GreHack WorkShop - System introspection for Web Offensive Research with Sysdig

Hello you !
Please be sure to have all these prerequisites working with similar expected output to not start the workshop with a half-broken sysdig setup, and prevent network issues during the session!
If you have everything described below, little to no internet connection will be required during the training! 🎉

Prerequisites 1 : Sysdig docker

Run the following :

```
sudo docker run --name sysdig --rm -i -t --privileged --net=host -v /var/run/docker.sock:/host/var/run/docker.sock
-v /dev:/host/dev -v /proc:/host/proc:ro -v /boot:/host/boot:ro -v /src:/src -v /lib/modules:/host/lib/modules:ro
-v /usr:/host/usr:ro -v /etc:/host/etc:ro docker.io/sysdig/sysdig sysdig -A container.name=sysdig
```

Expected result :

```
* Setting up /usr/src links from host
* Running scap-driver-loader for: driver version=3.0.1+driver, arch=x86_64, kernel release=5.15.0-82-generic,
kernel version=91
* Running scap-driver-loader with: driver=module, compile=yes, download=yes

================ Cleaning phase ================

* 1. Check if kernel module 'scap' is still loaded:
- Kernel module 'scap' is still loaded.
- Trying to unload it with 'rmmod scap'...
- OK! Unloading 'scap' module succeeded.

* 2. Check all versions of kernel module 'scap' in dkms:
- OK! There are no 'scap' module versions in dkms.

[SUCCESS] Cleaning phase correctly terminated.

================ Cleaning phase ================

* Looking for a scap module locally (kernel 5.15.0-82-generic)
* Filename 'scap_ubuntu-generic_5.15.0-82-generic_91.ko' is composed of:
 - driver name: scap
 - target identifier: ubuntu-generic
 - kernel release: 5.15.0-82-generic
 - kernel version: 91
* Trying to download a prebuilt scap module from
https://download.sysdig.com/scap-drivers/3.0.1%2Bdriver/x86_64/scap_ubuntu-generic_5.15.0-82-generic_91.ko
curl: (22) The requested URL returned error: 404
Unable to find a prebuilt scap module
* Trying to dkms install scap module with GCC /usr/bin/gcc
DIRECTIVE: MAKE="'/tmp/scap-dkms-make'"

Creating symlink /var/lib/dkms/scap/3.0.1+driver/source ->
                 /usr/src/scap-3.0.1+driver

DKMS: add completed.

Kernel preparation unnecessary for this kernel.  Skipping...

Building module:
cleaning build area...
'/tmp/scap-dkms-make'....
cleaning build area...

DKMS: build completed.

scap.ko:
Running module version sanity check.
 - Original module
```

```
   - No original module exists within this kernel
 - Installation
   - Installing to /lib/modules/5.15.0-82-generic/extra/
Adding any weak-modules
weak-modules: could not find dracut at /usr/bin/dracut

depmod...

DKMS: install completed.
* scap module installed in dkms
* scap module found: /var/lib/dkms/scap/3.0.1+driver/5.15.0-82-generic/x86_64/module/scap.ko
* Trying insmod
* Success: scap module found and loaded in dkms
25 10:57:59.869232687 2 sysdig (18510.18510) > switch next=0 pgft_maj=0 pgft_min=4010 vm_size=184704 vm_rss=23520
vm_swap=0
```

Prerequisites 2 : Php docker

Run the following :

```
docker run --rm -it --net=host --name php php:8 php -S 0.0.0:8000
curl http://127.0.0.1:8000/
```

Expected result :

```
[Thu Sep 14 11:06:46 2023] PHP 8.2.10 Development Server (http://0.0.0:8000) started
[Thu Sep 14 11:06:50 2023] 127.0.0.1:42496 Accepted
[Thu Sep 14 11:06:50 2023] 127.0.0.1:42496 [404]: GET / - No such file or directory
[Thu Sep 14 11:06:50 2023] 127.0.0.1:42496 Closing

<!doctype html><html><head><title>404 Not Found</title><style>
```

Prerequisites 3 : Jolokia docker

Run the following :

```
docker run --rm -it --net=host --name jolokia bodsch/docker-jolokia
curl http://127.0.0.1:8080/jolokia
```

