专注APT攻击与防御

https://micropoor.blogspot.com/

SNMP简介：

SNMP是一种简单网络管理协议，它属于TCP/IP五层协议中的应用层协议，用于网络管理的协议。SNMP主要用于网络设备的管理。SNMP协议主要由两大部分构成：SNMP管理站和SNMP代理。SNMP管理站是一个中心节点，负责收集维护各个SNMP元素的信息，并对这些信息进行处理，最后反馈给网络管理员；而SNMP代理是运行在各个被管理的网络节点之上，负责统计该节点的各项信息，并且负责与SNMP管理站交互，接收并执行管理站的命令，上传各种本地的网络信息。

nmap扫描：

root@John:~# nmap -sU --script snmp-brute 192.168.1.0/24 -T4

```
root@John:~# nmap -sU --script snmp-brute 192.168.1.0/24 -T4

Starting Nmap 7.40 ( https://nmap.org ) at 2017-12-03 23:11 EST
Warning: 192.168.1.101 giving up on port because retransmission cap hit (6).
Stats: 0:00:44 elapsed; 252 hosts completed (3 up), 3 undergoing UDP Scan
UDP Scan Timing: About 69.33% done; ETC: 23:12 (0:00:18 remaining)
Stats: 0:05:00 elapsed; 252 hosts completed (3 up), 3 undergoing UDP Scan
UDP Scan Timing: About 77.44% done; ETC: 23:18 (0:01:27 remaining)
Stats: 0:08:57 elapsed; 252 hosts completed (3 up), 3 undergoing UDP Scan
UDP Scan Timing: About 85.00% done; ETC: 23:22 (0:01:34 remaining)
Stats: 0:17:29 elapsed; 252 hosts completed (3 up), 3 undergoing UDP Scan
UDP Scan Timing: About 100.00% done; ETC: 23:29 (0:00:00 remaining)
Nmap scan report for 192.168.1.1
Host is up (0.0071s latency).
Not shown: 992 closed ports
PORT      STATE         SERVICE
53/udp    open          domain
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
1701/udp  open|filtered L2TP
1900/udp  open|filtered upnp
1901/udp  open|filtered fjicl-tep-a
49154/udp open|filtered unknown
49158/udp open|filtered unknown
MAC Address: [redacted]

Nmap scan report for 192.168.1.100
Host is up (0.012s latency).
Not shown: 999 open|filtered ports
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: [redacted]

Nmap scan report for 192.168.1.101
Host is up (0.16s latency).
Not shown: 996 closed ports
```

