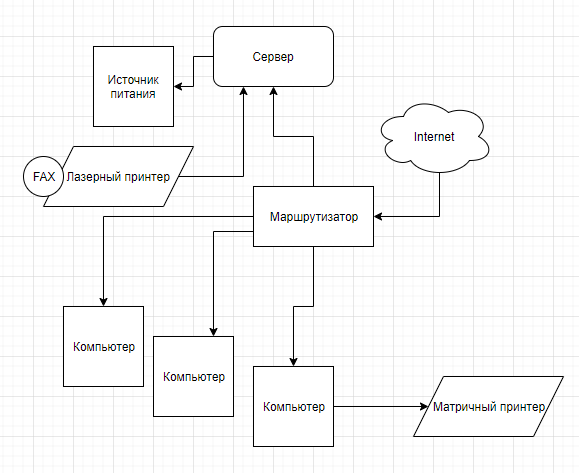
Лабораторная работа 9

Системы обнаружения вторжений

Постановка задачи:

1. Спроектировать физическую сеть для заданного расположения узлов
2. Установка и настройка системы IDS (системы обнаружения вторжений) Snort.

Ход работы:



**Установка и настройка Snort**

Установка:

rpm –i snort-1.9.1-1snort.i386.rpm

Настройка:

Открыть файл: snort.conf.

1. Установка переменных сети

var HOME\_NET 192.168.168.0/24

var EXTERNAL\_NET !$HOME\_NET

var DNS\_SERVERS $HOME\_NET

var SMTP\_SERVERS $HOME\_NET

var HTTP\_SERVERS $HOME\_NET

var SQL\_SERVERS $HOME\_NET

var TELNET\_SERVERS $HOME\_NET

var ORACLE\_PORTS 1521

var HTTP\_PORTS 80

var SHELLCODE\_PORTS !80

var RULE\_PATH /etc/snort

Подключить файлы содержащие классификацию обнаруженной атаки и ссылки на багтраки

include classification.config

include reference.config

2. Настройка механизма обнаружения атак

preprocessor frag2

preprocessor stream4: detect\_scans, disable\_evasion\_alerts

preprocessor stream4\_reassemble

preprocessor http\_decode: 80 unicode iis\_alt\_unicode double\_encode iis\_flip\_slash full\_whitespace

preprocessor rpc\_decode: 111 32771

preprocessor portscan: $HOME\_NET 4 3 portscan.log

preprocessor portscan-ignorehosts: 192.168.168.0/24

preprocessor arpspoof

preprocessor conversation: allowed\_ip\_protocols all, timeout 60, max\_conversations 32000

preprocessor portscan2: scanners\_max 3200, targets\_max 5000, target\_limit 5, port\_limit 20, timeout 60

include $RULE\_PATH/bad-traffic.rules

include $RULE\_PATH/exploit.rules

include $RULE\_PATH/scan.rules

include $RULE\_PATH/finger.rules

include $RULE\_PATH/ftp.rules

include $RULE\_PATH/dos.rules

include $RULE\_PATH/ddos.rules

include $RULE\_PATH/dns.rules

include $RULE\_PATH/web-cgi.rules

include $RULE\_PATH/web-iis.rules

include $RULE\_PATH/web-client.rules

include $RULE\_PATH/web-php.rules

include $RULE\_PATH/sql.rules

include $RULE\_PATH/icmp.rules

include $RULE\_PATH/netbios.rules

include $RULE\_PATH/misc.rules

include $RULE\_PATH/attack-responses.rules

include $RULE\_PATH/mysql.rules

include $RULE\_PATH/pop3.rules

include $RULE\_PATH/pop2.rules

include $RULE\_PATH/other-ids.rules

include $RULE\_PATH/web-attacks.rules

include $RULE\_PATH/backdoor.rules

include $RULE\_PATH/shellcode.rules