SAND2015-6361PE

Exceptional service in the national interest

Sandia National Laboratories

Easy Being a Bro, It is Not

MIDN 2/C Chadwick Riggins

U.S. DEPARTMENT OF ENERGY

National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP

Problem Statement

Sandia National Laboratories

- Intrusion Detection and Big Data
- Differing sources
  - Server Logs
  - Packets
  - Cookies
- Limitation
  - Time
  - Prior knowledge of software

What is Bro?

Sandia National Laboratories

- Network Security Monitor
- Open Source and Unix based
- Important to note
  - Looks at connections (broader capability)
    - Not signature based
  - Framework can be used as an IDS
  - Little documentation

The Goal

Sandia National Laboratories

- Add additional capabilities to current software using Bro
- Tasks:
  - Complete ingest of PCAPs
  - Complete integration into ELK stack
  - X509 Certificates
  - File Analysis

PCAP Ingestion

Sandia National Laboratories

```
#!/usr/bin/python
#Chad Riggins
#26Jun2015

import os
#path can be changed to search anywhere in the vm
os.system("sudo find /home/tyler/Desktop/newPcaps/* -name '*.pcap' > pcaps.tx")

#formatting to get pcaps into a list without new lines
fi = open("pcaps.tx", "r+")
pcaps = fi.readlines()
pcaps = "".join(pcaps)
pcaps.replace("/n", "")
pcaps = pcaps.split()


length = len(pcaps) #full number of pcaps

#for cap in range(0, length):#iterating through each pcap

    #currCap = pcaps[cap]
currCap = pcaps[0]
reverseCap = currCap

count = 1
for i in reverseCap[::-1]:#searching for a "/" from the end
    if i == "/":
        break
    count += 1

pcapDir = currCap[0: len(currCap) - count]#file path
actualPcap = currCap[len(currCap) - count+1:]#file(pcap)
    #os.chdir(pcapDir)#change to pcap path
cmd = "bro -Cr "
fullcmd = cmd + currCap
    #print fullcmd
os.system(fullcmd) #run bro

print "done"
```