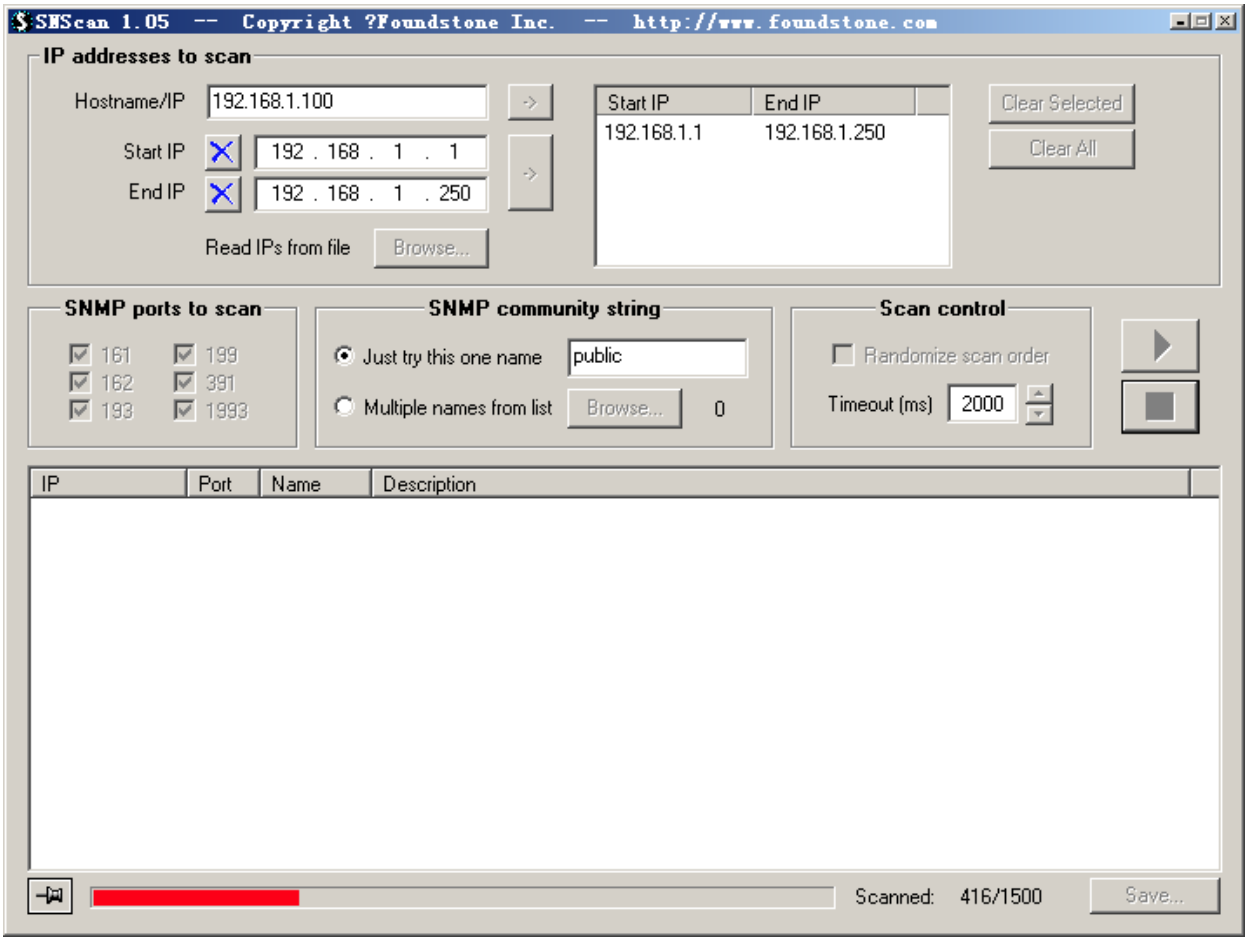
msf扫描：

msf > use auxiliary/scanner/snmp/snmp_enum

```
msf auxiliary(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>

msf auxiliary(snmp_enum) > set THREADS 10
THREADS => 10
msf auxiliary(snmp_enum) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
```

