In the name of GOD

security essentials practical homework

Amir H Pirhosseinloo

9531014

1. Question 1
   a) before deleting a character
      a. md5 result (hexadecimal digits): f868791dabbbba52bf6e7d9ca445a44b
      b. sha256 result (hexadecimal digits): aca0ba757235a44b8addac6f6419ecdbd37dcdd01661864e47de2ccf1bdef3b9
   b) after deleting a character (deleting 'l')
      a. md5 result (hexadecimal digits): 83ea6447a0563e99c435b5db113ef035
      b. sha256 result (hexadecimal digits): 3baaa93f259269a049190769479eeb6f2db4926f7b2f3df9b730c6fa4dc8fda6
   c) number of bytes changed (md5): 16
   d) number of bytes changed (sha256): 32
2. Question 2
3. Question 3
   a. key = -10 or 16 (shift 10 units to left, for example convert 't' to 'j')
   b. 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.
   c. 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.
4. 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:

```
C:\Users\amirphl>ping 192.168.146.129

Pinging 192.168.146.129 with 32 bytes of data:
Reply from 192.168.146.129: bytes=32 time<1ms TTL=64
Reply from 192.168.146.129: bytes=32 time<1ms TTL=64
Reply from 192.168.146.129: bytes=32 time<1ms TTL=64
Reply from 192.168.146.129: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.146.129:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\amirphl>ping 192.168.146.128

Pinging 192.168.146.128 with 32 bytes of data:
Reply from 192.168.146.128: bytes=32 time<1ms TTL=64
Reply from 192.168.146.128: bytes=32 time<1ms TTL=64
Reply from 192.168.146.128: bytes=32 time<1ms TTL=64
Reply from 192.168.146.128: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.146.128:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\amirphl>
```

ping 192.168.146.128 and 192.168.1.167 from 192.168.146.129:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# ping 192.168.1.167
PING 192.168.1.167 (192.168.1.167) 56(84) bytes of data.
64 bytes from 192.168.1.167: icmp_seq=1 ttl=128 time=0.518 ms
64 bytes from 192.168.1.167: icmp_seq=2 ttl=128 time=0.466 ms
64 bytes from 192.168.1.167: icmp_seq=3 ttl=128 time=0.548 ms
64 bytes from 192.168.1.167: icmp_seq=4 ttl=128 time=0.349 ms
^C
--- 192.168.1.167 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.349/0.470/0.548/0.077 ms
root@kali:~# ping 192.168.146.128
PING 192.168.146.128 (192.168.146.128) 56(84) bytes of data.
64 bytes from 192.168.146.128: icmp_seq=1 ttl=64 time=0.218 ms
64 bytes from 192.168.146.128: icmp_seq=2 ttl=64 time=0.210 ms
64 bytes from 192.168.146.128: icmp_seq=3 ttl=64 time=0.551 ms
64 bytes from 192.168.146.128: icmp_seq=4 ttl=64 time=0.294 ms
^C
--- 192.168.146.128 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.210/0.318/0.551/0.138 ms
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.146.129  netmask 255.255.255.0  broadcast 192.168.146.255
        inet6 fe80::20c:29ff:fecd:15d8  prefixlen 64  scopeid 0x20<link>
```

ping 192.168.146.129 and 192.168.1.167 from 192.168.146.128:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# ping 192.168.1.167
PING 192.168.1.167 (192.168.1.167) 56(84) bytes of data.
64 bytes from 192.168.1.167: icmp_seq=1 ttl=128 time=0.529 ms
64 bytes from 192.168.1.167: icmp_seq=2 ttl=128 time=1.12 ms
^C
--- 192.168.1.167 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.529/0.827/1.126/0.299 ms
root@kali:~# ping 192.168.146.129
PING 192.168.146.129 (192.168.146.129) 56(84) bytes of data.
64 bytes from 192.168.146.129: icmp_seq=1 ttl=64 time=0.343 ms
64 bytes from 192.168.146.129: icmp_seq=2 ttl=64 time=1.76 ms
64 bytes from 192.168.146.129: icmp_seq=3 ttl=64 time=0.257 ms
^C
--- 192.168.146.129 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.257/0.786/1.760/0.689 ms
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.146.128  netmask 255.255.255.0  broadcast 192.168.146.255
        inet6 fe80::20c:29ff:fef8:6b26  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:f8:6b:26  txqueuelen 1000  (Ethernet)
        RX packets 557  bytes 38971 (38.0 KiB)
```

