**In the name of GOD**

**security essentials practical homework**

**Amir H Pirhosseinloo**

**9531014**

1. Question 1
2. before deleting a character
   1. md5 result (hexadecimal digits): f868791dabbbba52bf6e7d9ca445a44b
   2. sha256 result (hexadecimal digits): aca0ba757235a44b8addac6f6419ecdbd37dcdd01661864e47de2ccf1bdef3b9
3. after deleting a character (deleting ‘I’)
   1. md5 result (hexadecimal digits): 83ea6447a0563e99c435b5db113ef035
   2. sha256 result (hexadecimal digits): 3baaa93f259269a049190769479eeb6f2db4926f7b2f3df9b730c6fa4dc8fda6
4. number of bytes changed (md5): 16
5. number of bytes changed (sha256): 32
6. Question 2
7. Question 3
   1. key = -10 or 16 (shift 10 units to left, for example convert ‘t’ to ‘j’)
   2. plain text:

the caesar cipher technique is one of the earliest and simplest method of encryption technique.

it’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter

some fixed number of positions down the alphabet. for example with a shift of 1, a would be

replaced by b, b would become c, and so on. the method is apparently named after julius caesar,

who apparently used it to communicate with his officials. thus to cipher a given text we need an

integer value, known as shift which indicates the number of position each letter of the text has

been moved down.

* 1. character ‘e’ is the most frequent letter in texts in English language, so the most frequent character in cipher text is equivalent to ‘e’ in plain text. so number of shift units will be determined according to difference between 2 letters.

1. 3 systems containing 2 kali system + 1 windows 10

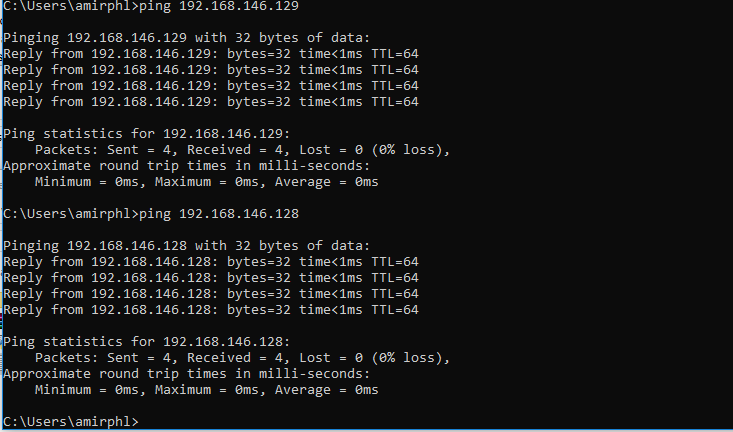
IP of first system(kali): 192.168.146.128

IP of second system(kali): 192.168.146.129

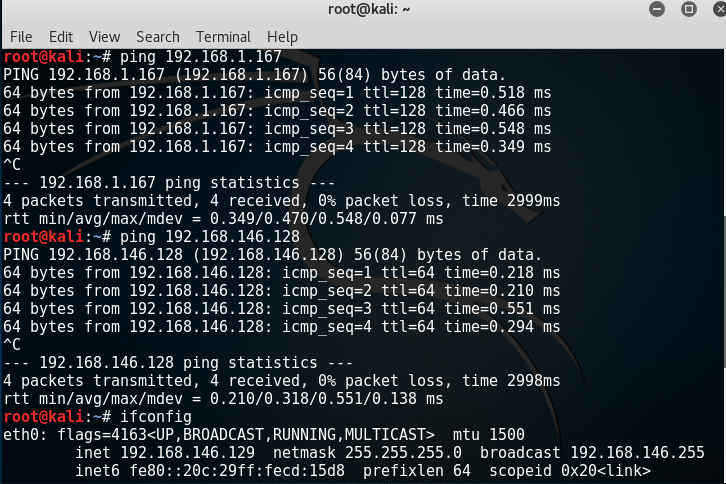
IP of third system(windows): 192.168.1.167

ping report:

