SCRIPTING WITH BASH

Thursday, July 22, 2021 11:49 PM

- **IF CONFIG-**
  - ```
    ┌──(atom㉿atom)-[~]
    └─$ ifconfig
    eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
            inet 10.28.1.235  netmask 255.255.255.0  broadcast 10.28.1.255
            inet6 fe80::20c:29ff:fe25:feae  prefixlen 64  scopeid 0x20<link>
            ether 00:0c:29:25:fe:ae  txqueuelen 1000  (Ethernet)
            RX packets 1118  bytes 70505 (68.8 KiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 61  bytes 5706 (5.5 KiB)
            TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

    lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
            inet 127.0.0.1  netmask 255.0.0.0
            inet6 ::1  prefixlen 128  scopeid 0x10<host>
            loop  txqueuelen 1000  (Local Loopback)
            RX packets 24  bytes 1360 (1.3 KiB)
            RX errors 0  dropped 0  overruns 0  frame 0
            TX packets 24  bytes 1360 (1.3 KiB)
            TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
    ```
- **PING SWEEPER-**
  - **ping 10.28.1.109** | **#Ping the specific IP address**
    - ```
      ┌──(atom㉿kali)-[~]
      └─$ ping 10.28.1.109
      PING 10.28.1.109 (10.28.1.109) 56(84) bytes of data.
      64 bytes from 10.28.1.109: icmp_seq=1 ttl=255 time=9.08 ms
      64 bytes from 10.28.1.109: icmp_seq=2 ttl=255 time=5.99 ms
      64 bytes from 10.28.1.109: icmp_seq=3 ttl=255 time=4.82 ms
      64 bytes from 10.28.1.109: icmp_seq=4 ttl=255 time=6.74 ms
      ^C
      --- 10.28.1.109 ping statistics ---
      4 packets transmitted, 4 received, 0% packet loss, time 3018ms
      rtt min/avg/max/mdev = 4.820/6.657/9.080/1.556 ms
      ```
  - **ping 10.28.1.109 -c 1** | **#Ping the specific IP address one time**
    - ```
      ┌──(atom㉿kali)-[~]
      └─$ ping 10.28.1.109 -c 1
      PING 10.28.1.109 (10.28.1.109) 56(84) bytes of data.
      64 bytes from 10.28.1.109: icmp_seq=1 ttl=255 time=5.39 ms

      --- 10.28.1.109 ping statistics ---
      1 packets transmitted, 1 received, 0% packet loss, time 0ms
      rtt min/avg/max/mdev = 5.391/5.391/5.391/0.000 ms
      ```
  - **ping 10.28.1.109 -c 1 > ping.txt** | **#Saves the specific ping command to a file**
    - ```
      ┌──(atom㉿kali)-[~/test]
      └─$ ping 10.28.1.109 -c 1 > ping.txt

      ┌──(atom㉿kali)-[~/test]
      └─$ cat ping.txt
      PING 10.28.1.109 (10.28.1.109) 56(84) bytes of data.
      64 bytes from 10.28.1.109: icmp_seq=1 ttl=255 time=5.13 ms

      --- 10.28.1.109 ping statistics ---
      1 packets transmitted, 1 received, 0% packet loss, time 0ms
      rtt min/avg/max/mdev = 5.130/5.130/5.130/0.000 ms
      ```
  - **cat ping.txt | grep "64 bytes"** | **#Prints the specific line from the file of the ping request which contains 64 bytes**
    - ```
      ┌──(atom㉿kali)-[~/test]
      └─$ cat ping.txt | grep "64 bytes"
      64 bytes from 10.28.1.109: icmp_seq=1 ttl=255 time=5.13 ms
      ```
  - **cat ping.txt | grep "64 bytes" | cut -d " " -f 4** | **#Prints the above line info after cutting the 4 part of the line one**
    - ```
      ┌──(atom㉿kali)-[~/test]
      └─$ cat ping.txt | grep "64 bytes" | cut -d " " -f 4
      10.28.1.109:
      ```
  - **cat ping.txt | grep "64 bytes" | cut -d " " -f 4 | tr -d ":"** | **#Prints the above line (IP address)without the ":"**
    - ```
      ┌──(atom㉿kali)-[~/test]
      └─$ cat ping.txt | grep "64 bytes" | cut -d " " -f 4 | tr -d ":"
      10.28.1.109
      ```
  - FINAL CODE IPSWEEPER-

#!/bin/bash
if ["$1" == ""]
then
echo "your forgot an ip address!"
echo "Syntax: ./ipsweep.sh 10.28.1"
else
for ip in `seq 1 254`; do
ping -c 1 $1.$ip | grep "64 bytes" | cut -d " " -f 4 | tr -d ":" &
done
fi
	#Decleration of the program (BASH)
	#If we forgot to give the IP address
	
	#For IP from (1 to 254)
	#Doing the ping command and pipe the IP ADDERSS
	Here $1 means argument one(IP Address) [$1.$ip]-> 192.168.1.1

    ~/test/ipsweep.sh - Mousepad

    File Edit Search View Document Help

    ```
    1 #!/bin/bash
    2
    3 if [ "$1" == "" ]
    4 then
    5 echo "your forgot an ip address!"
    6 echo "Syntax: ./ipsweep.sh 10.28.1"
    7 else
    8 for ip in `seq 1 254`; do
    9 ping -c 1 $1.$ip | grep "64 bytes" | cut -d " " -f 4 | tr -d ":" &
    10 done
    11 fi
    ```

    - ```
      ┌──(atom㉿kali)-[~/test]
      └─$ ./ipsweep.sh 10.28.1
      10.28.1.5
      10.28.1.6
      10.28.1.3
      10.28.1.4
      10.28.1.8
      10.28.1.7
      10.28.1.2
      10.28.1.15
      10.28.1.10
      10.28.1.65

      ┌──(atom㉿kali)-[~/test]
      └─$ 10.28.1.91
      10.28.1.55
      10.28.1.109
      10.28.1.110
      10.28.1.113
      10.28.1.114
      10.28.1.247
      10.28.1.242
      ```
  - **./ipsweeper.sh 10.28.1 > ping.txt**
    - ```
      ┌──(atom㉿kali)-[~/test]
      └─$ ./ipsweep.sh 10.28.1 > ping.txt

      ┌──(atom㉿kali)-[~/test]
      └─$ cat ping.txt
      10.28.1.65
      10.28.1.5
      10.28.1.114
      10.28.1.91
      10.28.1.3
      10.28.1.2
      10.28.1.15
      10.28.1.8
      10.28.1.109
      10.28.1.10
      10.28.1.6
      10.28.1.4
      10.28.1.7
      10.28.1.110
      10.28.1.16
      10.28.1.113
      10.28.1.247
      10.28.1.17
      10.28.1.55
      10.28.1.49
      ```
  - EX- **for ip in $(cat ping.txt); do nmap -T4 -A -p- -Pn $ip& done > nmap.txt**
    - For nmap scanning
      ```