Nmap & Flanscan Technical Segment

Paul Asadoorian, Paul's Security Weekly

Episode #709 (https://securityweekly.com/psw709)

Flanscan builds a Docker container with Nmap and the Vulners scripts. It does not build Nmap from source. However, it includes some Python scripts that can output the Nmap XML reports to HTML and even post them to AWS. The project has not been well-maintained, there is a Docker issue in the Makefile and a pull request not accepted that allows for CSV exporting (https://github.com/cloudflare/flan/pull/58). I've not merged the pull request for CSV exporting, but I did find a workaround for the Docker configuration.

```
$ git clone https://github.com/cloudflare/flan.git

$ cd flan

$ vi Makefile

# Original configuration, only adds the NET_RAW capability
html:
docker run --rm --cap-drop=all --cap-add=NET_RAW --name $(container_name) -v
"$(CURDIR)/shared:/shared:Z" -e format=html flan_scan

# I removed the capability filters altogether, and it runs, slightly less secure!
myhtml :
docker run --rm --name $(container_name) -v "$(CURDIR)/shared:/shared:Z" -e format=html
flan_scan

$ make build

$ vi shared/ips.txt

# Enter your target IPs and/or subnets

$  make myhtml

$ head shared/xml_files/2021.08.17-17.28/10.16.1.0-24.xml

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.91 scan initiated Tue Aug 17 17:28:15 2021 as: nmap -sV -oX
/shared/xml_files/2021.08.17-17.28/10.16.1.0-24.xml -oN - -v1 -&#45;script=vulners/vulners.nse
172.16.1.0/24 -->
```

<nmaprun scanner="nmap" args="nmap -sV -oX /shared/xml_files/2021.08.17-17.28/10.16.1.0-24.xml -oN - -v1 --script=vulners/vulners.nse 10.16.1.0/24" start="1629221295" startstr="Tue Aug 17 17:28:15 2021" version="7.91" xmloutputversion="1.05">

View the HTML:

$ **open shared/reports/report_2021.08.17-17.28.html**

What I discovered in that Flanscan uses whatever version comes with Alpine 3.9, which as of a few weeks ago, was an older version of Nmap. I set to create a small container that would build a user-specified version of Nmap with the latest Vulners NSE scripts.

My Dockerfile is as follows:

```
# You can use whatever distro you like, I prefer Ubuntu as that is
# what is installed on my systems, servers and VMs for Linux
FROM ubuntu:20.04

# Tell it which version of Nmap you'd like to build, I tested with
# 7.92
ARG nmap_ver=7.92
ARG build_rev=5

#
# Install all required packages and system dependencies
# I built this in a VM first to get all the requirements
#
RUN set -eux; \
    apt-get update; \
    apt-get install -y --no-install-recommends \
    build-essential \
    libgcrypt20-dev \
    openssl \
    zlib1g \
    ca-certificates \
    libssh-4 \
    liblua5.2-dev \
    libssl-dev \
    libssh2-1-dev \
    curl \
    git \
    ; \
    update-ca-certificates \
    ; \
    rm -rf /var/lib/apt/lists/*
```

```
# Compile and install Nmap from sources and download the vulners
# NSEs
RUN curl -fL -o /tmp/nmap.tar.bz2 \
    https://nmap.org/dist/nmap-${nmap_ver}.tar.bz2 \
    && tar -xjf /tmp/nmap.tar.bz2 -C /tmp \
    && cd /tmp/nmap* \
    && ./configure \
        --prefix=/opt \
        --sysconfdir=/opt/etc \
        --mandir=/opt/share/man \
        --infodir=/opt/share/info \
        --without-zenmap \
        --without-nmap-update \
        --without-ndiff \
        --without-nping \
        --without-ncat \
        --with-openssl=/usr/lib \
        --with-liblua=/usr/include \
    && make \
    && make install \
    && git clone https://github.com/vulnersCom/nmap-vulners \
      /opt/share/nmap/scripts/vulners \
    && /opt/bin/nmap --script-updatedb \
    && rm -rf /tmp/nmap*

ENTRYPOINT ["/opt/bin/nmap"]
```

