ATTACK DEFENSE

by PentesterAcademy

Name	T1057 : Process Discovery
URL	https://attackdefense.com/challengedetails?cid=1867
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.

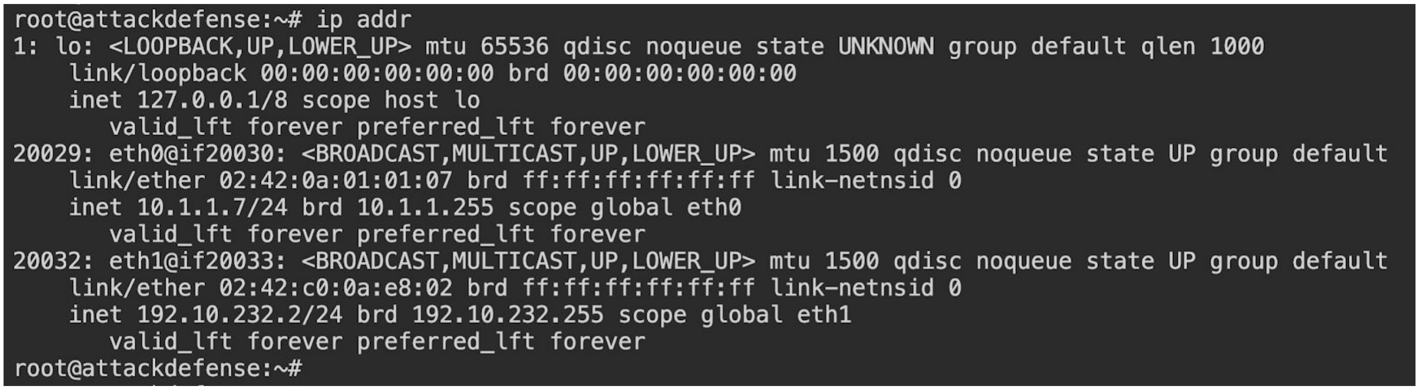
Objective:

- Identify the processes running on the target machine.
- Identify the password of user "bruce", The password and username are passed as an argument to a program.

Solution:

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

Commands: ip addr

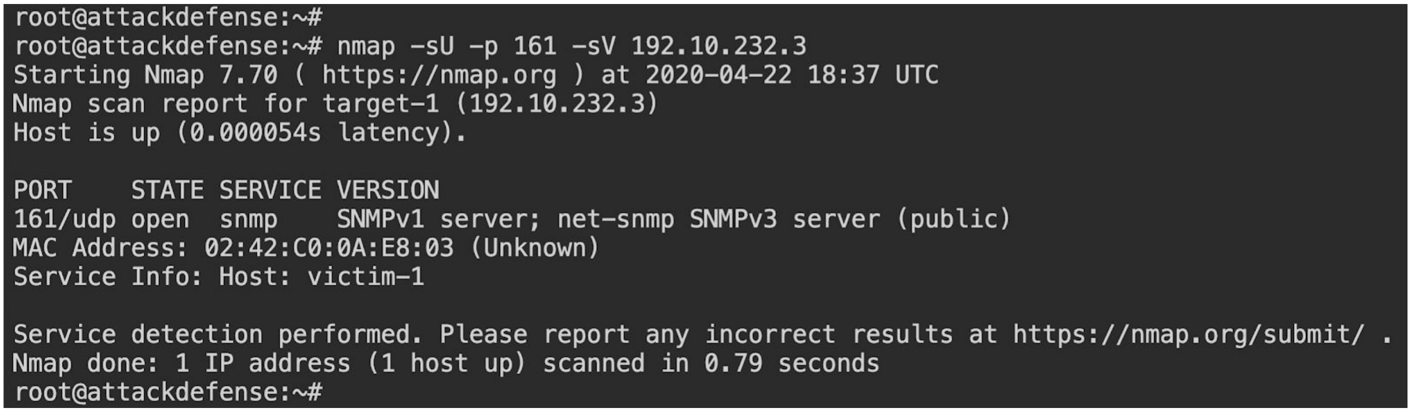


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
20029: eth0@if20030: <BROADCAST,MULTICAST,UP,LOWER_UP> 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
20032: eth1@if20033: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:0a:e8:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.10.232.2/24 brd 192.10.232.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.10.232.2. The target machine will be present at the IP address 192.10.232.3

Step 2: Scanning the default port used by SNMP Server.

