ATTACK DEFENSE

by PentesterAcademy

Name	T1518 : Software Discovery II
URL	https://attackdefense.com/challengedetails?cid=1863
Type	MITRE ATT&CK Linux : Discovery

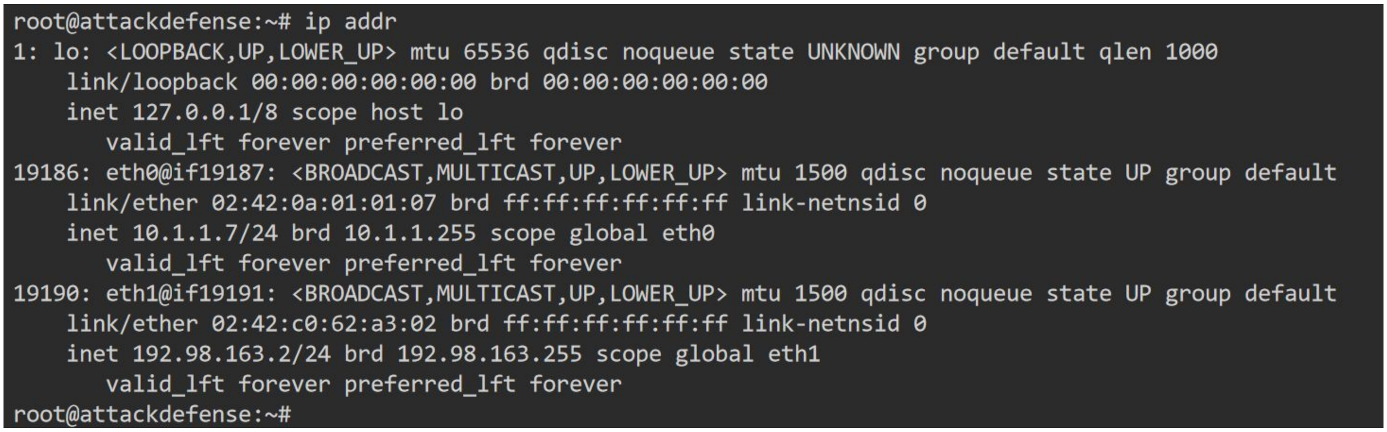
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Identify the softwares installed on the system

Solution:

Step 1: Check the IP address of the attacker machine.