项目地址：https://www.mcafee.com/us/downloads/free-tools/snscan.aspx

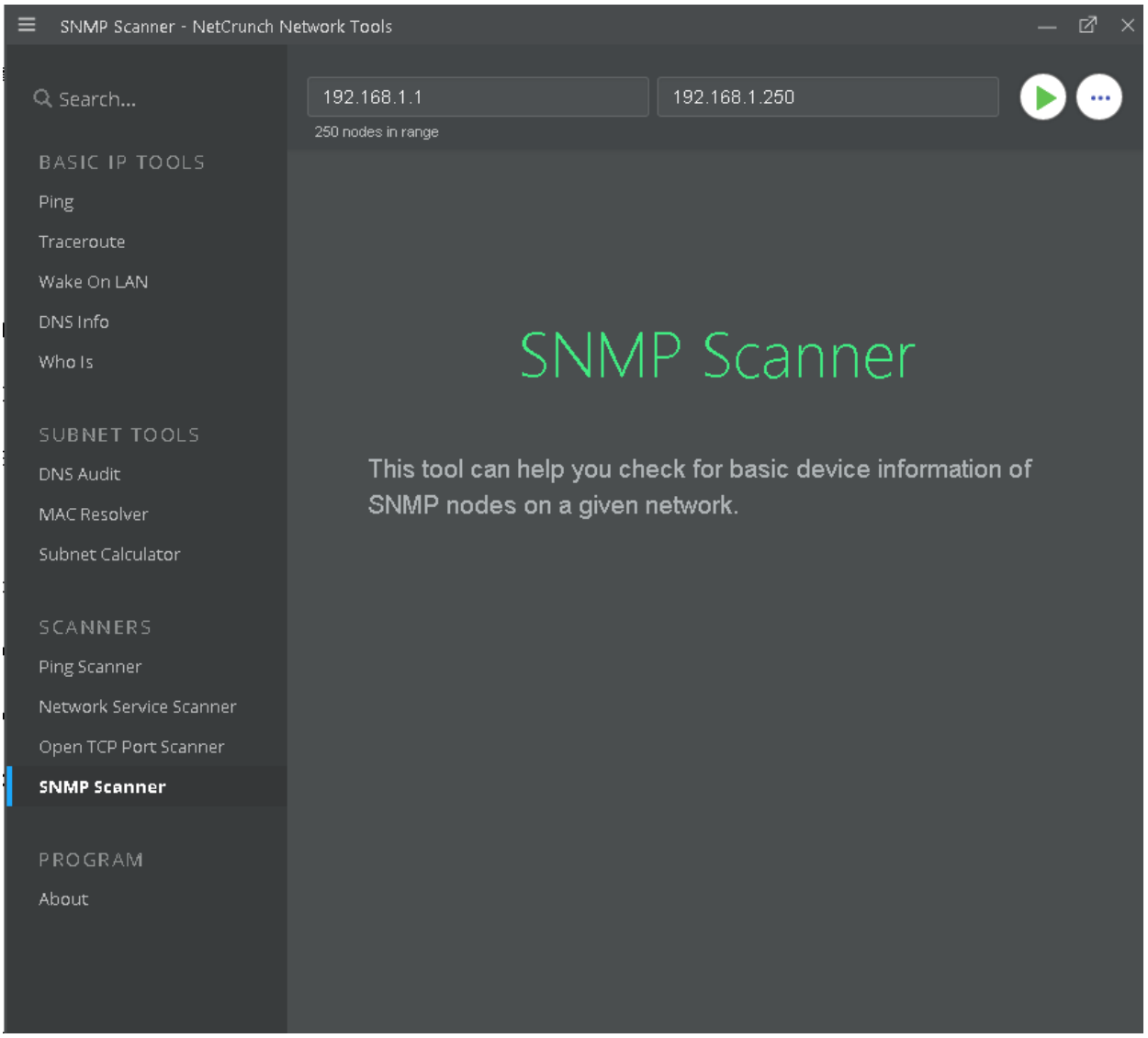
依然是一块macafee出品的攻击



NetCrunch :

项目地址：https://www.adremsoft.com/demo/

内网安全审计工具，包含了DNS审计，ping扫描，端口，　　网络服务等。



snmp for pl扫描：

项目地址：https://github.com/dheiland-r7/snmp

```
root@John:~/Desktop/snmp# ./snmpprs.pl

Syntax    "snmpprs.pl OutputFile"
-------------------------------------------------------------
example-1    ./snmpprs.pl results.txt
example-2    ./snmpprs.pl /home/location/results.txt
-------------------------------------------------------------
OutputFile :File name and path where you want the data writen too
```

其他扫描：

snmpbulkwalk：

```
root@John:~# snmpbulkwalk
Created directory: /var/lib/snmp/mib_indexes
No hostname specified.
USAGE: snmpbulkwalk [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
SNMP Version 3 specific
  -a PROTOCOL           set authentication protocol (MD5|SHA)
  -A PASSPHRASE         set authentication protocol pass phrase
  -e ENGINE-ID          set security engine ID (e.g. 800000020109840301)
  -E ENGINE-ID          set context engine ID (e.g. 800000020109840301)
  -l LEVEL              set security level (noAuthNoPriv|authNoPriv|authPriv)
  -n CONTEXT            set context name (e.g. bridge1)
  -u USER-NAME          set security name (e.g. bert)
  -x PROTOCOL           set privacy protocol (DES|AES)
  -X PASSPHRASE         set privacy protocol pass phrase
  -Z BOOTS,TIME         set destination engine boots/time
General communication options
```