Expected result :

```
Using CATALINA_BASE:   /opt/tomcat
Using CATALINA_HOME:   /opt/tomcat
Using CATALINA_TMPDIR: /opt/tomcat/temp
Using JRE_HOME:        /usr/lib/jvm/default-jvm
Using CLASSPATH:       /opt/tomcat/bin/bootstrap.jar:/opt/tomcat/bin/tomcat-juli.jar
Using CATALINA_PID:    /opt/tomcat/temp/catalina.pid
NOTE: Picked up JDK_JAVA_OPTIONS:  --add-opens=java.base/java.lang=ALL-UNNAMED
--add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
NOTE: Picked up JDK_JAVA_OPTIONS:  --add-opens=java.base/java.lang=ALL-UNNAMED
--add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be
removed in a future release.
[0.016s][warning][gc,ergo] NewSize was set larger than initial heap size, will use initial heap size.
14-Sep-2023 11:03:54.149 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server version name:
Apache Tomcat/9.0.16
14-Sep-2023 11:03:54.150 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server built:
Feb 4 2019 16:30:29 UTC
14-Sep-2023 11:03:54.151 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server version number:
9.0.16.0
14-Sep-2023 11:03:54.151 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log OS Name:
Linux
14-Sep-2023 11:03:54.151 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log OS Version:
5.15.0-82-generic
14-Sep-2023 11:03:54.151 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Architecture:
amd64
14-Sep-2023 11:03:54.151 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Java Home:
/usr/lib/jvm/java-11-openjdk
14-Sep-2023 11:03:54.151 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Version:
11.0.8+11-alpine-r0
```

14-Sep-2023 11:03:54.151 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Vendor:
Alpine
14-Sep-2023 11:03:54.151 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_BASE:
/opt/apache-tomcat-9.0.16
14-Sep-2023 11:03:54.151 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_HOME:
/opt/apache-tomcat-9.0.16
14-Sep-2023 11:03:54.153 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
--add-opens=java.base/java.lang=ALL-UNNAMED
14-Sep-2023 11:03:54.153 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
--add-opens=java.base/java.io=ALL-UNNAMED
14-Sep-2023 11:03:54.153 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
--add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
14-Sep-2023 11:03:54.153 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
--add-opens=java.base/java.lang=ALL-UNNAMED
14-Sep-2023 11:03:54.153 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
--add-opens=java.base/java.io=ALL-UNNAMED
14-Sep-2023 11:03:54.153 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
--add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
14-Sep-2023 11:03:54.153 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
-Djava.util.logging.config.file=/opt/tomcat/conf/logging.properties
14-Sep-2023 11:03:54.153 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
-Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
14-Sep-2023 11:03:54.154 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
-Djdk.tls.ephemeralDHKeySize=2048
14-Sep-2023 11:03:54.154 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
-Djava.protocol.handler.pkgs=org.apache.catalina.webresources
14-Sep-2023 11:03:54.154 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
-Dorg.apache.catalina.security.SecurityListener.UMASK=0027
14-Sep-2023 11:03:54.154 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
-Xms256M
14-Sep-2023 11:03:54.154 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
-Xmx1025m
14-Sep-2023 11:03:54.154 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
-XX:NewSize=256m
14-Sep-2023 11:03:54.154 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
-XX:MaxNewSize=256m
14-Sep-2023 11:03:54.154 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
-XX:+DisableExplicitGC
14-Sep-2023 11:03:54.154 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
-XX:HeapDumpPath=/var/logs/
14-Sep-2023 11:03:54.154 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument:
-XX:+HeapDumpOnOutOfMemoryError

{"request":{"type":"version"},"value":{"agent":"1.6.0","protocol":"7.2","config":{"listenForHttpService":"true","ma
xCollectionSize":"0","authIgnoreCerts":"false","agentId":"192.168.8.23-12-5baaae4c-servlet","agentType":"servlet","
policyLocation":"classpath:\/jolokia-access.xml","agentContext":"\/jolokia","mimeType":"text\/plain","discoveryEnab
led":"false","streaming":"true","historyMaxEntries":"10","allowDnsReverseLookup":"true","maxObjects":"0","debug":"f
alse","serializeException":"false","detectorOptions":"{}","dispatcherClasses":"org.jolokia.jsr160.Jsr160RequestDisp
atcher","maxDepth":"15","authMode":"basic","canonicalNaming":"true","allowErrorDetails":"true","realm":"jolokia","i
ncludeStackTrace":"true","useRestrictorService":"false","debugMaxEntries":"100"},"info":{"product":"tomcat","vendor
":"Apache","version":"9.0.16"}},"timestamp":1694689508,"status":200}

Prerequisites 4 : Up Your Spip Lab ! :]

