STAC Reference Platform[1]

1 Introduction

The following sections will detail the configuration of the STAC Reference Platform; consisting of:

- Hardware Platform (NUC)
- Disk partitions and volumes on the NUC SSD
- File System installed on the volumes
- Linux Kernel
- Linux Distribution
- Daemons started by Systemd
- Docker Server
- Docker Containers
- Challenge Programs and STAC Baseline Image
- Procedures for performing reference installation
- Reference Network Environment Configuration

2 Hardware

The hardware Platform will be a NUC, model NUC5i5RYH, with following key specifications:
(http://www.intel.com/content/www/us/en/nuc/nuc-kit-nuc5i5ryh.html)

- CPU
  - Intel(R) Core(TM) i5-5250U CPU @ 1.60GHz
    (http://ark.intel.com/products/84984/Intel-Core-i5-5250U-Processor-3M-Cache-up-to-2_70-GHz)
    - Two 64-bit Cores, each with base operating frequency of 1.6GHz
      - Support Intel Turbo Boost up to 2.7GHz however this will be disabled through BIOS for the reference platform
      - Support Intel Speed Step for lower frequency operation (will disable frequency reduction through cpupower.service configuration)
      - Support Intel Hyper Threading, providing 2 logical processors per Core for a total of 4 logical processors
    - Front Side Bus frequency of 1600 MHz

[1] The Apogee Research effort on STAC is funded by the United States Airforce Research Lab (AFRL) and the Defense Advanced Research Projects Agency (DARPA) under Contract Number FA8750-15-C-0089. THE VIEWS AND CONCLUSIONS CONTAINED IN THIS DOCUMENT ARE THOSE OF THE AUTHORS AND SHOULD NOT BE INTERPRETED AS REPRESENTING THE OFFICIAL POLICIES, EITHER EXPRESSED OR IMPLIED, OF THE DEFENSE ADVANCED RESEARCH PROJECTS AGENCY OR THE US GOVERNMENT.

- Memory Architecture
  - L1 cache (32 KiB I-cache, 32 KiB D-cache per Core)
  - L2 cache (256 KiB per Core)
  - L3 cache (3 MiB)
  - External Memory: 16GiB DDR3L, 1333/1600MHz (64 bit) – max transfer rate of 25.6GB/s
    (Memory Crucial 16GiB Kit 2-8GiB PC3-12800 DDR3 KIT - Model # ct2kit102464BF160B)
- Storage
  - 250 GB SSD (Samsung 850 EVO M.2 Sata 6Gb/s - Model # mz-n5e250bw)
    (see disk partitioning below)
- Network
  - 10/100/1000 Mbps Ethernet (Wi-Fi disabled)
    MTU size of loopback interface will be configured as 1500

3 Disk Partitioning and Logical Volumes

The solid state drive (/dev/sda) will be partitioned as follows:

- sda1: 200 MiB for EFI, GRUB2
- sda2: 500 MiB for kernel images
- sda3: 68 GiB, managed by LVM2 as 3 logical volumes:
  - centos-root (root filesystem, mounted at '/'): 50 GiB
  - centos-home (user home directories, mounted at '/home/') : 10 GiB
  - centos-swap (swap space) 8000 MiB
- sda4: 40 GiB, managed by LVM2 as 2 logical volumes:
  - vg-docker-data (pool of data for docker images): 35 GiB
  - vg-docker-metadata (metadata for managing above pool): 4.9 GiB
- sda5: Optional 20 GiB "Hot Partition" for installation of Docker Images on "Bare Metal"

4 File System

XFS File-system will be installed on centos-root and centos-home volumes.

5 Linux Kernel

The Linux kernel will be 3.10.0:

- 64 bit kernel 3.10.0-229.el7.x86_64
- Started as follows by GRUB2:

```
/vmlinuz-3.10.0-229.el7.x86_64 root=/dev/mapper/centos-root ro
rd.lvm.lv=centos/root rd.lvm.lv=centos/swap crashkernel=auto rhgb
quiet LANG=en_US.UTF-8
```

- For this engagement, no restrictions on processor selection will be enforced upon the kernel scheduler. All four logical processors (2 cores, each with 2 logical processors due to hyper

threading) may be allocated by the kernel scheduler to each thread, as well as the interrupt handlers.