Command: nmap -sU -p 161 -sV 192.10.232.3

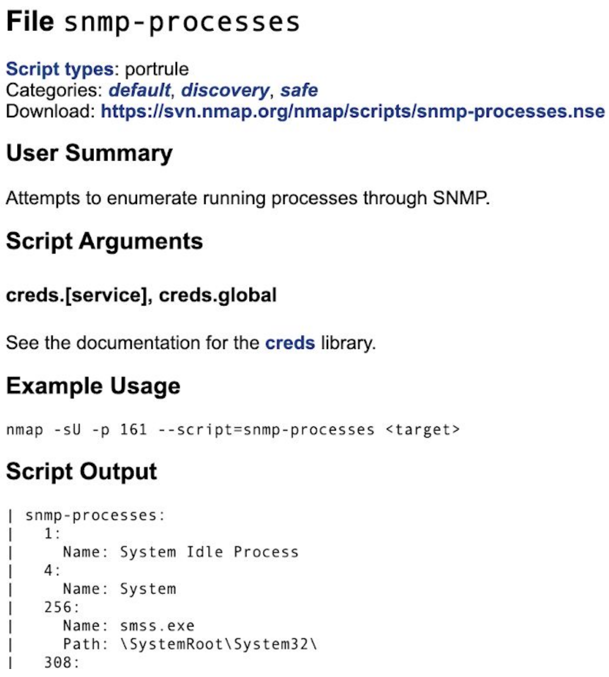


```
root@attackdefense:~#
root@attackdefense:~# nmap -sU -p 161 -sV 192.10.232.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-22 18:37 UTC
Nmap scan report for target-1 (192.10.232.3)
Host is up (0.000054s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)
MAC Address: 02:42:C0:0A:E8:03 (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 0.79 seconds
root@attackdefense:~#
```

The SNMP server is running on port 161 of the target machine. The snmp server is configured to use the community string "public"

Step 3: Identify the processes running on the target machine. Nmap script is available to identify the processes and the parameters passed to them.

https://nmap.org/nsedoc/scripts/snmp-processes.html



File snmp-processes

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

User Summary

Attempts to enumerate running processes through SNMP.

Script Arguments

creds.[service], creds.global

See the documentation for the creds library.

