Name: Hud Seidu Daannaa

Intrusion Detection System and Working with Snort

Components of an Intrusion Detection System (IDS):

Sensors: This collects data from various sources such as files, network packets and sends them to the analyzer. Analyzers: The data is processed from the sensors and determine intrusion has occurred. User interface: this helps to view the output and manage the behavior.

Network-based and host-based IDS with differences:

Network-based IDS's are used to monitor and analyze passing traffic on a network with the use of a dedicated platform, these are normally located inside the firewall or on the
DMZ.
Host-based IDS's are used on host computer (individual), it takes advantage of system resources to detect intrusions by analyzing logs of operating systems, system activities and monitor other applications.
The differences are that Network-based IDS's are placed within the network and are specialized for monitoring and analyzing passing traffic while Host-based IDS's use a host computer's resources, logs of the computers operating systems to detect intrusions

The difference between passive and reactive systems:

The difference between passive and reactive systems are, in a passive system, the IDS detects an intrusion, puts the information in a log and signals an alert. For reactive systems, the IDS respond to a suspicious activity or intrusion by logging off a user or by reconfiguring the IDS to block the flow of network traffic from the suspected source of intrusion.

4.2 HOME_NET set to 10.130.4.25 and EXTERNAL_NET set to any

Snort rule that alerts for FTP connections from IP address different from Home_net : *alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"foreign IP alert";*sid:1098760;*)*

Snort rule that alerts for "worm" in content outgoing from Home_net :
*alert tcp $HOME_NET any -> EXTERNAL_NET any (content: "worm"; msg: "outgoing content worm";*sid:1032231*)*

The rule written in the previous question will not raise an alert because, 'Internet Worm' is not case sensitive, due to the specification of the rule above (content: "worm";)

Snort rule that alerts for pings from External_Net :
*alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg: "Ping found";*sid:30987*)*

*alert tcp any any -> 10.1.1.0/24 6000:6010 (msg: "*X Windows service traffic*";)* The above rule alerts for detected tcp packets fr(that is to say, X windows trafic) on any address on any port to 10.1.1.0/24 network on ports ranging from '6000 to 6010 and output a message 'X Windows service traffic'.

Name: Hud Seidu Daannaa

4.3

How the following rules work:

alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"SCAN FIN"; flags: F; reference:arachnids,27;)
Make an alert on any tcp packet with a 'F' flag (FIN) leaving any port on an external_net to any port on a home_net and output a message 'SCAN FIN' and with reference to arachmids external attack identification systems.

alert tcp $HOME_NET 23 -> EXTERNAL_NET any (msg: "Telnet login incorrect"; content: "Login incorrect" ; flag A+ reference:arachnids,127;)
Alert any Telnet connection attempted from some home_net on port 23 to an outside network(external_net) on any port, with Tcp flag bits set to Ack and other set flag bits,the packet is to be filtered for a 'Login incorrect' content,display a message 'Telnet login incorrect' with reference to arachmids external attack identification systems.

Alert icmp any any → any any (msg:"ICMP Source Quench"; itype: 4; icode:0;) For an icmp packet, from any port of any address to a destination of any port on any address, with 'itype:4' which means ICMP source Quench,it is described as 'no code ' or "code 0" and for the ''icode:0 , this shoud create an an alert with the message 'ICMP Source Quench'.

4.4 OpenSSL Heartbleed Vulnerability

alert tcp $EXTERNAL_NET any -> $HOME_NET 443
msg:"SERVEROTHER OpenSSL TLSv1.2 heartbeat read overrun attempt"
flow:to_server,established content:"|18 03 03|"
depth:3 dsize:>40
detection_filter:track by_src, count 3, seconds 1
metadata:policy balanced-ips drop, policy security-ips drop, service ssl
reference:cve,2014-0160 classtype:attempted-recon sid:30513 rev:2

Description and analysis:

