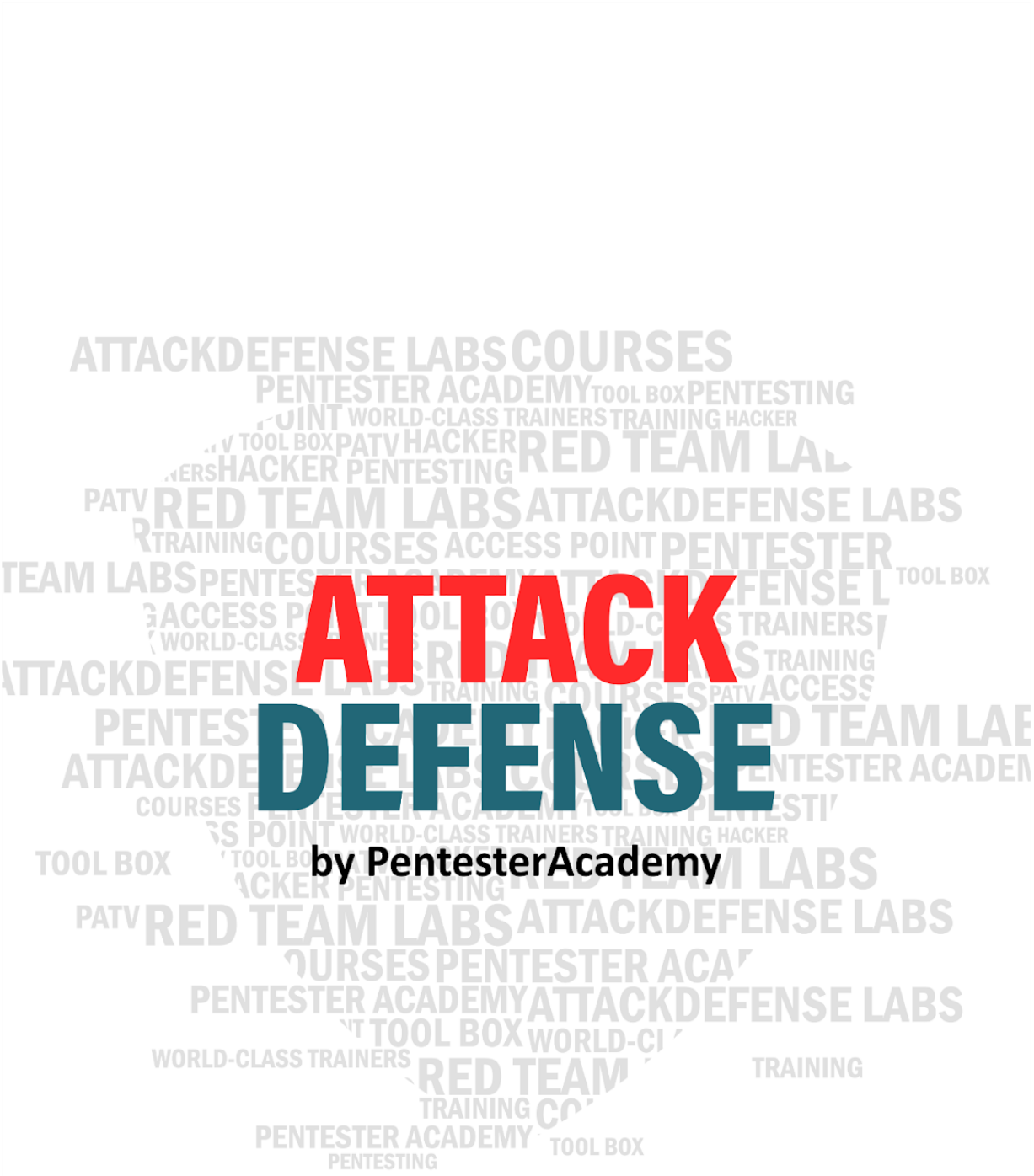

ATTACK
DEFENSE
by PentesterAcademy

Name	T1016 : System Network Configuration Discovery II
URL	https://attackdefense.com/challengedetails?cid=1866
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 interfaces on the target machine

