Network Security Lab 12

Network Security Lab 12

David Ayeke Mar 6. 2017

Rule to capture all TCP packets and alert

sudo snort -A fast -dev -l ~/.log2 -h 0.0.0.0/0 -i wlp3s0 -c /etc/snort/snort.conf

Contents of alert file

```
cat ~/.log2/alert
03/06-11:28:06.660698  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification:
Detection of a Network Scan] [Priority: 3] {UDP} 192.168.1.2:41017 -> 239.255.255.250:1900
03/06-11:28:07.661390  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification:
Detection of a Network Scan] [Priority: 3] {UDP} 192.168.1.2:41017 -> 239.255.255.250:1900
03/06-11:28:08.662061  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification:
Detection of a Network Scan] [Priority: 3] {UDP} 192.168.1.2:41017 -> 239.255.255.250:1900
03/06-11:28:09.662742  [**] [1:1917:6] SCAN UPnP service discover attempt [**] [Classification:
Detection of a Network Scan] [Priority: 3] {UDP} 192.168.1.2:41017 -> 239.255.255.250:1900
```