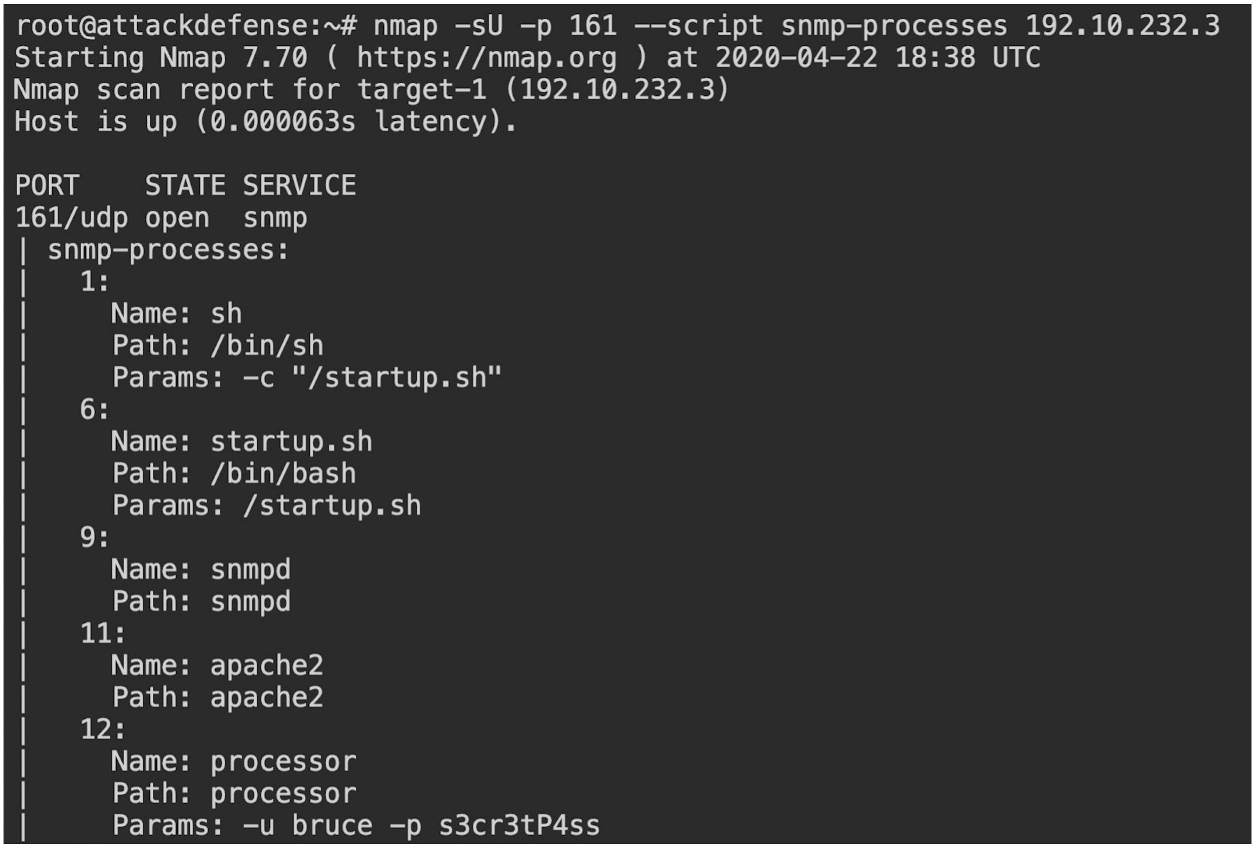
Example Usage

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

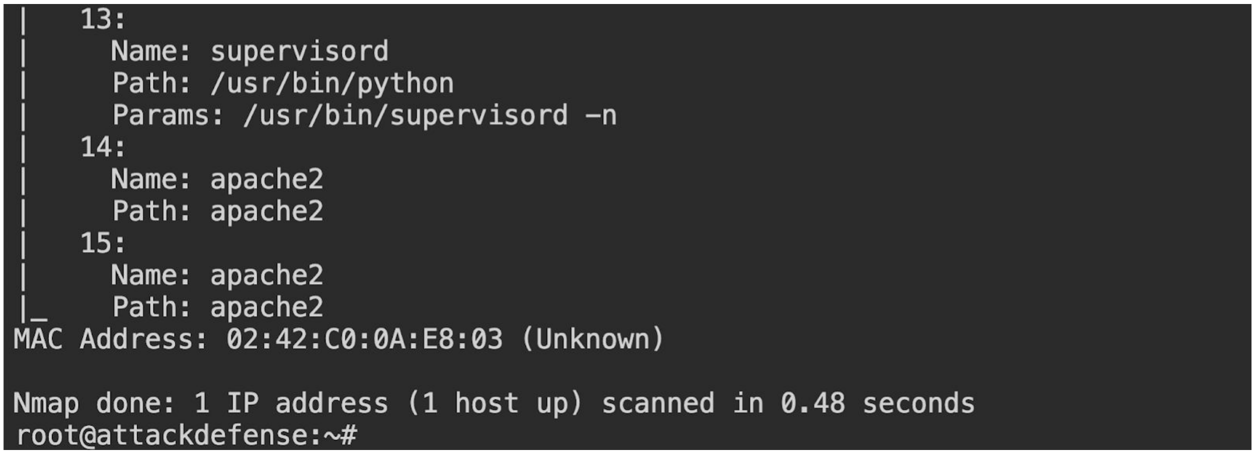
Script Output

```
| snmp-processes:
|   1:
|     Name: System Idle Process
|   4:
|     Name: System
|   256:
|     Name: smss.exe
|     Path: \SystemRoot\System32\
|   308:
```