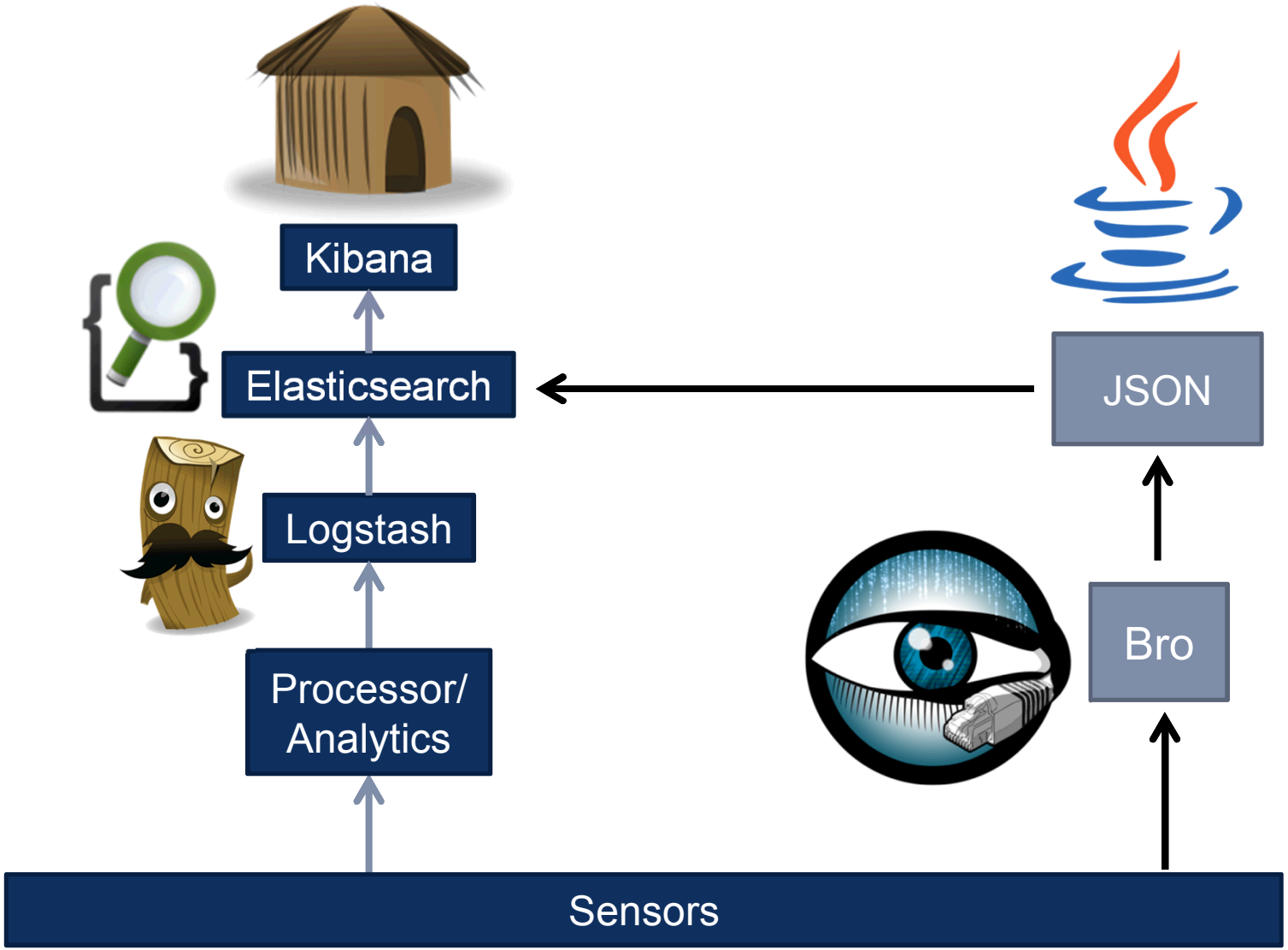
```
logLength = len(logs)
length = len(pcaps) #full number of pcaps

for cap in range(0, length):#iterating through each pcap
    currCap = pcaps[cap]
    #currCap = pcaps[0]
    reverseCap = currCap
    #print "curr pcap is", currCap

    count = 1
    for i in reverseCap[::-1]:#searching for a "/" from the end
        if i == "/":
            break
        count += 1
    pcapDir = currCap[0: len(currCap) - count]#file path
    actualPcap = currCap[len(currCap) - count+1:]#file(pcap)
    os.chdir(pcapDir)#change to pcap path
    print "curr directory is", os.getcwd()
    print
    for curr in range(0, logLength):
        logCount = 1
        currLog = logs[curr]
        reverseLog = currLog
        #print "curr log is", currLog
        #print
        for j in reverseLog[::-1]:

            if j == "/":
                break
            logCount += 1

        logDir = currLog[0: len(currLog) - logCount]
        actualLog = currLog[len(currLog) - logCount+1:]

        if logDir == pcapDir:
            newLog = actualLog + "." + actualPcap
            mvCmd = "mv "
            cpCmd ="cp "
            logCmd = mvCmd + actualLog + " "
            logFullCmd = logCmd + newLog

            os.system(logFullCmd)
            collectiveDir = "/home/tyler/Desktop/logs/"
            moveCmd = cpCmd + newLog + " "+ collectiveDir
            os.system(moveCmd)

print "done"
```

```
/home/tyler/Desktop/newPcaps/2013/07/28/2013-07-28-phishing-malware-traffic.pcap
/home/tyler/Desktop/newPcaps/2013/07/14/2013-07-14-DotkaChef-EK-traffic.pcap
/home/tyler/Desktop/newPcaps/2013/07/08/2013-07-08-DotkaChef-EK-traffic.pcap
/home/tyler/Desktop/newPcaps/2013/07/21/2013-07-21-Blackhole-EK-traffic.pcap
/home/tyler/Desktop/newPcaps/2013/10/28/2013-10-28.pcap
/home/tyler/Desktop/newPcaps/2013/11/23/2013-11-23.pcap
/home/tyler/Desktop/newPcaps/2013/11/29/2013-11-29-unsuccessful-infection.pcap
/home/tyler/Desktop/newPcaps/2013/11/29/2013-11-29-successful-infection.pcap
/home/tyler/Desktop/newPcaps/2013/11/15/2013-11-15.pcap
/home/tyler/Desktop/newPcaps/2013/12/23/2013-12-23.pcap
```

```
/home/tyler/Desktop/newPcaps/2013/07/28/files.log
/home/tyler/Desktop/newPcaps/2013/07/28/http.log
/home/tyler/Desktop/newPcaps/2013/07/28/dns.log
/home/tyler/Desktop/newPcaps/2013/07/28/conn.log
/home/tyler/Desktop/newPcaps/2013/07/28/packet_filter.log
/home/tyler/Desktop/newPcaps/2013/07/14/files.log
/home/tyler/Desktop/newPcaps/2013/07/14/http.log
/home/tyler/Desktop/newPcaps/2013/07/14/conn.log
/home/tyler/Desktop/newPcaps/2013/07/14/packet_filter.log
/home/tyler/Desktop/newPcaps/2013/07/08/files.log
/home/tyler/Desktop/newPcaps/2013/07/08/http.log
/home/tyler/Desktop/newPcaps/2013/07/08/conn.log
/home/tyler/Desktop/newPcaps/2013/07/08/packet_filter.log
/home/tyler/Desktop/newPcaps/2013/10/28/ssl.log
```