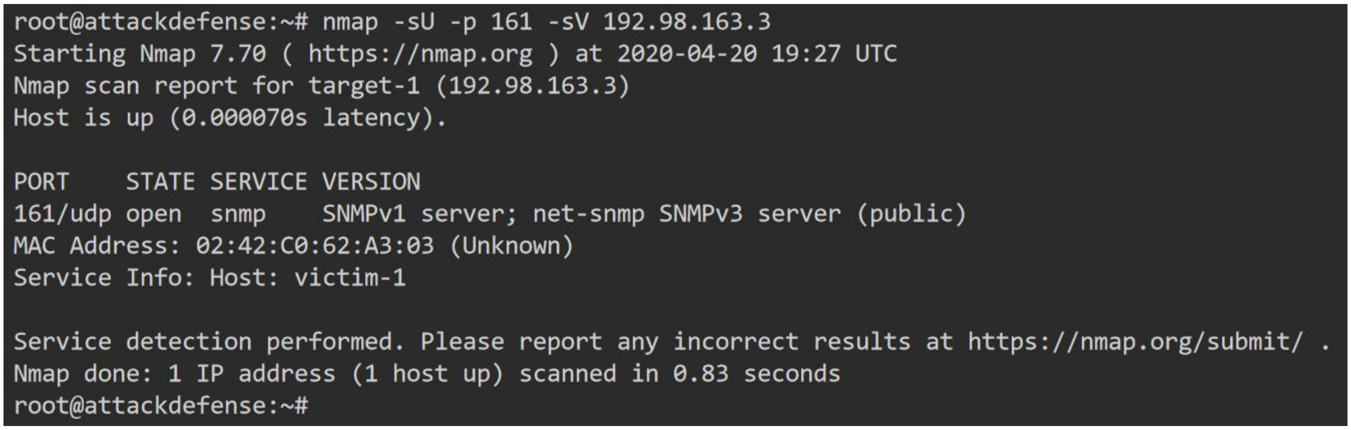
Commands: ip addr



```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
19186: eth0@if19187: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:07 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.7/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
19190: eth1@if19191: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:62:a3:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.98.163.2/24 brd 192.98.163.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Run Nmap scan on the target machine.

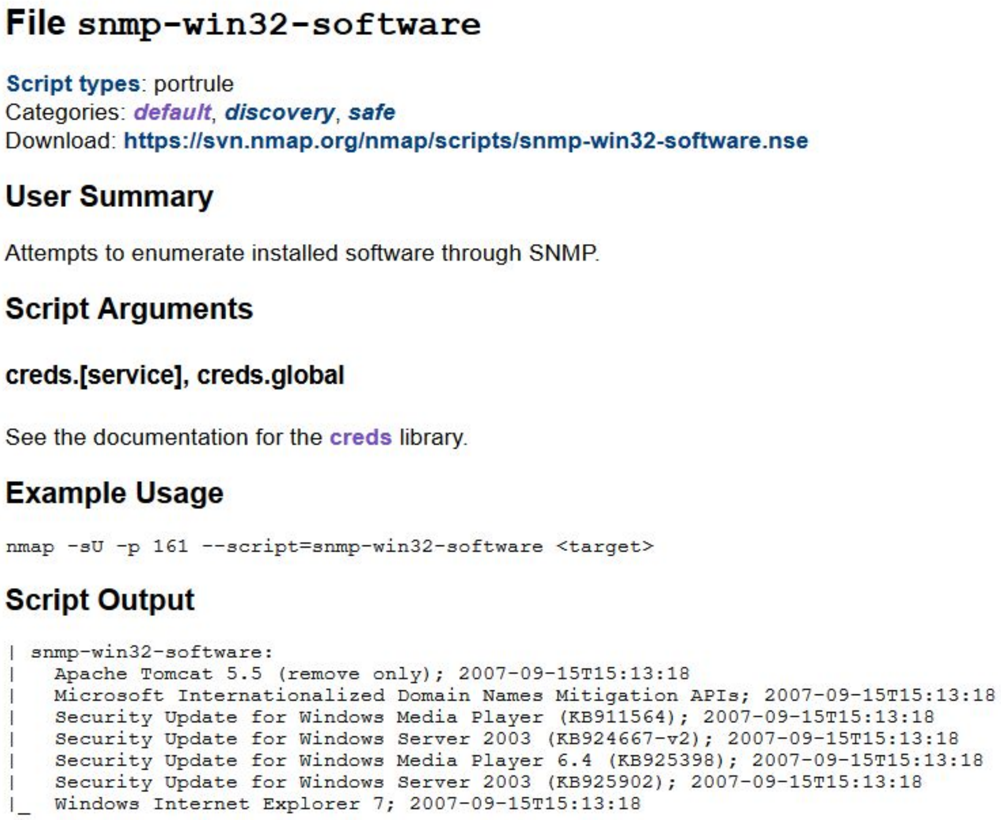
Command: nmap -sU -p 161 -sV 192.98.163.3