snmp-check：

```
root@John:~# snmp-check
[!] You need specify a IP address target!
root@John:~# snmp-check -h
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

 Usage: snmp-check [OPTIONS] <target IP address>

  -p --port        : SNMP port. Default port is 161;
  -c --community   : SNMP community. Default is public;
  -v --version     : SNMP version (1,2c). Default is 1;

  -w --write       : detect write access (separate action by enumeration);

  -d --disable_tcp : disable TCP connections enumeration!
  -t --timeout     : timeout in seconds. Default is 5;
  -r --retries     : request retries. Default is 1;
  -i --info        : show script version;
  -h --help        : show help menu;
```

snmptest：

```
root@John:~# snmptest
No hostname specified.
USAGE: snmptest [OPTIONS] AGENT

  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
SNMP Version 3 specific
  -a PROTOCOL           set authentication protocol (MD5|SHA)
  -A PASSPHRASE         set authentication protocol pass phrase
  -e ENGINE-ID          set security engine ID (e.g. 800000020109840301)
  -E ENGINE-ID          set context engine ID (e.g. 800000020109840301)
  -l LEVEL              set security level (noAuthNoPriv|authNoPriv|authPriv)
  -n CONTEXT            set context name (e.g. bridge1)
  -u USER-NAME          set security name (e.g. bert)
  -x PROTOCOL           set privacy protocol (DES|AES)
  -X PASSPHRASE         set privacy protocol pass phrase
  -Z BOOTS,TIME         set destination engine boots/time
General communication options
  -r RETRIES            set the number of retries
  -t TIMEOUT            set the request timeout (in seconds)
Debugging
  -d                    dump input/output packets in hexadecimal
```

附录：

use auxiliary/scanner/snmp/aix_version

use auxiliary/scanner/snmp/snmp_enum

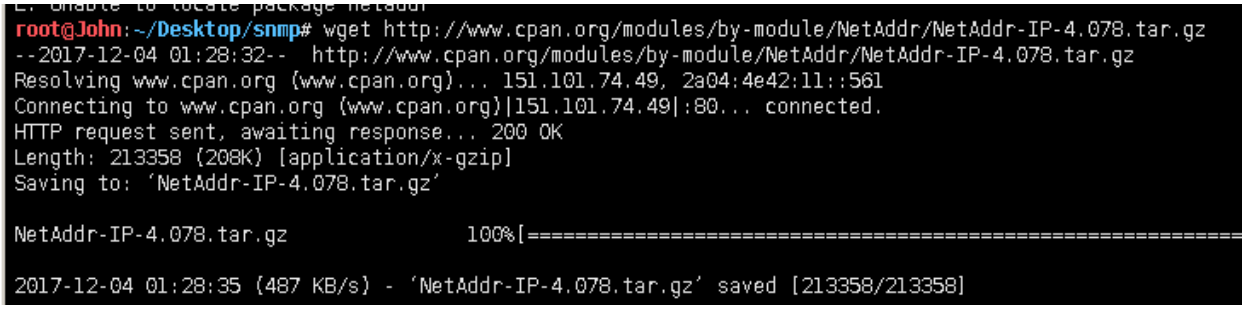
use auxiliary/scanner/snmp/arris_dg950
use auxiliary/scanner/snmp/snmp_enum_hp_laserjet
use auxiliary/scanner/snmp/brocade_enumhash
use auxiliary/scanner/snmp/snmp_enumshares
use auxiliary/scanner/snmp/cambium_snmp_loot
use auxiliary/scanner/snmp/snmp_enumusers
use auxiliary/scanner/snmp/cisco_config_tftp
use auxiliary/scanner/snmp/snmp_login
use auxiliary/scanner/snmp/cisco_upload_file
use auxiliary/scanner/snmp/snmp_set
use auxiliary/scanner/snmp/netopia_enum
use auxiliary/scanner/snmp/ubee_ddw3611
use auxiliary/scanner/snmp/sbg6580_enum
use auxiliary/scanner/snmp/xerox_workcentre_enumusers

