How to Use ARPing Command on a Security Test

MERIMETSO

The **arping** tool is designed to allow us to identify every machine on a local area network by means sending a broadcast ARP request. The basic arguments to use the tool are defined as follows. Please note that to use this tool you must be root.

```
kali@kali:~$ arping
ARPing 2.23, by Thomas Habets <thomas@habets.se>
usage: arping [ -0aAbdDeFpPqrRuUvzZ ] [ -w <sec> ] [ -W <sec> ] [ -S <host/ip> ]
              [ -T <host/ip ] [ -s <MAC> ] [ -t <MAC> ] [ -c <count> ]
              [ -C <count> ] [ -i <interface> ] [ -m <type> ] [ -g <group> ]
              [ -V <vlan> ] [ -Q <priority> ] <host/ip/MAC | -B>
For complete usage info, use --help or check the manpage.

kali@kali:~$
```

We can use **arping** to identify if a specific IP is connected to the network, as follows:

```
kali@kali:~$ sudo arping -i eth0 192.168.2.12
ARPING 192.168.2.12
60 bytes from 00:0c:29:19:59:34 (192.168.2.12): index=0 time=606.833 usec
. . . . . . . . . . . . .
```

The following options are useful when performing an arping scan.

-c count	Only send count requests.
-i interface	Send the data out on a specific interface.
-p MAC	Turn on promiscuous mode on interface, use this if you don't "own" the MAC address you are using.
-s MAC	Set source MAC address. You may need to use `-p` with this
-S IP	Set the source IP address to be used
-T IP	Use `-T` as target address when pinging MACs that won't respond to a broadcast ping but perhaps to a directed broadcast. For example, to check the address of MAC-A, use knowledge of MAC-B and IP-B. `$ arping -S <IP-B> -s <MAC-B> -p <MAC-A>`
-t MAC	Set target MAC address to use when pinging IP address.
-v	Verbose output. Use twice for more messages.
-V vlan	VLAN tag to set. Defaults to no VLAN tag.
-W sec	Time to wait between pings.

So, via a bit of BASH scripting we can use arping to scan all machines on a local area network. In the following example we can arping every machine on a class C network via the command **arpinhsh.sh 192.168.2**. This command will then perform a single arping against every machine on the network 192.168.2.0/24

```
kali@kali:~$ cat arpingsh.sh
#/usr/bin/bash
ARGV1=$1
for ((i=1;i<=254;i++))
do
       /usr/sbin/arping -c1 $ARGV1.$i
done
```

Just as a note to end on we can as to an arp ping scan using NMAP as follows:

```
kali@kali:~$ nmap -sP -PR 192.168.2.0/24
```