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
19924: eth0@if19925: <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
19930: eth1@if19931: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:f1:da:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.241.218.2/24 brd 192.241.218.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.241.218.2. The target machine will be present at the IP address 192.241.218.3

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

Command: nmap -sU -p 161 -sV 192.241.218.3

```
root@attackdefense:~# nmap -sU -p 161 -sV 192.241.218.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-22 15:06 UTC
Nmap scan report for target-1 (192.241.218.3)
Host is up (0.000053s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; net-snmp SNMPv3 server (public)
MAC Address: 02:42:C0:F1:DA: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:~#
```

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 interfaces on the target machine. Nmap script is available to identify the interfaces.

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

File `snmp-interfaces`

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

User Summary

Attempts to enumerate network interfaces through SNMP.

This script can also be run during Nmap's pre-scanning phase and can attempt to add the SNMP server's interface addresses to the target list. The script argument `snmp-interfaces.host` is required to know what host to probe. To specify a port for the SNMP server other than 161, use `snmp-interfaces.port`. When run in this way, the script's output tells how many new targets were successfully added.

Script Arguments

snmp-interfaces.host

Specifies the SNMP server to probe when running in the "pre-scanning phase".

snmp-interfaces.port

The optional port number corresponding to the host script argument. Defaults to 161.

max-newtargets, newtargets

See the documentation for the **target** library.

creds.[service], creds.global

See the documentation for the **creds** library.

Example Usage

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

Command: nmap -sU -p 161 --script snmp-interfaces 192.241.218.3

```
root@attackdefense:~# nmap -sU -p 161 --script snmp-interfaces 192.241.218.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-22 15:06 UTC
Nmap scan report for target-1 (192.241.218.3)
Host is up (0.000059s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-interfaces:
|   lo
|     IP address: 127.0.0.1  Netmask: 255.0.0.0
|     Type: softwareLoopback  Speed: 10 Mbps
|     Status: up
|     Traffic stats: 3.85 Kb sent, 3.85 Kb received
|   eth0
|     IP address: 192.241.218.3  Netmask: 255.255.255.0
|     MAC address: 02:42:c0:f1:da:03 (Unknown)
|     Type: ethernetCsmacd  Speed: 4 Gbps
|     Status: up
|     Traffic stats: 0.77 Kb sent, 2.95 Kb received
|   eth1
|     IP address: 192.39.12.2  Netmask: 255.255.255.0
|     MAC address: 02:42:c0:27:0c:02 (Unknown)
|     Type: ethernetCsmacd  Speed: 4 Gbps
|     Status: up
|     Traffic stats: 0.00 Kb sent, 2.15 Kb received
|   eth2
|     IP address: 192.34.109.2  Netmask: 255.255.255.0
|     MAC address: 02:42:c0:22:6d:02 (Unknown)
|     Type: ethernetCsmacd  Speed: 4 Gbps
|     Status: up
|     Traffic stats: 0.00 Kb sent, 2.15 Kb received
|   eth3
|     IP address: 192.34.48.2  Netmask: 255.255.255.0
|     MAC address: 02:42:c0:22:30:02 (Unknown)
|     Type: ethernetCsmacd  Speed: 4 Gbps
|     Status: up
|_    Traffic stats: 0.00 Kb sent, 2.15 Kb received
MAC Address: 02:42:C0:F1:DA:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.53 seconds
root@attackdefense:~#
```

Excluding the lo interface, there are 4 interfaces on the target machine, eth0, eth1, eth2, eth3.

Alternate Method: Using snmpwalk

Step 4: Check the help of snmpwalk.

