NAMA : DWI KURNIA PUTRA

NIM : 09011181320019

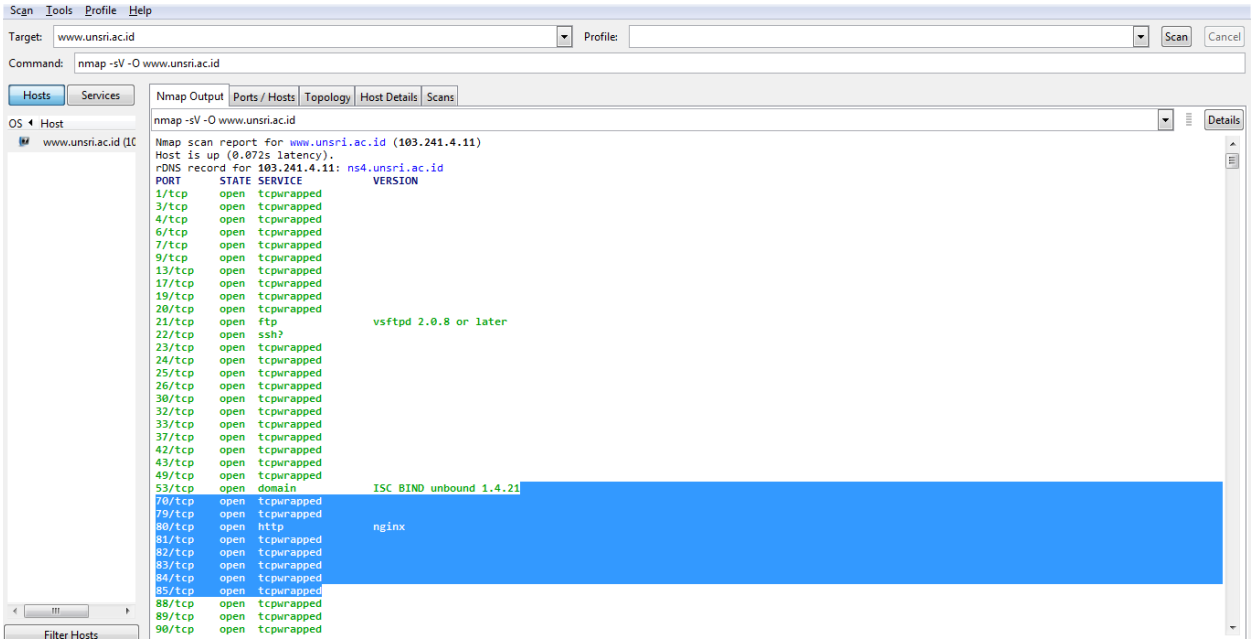
MK : KEAMANAN JARINGAN KOMPUTER

INSTRUCTION DETECTION SYSTEM MENGGUNAKAN SNORT

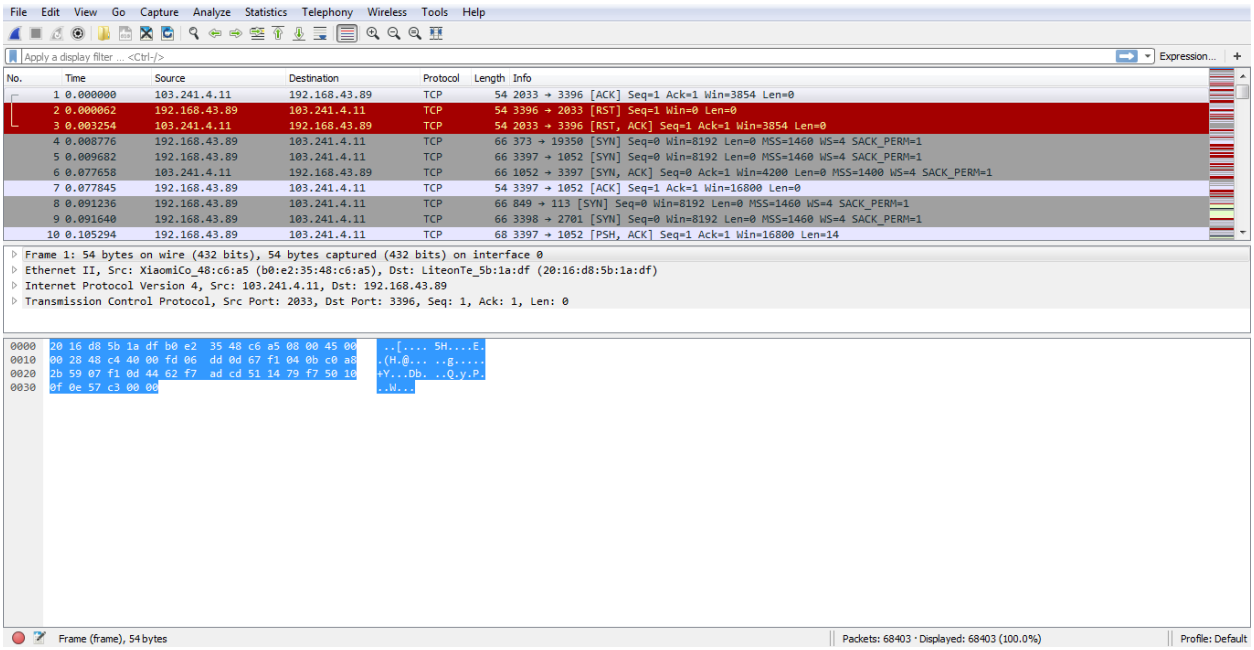
Instruction Detection System (IDS) merupakan sebuah system yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan kegiatan yang mencurigakan didalam sebuah system jaringan. Dimana pada Tugas kali ini saya akan melihat traffic yang ada pada situs Krakatausteel.com dengan menggunakan aplikasi snort. Aplikasi snort sendiri berfungsi sebagai sniffer dan packet logger pada sebuah jaringan selain itu snort dapat digunakan untuk mendeteksi sebuah serangan.