Command: nmap -sU -p 161 --script snmp-processes 192.10.232.3



```
root@attackdefense:~# nmap -sU -p 161 --script snmp-processes 192.10.232.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-22 18:38 UTC
Nmap scan report for target-1 (192.10.232.3)
Host is up (0.000063s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-processes:
|   1:
|     Name: sh
|     Path: /bin/sh
|     Params: -c "/startup.sh"
|   6:
|     Name: startup.sh
|     Path: /bin/bash
|     Params: /startup.sh
|   9:
|     Name: snmpd
|     Path: snmpd
|   11:
|     Name: apache2
|     Path: apache2
|   12:
|     Name: processor
|     Path: processor
|     Params: -u bruce -p s3cr3tP4ss
```



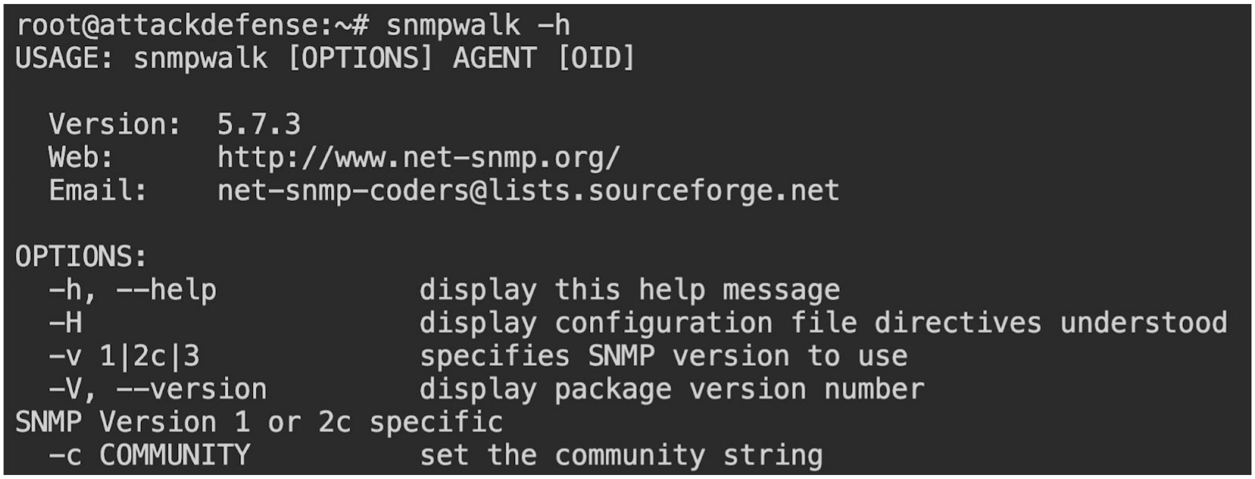
```
|   13:
|     Name: supervisord
|     Path: /usr/bin/python
|     Params: /usr/bin/supervisord -n
|   14:
|     Name: apache2
|     Path: apache2
|   15:
|     Name: apache2
|_    Path: apache2
MAC Address: 02:42:C0:0A:E8:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
root@attackdefense:~#
```

The processes running on the target machine are, sh interpreter, bash script, snmpd, apache, supervisor and processor.

The username and password are passed as parameters to the processor program. The password of user bruce is "s3cr3tP4ss"

Alternate Method: Using snmpwalk

Step 4: Check the help of snmpwalk.

