



# 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<X0a00}0000000}10X0aX0a000^00040*PE0J0@|00000000}100M-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<X0a05}0000000}10X0aX0a050^00040*PE0J0@|00000000}100M-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<X0a0}0000000}10X0aX0a00^00040*PE0K@|p0000000}100M-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<X0a>
0a}0000000|10X0a>X0a>
0a0^00040*PE0P0@v00000000|100M-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<X0a?
0F}0000000|10X0a?X0a?
0F0^00040*PE0P0@v00000000|100M-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

hX0a@
```

00}0000000|lX0a@X0a@

000^00040\*PE0Q!@v`0000000|l00M-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< X0aA

00}0000000|l0 X0aAX0aA

000^00040\*PE0Q)@vX0000000|l00M-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<

X0a009}0000000Tl0

X0a0X0a0090^00040\*PE0{0@K0000000Tl100M-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<

X0a00}%000000Tl0

X0a0X0a000%0^00040\*PE0|0@J0000000Tl100M-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<

X0a00N}000000Tl0

X0a0X0a00N0^00040\*PE0}G@J:000000Tl100M-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

X0a0X0a000^00040\*PE0}}@J000000Tl100M-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<X0b0p}0000000:10X0bX0b0p0^00040\*PEDž@B0000000:100\_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<X0b0X}0000000:10X0bX0b0X0^00040\*PEDžv@A

0000000:100\_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