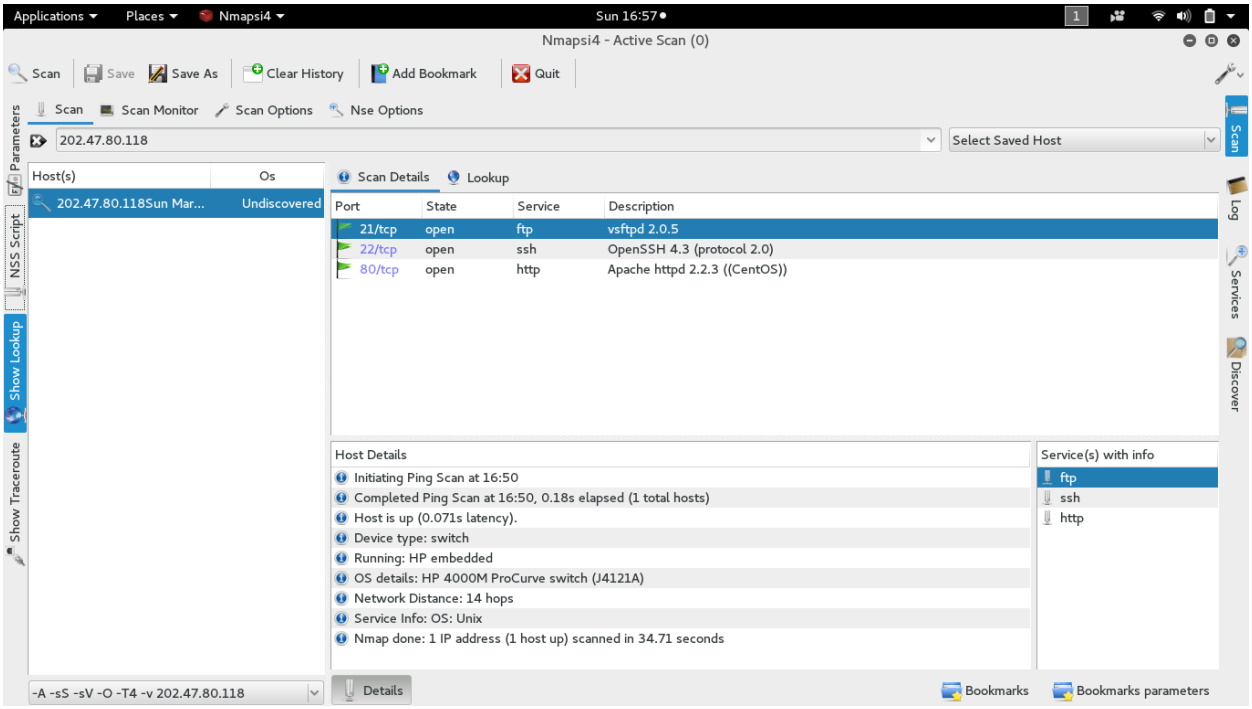
   Solusi: Hubungi vendor atau konsul produk dokumentasi untuk menonaktifkan MD5 dan algoritma 96-bit MAC.

   Output:

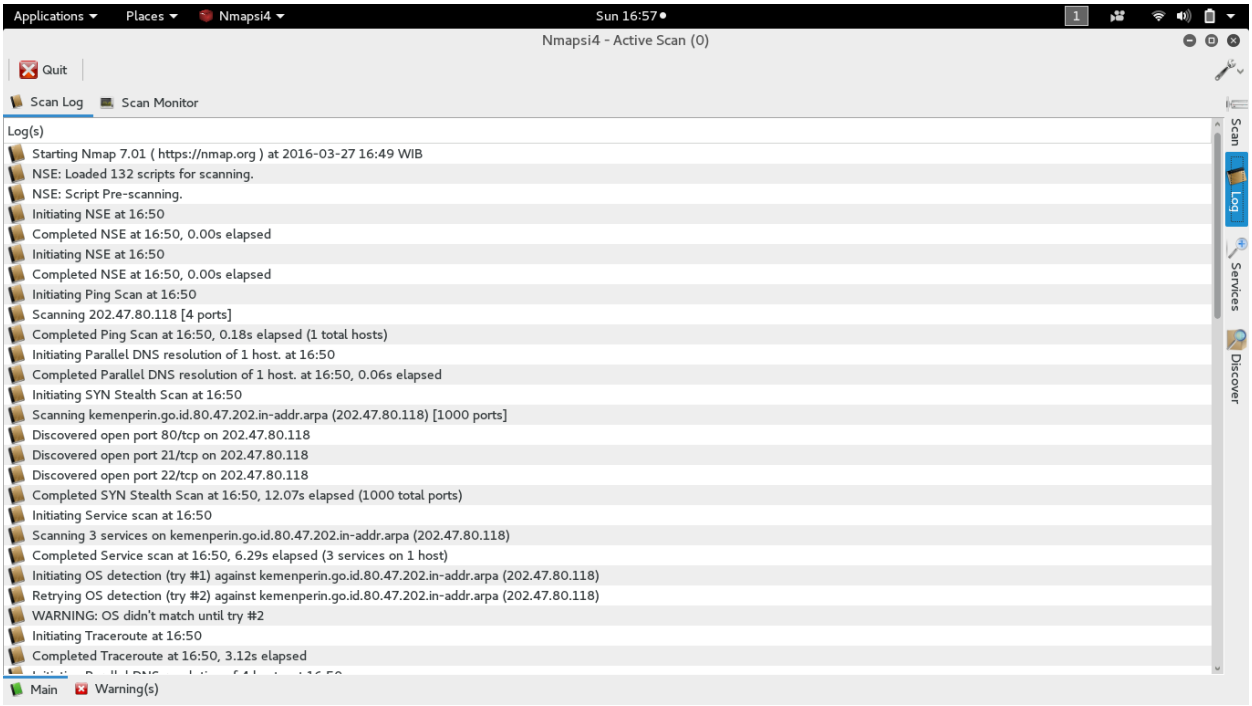
```
The following client-to-server Message Authentication Code (MAC) algorithms
are supported :

  hmac-md5
  hmac-md5-96
  hmac-sha1-96

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

  hmac-md5
  hmac-md5-96
  hmac-sha1-96
```