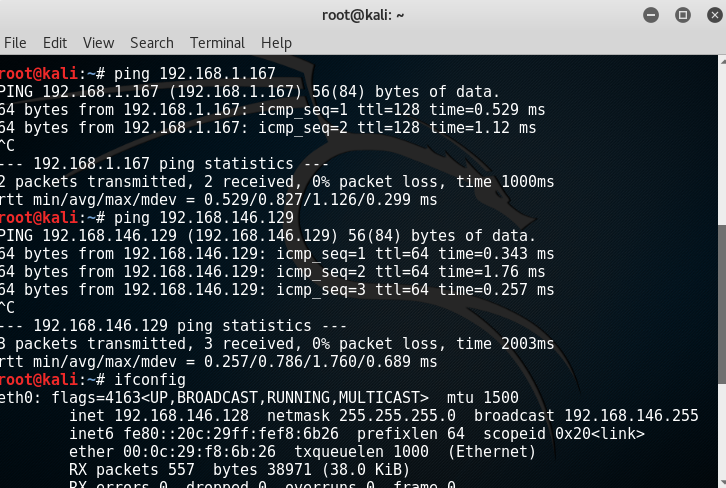
ping 192.168.146.128 and 192.168.146.129 from 192.168.1.167:



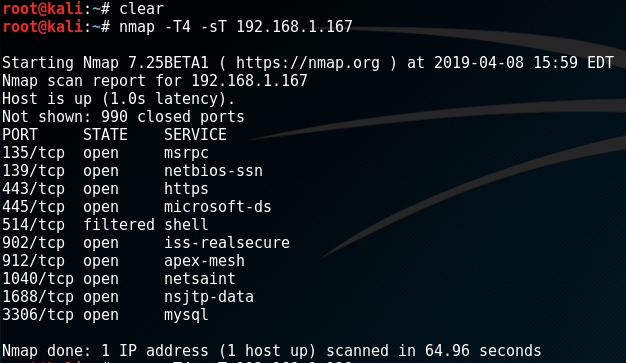
ping 192.168.146.128 and 192.168.1.167 from 192.168.146.129:

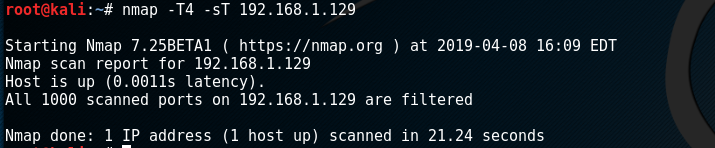
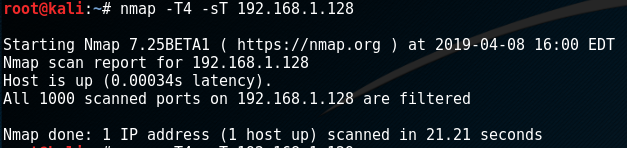


ping 192.168.146.129 and 192.168.1.167 from 192.168.146.128:

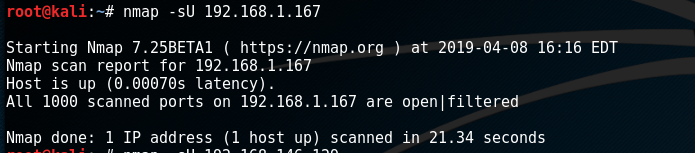


TCP full scan result from 192.168.146.128:

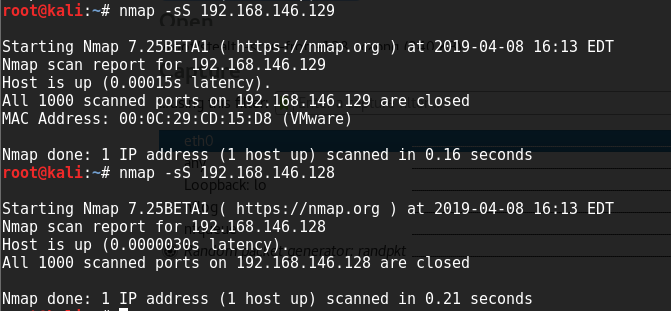


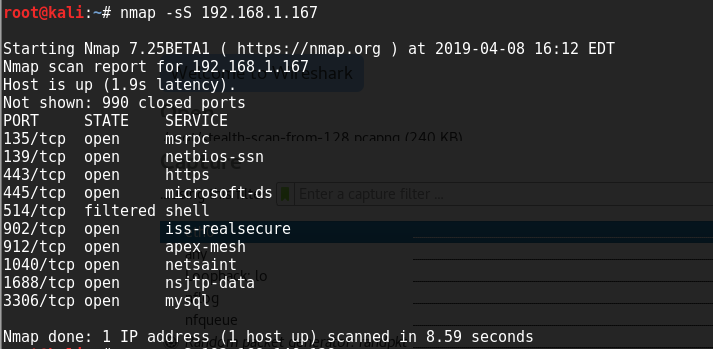


UDP scan result from 192.168.146.128:

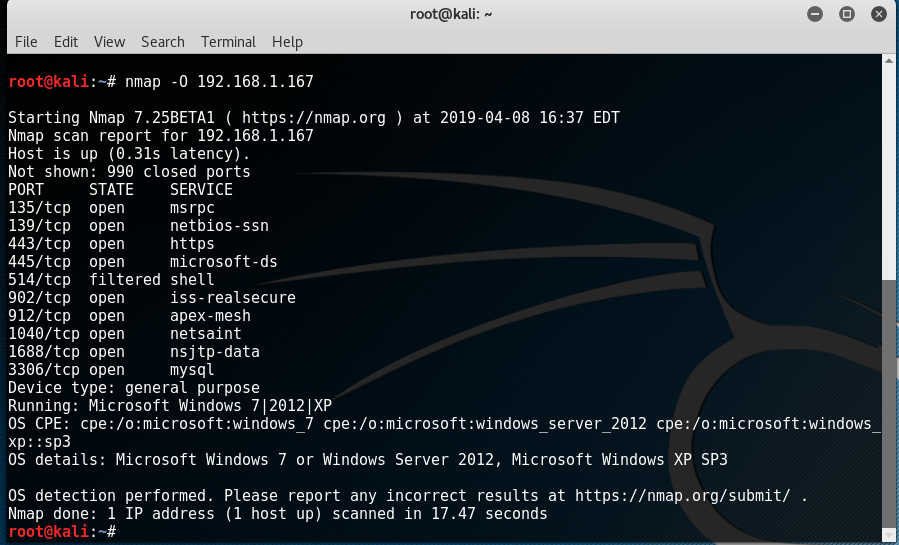


Stealth scan result from 192.168.146.128:

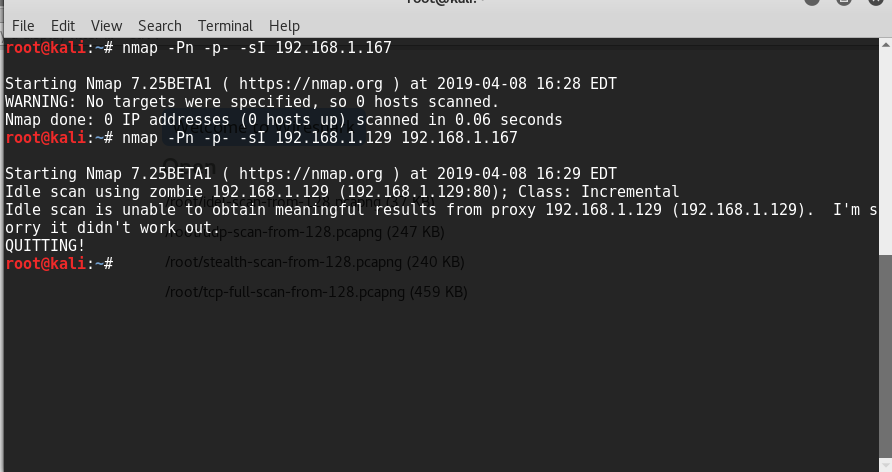




Fingerprint scan result from 192.168.146.128:



Idle scan result from 192.168.146.128:



Wireshark files are available in Wireshark folder.