Detailed kernel configuration may be provided separately.

6 Linux Distribution

The Linux distribution will be Centos 7:

- CentOS Linux release 7.1.1503 (Core)
- Minimal installation w. Ethernet enabled (DHCP) (as reference, see anaconda-ks.cfg below)
- Systemd target “multi-user.target” (login through ssh or console)
- User ‘stac’ with ‘/home/stac’ home directory and ‘wheel’ group membership (for sudo access)

```
#version=RHEL7
# System authorization information
auth --enableshadow --passalgo=sha512
# Use CDROM installation media
cdrom
# Use graphical install
graphical
# Run the Setup Agent on first boot
firstboot –enable
ignoredisk --only-use=sda
# Keyboard layouts
keyboard --vckeymap=us --xlayouts='us'
# System language
lang en_US.UTF-8
# Network information
network  --bootproto=dhcp --device=enp0s25 --ipv6=auto –activate
network  --hostname=localhost.localdomain
#Root password
rootpw –lock
# System timezone
timezone America/New_York –isUtc
user --groups=wheel --name=stac --
password=$6$O41JeGbbtBigPt6Z$d.lhTowUG.iFIJFC/BnOfiICrBuk57qJK1fbLDNXqtqs2EN0C3
me.Ainliq5yoVd.Nlbl/.Uzn5Xy/sXKy.9T0 --iscrypted --gecos="stac"
# System bootloader configuration
bootloader --append=" crashkernel=auto" --location=mbr --boot-drive=sda
# Partition clearing information
clearpart  --initlabel --list=sda5,sda4,sda3,sda2,sda1
# Disk partitioning information
part /boot --fstype="xfs" --ondisk=sda --size=500
part pv.695 --fstype="lvmpv" --ondisk=sda --size=69448
part /boot/efi --fstype="efi" --ondisk=sda --size=200 --
fsoptions="umask=0077,shortname=winnt"
volgroup centos --pesize=4096 pv.695
logvol /  --fstype="xfs" --size=51200 --name=root --vgname=centos
logvol swap  --fstype="swap" --size=8000 --name=swap --vgname=centos
logvol /home  --fstype="xfs" --size=10240 --name=home --vgname=centos
%packages
@core
```

```
kexec-tools
%end
%addon com_redhat_kdump --enable --reserve-mb='auto'
%end
```

7 Daemons

The minimal installation includes the following running daemons (after the install script described in section 11 has installed `docker`, and disabled `firewalld, tuned, crond, Postfix, and NetworkManager`):

```
systemd-journal
lvmetad
systemd-udevd
auditd
irqbalance
rsyslogd
systemd-logind
dbus-daemon
login
sshd
dhclient
docker
```

Note: In future engagements, the `irqbalance` daemon may become configured such as to process interrupts on specific processors.

8 Docker Server

Docker will be installed on the reference platform:

- Docker version 1.9.1 (docker-engine-1.9.1-1.el7.centos.x86_64.rpm); installed through a script provided by STAC-EL (see section 11).
- The following Docker configuration options will be set; such as to apply direct-lvm storage (dedicated volumes for storage of docker images; managed as a pool of logical volumes)
  - –storage-driver=devicemapper
  - –storage-opt dm.datadev=/dev/vg-docker/data
  - –storage-opt dm.metadatadev=/dev/vg-docker/metadata
- The following Docker configuration option will be set; such as to apply XFS filesystem for docker images:
  - –storage-opt dm.fs=xfs
- The following Docker configuration option will be set; as workaround for a bug in docker related to Systemd management of Docker cgroup settings (the default w/o this option):
  - –exec-opt native.cgroupdriver=cgroupfs
- The Linux user ‘stac’ will be added to the Linux group ‘docker’, such as to allow execution of docker commands without sudo.