Berikut merupakan aktifitas IDS yang dilakukan, dimulai dari proses scaning dengan zenmap dan traffic data dengan wireshark dan mengompile data menggunakan snort.

Proses Scanning dan Traffic Data

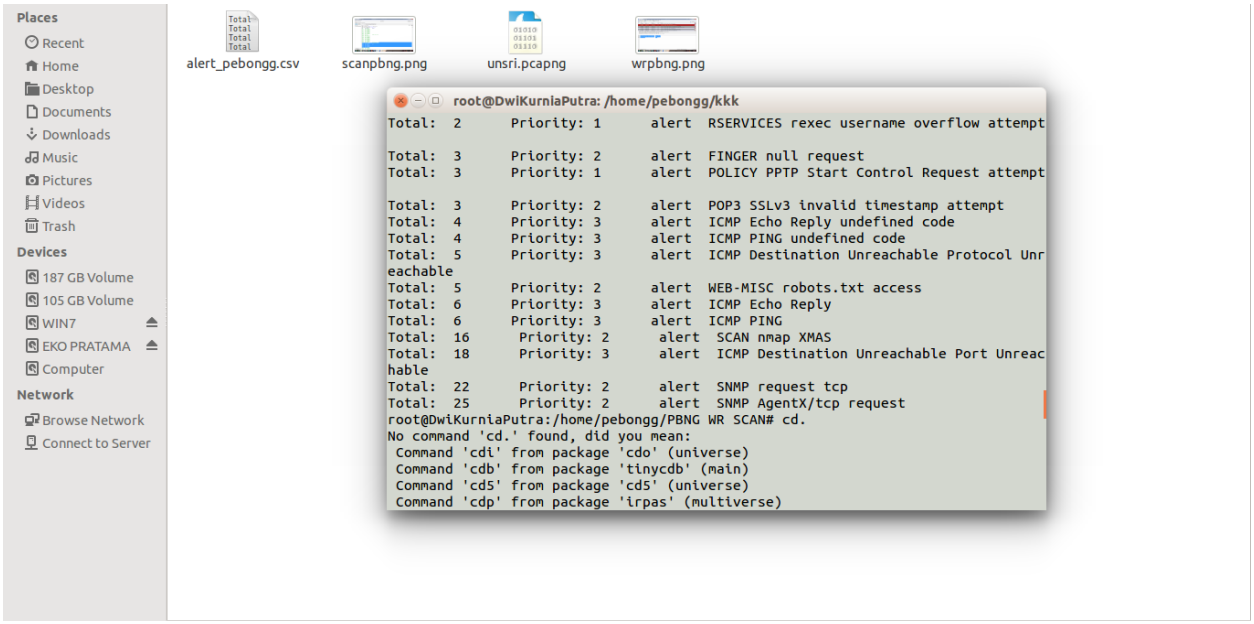


Proses scanning menggunakan tool zenmap, target ke website www.unsri.ac.id dengan ip **103.241.4.11 .** Saat proses scanning berjalan, selanjutnya melakukan traffic data menggunakan wireshark.