```
root@attackdefense:~# nmap -sU -p 161 -sV 192.98.163.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-20 19:27 UTC
Nmap scan report for target-1 (192.98.163.3)
Host is up (0.000070s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)
MAC Address: 02:42:C0:62:A3:03 (Unknown)
Service Info: Host: victim-1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.83 seconds
root@attackdefense:~#
```

SNMP server is running on the target machine.

Step 3: Use available nmap script to list the packages installed on the target machine,



File snmp-win32-software

Script types: portrule
Categories: *default*, *discovery*, *safe*
Download: https://svn.nmap.org/nmap/scripts/snmp-win32-software.nse

User Summary

Attempts to enumerate installed software through SNMP.

Script Arguments

creds.[service], creds.global

See the documentation for the creds library.

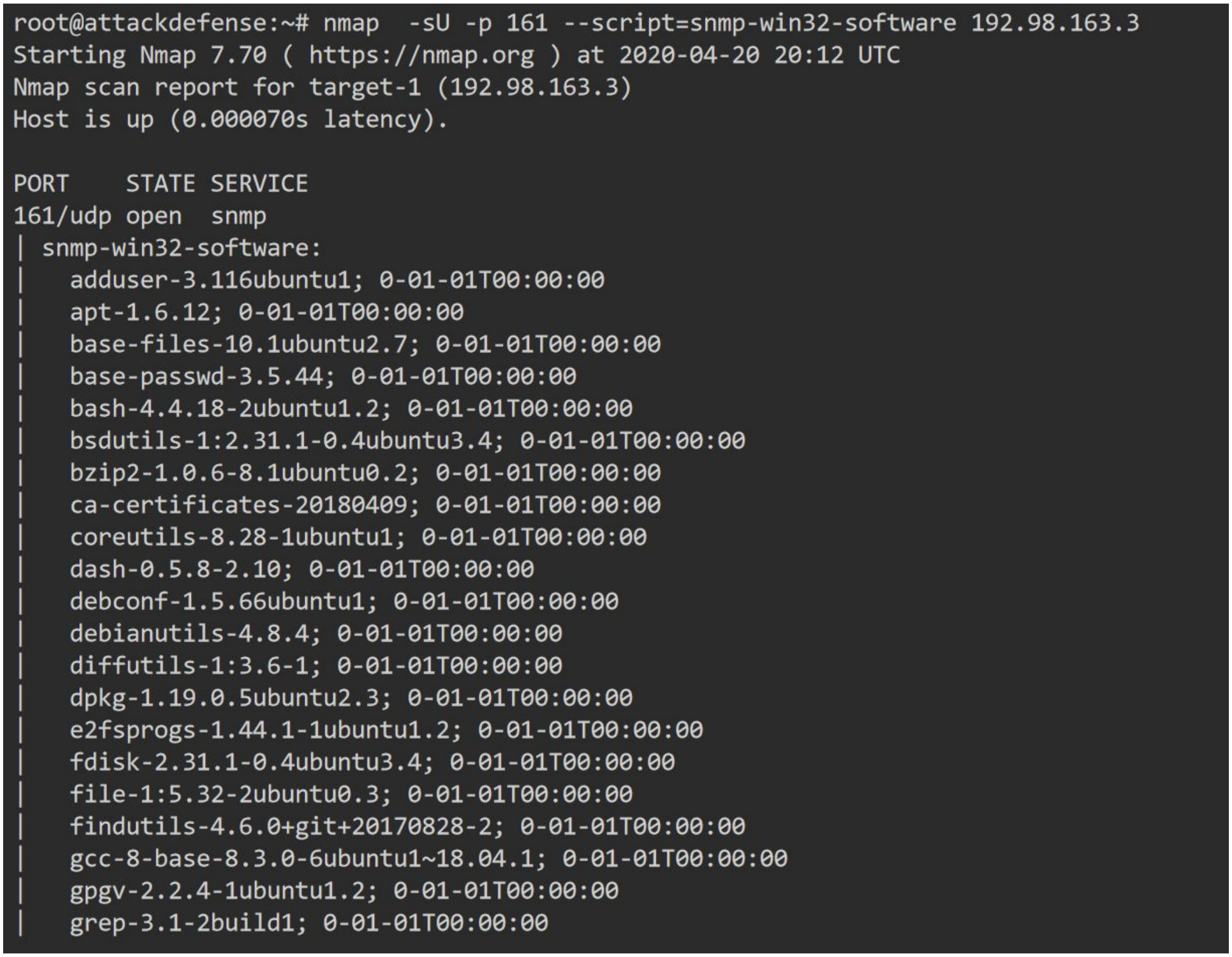
Example Usage

```
nmap -sU -p 161 --script=snmp-win32-software <target>
```

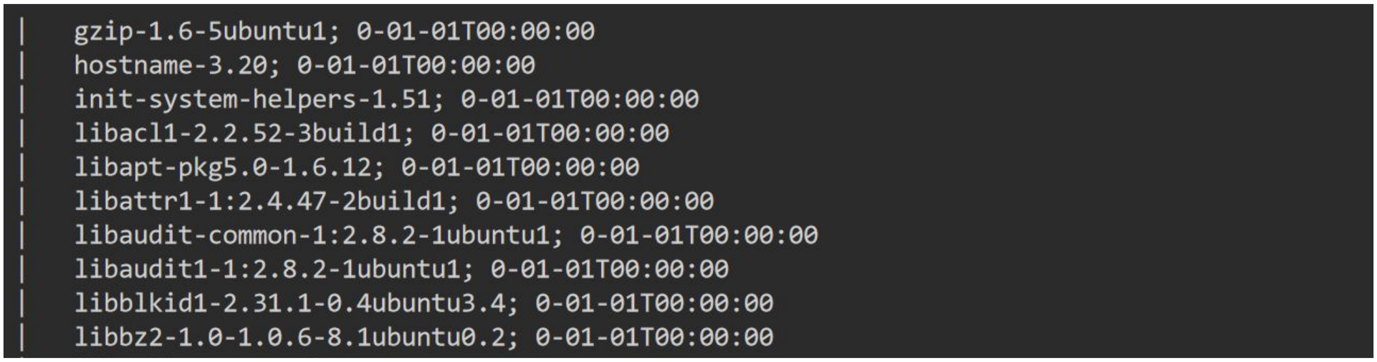
Script Output