9 Docker Containers

Challenge Programs will be managed as Docker Containers, hosted by a STAC Docker Registry installed on the reference platform. Challenge Programs will be pulled and run from this STAC Registry through a script (`manage_stac_docker_registry_<version>.sh`).

- Challenge Programs will be run within Docker Containers; started with the following options:
  - –net=host (in order to disable NAT'ing between Docker container and localhost)
- No (cgroup) restrictions will be enforced on Docker Containers for access to the resources of the reference platform.

10 Challenge Programs and STAC Baseline Image

Challenge Programs will be Java bytecode, run within a Docker Container consisting of an XFS filesystem with the following layers:

- STAC Base Image:
  - Centos 7.1.1503 (tag centos:7.1.1503 from `hub.docker.com`)
    - No services/daemons running within container unless installed by Challenge Program
  - Java Runtime Environment java-1.8.0-openjdk-1:1.8.0.65-2.b17.el7_1.x86_64.rpm (available at http://vault.centos.org/7.1.1503/updates/x86_64)
- Challenge Program and its dependencies
  - Challenge Programs will be run with JIT enabled

11 Installation Walk-through

The following describes procedures for performing a STAC Reference Installation on a fresh NUC:

1) Connect NUC to a monitor, keyboard, mouse, and Ethernet (with DHCP server reachable on the network)

2) Disable Intel Turbo Boost through BIOS Settings (boot + f2)

3) Install CentOS 7.1.1503 from Minimal Installation CD/DVD, as downloaded from e.g.:

   `http://vault.centos.org/7.1.1503/isos/x86_64/CentOS-7-x86_64-Minimal-1503-01.iso`

   NOTE: After powering up the NUC, press F10, then select the **UEFI** Bootloader option from the CD/DVD.

   Apply following selections:

   - Select "Minimal Install" with no Add-Ons
   - Select "I will configure partitioning", do not select "Encrypt my data"

- Configure the following partitions:
  - /boot/efi
    - Mount Point /boot/efi
    - Device Type "Standard Partition"
    - File System "EFI System Partition"
    - Desired Capacity 200MiB
  - /boot
    - Mount Point /boot
    - Device Type “Standard Partition”
    - File System XFS
    - Desired Capacity 500MiB
  - /
    - Mount Point /
    - Device Type LVM
    - File System XFS
    - Volume Group centos
    - Name root
    - Desired Capacity 50 GiB
  - /home
    - Mount Point /home
    - Device Type LVM
    - File System XFS
    - Volume Group centos
    - Name home
    - Desired Capacity 25 GiB
  - Swap
    - Mount Point : None
    - Device Type LVM
    - File System swap
    - Volume Group centos
    - Name swap
    - Desired Capacity 8000 MiB
- Select following network settings:
  - Ethernet ON
  - Wireless OFF
- Create stac user:
  - Full name stac
  - User name stac
  - Make user administrator
  - Require a password to use this account
  - Password stacme (click Done twice since password is weak)

4) Following CentOS installation, reboot and login as stac. Then determine the IP address assigned by DHCP by typing “`ip addr list`”

5) Download the following "STAC Reference Platform Configuration" script, found in the STAC GIT Repository to the NUC (e.g. using scp):

```
STAC_Reference_Platform_Install.v2.3.sh
```

6) From the NUC (console or through ssh connection), run the script:

```
sudo ./STAC_Reference_Platform_Install.v2.3.sh all
```

The script will remove some daemons, install the `cpupower Systemd` service, and finally download and install the `docker` service.

7) Reboot the NUC

12 Reference Network Environment

For Engagement 5 onward, we will be moving from the current localhost implementation of all server and client interactions. This section provides configurations for the reference network environment as well as an example implementation of the reference network configuration to be used by Apogee for testing future challenge programs. The reference network environment components are as follows:

- 2 NUCs running the reference platform established in sections 1 through 11 of this document
- 1 Netgear GS108Ev3 managed switch
- 1 device (unspecified configuration; we use a NUC running the reference platform) for observing packets on the mirrored port
- Optional: 1 device for managing and monitoring the switch (we use a laptop running windows 10)

Given that the specs of the refence network environment have been enumerated we will proceed to setup the switch.

