Ping Sweeper Bash Scripting with NMAP

הסבר

אראה באמצעות כמה פקודות כיצד ניתן ליצור סקריפט בסביבת לינוקס שסורק את כתובות ה **IP** ברשת המקומית ולאחר מכן באמצעות הקובץ עם הכתובת, כיצד ניתן להשתמש בו בסריקת רשת ב **NMAP**.

1. ראשית נכנס לטרמינל ונזין את הפקודה הבאה:

```
┌──(kali㉿kali)-[~]
└─$ ping -c 1 8.8.8.8 > ping.txt
```

בפקודה זאת אנחנו עושים פינג עם חבילה 1 לגוגל ומייצאים את התשובה לקובץ ping.txt.

ניתן לראות את תוכן הקובץ באמצעות הפקודה cat:

```
┌──(kali㉿kali)-[~]
└─$ cat ping.txt
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=10.7 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 10.696/10.696/10.696/0.000 ms

┌──(kali㉿kali)-[~]
└─$
```

2. כעת נרצה "לחתוך" מהפלט את כתובת ה IP לצורך שימוש בו באוטומציה בהמשך:

```
┌──(kali㉿kali)-[~]
└─$ cat ping.txt | grep "64 bytes"
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=10.7 ms

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ cat ping.txt | grep "64 bytes" | cut -d " " -f 4 | tr -d ":"
8.8.8.8

┌──(kali㉿kali)-[~]
└─$
```

הסבר:

- הפקודה GREP משתמש לחיפוש.
- הפקודה cut משמשת לחיתוך
- d flag משתייך לפקודת cut, ומתפקד בתור delimiter (מפריד) באמצעות רווח.
- f flag משתייך לפקודת cut, ומתפקד בתור Field (שדה). כלומר הוא מייצג את השדה הרביעי, במקרה הזה כתובת ה IP.
- Tr -d מאפשר לעשות שימוש דומה לפקודה cut אך "משמיט" את : מהכתובת IP.

3. כעת ניצור סקריפט שיאפשר לנו לשלוח פינגים לכתובות ה IP ברשת המקומית באמצעות אוטומציה. הסבר נמצא בתוך הסקריפט:

```
1 #! /bin/bash
2
3
4
5 if [ "$1" == "" ]    #The variable after the command .ipsweep.sh ..
6 then
7 echo "You Forgot an IP Adress!" #print it
8 echo "Syntax: ./ipsweep.sh 192.168.1" #print it
9
10 else
11 for ip in `seq 1 254`; do #loop in range
12 ping -c 1 $1.$ip| grep "64 bytes" | cut -d " " -f 4 | tr -d ":" & #ping 1 time, use the syntax $1.$ip
13 done
14 fi
```

כעת נריץ את הסקריפט ונראה אותו בפעולה:

```
┌──(kali㉿kali)-[~]
└─$ ./ipsweep.sh
You Forgot an IP Adress!
Syntax: ./ipsweep.sh 192.168.1
```

```
┌──(kali㉿kali)-[~]
└─$ ./ipsweep.sh 192.168.1
192.168.1.1
192.168.1.62
192.168.1.63
192.168.1.61
192.168.1.100
192.168.1.104
192.168.1.152
192.168.1.158
192.168.1.170
192.168.1.234
```

נראה שהוא עובד מעולה.

כעת נייצא את כל הכתובות IP לתוך קובץ TXT על מנת שנוכל להשתמש בהם בסריקה ב NMAP:

```
┌──(root💀kali)-[/home/kali]
└─# ./ipsweep.sh 192.168.1 > ips.txt
```

```
┌──(root💀kali)-[/home/kali]
└─# cat ips.txt
92.168.1.1
92.168.1.62
92.168.1.63
92.168.1.61
92.168.1.104
92.168.1.100
92.168.1.152
92.168.1.158
92.168.1.170
92.168.1.234
92.168.1.221
```

כעת באמצעות הפקודה הבאה נשתמש בקובץ עם כתובות ה IP שסרקנו ונסרוק אותם עם NMAP:

```
┌──(root💀 kali)-[/home/kali]
└─# for ip in $(cat ips.txt); do nmap $ip & done
[2] 53022
[3] 53023
[4] 53024
[5] 53025
[6] 53026
[7] 53027
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-26 07:12 EST
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-26 07:12 EST
[8] 53031
[9] 53035
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-26 07:12 EST
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-26 07:12 EST
[10] 53036
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-26 07:12 EST
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-26 07:12 EST
[11] 53052
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-26 07:12 EST
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-26 07:12 EST
[12] 53053

Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-26 07:12 EST
┌──(root💀 kali)-[/home/kali]
└─# Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-26 07:12 EST
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-26 07:12 EST
```