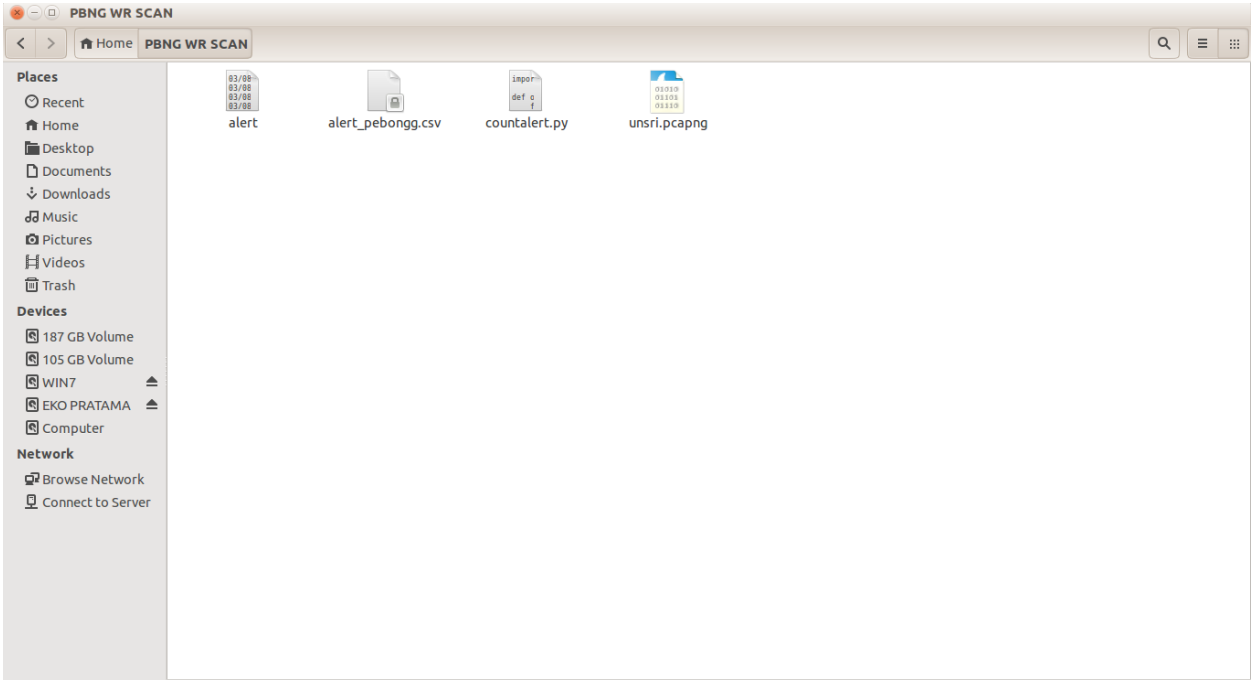


Proses Compile Data Menggunakan Snort

Setelah mendapatkan hasil pcap dari wireshark lakukan compile file pcap dengan perintah *snort –A fast –c /etc/snort/snort.conf –r* dan *Phyton countalert.py alert alert_pebongg.csv*, pada direktori file yang tersimpan kemuddian jika tidak terdapat error lihat apakah data alert berhasil didapatkan.



```
Total:  1      Priority: 3      alert  FTP format string attempt
Total:  1      Priority: 2      alert  ICMP PING NMAP
Total:  1      Priority: 3      alert  ICMP Timestamp Reply
Total:  1      Priority: 3      alert  ICMP Timestamp Request
Total:  1      Priority: 2      alert  RPC portmap listing TCP 111
Total:  1      Priority: 2      alert  SNMP request tcp
Total:  2      Priority: 2      alert  DNS named version attempt
Total:  2      Priority: 3      alert  FTP command overflow attempt
Total:  2      Priority: 3      alert  ICMP Echo Reply undefined code
Total:  2      Priority: 3      alert  ICMP PING undefined code
Total:  2      Priority: 2      alert  INFO FTP Bad login
Total:  2      Priority: 3      alert  POLICY FTP anonymous login attempt
Total:  2      Priority: 2      alert  SNMP AgentX/tcp request
Total:  2      Priority: 2      alert  WEB-MISC robots.txt access
Total:  3      Priority: 3      alert  ICMP Destination Unreachable Protocol Unr
eachable
Total:  4      Priority: 3      alert  ICMP Destination Unreachable Port Unreach
able
Total:  4      Priority: 3      alert  ICMP PING Windows
Total:  5      Priority: 3      alert  ICMP Time-To-Live Exceeded in Transit
Total:  6      Priority: 3      alert  ICMP Destination Unreachable Host Unreach
able
Total:  8      Priority: 3      alert  ICMP Echo Reply
Total:  8      Priority: 3      alert  ICMP PING
Total:  8      Priority: 2      alert  SCAN nmap XMAS
Total:  24      Priority: 3      alert  COMMUNITY WEB-MISC Proxy Server Access
Total:  76      Priority: 3      alert  SCAN UPnP service discover attempt
Total:  183      Priority: 2      alert  MISC UPnP malformed advertisement
root@DwiKurniaPutra:/home/pebongg/kkk# python countalert.py alert alert_pebongg.
csv
```



Setelah berhasil mendapatkan alert kita melakukan compile terhadap data alert dengan alat bantu countalert.py yang dimana alat bantu tersebut merupakan tools dengan bahasa python yang berfungsi untuk mengekstrak data alert yang telah didapatkan. Setelah melakukan ekstrak didapatlah hasil dari traffic yang telah kita lakukan dengan wireshark.

Hasil Data PCAP

1	Alert	Total
2	alert FTP wu-ftp bad file completion attempt [	1
3	alert FTP wu-ftp bad file completion attempt {	1
4	alert RPC portmap listing TCP 111	1
5	alert RSERVICES rexec password overflow attempt	1
6	alert X11 xopen	2
7	alert CHAT IRC nick change	2
8	alert ICMP PING	6
9	alert SNMP AgentX/tcp request	25