SAND2016-6898C

The Center for Cyber Defenders

Expanding computer security knowledge

TracerFIRE Forensic Team

Aliyah Carter, Norfolk State University;
Ryan Jacobson, University of California, Santa Cruz; Katrina Gilmore, Paine College

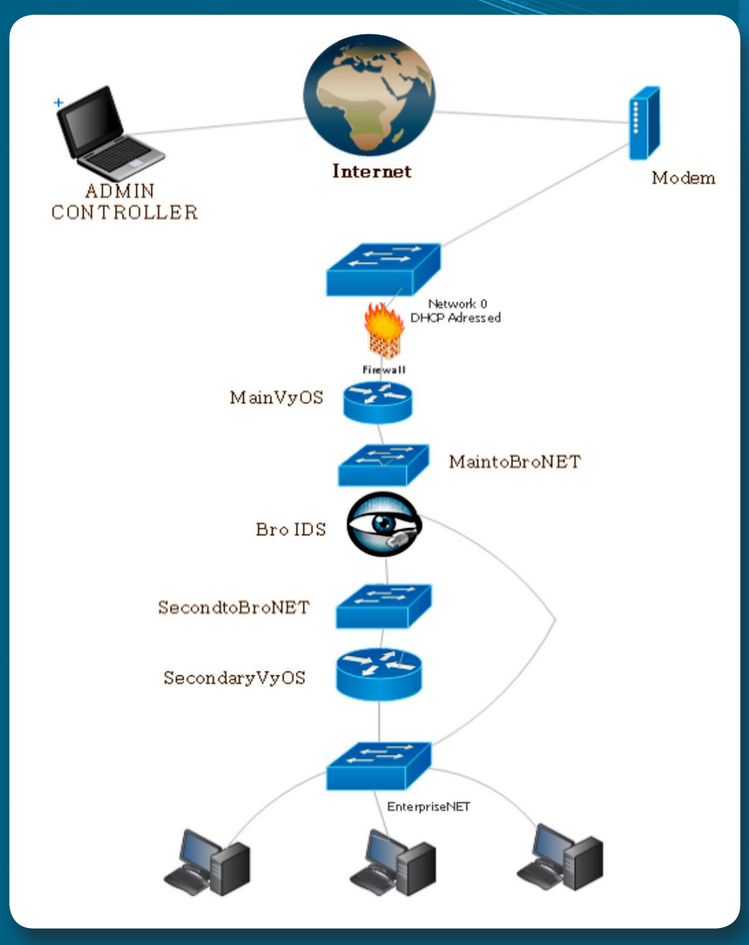
Project Mentor: SeanMichael Galvin, Org. 9312

Problem Statement:

As the use of technology increases the need for cyber security escalates. Without security efforts malicious hackers attempting to compromise or steal information can enter a system without being detected. TracerFIRE uses several tools to protect from and analyze malware but this Forensics team specifically focused on the Bro Network Security Monitor. TracerFire is incorporating Bro into the competition in order to give players a closer look at what exploits look like in real-time.

```
root@ubuntu: /opt/bro/logs/current
root@ubuntu:/opt/bro/logs/current# ls
communication.log  dns.log             packet_filter.log  stdout.log
conn.log           known_services.log  reporter.log       weird.log
dhcp.log           loaded_scripts.log  stderr.log
root@ubuntu:/opt/bro/logs/current#
```

The Bro Network Security Monitor:



Objective and Approach of Bro IDS:

- The Bro software serves as a flexible network traffic analyzer
- The framework of the software differs from other IDS's because it allows users to write specific policy scripts which filter results from large amounts of traffic.
- Bro provides users with real time traffic monitoring, and separates the packets received into a set of log files based on the different network activity. A few examples of log files:
  - conn.log - all connections formed on the network
  - http.log - only HTTP connections
  - files.log - all files transferred over the network
  - weird.log - all unexpected protocol-level activity

```
aliyah@ubuntu: /opt/bro/bin
aliyah@ubuntu:/opt/bro/bin$ sudo ./broctl
[sudo] password for aliyah:

Welcome to BroControl 1.4

Type "help" for help.

[BroControl] > start
'starting bro ...
[BroControl] > capstats

Interface              kpps       mbps       (10s average)
-----------------------------------------
localhost/eth0         0.0        0.0
[BroControl] >
```

Impact and Benefits:

Using a network security traffic analyzer such as Bro can improve a users chance of understanding network traffic as a whole as well as the different categories of traffic and how each could potentially be a security risk. In addition to the library of pre-loaded scripts, Bro provides a framework for users to create and manage their own network monitoring scripts to implement site-specific policies. It provides an integrated method for detecting and automatically responding to threats on the network. Incorporating Bro into TracerFire will give attendees hands-on training when dealing with live malware on a network.

Results:

- Analyzed network traffic in real time using provided logs
- Created policies to notify/respond to threats
- Analyzed Bro packet capture file in to identify malicious code

```
3.48    443     tcp     -       -       -       -       OTH     T       F       0
:       0       0       0       0       (empty)
1467991894.723613       CZVWYr4CTDlV1E34H3      192.168.61.133  54471   162.213.
3.48    443     tcp     -       -       -       -       OTH     T       F       0
:       0       0       0       0       (empty)
1467991900.696304       CPcRni2Q35e63E4Vce      192.168.61.133  59914   162.213.
3.49    443     tcp     -       -       -       -       OTH     T       F       0
:       0       0       0       0       (empty)
1467991901.695883       CFCe4U21dG7ZI70Xjk      192.168.61.133  59914   162.213.
3.49    443     tcp     -       -       -       -       OTH     T       F       0
:       0       0       0       0       (empty)
1467991900.696033       CXrfajK4PxTaX2A36       192.168.61.133  54471   162.213.
3.48    443     tcp     -       -       -       -       RSTRH   T       F       0
:       0       0       1       40      (empty)
1467991903.699565       C4e3wW3bg9qvyqPfj1      192.168.61.133  59914   162.213.
3.49    443     tcp     -       -       -       -       OTH     T       F       0
:       0       0       0       0       (empty)
1467991907.707988       CIPqNXbl6wxtrcLt8       192.168.61.133  59914   162.213.
3.49    443     tcp     -       -       -       -       OTH     T       F       0
:       0       0       0       0       (empty)
1467991915.715873       CeScaq3z5TSlfwPaI       192.168.61.133  59914   162.213.
3.49    443     tcp     -       -       -       -       OTH     T       F       0
:       0       0       0       0       (empty)
```

Sandia National Laboratories
LOCKHEED MARTIN

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-84AL8500. SAND2016-XXXXC.

U.S. DEPARTMENT OF ENERGY
NNSA National Nuclear Security Administration