```
| snmp-win32-software:
|   Apache Tomcat 5.5 (remove only); 2007-09-15T15:13:18
|   Microsoft Internationalized Domain Names Mitigation APIs; 2007-09-15T15:13:18
|   Security Update for Windows Media Player (KB911564); 2007-09-15T15:13:18
|   Security Update for Windows Server 2003 (KB924667-v2); 2007-09-15T15:13:18
|   Security Update for Windows Media Player 6.4 (KB925398); 2007-09-15T15:13:18
|   Security Update for Windows Server 2003 (KB925902); 2007-09-15T15:13:18
|_  Windows Internet Explorer 7; 2007-09-15T15:13:18
```

Command: nmap -sU -p 161 --script=snmp-win32-software 192.98.163.3



```
root@attackdefense:~# nmap  -sU -p 161 --script=snmp-win32-software 192.98.163.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-20 20:12 UTC
Nmap scan report for target-1 (192.98.163.3)
Host is up (0.000070s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-win32-software:
|   adduser-3.116ubuntu1; 0-01-01T00:00:00
|   apt-1.6.12; 0-01-01T00:00:00
|   base-files-10.1ubuntu2.7; 0-01-01T00:00:00
|   base-passwd-3.5.44; 0-01-01T00:00:00
|   bash-4.4.18-2ubuntu1.2; 0-01-01T00:00:00
|   bsdutils-1:2.31.1-0.4ubuntu3.4; 0-01-01T00:00:00
|   bzip2-1.0.6-8.1ubuntu0.2; 0-01-01T00:00:00
|   ca-certificates-20180409; 0-01-01T00:00:00
|   coreutils-8.28-1ubuntu1; 0-01-01T00:00:00
|   dash-0.5.8-2.10; 0-01-01T00:00:00
|   debconf-1.5.66ubuntu1; 0-01-01T00:00:00
|   debianutils-4.8.4; 0-01-01T00:00:00
|   diffutils-1:3.6-1; 0-01-01T00:00:00
|   dpkg-1.19.0.5ubuntu2.3; 0-01-01T00:00:00
|   e2fsprogs-1.44.1-1ubuntu1.2; 0-01-01T00:00:00
|   fdisk-2.31.1-0.4ubuntu3.4; 0-01-01T00:00:00
|   file-1:5.32-2ubuntu0.3; 0-01-01T00:00:00
|   findutils-4.6.0+git+20170828-2; 0-01-01T00:00:00
|   gcc-8-base-8.3.0-6ubuntu1~18.04.1; 0-01-01T00:00:00
|   gpgv-2.2.4-1ubuntu1.2; 0-01-01T00:00:00
|   grep-3.1-2build1; 0-01-01T00:00:00
```

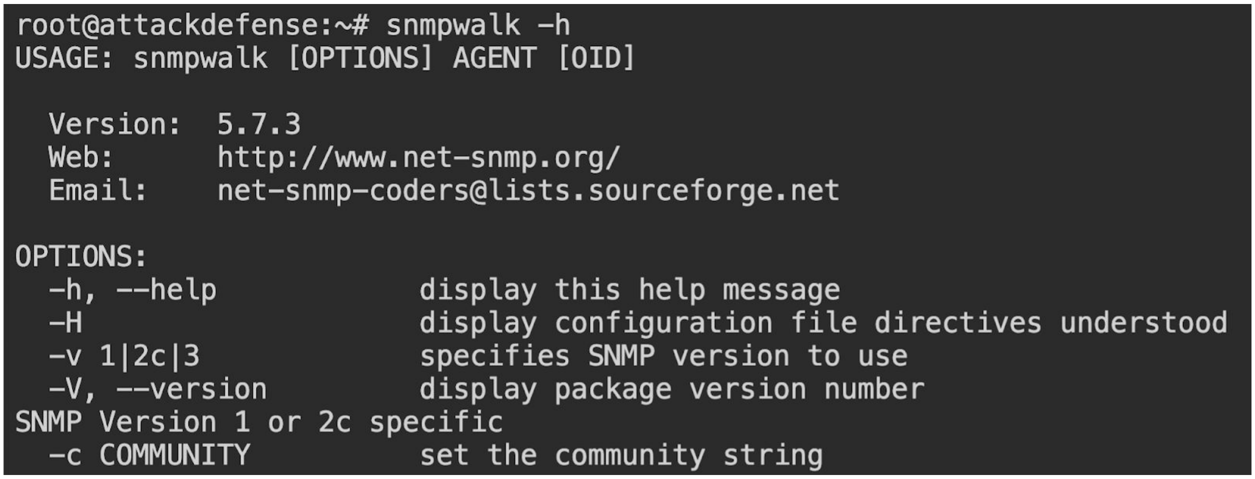