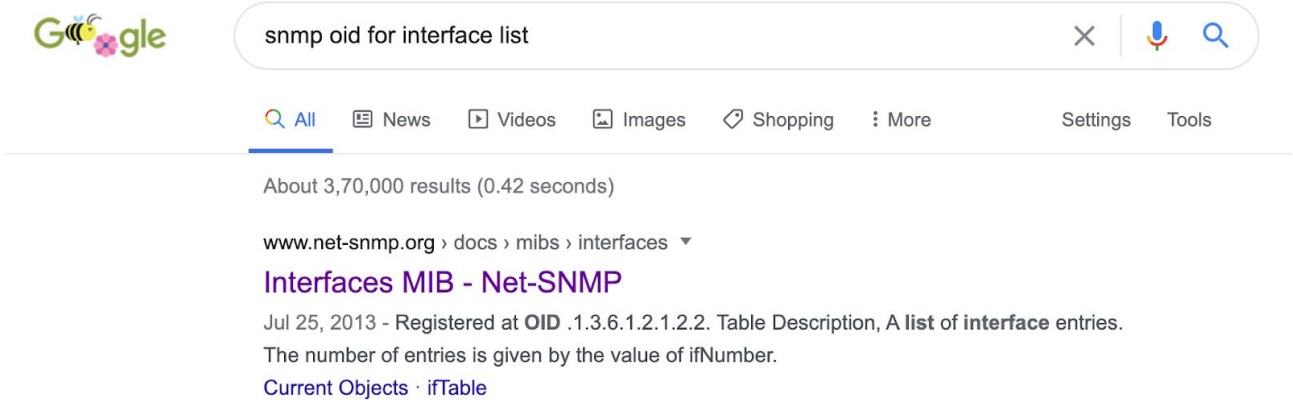
```
root@attackdefense:~# snmpwalk -h
USAGE: snmpwalk [OPTIONS] AGENT [OID]

  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
```

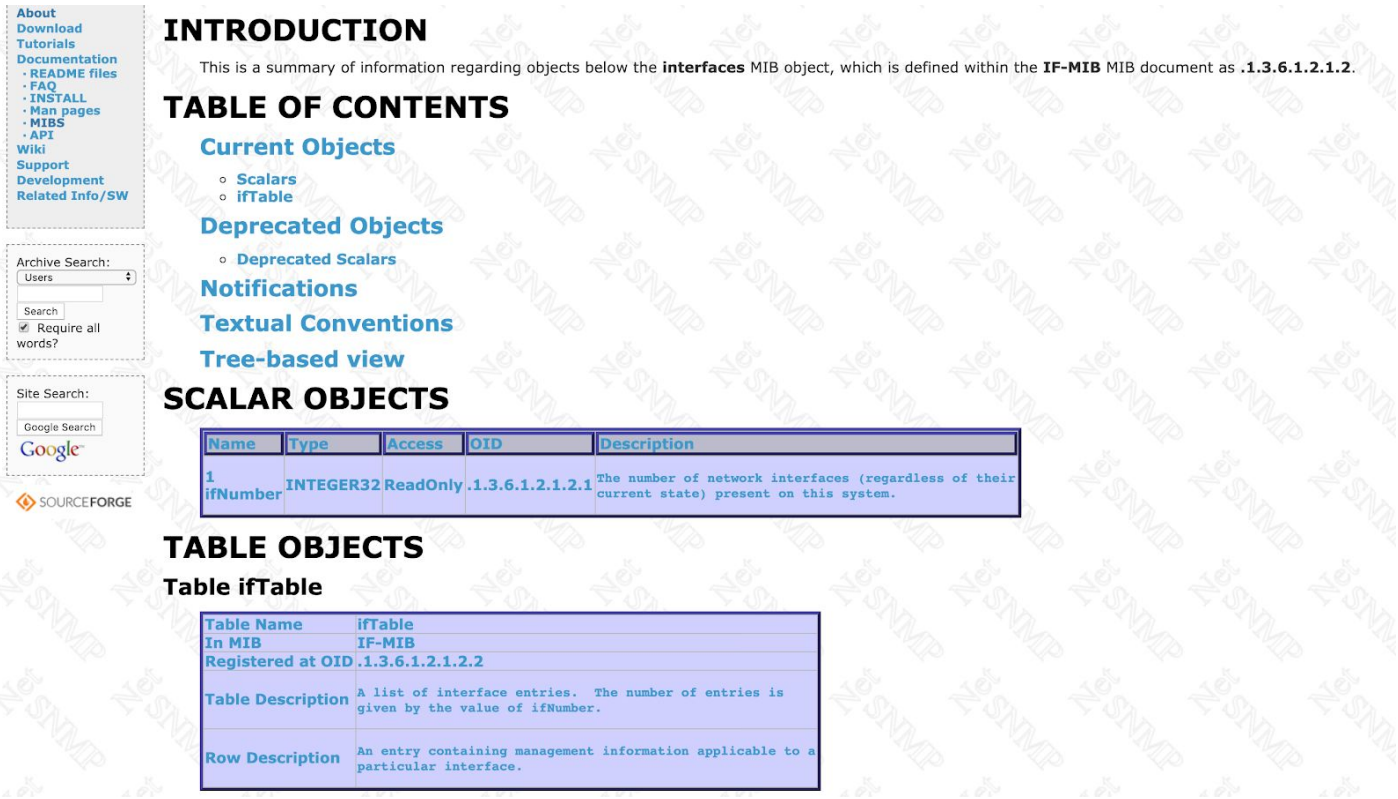
Snmpwalk requires the options and oid to be passed along with the IP address of the remote machine.