其他内网安全审计工具（snmp）：
项目地址：https://www.solarwinds.com/topics/snmp-scanner
项目地址：https://www.netscantools.com/nstpro_snmp.html

snmp for pl ：

Can't locate NetAddr/IP

root@John:~/Desktop/snmp# wget http://www.cpan.org/modules/by-module/NetAddr/NetAddr-IP-4.078.tar.gz



root@John:~/Desktop/snmp# tar xvzf ./NetAddr-IP-4.078.tar.gz

```
root@John:~/Desktop/snmp# tar xvzf ./NetAddr-IP-4.078.tar.gz
NetAddr-IP-4.078/
NetAddr-IP-4.078/Lite/
NetAddr-IP-4.078/Lite/Util/
NetAddr-IP-4.078/Lite/Util/t/
NetAddr-IP-4.078/Lite/Util/t/inet_4map6.t
NetAddr-IP-4.078/Lite/Util/t/binet_n2ad.t
NetAddr-IP-4.078/Lite/Util/t/badd.t
NetAddr-IP-4.078/Lite/Util/t/addconst.t
NetAddr-IP-4.078/Lite/Util/t/binet_n2dx.t
NetAddr-IP-4.078/Lite/Util/t/naip_gethostbyname.t
NetAddr-IP-4.078/Lite/Util/t/mode.t
NetAddr-IP-4.078/Lite/Util/t/bin.t
NetAddr-IP-4.078/Lite/Util/t/leftshift.t
NetAddr-IP-4.078/Lite/Util/t/ipv6_ntoa.t
NetAddr-IP-4.078/Lite/Util/t/binet_pton.t
NetAddr-IP-4.078/Lite/Util/t/anyto6.t
NetAddr-IP-4.078/Lite/Util/t/bipv6func.t
NetAddr-IP-4.078/Lite/Util/t/bpackzeros.t
NetAddr-IP-4.078/Lite/Util/t/bcdn2bin.t
NetAddr-IP-4.078/Lite/Util/t/notcontiguous.t
NetAddr-IP-4.078/Lite/Util/t/bcd2bin.t
NetAddr-IP-4.078/Lite/Util/t/ipv6to4.t
NetAddr-IP-4.078/Lite/Util/t/ipv6func.t
NetAddr-IP-4.078/Lite/Util/t/inet_n2ad.t
NetAddr-IP-4.078/Lite/Util/t/binet_ntoa.t
NetAddr-IP-4.078/Lite/Util/t/bipv4_inet.t
NetAddr-IP-4.078/Lite/Util/t/inet_n2dx.t
NetAddr-IP-4.078/Lite/Util/t/4to6.t
NetAddr-IP-4.078/Lite/Util/t/isIPv4.t
NetAddr-IP-4.078/Lite/Util/t/bipv6_any2n.t
NetAddr-IP-4.078/Lite/Util/t/inet_pton.t
NetAddr-IP-4.078/Lite/Util/t/compl28.t
```

root@John:~/Desktop/snmp# cd NetAddr-IP-4.078/

root@John:~/Desktop/snmp/NetAddr-IP-4.078# ls

About-NetAddr-IP.txt Artistic Changes Copying docs IP.pm Lite Makefile.PL MANIFEST MANIFEST.SKIP META.yml t TODO

root@John:~/Desktop/snmp/NetAddr-IP-4.078# perl Makefile.PL

```
root@John:~/Desktop/snmp/NetAddr-IP-4.078# perl Makefile.PL

This build requires a C compiler by default except on Windows where
the Pure Perl version is mandatory. The Pure Perl version, which does
not require compilation of XS code, can be used by invoking this as:

  perl Makefile.PL -noxs


================================================================
W A R N I N G - Please do read below if you have legacy code
================================================================

Versions 3.21 and above of NetAddr::IP, include hooks for the Storable
class that are incompatible with the old (automatic) method of storing
data. To regain backwards compatibility, the module must be use()d as

    use NetAddr::IP ':old_storable';

which will disable the new hooks and revert back to the old ways.

If you do not use Storable along with NetAddr::IP, or just don't know
what this all means, most likely you're safe to go ahead.

Versions before 3.25 recognized by default IP addresses as returned by
inet_aton. This is no longer the default. To enable this behavior
again, the module must be use()d as

    use NetAddr::IP ':aton';

Versions before 4.000 recognized the above syntax. This behavior is
```