Integration into stack

Sandia National Laboratories



Certificates

Sandia National Laboratories

- X509 certificates not currently being looked at
- What Bro found:
  - Cert. valid before/after
  - Cert. issuer
  - Cert. algorithm
  - Cert. subject

AU6H7a83qyOg4qthiNV9	bro-x509_log	2004-06-30T00:06:20.000Z	2034-06-30T00:06:20.000Z	OU=Go Daddy Class 2 Certification Authority,O=The Go Daddy G...

View: **Table** / JSON / Raw

Field	Action	Value
@timestamp		2015-07-13T14:59:36.681Z
@version		1
DATETIME		2014-05-01T02:57:26.965Z
_id		AU6H7a83qyOg4qthiNV9
_index		logstash-2015.07.13
_type		bro-x509_log
basic_constraints.ca		T
basic_constraints.path_len		-
cert.not_valid_after		2034-06-30T00:06:20.000Z
cert.not_valid_before		2004-06-30T00:06:20.000Z
certificate.curve		-
certificate.exponent		3
certificate.issuer		OU=Go Daddy Class 2 Certification Authority,O=The Go Daddy Group\, Inc.,C=US
certificate.key_alg		rsaEncryption
certificate.key_length		2048
certificate.key_type		rsa
certificate.serial		00
certificate.sig_alg		sha1WithRSAEncryption
certificate.subject		OU=Go Daddy Class 2 Certification Authority,O=The Go Daddy Group\, Inc.,C=US
certificate.version		3
host		localhost.localdomain
id		FYVWlV1qH7uo9iOtCk
path		/home/tyler/Desktop/logs/x509.log.2014-05-01-Magnitude-EK-traffic.pcap
san.dns		-
san.email		-
san.ip		-
san.uri		-
ts		1398913046.965874
type		bro-x509_log

ELK Stack

- Goal: To push our Bro logs through the stack and display our findings through Kibana.
- Problems:
  - Where to start off
  - Kibana interface

Project Outcomes

Sandia National Laboratories

- Bro is powerful
- Could and should be used in concert with current software
- Future Bro expansions
  - Formatting (epoch problem)
  - Pivoting between Bro and current software

Internship Outcomes

- Sandia plays an integral role in the National Mission
- Nukes are pretty neat
- This internship should be extended to a longer period

Acknowledgements

- Staci Dorsey
- Dr. Alex Roesler
- Mayuri Shakamuri, Jay Patel, and Ryan Birmingham
- David Reed
- Cherri Porter
- MIDN 2/c Jason Mapa and MIDN 1/c Joseph Zobel
- The people of the CCD