Knowing Your Network with OpenAppID

Rafeeq dot Rehman at Gmail
@rafeeq_rehman

Agenda

- What is OpenAppID
- How to Enable OpenAppID in Snort
- How to use OpenAppID

What Security Has to Do with Applications?

Unauthorized applications? Mobile Apps? Online Data Storage Apps? Etc.

What is OpenAppID

- Traditionally Snort Rules are based upon IP packet analysis
- OpenAppID enables detection of Applications
- An excellent way of detecting Cloud Applications
- Create alerts based upon use of specific apps in a network
- Find data amount used by each application
- Detects “more than 1400 apps” (1550), enables writing custom detectors
- Still in Alpha!!!

Enable in Snort

- Download Snort Alpha, compile, install dependencies
  - tar zxvf snort-2.9.7.0_alpha.tar.gz
  - cd snort-2.9.7.0.alpha
  - ./configure --prefix=/opt/snort --enable-sourcefire --enable-open-appid
  - make
  - make install
- Add OpenAppID detector files - snort-openappid-detectors. 2014-02-22.187-0.tgz
- OpenAppID requires Lua

Configure and Start Snort

- Configure snort.conf

  *preprocessor appid: *

  *app_stats_filename appstats-unified.log, *

  *app_stats_period 60, *

  app_detector_dir /opt/snort/lib/openappid

- Start Snort

  /opt/snort/bin/snort -c /opt/snort/etc/snort.conf -k none -D -A fast

Application Data Usage

- Viewing OpenAppID Unified Logs

  /opt/snort/bin/u2openappid /var/log/snort/appstats-unified.log.1398999240

  statTime="1398263040",appName="dropbox",txBytes="6494",rxBytes="4981”

  statTime="1398263040",appName="http",txBytes="6494",rxBytes="4981”

  statTime="1398263640",appName="https",txBytes="2401",rxBytes="1569”

  statTime="1398263760",appName="dns",txBytes="80",rxBytes="140”

  statTime="1398263820",appName="https",txBytes="855",rxBytes="563”

  statTime="1398263880",appName="dns",txBytes="148",rxBytes="358”

  statTime="1398263880",appName="firefox",txBytes="752",rxBytes="1983”

- Get surprised (vonage, slingbox, …)

Addition to Snort Rules

- The appid keyword (appid: facebook;)
- Write Rules specific to certain application (in addition to other criteria)
- Can match with multiple apps

Alerting for specific Applications

- Add a new rules for specific application in local.rules

  alert tcp any any -> any any (msg:"OpenAppID: Use of dropbox"; appid: dropbox; sid:100005; rev:1;)

- View alerts

  05/02-07:44:49.314989 [**] [1:100000:4] "OpenAppID: Use of dropbox" [**] [Priority: 0] {TCP} xxx.xxx.167.39:80 -> xxx.xxx.2.15:45316

- You can use multiple applications in one Snort rule.

Apps Mapping (appMapping.data)

117 Digg	0	0	31 ~ digg
11 Direct Connect	20040	0	0 direct_connect direct_connect
125 Dropbox	0	300	98 ~ dropbox
133 eBay Bid	0	0	32 ~ ebay_bid
134 eBay Search	0	0	33 ~ ebay_search
135 eBay Watch	0	0	34 ~ ebay_watch
136 eBuddy		0	0 35 ~ ebuddy
149 Facebook Apps		0	0 852 ~ facebook_apps

Writing Detectors

- Excerpt from Detector Lua File

```
DetectorPackageInfo = {
   name =  "AirPlay",
   proto =  DC.ipproto.tcp,
   client = {
      init =  'DetectorInit',
      clean =  'DetectorClean',
      validate =  'DetectorValidator',
      minimum_matches =  1
   }
}
```

- Present in openappid/odp/lua directory

The Initialization Function

- Detect based upon URLs, HTTP Patterns, src/dst ports, SSL Certificate fields, etc.

```
function DetectorInit(detectorInstance)
   gDetector = detectorInstance
      gDetector:addHttpPattern(2, 5, 0, 215, 1, 0, 0, 'AirPlay', 1681, 1);
   return gDetector
end
```

Where to use OpenAppID

- Data usages by different apps
  - *Will require some scripting!*
- Alerting based upon apps
- Network app inventory
- Application Blocking (Depending upon how Snort is deployed)