Step 5: Identifying the OID required to view the interface information. The OID can be searched online, search "snmp oid for interface list" on google.



The first link contains the information regarding the ifTable OID.

Net-SNMP MIB Interfaces : http://www.net-snmp.org/docs/mibs/interfaces.html



About
Download
Tutorials
Documentation
· README files
· FAQ
· INSTALL
· Man pages
· MIBS
· API
Wiki
Support
Development
Related Info/SW

Archive Search:
Users
Search
Require all words?

Site Search:
Google Search
Google

SOURCEFORGE

INTRODUCTION

This is a summary of information regarding objects below the **interfaces** MIB object, which is defined within the **IF-MIB** MIB document as **.1.3.6.1.2.1.2**.

TABLE OF CONTENTS

Current Objects
- Scalars
- ifTable

Deprecated Objects
- Deprecated Scalars

Notifications

Textual Conventions

Tree-based view

SCALAR OBJECTS

Name	Type	Access	OID	Description
1 ifNumber	INTEGER32	ReadOnly	.1.3.6.1.2.1.2.1	The number of network interfaces (regardless of their current state) present on this system.

TABLE OBJECTS

Table ifTable

Table Name	ifTable
In MIB	IF-MIB
Registered at OID	.1.3.6.1.2.1.2.2
Table Description	A list of interface entries. The number of entries is given by the value of ifNumber.
Row Description	An entry containing management information applicable to a particular interface.

The OID for listing interfaces is 1.3.6.1.2.1.2

Step 6: Pass the OID along with other required arguments to the snmpwalk tool.

Command: snmp -v 2c -c public 192.241.218.3 .1.3.6.1.2.1.2 | grep STRING

```
root@attackdefense:~# snmpwalk -v 2c -c public 192.241.218.3 .1.3.6.1.2.1.2 | grep STRING
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "lo"
iso.3.6.1.2.1.2.2.1.2.19932 = STRING: "eth0"
iso.3.6.1.2.1.2.2.1.2.19934 = STRING: "eth1"
iso.3.6.1.2.1.2.2.1.2.19936 = STRING: "eth2"
iso.3.6.1.2.1.2.2.1.2.19938 = STRING: "eth3"
iso.3.6.1.2.1.2.2.1.6.19932 = Hex-STRING: 02 42 C0 F1 DA 03
iso.3.6.1.2.1.2.2.1.6.19934 = Hex-STRING: 02 42 C0 27 0C 02
iso.3.6.1.2.1.2.2.1.6.19936 = Hex-STRING: 02 42 C0 22 6D 02
iso.3.6.1.2.1.2.2.1.6.19938 = Hex-STRING: 02 42 C0 22 30 02
root@attackdefense:~#
```

Excluding the lo interface, there are 4 interfaces on the target machine, eth0, eth1, eth2, eth3.

References:

1. System Network Configuration Discovery (https://attack.mitre.org/techniques/T1016/)
2. Nmap Script SNMP Interfaces (https://nmap.org/nsedoc/scripts/snmp-interfaces.html)
3. Snmpwalk (https://linux.die.net/man/1/snmpwalk)