```
|   gzip-1.6-5ubuntu1; 0-01-01T00:00:00
|   hostname-3.20; 0-01-01T00:00:00
|   init-system-helpers-1.51; 0-01-01T00:00:00
|   libacl1-2.2.52-3build1; 0-01-01T00:00:00
|   libapt-pkg5.0-1.6.12; 0-01-01T00:00:00
|   libattr1-1:2.4.47-2build1; 0-01-01T00:00:00
|   libaudit-common-1:2.8.2-1ubuntu1; 0-01-01T00:00:00
|   libaudit1-1:2.8.2-1ubuntu1; 0-01-01T00:00:00
|   libblkid1-2.31.1-0.4ubuntu3.4; 0-01-01T00:00:00
|   libbz2-1.0-1.0.6-8.1ubuntu0.2; 0-01-01T00:00:00
```

The nmap script was able to identify the packages installed on the target machine.

Alternate Method: Using snmpwalk

Step 4: Check the help of snmpwalk.

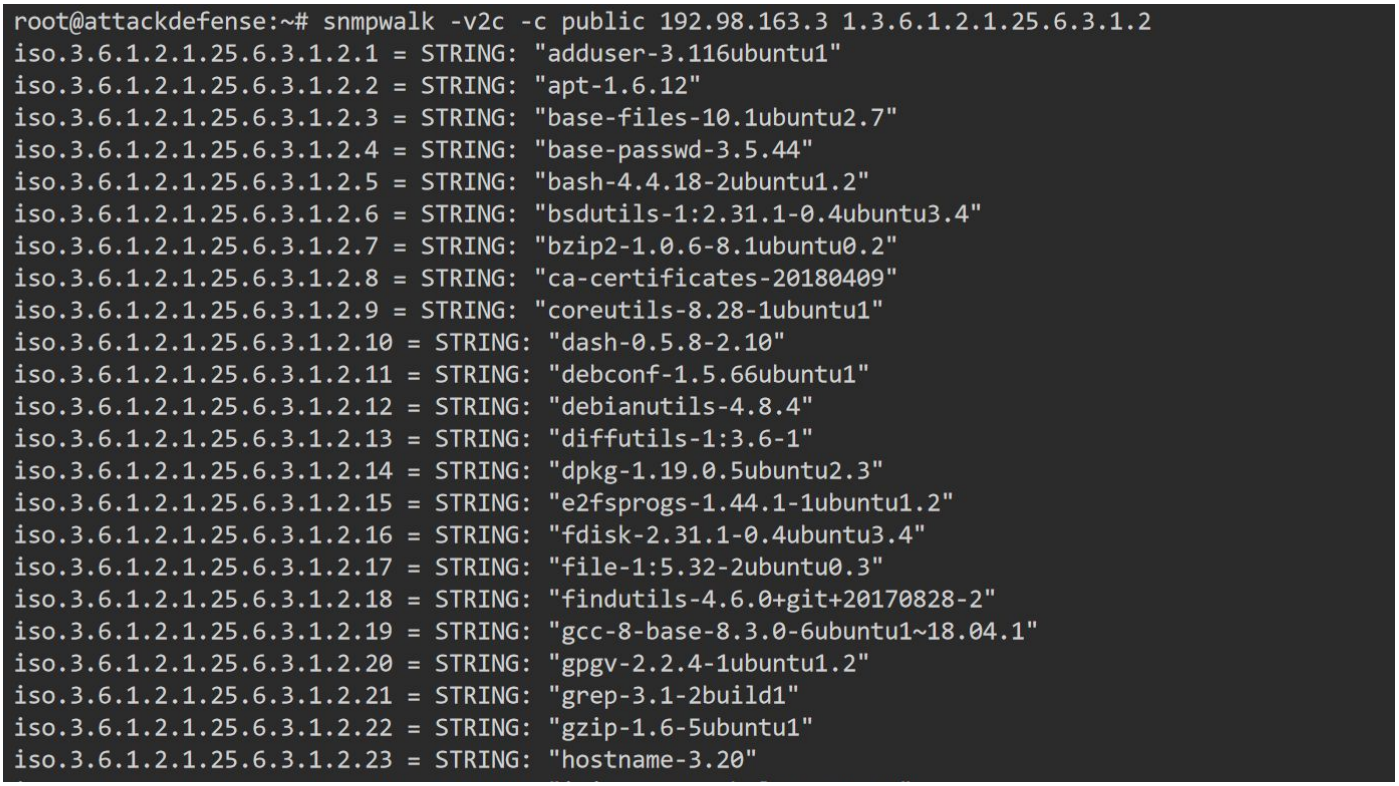