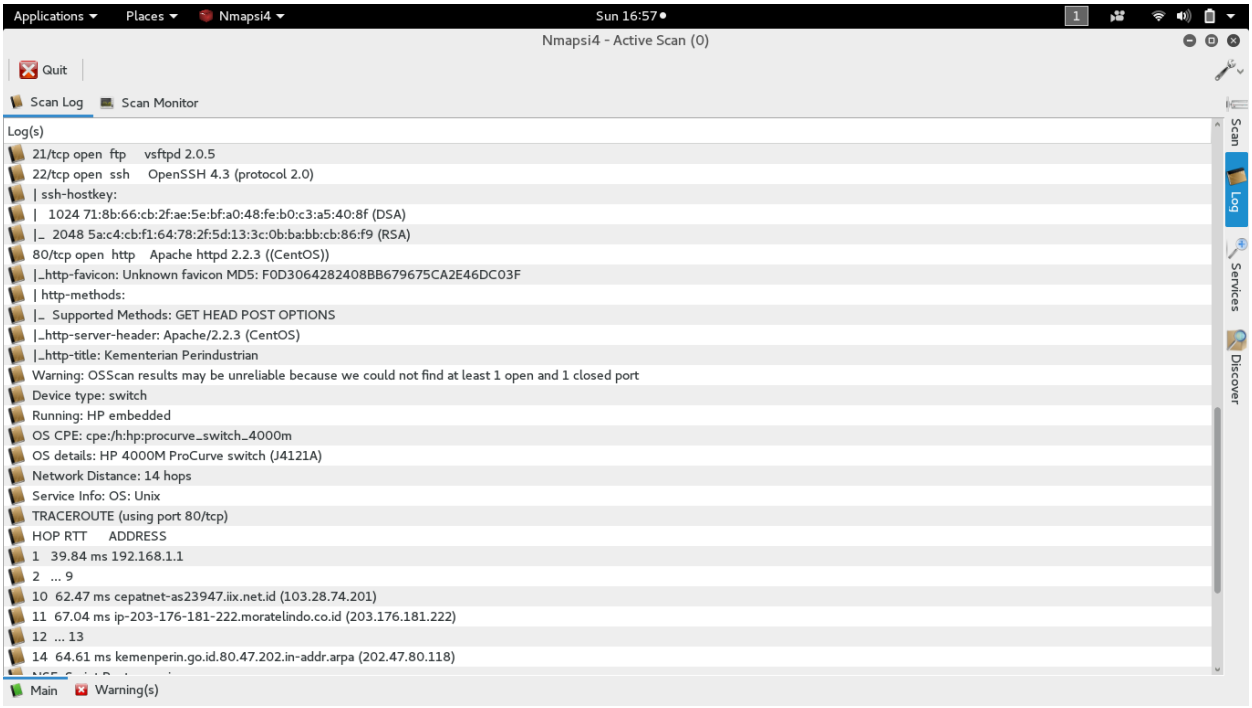
Port	Hosts
22 / tcp / ssh	202.47.80.118

3. Scanning menggunakan Nmapsi4



Gambar 3.1 Hasil scanning Nmapsi4

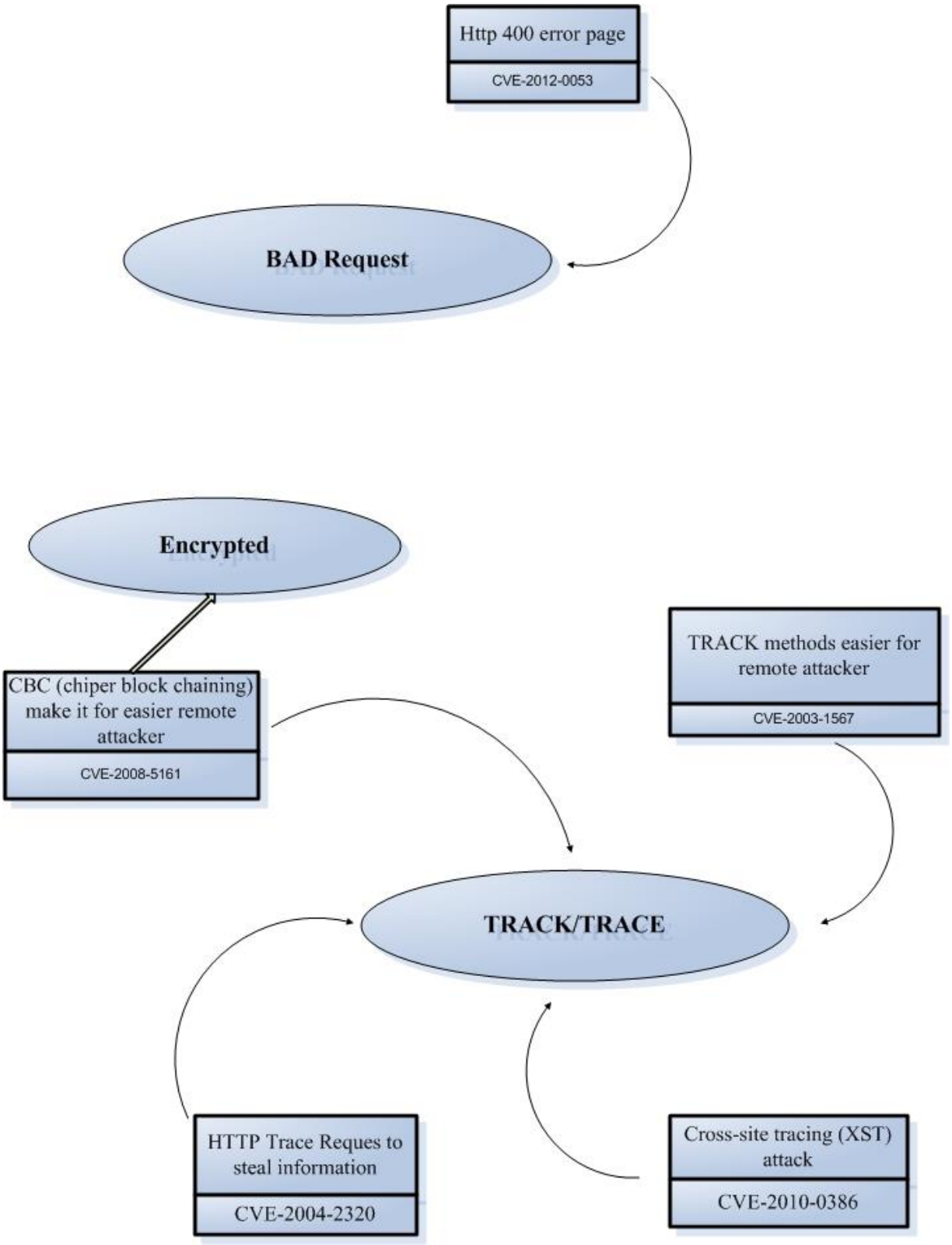




Gambar 3.2 Log Nmapsi4

Jumlah port open pada hasil scanning nmapsi4 adalah 3 port yaitu 21,22 dan 80. Jumlah port yang terscan lebih sedikit jika dibangdikan dengan jumlah scanning menggunakan zenmap. OS yang terscan di nmapsi4 adalah UNIX sedangkan pada zenmap adalah Linux.

CVE Mapping


Http 400 error page
CVE-2012-0053
BAD Request
Encrypted
CBC (chiper block chaining) make it for easier remote attacker
CVE-2008-5161
TRACK methods easier for remote attacker
CVE-2003-1567
TRACK/TRACE
HTTP Trace Reques to steal information
CVE-2004-2320
Cross-site tracing (XST) attack
CVE-2010-0386