Run the following :

```
mkdir grehack-spip
cd grehack-spip
git clone https://github.com/ashledombos/docker-spip
cd docker-spip/compose_samples
sudo docker-compose -f docker-compose.txt up --build --force-recreate --remove-orphans
# Then login with the account admin:adminadmin at
http://127.0.0.1:13080/spip.php?page=login
# Ensure everything works, that you can create articles, sections, accounts, etc!
```

Expected result :

```
Cloning into 'docker-spip'...
remote: Enumerating objects: 588, done.
remote: Counting objects: 100% (77/77), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 588 (delta 64), reused 61 (delta 61), pack-reused 511
Receiving objects: 100% (588/588), 118.02 KiB | 3.11 MiB/s, done.
Resolving deltas: 100% (249/249), done.
Recreating compose_samples_mysql_1 ... done
Recreating compose_samples_php_1   ... done
Recreating compose_samples_apache_1 ... done
Attaching to compose_samples_mysql_1, compose_samples_php_1, compose_samples_apache_1
apache_1  | [Thu Sep 28 12:30:21.798095 2023] [mpm_event:notice] [pid 1:tid 139913273707336] AH00489: Apache/2.4.48
(Unix) configured -- resuming normal operations
apache_1  | [Thu Sep 28 12:30:21.798131 2023] [core:notice] [pid 1:tid 139913273707336] AH00094: Command line:
'/usr/local/apache2/bin/httpd -D FOREGROUND'
mysql_1   | [i] mysqld not found, creating....
mysql_1   | [i] MySQL directory already present, skipping creation
mysql_1   | 2023-09-28 12:30:21 0 [Note] /usr/bin/mysqld (server 10.6.11-MariaDB) starting as process 1 ...
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: Compressed tables use zlib 1.2.13
php_1     | Setting SPIP core in /var/www/html/core/
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: Number of pools: 1
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: Using crc32 + pclmulqdq instructions
mysql_1   | 2023-09-28 12:30:21 0 [Note] mysqld: O_TMPFILE is not supported on /var/tmp (disabling future attempts)
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: Using Linux native AIO
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: Initializing buffer pool, total size = 134217728, chunk size =
134217728
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: Completed initialization of buffer pool
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: 128 rollback segments are active.
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: Creating shared tablespace for temporary tables
php_1     | Complete! SPIP has been successfully copied to /var/www/html/core/
php_1     | Move IMG and config in /var/www/html/data/ if needed
php_1     | Apache uses /var/www/html/data/htaccess.txt instead of .htaccess
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: Setting file './ibtmp1' size to 12 MB. Physically writing the file
full; Please wait ...
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: File './ibtmp1' size is now 12 MB.
php_1     | Apache uses /var/www/html/data/htdir.txt for location and directory rules
php_1     | Create and/or link robots-cdn.txt
php_1     | Create plugins, libraries and template directories in /var/www/html/data/ if they don't exist
php_1     | change rights
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: 10.6.11 started; log sequence number 42180; transaction id 14
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: Loading buffer pool(s) from /var/lib/mysql/ib_buffer_pool
php_1     | create all symlinks
php_1     | [28-Sep-2023 12:30:21] NOTICE: fpm is running, pid 1
mysql_1   | 2023-09-28 12:30:21 0 [Note] Plugin 'FEEDBACK' is disabled.
mysql_1   | 2023-09-28 12:30:21 0 [Note] InnoDB: Buffer pool(s) load completed at 230928 12:30:21
php_1     | [28-Sep-2023 12:30:21] NOTICE: ready to handle connections
mysql_1   | 2023-09-28 12:30:21 0 [Note] Server socket created on IP: '0.0.0.0'.
mysql_1   | 2023-09-28 12:30:21 0 [Note] Server socket created on IP: '::'.
mysql_1   | 2023-09-28 12:30:21 0 [Warning] 'user' entry '@356fdbf8d67f' ignored in --skip-name-resolve mode.
mysql_1   | 2023-09-28 12:30:21 0 [Warning] 'proxies_priv' entry '@% root@356fdbf8d67f' ignored in
--skip-name-resolve mode.
mysql_1   | 2023-09-28 12:30:21 0 [Note] /usr/bin/mysqld: ready for connections.
mysql_1   | Version: '10.6.11-MariaDB'  socket: '/run/mysqld/mysqld.sock'  port: 3306  MariaDB Server
php_1     | 172.30.0.4 -  28/Sep/2023:12:30:32 +0000 "GET /index.php" 200
```