root@John:~/Desktop/snmp/NetAddr-IP-4.078# make

```
root@John:~/Desktop/snmp/NetAddr-IP-4.078# make
cp IP.pm blib/lib/NetAddr/IP.pm
AutoSplitting blib/lib/NetAddr/IP.pm (blib/lib/auto/NetAddr/IP)
make[1]: Entering directory '/root/Desktop/snmp/NetAddr-IP-4.078/Lite'
cp Lite.pm ../blib/lib/NetAddr/IP/Lite.pm
make[2]: Entering directory '/root/Desktop/snmp/NetAddr-IP-4.078/Lite/Util'
cp Util.pm ../../blib/lib/NetAddr/IP/Util.pm
AutoSplitting ../../blib/lib/NetAddr/IP/Util.pm (../../blib/lib/auto/NetAddr
cp lib/NetAddr/IP/UtilPP.pm ../../blib/lib/NetAddr/IP/UtilPP.pm
AutoSplitting ../../blib/lib/NetAddr/IP/UtilPP.pm (../../blib/lib/auto/NetAd
cp lib/NetAddr/IP/InetBase.pm ../../blib/lib/NetAddr/IP/InetBase.pm
AutoSplitting ../../blib/lib/NetAddr/IP/InetBase.pm (../../blib/lib/auto/Net
cp Util_IS.pm ../../blib/lib/NetAddr/IP/Util_IS.pm
Running Mkbootstrap for NetAddr::IP::Util ()
chmod 644 "Util.bs"
"/usr/bin/perl" "/usr/share/perl/5.24.1/ExtUtils/xsubpp"  -typemap "/usr/sha
mv Util.xsc Util.c
x86_64-linux-gnu-gcc -c   -D_REENTRANT -D_GNU_SOURCE -DDEBIAN -fwrapv -fno-s
SET_BITS=64 -O2 -g   -DVERSION=\"1.53\" -DXS_VERSION=\"1.53\" -fPIC "-I/usr/
rm -f ../../blib/arch/auto/NetAddr/IP/Util/Util.so
x86_64-linux-gnu-gcc  -shared -L/usr/local/lib -fstack-protector-strong Util
        \

chmod 755 ../../blib/arch/auto/NetAddr/IP/Util/Util.so
"/usr/bin/perl" -MExtUtils::Command::MM -e 'cp_nonempty' -- Util.bs ../../bl
Manifying 3 pod documents
```

root@John:~/Desktop/snmp/NetAddr-IP-4.078# make install

```
root@John:~/Desktop/snmp/NetAddr-IP-4.078# make install
make[1]: Entering directory '/root/Desktop/snmp/NetAddr-IP-4.078/Lite'
make[2]: Entering directory '/root/Desktop/snmp/NetAddr-IP-4.078/Lite/Util'
Running Mkbootstrap for NetAddr::IP::Util ()
chmod 644 "Util.bs"
Manifying 3 pod documents
make[2]: Leaving directory '/root/Desktop/snmp/NetAddr-IP-4.078/Lite/Util'
Manifying 1 pod document
make[1]: Leaving directory '/root/Desktop/snmp/NetAddr-IP-4.078/Lite'
Manifying 1 pod document
Files found in blib/arch: installing files in blib/lib into architecture dependent library tree
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/Util/Util.so
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/_splitref.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/re.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/_compV6.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/_splitplan.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/wildcard.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/nprefix.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/canon.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/re6.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/prefix.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/coalesce.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/compactref.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/autosplit.ix
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/do_prefix.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/hostenum.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/short.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/_compact_v6.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/mod_version.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/Util/autosplit.ix
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/InetBase/ipv6_aton.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/InetBase/inet_n2ad.al
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/InetBase/autosplit.ix
Installing /usr/local/lib/x86_64-linux-gnu/perl/5.24.1/auto/NetAddr/IP/InetBase/_inet_ntop.al
```

> _ < !!

```
root@John:~/Desktop/snmp# ./snmpbw.pl

Syntax    "snmpbw.pl target community timeout threads"
-------------------------------------------------------
example-1   ./snmpbw.pl 192.168.0.1 public 2 1
example-2   ./snmpbw.pl ipfile.txt  public 2 4
-------------------------------------------------------
community :public or what ever the community string is
timeout   :Timeout is in seconds
threads   :number of threads to run
```

- Micropoor