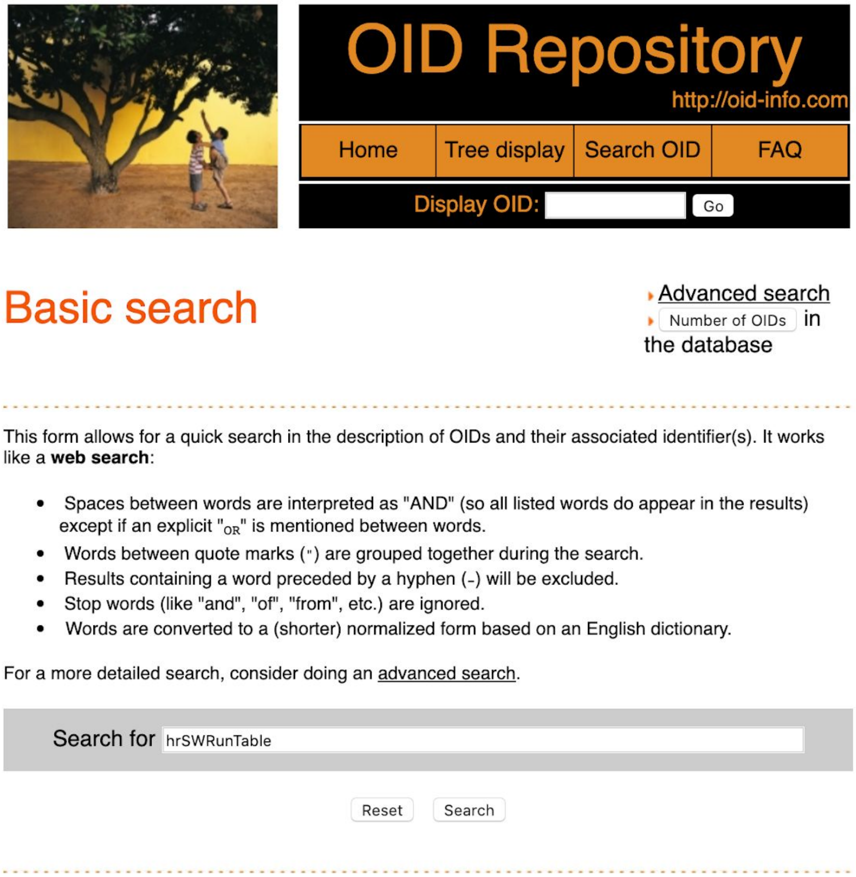


```
root@attackdefense:~# snmpwalk -h
USAGE: snmpwalk [OPTIONS] AGENT [OID]

  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.

Step 5: Identifying the OID required to view the interface information. The information regarding processes are stored in the hrSWRunTable. Search for hrSWRunTable in the OID repository.

OID Repository Link: http://www.oid-info.com/basic-search.htm



Basic search

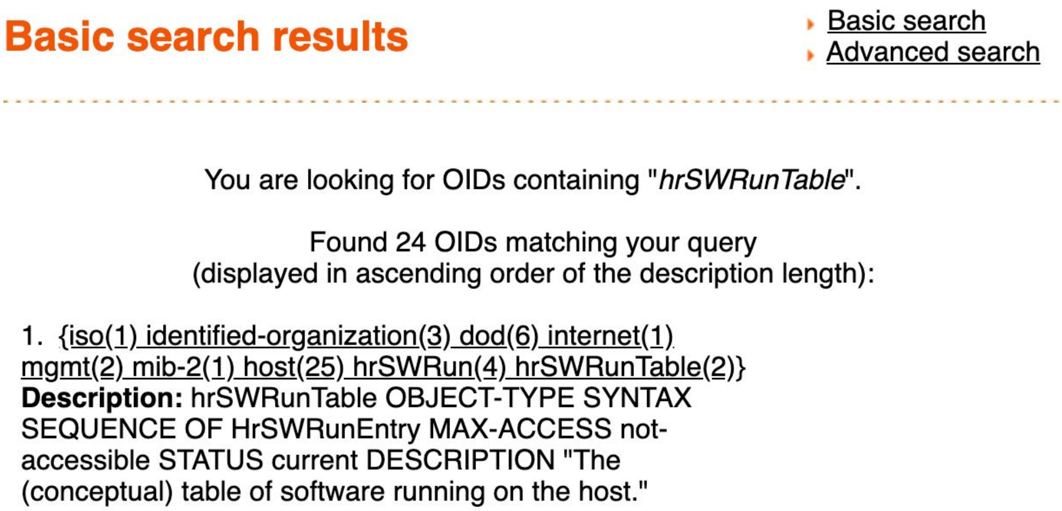
This form allows for a quick search in the description of OIDs and their associated identifier(s). It works like a **web search**:

- Spaces between words are interpreted as "AND" (so all listed words do appear in the results) except if an explicit "OR" is mentioned between words.
- Words between quote marks (") are grouped together during the search.
- Results containing a word preceded by a hyphen (-) will be excluded.
- Stop words (like "and", "of", "from", etc.) are ignored.
- Words are converted to a (shorter) normalized form based on an English dictionary.

For a more detailed search, consider doing an advanced search.