TCP full scan result from 192.168.146.128:

```
root@kali:~# clear
root@kali:~# nmap -T4 -sT 192.168.1.167

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2019-04-08 15:59 EDT
Nmap scan report for 192.168.1.167
Host is up (1.0s latency).
Not shown: 990 closed ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
443/tcp  open     https
445/tcp  open     microsoft-ds
514/tcp  filtered shell
902/tcp  open     iss-realsecure
912/tcp  open     apex-mesh
1040/tcp open     netsaint
1688/tcp open     nsjtp-data
3306/tcp open     mysql

Nmap done: 1 IP address (1 host up) scanned in 64.96 seconds
```

```
root@kali:~# nmap -T4 -sT 192.168.1.128

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2019-04-08 16:00 EDT
Nmap scan report for 192.168.1.128
Host is up (0.00034s latency).
All 1000 scanned ports on 192.168.1.128 are filtered

Nmap done: 1 IP address (1 host up) scanned in 21.21 seconds
```

```
root@kali:~# nmap -T4 -sT 192.168.1.129

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2019-04-08 16:09 EDT
Nmap scan report for 192.168.1.129
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.1.129 are filtered

Nmap done: 1 IP address (1 host up) scanned in 21.24 seconds
```

UDP scan result from 192.168.146.128:

```
root@kali:~# nmap -sU 192.168.1.167

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2019-04-08 16:16 EDT
Nmap scan report for 192.168.1.167
Host is up (0.00070s latency).
All 1000 scanned ports on 192.168.1.167 are open|filtered

Nmap done: 1 IP address (1 host up) scanned in 21.34 seconds
```

Stealth scan result from 192.168.146.128:

```
root@kali:~# nmap -sS 192.168.146.129

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2019-04-08 16:13 EDT
Nmap scan report for 192.168.146.129
Host is up (0.00015s latency).
All 1000 scanned ports on 192.168.146.129 are closed
MAC Address: 00:0C:29:CD:15:D8 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
root@kali:~# nmap -sS 192.168.146.128

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2019-04-08 16:13 EDT
Nmap scan report for 192.168.146.128
Host is up (0.0000030s latency).
All 1000 scanned ports on 192.168.146.128 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

```
root@kali:~# nmap -sS 192.168.1.167

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2019-04-08 16:12 EDT
Nmap scan report for 192.168.1.167
Host is up (1.9s latency).
Not shown: 990 closed ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
443/tcp  open     https
445/tcp  open     microsoft-ds
514/tcp  filtered shell
902/tcp  open     iss-realsecure
912/tcp  open     apex-mesh
1040/tcp open     netsaint
1688/tcp open     nsjtp-data
3306/tcp open     mysql

Nmap done: 1 IP address (1 host up) scanned in 8.59 seconds
```

Fingerprint scan result from 192.168.146.128:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help

root@kali:~# nmap -O 192.168.1.167

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2019-04-08 16:37 EDT
Nmap scan report for 192.168.1.167
Host is up (0.31s latency).
Not shown: 990 closed ports
PORT     STATE    SERVICE
135/tcp  open     msrpc
139/tcp  open     netbios-ssn
443/tcp  open     https
445/tcp  open     microsoft-ds
514/tcp  filtered shell
902/tcp  open     iss-realsecure
912/tcp  open     apex-mesh
1040/tcp open     netsaint
1688/tcp open     nsjtp-data
3306/tcp open     mysql
Device type: general purpose
Running: Microsoft Windows 7|2012|XP
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012 cpe:/o:microsoft:windows_
xp::sp3
OS details: Microsoft Windows 7 or Windows Server 2012, Microsoft Windows XP SP3

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.47 seconds
root@kali:~#
```

Idle scan result from 192.168.146.128:

```
File  Edit  View  Search  Terminal  Help
root@kali:~# nmap -Pn -p- -sI 192.168.1.167

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2019-04-08 16:28 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.06 seconds
root@kali:~# nmap -Pn -p- -sI 192.168.1.129 192.168.1.167

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2019-04-08 16:29 EDT
Idle scan using zombie 192.168.1.129 (192.168.1.129:80); Class: Incremental
Idle scan is unable to obtain meaningful results from proxy 192.168.1.129 (192.168.1.129).  I'm s
orry it didn't work out.
QUITTING!
root@kali:~#
```

Wireshark files are available in Wireshark folder.