12.1 Switch Configuration Walk-through

The Netgear GS108Ev3 switch can be configured by navigating to the device IP address. Ensure that the switch is not connected to a DHCP server during the entire configuration process. To access the web-management interface:

1) Connect a device with a browser to any of the ports on the switch, and navigate to the default static IP address (192.168.0.239). Before you can navigate to the switch address the network interface card (NIC) connected to the switch must have the same 192.168.0.x IP address name and the same 255.255.255.0 subnet mask. Instructions for implementing these settings are as follows:
    a. Windows 10 OS:
        i. Control Panel → *Control Panel\Network and Internet\Network and Sharing Center*

ii. Right click on network device connected to switch and click on *properties* tab
iii. Click on *Internet Protocol Version 4 (TCP/IPv4)* and click on *properties* tab
iv. Set IP address to *192.168.0.90* and subnet mask to *255.255.255.0*. Leave default gateway field empty.

b. CentOS 7:
i. Navigate to */etc/sysconfig/network-scripts*
ii. Identify the network interface config file (e.g *ifcfg-enp0s25*) and save a copy before proceeding
iii. Ensure that the following settings are changed:
1. *TYPE="Ethernet"*
2. *BOOTPROTO="static"*
3. *IPADDR="192.168.0.90"*
4. *NETMASK="255.255.255.0"*
iv. Run *sudo ifdown <device name e.g enp0s25>*
v. Run *sudo ifup <device name e.g enp0s25>*

2) Use the default username *admin* (may not be required) and default password *password* to log in.
3) Upgrade to firmware version 2.00.09
a. Download the firmware upgrade from: http://www.downloads.netgear.com/files/GDC/GS108EV3/GS108Ev3_V2.00.09.zip
b. Unzip the file
c. In the web interface navigate to the *System* tab then the *Maintenance* tab
d. Click on the *Firmware Upgrade* link
e. Click on the *Enter Loader Mode* link
f. Click on the *Firmware Upgrade* link and browse to the *GS108Ev3_V2.00.09.bin* file extracted from the *GS108Ev3_V2.00.09.zip* file
g. Wait for the firmware upgrade to complete and the switch to reboot
4) Log in with the default password *password* to the web-management interface
5) Proceed to the *System* tab then the *Maintenance* tab
6) Download the *GS108Ev3.cfg* file from the *STAC* repo
7) Click on the *Restore Configuration* link and browse to the *GS108Ev3.cfg* file
8) Wait for the settings to be loaded and the switch to reboot. The updated settings are as follows:
a. Change of the Switch Name to *STAC Switch*
b. DHCP Mode Disabled
c. Change of the switch IP address to 192.168.100.50
d. Change of the switch subnet mask to 255.255.255.0
e. Change of the switch gateway address to 192.168.100.1
f. Change of the port mirroring configuration to mirror port 2 and port 4 traffic on port 3

Note: the port mirroring configuration is required for the reference network environment; however, the specific ports used and the specific assigned IP addresses, subnet mask, and gateway address are not required. Teams may choose to use

different values but these are the values and specific configurations that will be used to test engagement challenges.

9) Use the instructions in "1)" to change the IP address of the device connected to the switch to a *192.168.100.x* name e.g *192.168.100.90* and ensure that the device is connected to a port other than 1,2,3 or 4.
10) Log in with the default password *password* to the web-management interface and confirm that the settings in "8)" are applied.

12.2 Network Configuration

As stated in the previous section the reference network environment calls for 2 NUCs running the reference hardware, a Netgear GS108Ev3 switch running firmware version 2.00.09 and the configurations specified in the *GS108Ev3.cfg*, and a device of unspecified configuration to be used for monitoring traffic on the mirrored port (set as port 2 traffic mirrored to port 3 for EL configuration). The device configuration used by the EL is as follows:

Device	Static IPv4 Address	Switch Port Number
Reference NUC A (Remote/Server Device)	192.168.100.20	1
Reference NUC B (Benign User Device)	192.168.100.30	2
Mirrored port monitor NIC (Device #3)	NA	3
Attacker NIC (Device #3)	192.168.100.10	4
Optional Switch setup/maintenance PC	192.168.100.90	8
Netgear GS108Ev3 Switch	192.168.100.50	NA

*Device #3 is a single device of unspecified configuration with two network interface cards (NICs) that serves as both the observable instrument and the attacker device when required.