Search for: hrSWRunTable

Result:



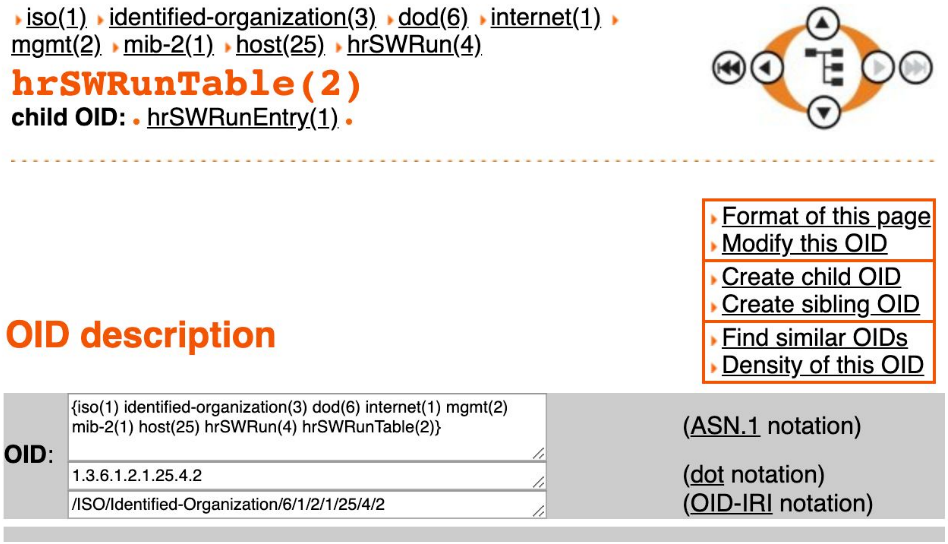
Basic search results

You are looking for OIDs containing "*hrSWRunTable*".

Found 24 OIDs matching your query
(displayed in ascending order of the description length):

1. {iso(1) identified-organization(3) dod(6) internet(1) mgmt(2) mib-2(1) host(25) hrSWRun(4) hrSWRunTable(2)}
Description: hrSWRunTable OBJECT-TYPE SYNTAX SEQUENCE OF HrSWRunEntry MAX-ACCESS not-accessible STATUS current DESCRIPTION "The (conceptual) table of software running on the host."

Step 6: Click on the first link.



iso(1) identified-organization(3) dod(6) internet(1) mgmt(2) mib-2(1) host(25) hrSWRun(4)

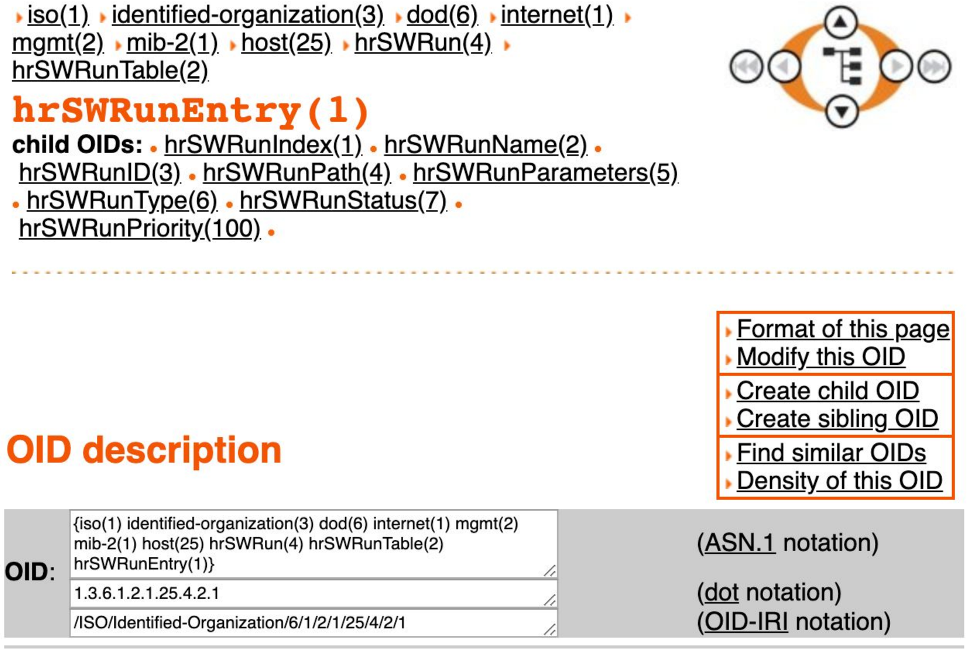
hrSWRunTable(2)

child OID: hrSWRunEntry(1)

OID description

OID:		
	{iso(1) identified-organization(3) dod(6) internet(1) mgmt(2) mib-2(1) host(25) hrSWRun(4) hrSWRunTable(2)}	(ASN.1 notation)
	1.3.6.1.2.1.25.4.2	(dot notation)
	/ISO/Identified-Organization/6/1/2/1/25/4/2	(OID-IRI notation)

Step 7: Expand the hrSWRUNEntry child OID