- The above rule will create an alert for some tcp packet leaving the external_net on any port to the home_net on port 443, .
- A message should flow the alert saying "SERVEROTHER OpenSSL TLSv1.2 heartbeat read overrun attempt".
- The flow option, helps to verify this is traffic going to the server on an established session
- The class type: attempted-recon,categorize a rule as detecting an intrusion or an attack that is known to be part of a more general type of attack class.
- The sid '30513' is normally used with rev, the sid acts as a unique snort rule identifier, it enables output plugins to identify rules easily.
- Rev is 2, it serves as an identifier for revisions on snort rules,it helps signatures and other description informations to be updated or replaced.
- The meta data allow the person writing the rules to add or embedd additional information in this case metadata:policy balanced-ips drop, policy security-ips drop, service ssl.

Name: Hud Seidu Daannaa

- The content:"|18 03 03|”, this is to find the 3 bytes data patterns "|18 03 03|"inside a packet eg.ASCII string or as binary data.,in this case ,the first three bytes ,"|18 03 03|" is meant to raise an alert if found in a packet.
- reference: cve,2014-0160, references are made to an external attack identification systems, eg. cve,2014-0160.
- The depth is 3, this enables the one writing the rule to specify how far a packet rule writer to specify how far into a packet, snort should search.
- The dsize:>40, this helps to test the packet payload size.
- Detection_filter is the rate which must be exceeded by a party (source or destination) before a rule can put out an event, counts are 3, which is the number matching rules in s seconds that will make an event filter limit to be exceeded. 1 seconds is the time over which count is accrued. “track by_dst” is the rate which is tracked by the source IP address.

```
alert tcp $HOME_NET 443 -> $EXTERNAL_NET any
msg:"SERVER-OTHER `TLSv1 large heartbeat response – possible ssl Heartbleed attempt"
flow:to_client,established content:"|18 03 01|"
depth:3
byte_test:2,>,128,0, relative
detection_filter:track by_dst,count 5, seconds 60
metadata:,policy balanced-ips drop, policy security-ips drop, service ssl reference:cve,2014-
0160 classtype:attempted-recon
sid:30515 rev:3
```

Description and analysis:

- The above rule will create an alert for some tcp packet leaving a home_net on port 443 to any port on the external_net.
- A message should flow the alert saying "SERVER-OTHER `TLSv1 large heartbeat response – possible ssl Heartbleed attempt"
- The flow option, helps to verify this is traffic going to the server on an established session
- The class type: attempted-recon, categorize a rule as detecting an intrusion or an attack that is known to be part of a more general type of attack class.
- The sid ‘30515’ is normally used with rev, the sid acts as a unique snort rule identifier, it enables output plugins to identify rules easily.
- Rev is 3, it serves as an identifier for revisions on snort rules,it helps signatures and other description information to be updated or replaced
- The meta data allow the person writing the rules to add or embedd additional information in this case metadata:policy balanced-ips drop, policy security-ips drop, service ssl.
- The content:"|18 03 01|”, this is to find the 3 bytes data patterns "|18 03 03|"inside a packet eg.ASCII string or as binary data.,in this case ,the first three bytes ,"|18 03 03|" is meant to raise an alert if found in a packet.
- reference: cve,2014-0160, references are made to an external attack identification systems, eg. cve,2014-0160
- Detection_filter is the rate which must be exceeded by a party (source or destination) before a rule can put out an event,counts is 5,which is the number matching rules in s seconds that will make an event filterlimit to be exceeded. 60 seconds is the time period over which count is accrued.”track by_dst” is the rate which is tracked by the destination IP address.

- The byte_test argument is used in addition with an operator to test against a specific value,in this case ,byte_test:2,>,128,0,relative.

4.6 A Computer Worm

The snort rule to detect the worm is:

alert tcp $EXTERNAL_NET any -> $HOME_NET 1045 (msg:” Internet Worm to be stopped”; sid:1000006; content: “07”; rawbytes; within:1; content:”71 f2 03 01 04 9b 71 f2 01”; rawbytes;distance:0; content:”tire”;distance:-100;)