Lembar Kerja Peraktek Mandiri
Kegiatan Belajar 7

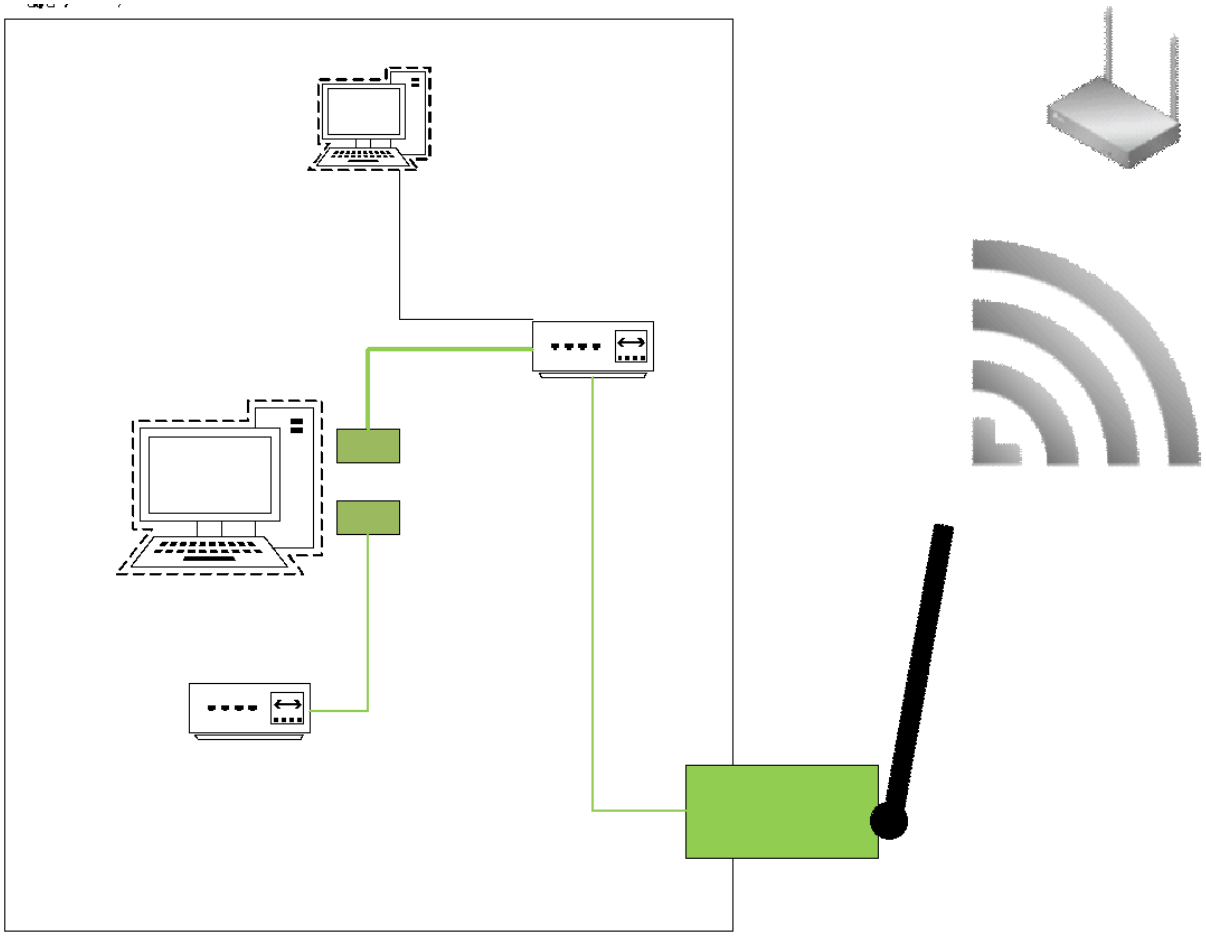
Menganalisis Sistem Pendeteksi Dan Penahan Ancaman/Serangan Yang Masuk Ke Jaringan (Snort)

Pada Kegiatan pembelajaran 7 dilakukan pengujian sistem pendeteksian dan penahanan ancaman/serangan yang masuk kejaringan (IDS) menggunakan snort

Skenario pengujian

1. Snort akan di install di router debian
2. Kali linux akan melakukan pengetesan dengan NMAP dari jaringan external

Skema Pengujian



Lembar Kerja Peraktek Mandiri
Kegiatan Belajar 7

Langkah Kerja

No	Steps	Information
A. Installasi		
1.	1. Installasi SNORT	apt-get install snort
B. Konfigurasi utama		
2.	Edit file konfigurasi utama	1. nano /etc/snort/snort.conf
		2. modifikasi *ipvar HOME_NET* menjadi *ipvar HOME_NET 192.168.1.0/24*
C. Konfigurasi aturan		
3.	Edit file konfigurasi aturan	1. nano /etc/snort/rules/local.rules
4.		2. Tambahkan baris paling bawah alert icmp any any -> any any (msg:"PING DETECTED!";sid:10000001;rev:0) alert tcp any any -> any 161 (msg:"NMAP SCAN DETECTED";sid:10000002;rev:1) alert tcp any any -> any 22 (msg:"SSH login DETECTED";sid:10000003;rev:1)
5.	Restart service	3. /etc/init.d/snort restart
6.	Jalankan snort sebagai IDS	4. snort -A console -q -c /etc/snort/snort.conf -i ens33
D. Pengujian		
7.	Konfigurasi kalilinux sebagai pc guest external	5. Ubah network ke vmnet 0
8.	Konfigurasi alamat IP menjadi external	6. Gunakan GUI , pilih icon configurasi
9.		7. Pilih networking

Lembar Kerja Peraktek Mandiri
Kegiatan Belajar 7

10.		8. Pada menu networking ubah ip menjadi: Ip :192.168.1.12 Netmask : 255.255.255.0 Gateway 192.168.1.1 Dns : 192.168.1.1
11.	Pengujian dari Kalilinux	9. Ketik perintah nmap : nmap -sN -p22 192.168.1.11

Kegiatan Laporan Peraktek yang harus diisi adalah sebagai berikut : :

No	testing	langkah	penjelasan	Capture scrren (minimize pic)
1.	Jalankan Perintah IDS	Gunakan perintah Snort –help untuk menjelaskan arti: snort -A console -q -c /etc/snort/snort.conf -i ens33	-A : …… -q : …… -c:……. ….. -I :…… ….	Capture hasil Jalankan Perintah IDS
2.	Pengujian dari Kalilinux	Ketik perintah nmap : *nmap -sN -p22 192.168.1.11*	Tidak ada penjelasan	**Capture hasil snort di debian**