iso(1) identified-organization(3) dod(6) internet(1) mgmt(2) mib-2(1) host(25) hrSWRun(4) hrSWRunTable(2)

hrSWRunEntry(1)

child OIDs: hrSWRunIndex(1) • hrSWRunName(2) • hrSWRunID(3) • hrSWRunPath(4) • hrSWRunParameters(5) • hrSWRunType(6) • hrSWRunStatus(7) • hrSWRunPriority(100)

OID description

OID:		
	{iso(1) identified-organization(3) dod(6) internet(1) mgmt(2) mib-2(1) host(25) hrSWRun(4) hrSWRunTable(2) hrSWRunEntry(1)}	(ASN.1 notation)
	1.3.6.1.2.1.25.4.2.1	(dot notation)
	/ISO/Identified-Organization/6/1/2/1/25/4/2/1	(OID-IRI notation)

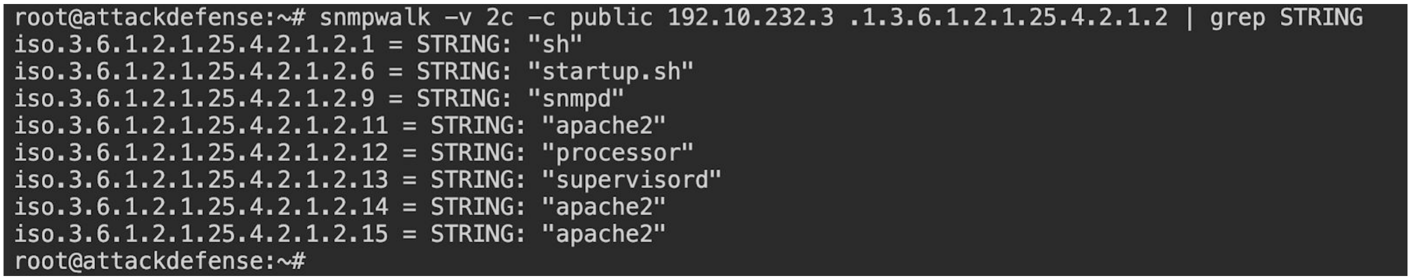
There are 8 child OIDs for hrSWRUNEntry. Two of the child OID are hrSWRunName and hrSWRunParameters. The first OID will reveal the name of the process and the second OID will reveal the parameters passed to the program.

hrSWRunName OID: 1.3.6.1.2.1.25.4.2.1.2

hrSWRunParameters OID: 1.3.6.1.2.1.25.4.2.1.5

Step 8: Pass the hrSWRunName OID along with other required arguments to the snmpwalk tool.

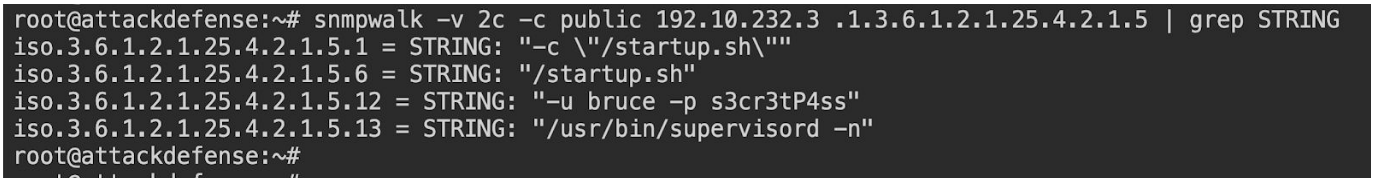
Command: snmpwalk -v 2c -c public 192.10.232.3 .1.3.6.1.2.1.25.4.2.1.2