Next, build the container and run it:

```
$ docker build -t nmap .

$ docker run --rm -it nmap -sV --script vulners 172.16.1.33

Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-28 16:37 UTC
Nmap scan report for leopard.int.psw.io (172.16.1.33)
Host is up (0.0016s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Raspbian 10+deb10u2 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:7.9p1:
|           EDB-ID:21018      10.0  https://vulners.com/exploitdb/EDB-
ID:21018    *EXPLOIT*
|           CVE-2001-0554     10.0  https://vulners.com/cve/CVE-2001-0554
|           MSF:ILITIES/UBUNTU-CVE-2019-6111/   5.8
      https://vulners.com/metasploit/MSF:ILITIES/UBUNTU-CVE-2019-6111/
      *EXPLOIT*
|           MSF:ILITIES/SUSE-CVE-2019-6111/     5.8
      https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2019-6111/
      *EXPLOIT*
```

```
|           MSF:ILITIES/SUSE-CVE-2019-25017/    5.8
      https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2019-25017/
      *EXPLOIT*
|           MSF:ILITIES/REDHAT_LINUX-CVE-2019-6111/   5.8
      https://vulners.com/metasploit/MSF:ILITIES/REDHAT_LINUX-CVE-2019-6111/
      *EXPLOIT*
|           MSF:ILITIES/REDHAT-OPENSHIFT-CVE-2019-6111/     5.8
      https://vulners.com/metasploit/MSF:ILITIES/REDHAT-OPENSHIFT-CVE-2019-
6111/ *EXPLOIT*
|           MSF:ILITIES/ORACLE-SOLARIS-CVE-2019-6111/ 5.8
      https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2019-
6111/ *EXPLOIT*
|           MSF:ILITIES/OPENBSD-OPENSSH-CVE-2019-6111/      5.8
      https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-OPENSSH-CVE-2019-
6111/ *EXPLOIT*
|           MSF:ILITIES/IBM-AIX-CVE-2019-6111/  5.8
      https://vulners.com/metasploit/MSF:ILITIES/IBM-AIX-CVE-2019-6111/
      *EXPLOIT*
|           MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2019-6111/     5.8
      https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-
2019-6111/  *EXPLOIT*
|           MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2019-6111/     5.8
      https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-
2019-6111/  *EXPLOIT*
|           MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-2019-6111/     5.8
      https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP3-CVE-
2019-6111/  *EXPLOIT*
|           MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-2019-6111/     5.8
      https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP2-CVE-
2019-6111/  *EXPLOIT*
|           MSF:ILITIES/GENTOO-LINUX-CVE-2019-6111/   5.8
      https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-CVE-2019-6111/
      *EXPLOIT*
|           MSF:ILITIES/F5-BIG-IP-CVE-2019-6111/      5.8
      https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-CVE-2019-6111/
      *EXPLOIT*
|           MSF:ILITIES/DEBIAN-CVE-2019-6111/   5.8
      https://vulners.com/metasploit/MSF:ILITIES/DEBIAN-CVE-2019-6111/
      *EXPLOIT*
|           MSF:ILITIES/CENTOS_LINUX-CVE-2019-6111/   5.8
      https://vulners.com/metasploit/MSF:ILITIES/CENTOS_LINUX-CVE-2019-6111/
      *EXPLOIT*
|           MSF:ILITIES/AMAZON_LINUX-CVE-2019-6111/   5.8
      https://vulners.com/metasploit/MSF:ILITIES/AMAZON_LINUX-CVE-2019-6111/
      *EXPLOIT*
|           MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-2019-6111/   5.8
      https://vulners.com/metasploit/MSF:ILITIES/AMAZON-LINUX-AMI-2-CVE-
2019-6111/  *EXPLOIT*
|           MSF:ILITIES/ALPINE-LINUX-CVE-2019-6111/   5.8
      https://vulners.com/metasploit/MSF:ILITIES/ALPINE-LINUX-CVE-2019-6111/
      *EXPLOIT*
