Example of snort rules report

Law, Security

Question 1: What does each of the flags in this snort command line do?

snort -r snort. out -P 5000 -c csec640. rules -e -X -v ""? k none -l log

There are various flags which are used in snort. There is only one flag in the command that has been given. This is –P flag. This is the push flag. It is used for pushing execution commands to be executed.

Question 2

My new rules are stated below:

Rule 1:

alert tcp 192. 168. 1. 4 any -> any any (msg:" Detected packets from 192. 168. 1. 4";)

The snort rule that is shown above alerts snort system any time there is traffic and packets from host with the IP address. It will send an alert message to the system network.

Rule 2:

Another option which si useful hen writing snort rule is about the content of the packets that are being received. There are some times when snbort can search through the packjets looking for a particular string. The snort rule bewlow will send a trigger when there is a content with digit 0x80.

alert tcp any any -> any any (msg: “ exploit could be possible”; content: “| 80|”;)

snort 3:

there is also the option of checking for flags. Snort gives snort option. This option aids in situations when portscan is being done where flag combinations are invalid.

```
alert tcp any any -> any any (flags: SF, 12 msg: “ There is a possibility of
SYN FIN in the scan”;)
```

Rule 4:

It is also possible to build rules apart from the ones that snort has built inside.

```
ruletype redalert
{
type alert
output alert_syslog: LOG_AUTH LOG ALERT
output database: log, database path
```

The rule above tells snort to have an alert but the alert should be sent to the daemon of syslog. The output should be directed to a database where the path is given.

Rule 5:

Another rule is oen that suppresses a network which uses public in polling devices that use SNMP. It is not secure to have this in place.

```
suppress gen_id 4, sig_id 5422, track by_src, ip 13. 4. 3. 2
```

Rule 6:

```
alert icmp any any -> any any (msg: " Ping with TTL= 100";
ttl: 100;)
```

Question 3

The statement that has just been stated means that the threat is aware of the network and the hosts that are operating in the network. The threat gets installed in a network of hosts by making use of a vulnerability service. There is the use of RPC which has been handled poorly and this is where the threat takes advantage. It then attacks the host on the network by making use of the weaknesses. The routine of checking the hosts and attacking them, this threat connects to the server which is remote and will record the version of the operating system and the security features and applications that have been installed in the system.

This threat can be detected by making sure that the hosts are registered with an antivirus program. Most antivirus programs are able to detect this threat. Another method is to check at the attempts made to access the hosts that are installed in the network. The attempts should be initiated by an administrator.

It is recommended that spyware removers are used in the process of removing the spyware Gimmiv. a. Manual renmoval is a preserve of the experts in technology like the system administratrors and IT experts only. This is because if the manual process is not done properly, there are some system files which can be damaged.

Question 4

Snort can not be used to detect covert channels. Although snort is the best security project that has been developed in the world, it has not been used in detecting covert channels. This capability has not yet been achieved. This is the reason as to why manual detection of covert channels is recommended. There is no command that will enable snort to detect a covert channel.