Network Security Lab 11

Network Security Lab 11

David Ayeke Feb 27. 2017

Rule to capture all TCP packets

```
sudo snort -de -l ~/.log -h 0.0.0.0/0 -i wlp3s0
```

Snort first 10 packets

```
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

h<X@a@@}@@@@@@@}l@X@aX@a@@@^@@@4@*PE@J@@|@@@@@@@@}l@@M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

h<X@a@5}@@@@@@@}l@X@aX@a@5@^@@@4@*PE@J@@|@@@@@@@@}l@@M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

h<X@a@}@@@@@@@}l@X@aX@a@@^@@@4@*PE@K@|p@@@@@@@}l@@M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

h<X@a>
       @a}@@@@@@@|l@X@a>X@a>
                                    @a@^@@@4@*PE@P@@v@@@@@@@@|l@@M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

h<X@a?
      @F}@@@@@@@|l@X@a?X@a?
                                  @F@^@@@4@*PE@P@@v@@@@@@@@|l@@M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

hX@a@
```

```
     ��}�������|lX�a@X�a@
                                    ���^���4�*PE�Q!@v`�������|l��M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

h<    X�aA
           ��}�������|l�    X�aAX�aA
                                                  ���^���4�*PE�Q)@vX�������|l��M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

h<
X�a��9}������Ц̧l�
X�a�X�a��9�^���4�*PE�{@@K�������Ц̧l���M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

h<
  X�a��%}������Ц̧l�
                           X�a�X�a��%�^���4�*PE�|@@J�������Ц̧l���M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

h<
  X�a��N}������Ц̧l�
                           X�a�X�a��N�^���4�*PE�}G@J:������Ц̧l���M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

X�a�X�a���^���4�*PE�}}@J������Ц̧l���M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

h<X�b�p}�������:l�X�bX�b�p�^���4�*PEDž@B�������:l��_M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux

h<X�b�X}�������:l�X�bX�b�X�^���4�*PEdžv@A
                                                        ��������:l��_M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
```

```
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/54.0.2840.59 Linux
```