|           EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8
      https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837
551A19      *EXPLOIT*
|           EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8
      https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD9
7F9E97      *EXPLOIT*
```

```
|           EDB-ID:46516      5.8   https://vulners.com/exploitdb/EDB-
ID:46516    *EXPLOIT*
|           CVE-2019-6111     5.8   https://vulners.com/cve/CVE-2019-6111
|           CVE-2019-16905    4.4   https://vulners.com/cve/CVE-2019-16905
|           MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/     4.3
      https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-
14145/      *EXPLOIT*
|           MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/    4.3
      https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-
2020-14145/ *EXPLOIT*
|           MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/    4.3
      https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-
2020-14145/ *EXPLOIT*
|           MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/    4.3
      https://vulners.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-
2020-14145/ *EXPLOIT*
|           MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/     4.3
      https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/
      *EXPLOIT*
|           CVE-2020-14145    4.3   https://vulners.com/cve/CVE-2020-14145
|           CVE-2007-2768     4.3   https://vulners.com/cve/CVE-2007-2768
|           CVE-2019-6110     4.0   https://vulners.com/cve/CVE-2019-6110
|           CVE-2019-6109     4.0   https://vulners.com/cve/CVE-2019-6109
|           CVE-2018-20685    2.6   https://vulners.com/cve/CVE-2018-20685
|           PACKETSTORM:151227      0.0
      https://vulners.com/packetstorm/PACKETSTORM:151227    *EXPLOIT*
|           EDB-ID:46193      0.0   https://vulners.com/exploitdb/EDB-
ID:46193    *EXPLOIT*
|_          1337DAY-ID-32009  0.0   https://vulners.com/zdt/1337DAY-ID-32009
      *EXPLOIT*
53/tcp open  domain  ISC BIND 9.11.5-P4-5.1+deb10u5 (Raspbian Linux)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.54 seconds

# Save the results to a directory:

$ docker run --rm -v ${PWD}/results:/results:Z nmap -sV --open -oA
/results/scan1 -p 22 172.16.1.1-10

# Next up, create an alias that runs the container version of Nmap:

$ nmap --version
Nmap version 7.80 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1d nmap-libssh2-1.8.2 libz-1.2.11
libpcre-8.39 libpcap-1.9.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

$ alias nmap="docker run --rm -v $(pwd):/results:Z -w /results nmap"

$ nmap --version
Nmap version 7.92 ( https://nmap.org )
Platform: x86_64-unknown-linux-gnu
```

```
Compiled with: nmap-liblua-5.3.5 openssl-1.1.1f libssh2-1.8.0 nmap-libz-
1.2.11 nmap-libpcre-7.6 nmap-libpcap-1.9.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

# Refreshing

$ docker rmi nmap:latest
Untagged: nmap:latest
Deleted:
sha256:5880b4e5022994f78a804ff6698f92414bdad764199beb363d6b7590813cce91
Deleted:
sha256:8c2e1683ad75108ea7033760118abe70b8ecc0de947ad534a8745b1f0c9ca181
Deleted:
sha256:693c7d0ee9a6b04caec9f64aaeac1d783838555afa4f989b2f75345a934668dc
Deleted:
sha256:093e8824df51443cd4ec3ffdbe1564f885eb1e80a80dcb9ef25246b256c78ed0
Deleted:
sha256:bf13df283420ebe56c5493ab8a379696fc3ebbe01612727298cfe3e825f74cd2
Deleted:
sha256:df22f17764631dea6c0a4eff1ea57258918ada3a3a92c72cdd6bf05d5b0a3927
Deleted:
sha256:d124734b86bc42d97648fdefda15152f3bac5015b165047c0717a504fb9ad4b3

$ docker build -t nmap ~/nmap-vulners/.
```