To allow for the mirrored port NIC to capture all traffic, the device must be set to *promiscuous mode*. Instructions to setup *promiscuous mode* in Windows 10 are as follows:

- Assuming the use of *Wireshark* to collect packet data, under *Capture* → *Options*, ensures that *Promiscuous* is *enabled* on the interface to be used for capture

Instructions to setup *promiscuous mode* in CentOS 7 are as follows:

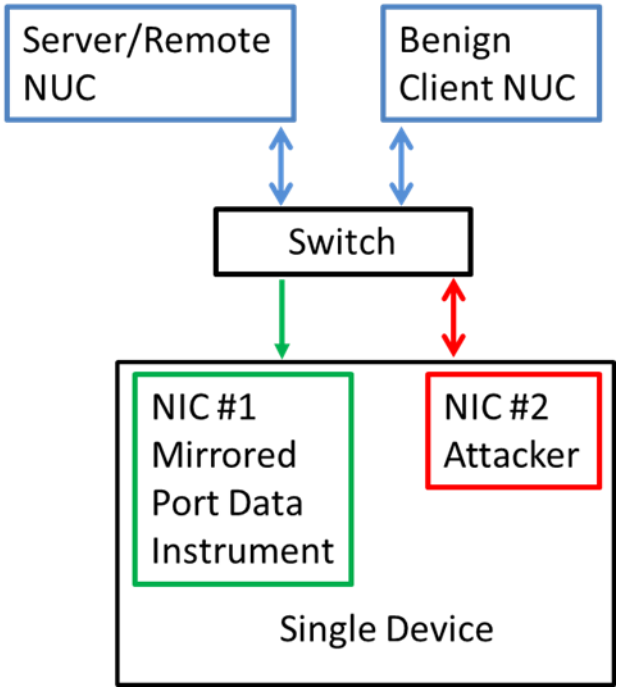
- In command line enter: *sudo ip link set <device e.g. enp0s25> promisc on*

12.3 Observing Vulnerabilities

Sections 12.1 and 12.2 establish the reference network environment requirements and provide an example implementation. This section provides further details on how vulnerabilities as specified in the E5+ operational definition document (*2017-03-24-opdef-v08.0*) will be measured.

The reference network environment has 2 NUCs running the reference hardware. One of these NUCs will **always** serve as the remote or server device; the other will **always** serve as the benign user device. Device #3 has two NICs, one listening on the mirrored port of the switch and the other which will, in cases where an active attacker is needed, be used to send the attack to the server/remote device.

Device #3 has an unspecified configuration; the EL will be using a NUC running the reference platform. Since the reference platform only has one NIC, we have attached a USB-to-Ethernet device (*StarTech USB 3.0 to Gigabit Ethernet NIC* model number: *USB31000SW*). In the EL's configuration, we use the USB-to-Ethernet device (NIC #1) as the NIC for collecting data on STAC observables (e.g. timing, packet sizes etc.). The internal NIC (NIC #2) which came with the NUC is used as the attacker when an active attacker is required. The diagram below shows the resulting network configuration.



NIC #1 collects data from both the active attacker's interaction and from the benign client's interaction. For algorithmic complexity attacks, the attacker does not have access to the data collected on NIC #1. The data collected on NIC #1 will be used to confirm the success of a remote-DoS AC Time attack (see *2017-03-24-opdef-v08.0*). The success of an AC Space attack will be confirmed via an observable (e.g. disk space, RSS memory usage etc.) on the server/remote NUC. The success of a self-DoS AC Time attack will continue to be confirmed via the time from the command submission to the applications response measured on a single reference platform NUC.

For side channel attacks, the attacker has access to the data collected on NIC #1. Note that all observables provided in the side channel challenge question must be observed through NIC #1.