Лабораторна робота №3

Мета роботи: Ознайомитись з системами виявлення вторгнень (IDS)/системами запобігання вторгненням на прикладі Snort.

Підготовка до виконання роботи

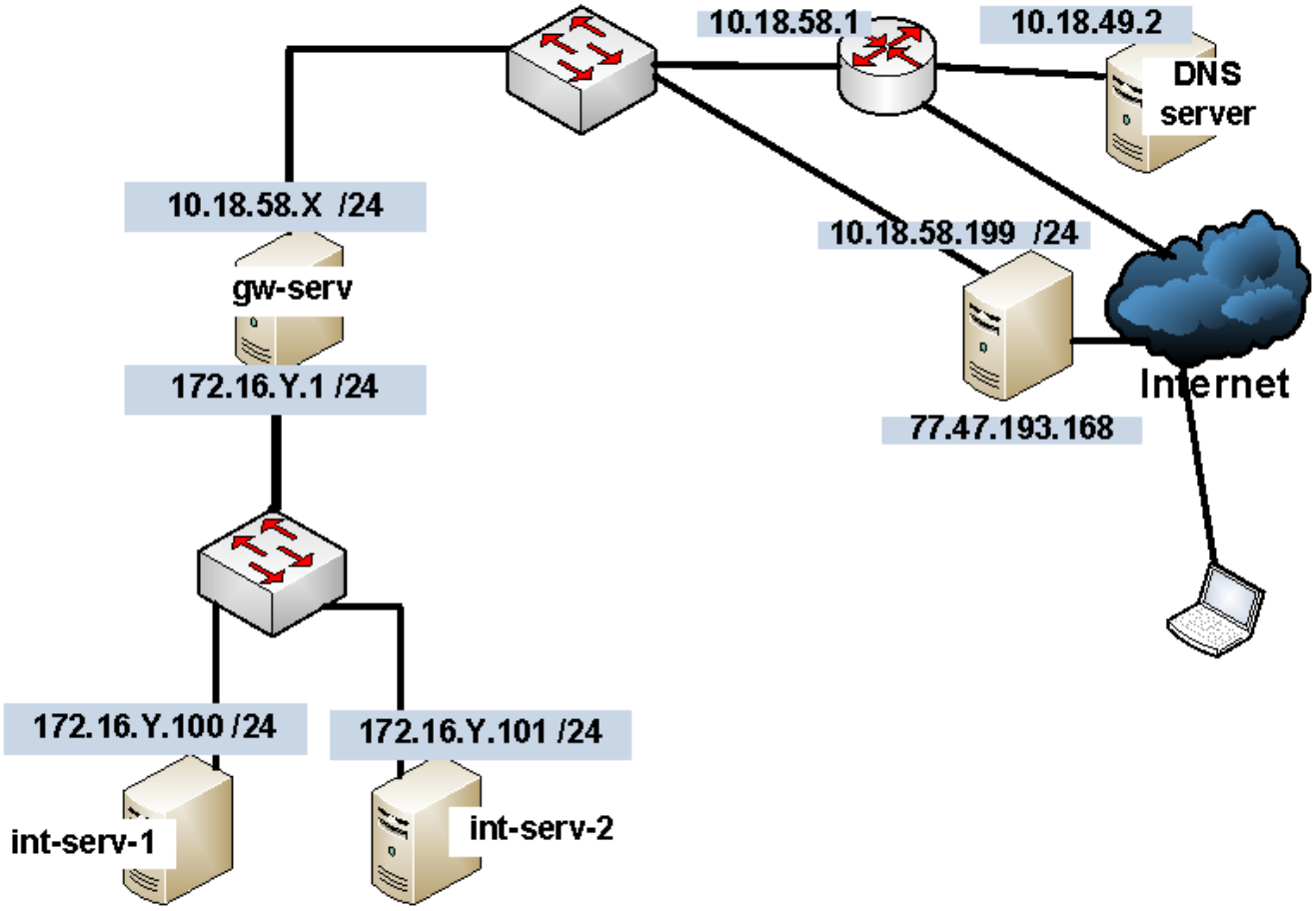
1. Переглянути теоретичні відомості з IDS/IPS, їх призначення, видів та принципів роботи, варіантів розташування у мережі.
2. Ознайомитись з документацією з установки та налаштування Snort

Порядок виконання роботи

1. Встановити та налаштувати Snort на сервері gw-serv згідно з варіантом (див. таблицю) для виявлення вторгнень у внутрішню мережу 172.16.Y.0/24(на сервери int-serv-1, int-serv-2, див. малюнок)
2. Перевірити чи працює система виявлення вторгнень, для цього з хоста в іншій мережі (наприклад, з 10.18.58.199)
   2.1. просканувати за допомогою nmap хости в мережі 172.16.Y.0/24
   2.2. згенерувати “підозрілий” трафік, який підпадає під правило згідно варіанту

№	X	Y	підозрілий трафік
1	201	1	ftp до int-serv-1
2	202	2	ftp до int-serv-2
3	203	3	telnet до int-serv-1
4	204	4	telnet до int-serv-2
5	205	5	telnet до будь-якого сервера
6	206	6	http на порти окрім 80
7	207	7	будь-який трафік на порт 8006
8	208	8	HTTP-запит GET /admin до будь-якого сервера
9	209	9	HTTP-запит GET /wp-admin до будь-якого сервера
10	210	10	HTTP-запит GET /admin.php до будь-якого сервера
11	211	11	SSH на сервер int-serv-1
12	212	12	SSH на сервер int-serv-2
13	213	13	DNS запит до сервера int-serv-2
14	214	14	DNS запит до сервера int-serv-1
15	215	15	http на порт 8080 будь-якого сервера
16	216	16	ftp до int-serv-1
17	217	17	ftp до int-serv-2
18	218	18	telnet до int-serv-1
19	219	19	telnet до int-serv-2
20	220	20	telnet до будь-якого сервера
21	221	21	http на порти окрім 80
22	222	22	будь-який трафік на порт 8006

23	223	23	HTTP-запит GET /admin до будь-якого сервера
24	224	24	HTTP-запит GET /wp-admin до будь-якого сервера
25	225	25	HTTP-запит GET /admin.php до будь-якого сервера
26	226	26	SSH на сервер int-serv-1
27	227	27	SSH на сервер int-serv-2
28	228	28	DNS запит до сервера int-serv-2
29	229	29	DNS запит до сервера int-serv-1
30	230	30	http на порт 8080 будь-якого сервера



https://www.snort.org/documents/snort-users-manual