```
root@attackdefense:~# snmpwalk -v 2c -c public 192.10.232.3 .1.3.6.1.2.1.25.4.2.1.2 | grep STRING
iso.3.6.1.2.1.25.4.2.1.2.1 = STRING: "sh"
iso.3.6.1.2.1.25.4.2.1.2.6 = STRING: "startup.sh"
iso.3.6.1.2.1.25.4.2.1.2.9 = STRING: "snmpd"
iso.3.6.1.2.1.25.4.2.1.2.11 = STRING: "apache2"
iso.3.6.1.2.1.25.4.2.1.2.12 = STRING: "processor"
iso.3.6.1.2.1.25.4.2.1.2.13 = STRING: "supervisord"
iso.3.6.1.2.1.25.4.2.1.2.14 = STRING: "apache2"
iso.3.6.1.2.1.25.4.2.1.2.15 = STRING: "apache2"
root@attackdefense:~#
```

The processes running on the target machine are, sh interpreter, startup.sh script, snmpd, apache, supervisor and processor.

Step 9: Pass the hrSWRunParameters OID along with other required arguments to identify the parameters to the process.



```
root@attackdefense:~# snmpwalk -v 2c -c public 192.10.232.3 .1.3.6.1.2.1.25.4.2.1.5 | grep STRING
iso.3.6.1.2.1.25.4.2.1.5.1 = STRING: "-c \"/startup.sh\""
iso.3.6.1.2.1.25.4.2.1.5.6 = STRING: "/startup.sh"
iso.3.6.1.2.1.25.4.2.1.5.12 = STRING: "-u bruce -p s3cr3tP4ss"
iso.3.6.1.2.1.25.4.2.1.5.13 = STRING: "/usr/bin/supervisord -n"
root@attackdefense:~#
```

The parameters can be related to the processes by relating the last digit (Process ID) in the OID string. For example, the OID string for the "processor" process has "12" in the end, therefore the OID string for the parameters will also have the same digit in the end.

The username and password are passed as parameters to the processor program. The password of user bruce is "s3cr3tP4ss"

References:

1. Process Discovery (https://attack.mitre.org/techniques/T1057/)
2. Nmap Script SNMP Processes (https://nmap.org/nsedoc/scripts/snmp-processes.html)
3. OID Repository (http://www.oid-info.com)
4. Snmpwalk (https://linux.die.net/man/1/snmpwalk)