```
root@attackdefense:~# snmpwalk -h
USAGE: snmpwalk [OPTIONS] AGENT [OID]

  Version:  5.7.3
  Web:      http://www.net-snmp.org/
  Email:    net-snmp-coders@lists.sourceforge.net

OPTIONS:
  -h, --help            display this help message
  -H                    display configuration file directives understood
  -v 1|2c|3             specifies SNMP version to use
  -V, --version         display package version number
SNMP Version 1 or 2c specific
  -c COMMUNITY          set the community string
```

Snmpwalk requires the options and oid to be passed along with the IP address of the remote machine. The OID for listing packages is 1.3.6.1.2.1.25.6.3.1.2

Step 5: Use snmpwalk to identify the packages installed on the target machine.

Command: snmpwalk -v2c -c public 192.98.163.3 1.3.6.1.2.1.25.6.3.1.2



```
root@attackdefense:~# snmpwalk -v2c -c public 192.98.163.3 1.3.6.1.2.1.25.6.3.1.2
iso.3.6.1.2.1.25.6.3.1.2.1 = STRING: "adduser-3.116ubuntu1"
iso.3.6.1.2.1.25.6.3.1.2.2 = STRING: "apt-1.6.12"
iso.3.6.1.2.1.25.6.3.1.2.3 = STRING: "base-files-10.1ubuntu2.7"
iso.3.6.1.2.1.25.6.3.1.2.4 = STRING: "base-passwd-3.5.44"
iso.3.6.1.2.1.25.6.3.1.2.5 = STRING: "bash-4.4.18-2ubuntu1.2"
iso.3.6.1.2.1.25.6.3.1.2.6 = STRING: "bsdutils-1:2.31.1-0.4ubuntu3.4"
iso.3.6.1.2.1.25.6.3.1.2.7 = STRING: "bzip2-1.0.6-8.1ubuntu0.2"
iso.3.6.1.2.1.25.6.3.1.2.8 = STRING: "ca-certificates-20180409"
iso.3.6.1.2.1.25.6.3.1.2.9 = STRING: "coreutils-8.28-1ubuntu1"
iso.3.6.1.2.1.25.6.3.1.2.10 = STRING: "dash-0.5.8-2.10"
iso.3.6.1.2.1.25.6.3.1.2.11 = STRING: "debconf-1.5.66ubuntu1"
iso.3.6.1.2.1.25.6.3.1.2.12 = STRING: "debianutils-4.8.4"
iso.3.6.1.2.1.25.6.3.1.2.13 = STRING: "diffutils-1:3.6-1"
iso.3.6.1.2.1.25.6.3.1.2.14 = STRING: "dpkg-1.19.0.5ubuntu2.3"
iso.3.6.1.2.1.25.6.3.1.2.15 = STRING: "e2fsprogs-1.44.1-1ubuntu1.2"
iso.3.6.1.2.1.25.6.3.1.2.16 = STRING: "fdisk-2.31.1-0.4ubuntu3.4"
iso.3.6.1.2.1.25.6.3.1.2.17 = STRING: "file-1:5.32-2ubuntu0.3"
iso.3.6.1.2.1.25.6.3.1.2.18 = STRING: "findutils-4.6.0+git+20170828-2"
iso.3.6.1.2.1.25.6.3.1.2.19 = STRING: "gcc-8-base-8.3.0-6ubuntu1~18.04.1"
iso.3.6.1.2.1.25.6.3.1.2.20 = STRING: "gpgv-2.2.4-1ubuntu1.2"
iso.3.6.1.2.1.25.6.3.1.2.21 = STRING: "grep-3.1-2build1"
iso.3.6.1.2.1.25.6.3.1.2.22 = STRING: "gzip-1.6-5ubuntu1"
iso.3.6.1.2.1.25.6.3.1.2.23 = STRING: "hostname-3.20"
```

References:

1. Software Discovery (https://attack.mitre.org/techniques/T1518/)