ASTANA IT UNIVERSITY

Report

Assignment 7

Student of Group: CS-2115N
Full name: Adil Ergazin

Astana 2023

Tryhachkme assignments

Objective

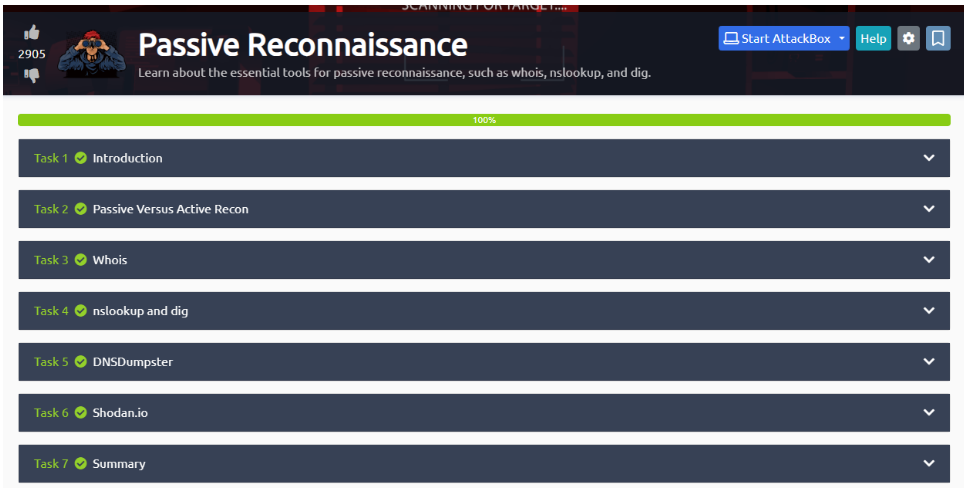
Part 1. Passive Reconnaissance

Part 2. Active Reconnaissance

Part 3. Introduction to Cryptography

Part 4. Encryption – Crypto 101

Part 1. Passive Reconnaissance



Passive Reconnaissance

Learn about the essential tools for passive reconnaissance, such as whois, nslookup, and dig.

Task 1 ✓ Introduction

Task 2 ✓ Passive Versus Active Recon

Task 3 ✓ Whois

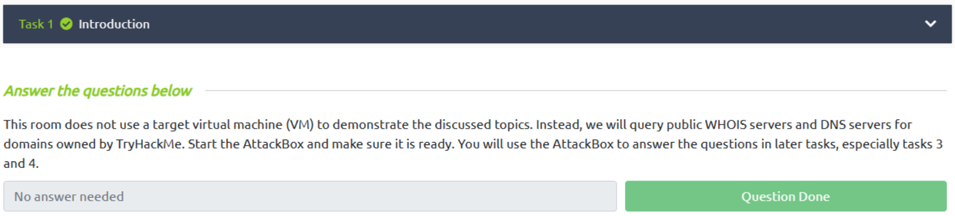
Task 4 ✓ nslookup and dig

Task 5 ✓ DNSDumpster

Task 6 ✓ Shodan.io

Task 7 ✓ Summary

1. Introduction



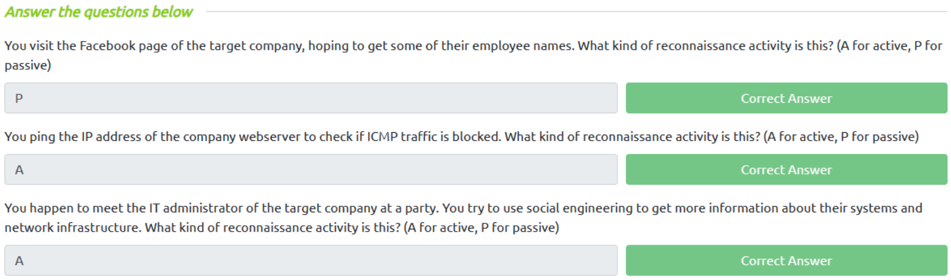
Task 1 ✓ Introduction

Answer the questions below

This room does not use a target virtual machine (VM) to demonstrate the discussed topics. Instead, we will query public WHOIS servers and DNS servers for domains owned by TryHackMe. Start the AttackBox and make sure it is ready. You will use the AttackBox to answer the questions in later tasks, especially tasks 3 and 4.

2. Passive Versus Active Recon

Task 2 ✓ Passive Versus Active Recon



Answer the questions below

You visit the Facebook page of the target company, hoping to get some of their employee names. What kind of reconnaissance activity is this? (A for active, P for passive)

P

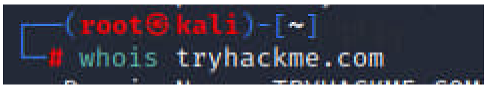
You ping the IP address of the company webserver to check if ICMP traffic is blocked. What kind of reconnaissance activity is this? (A for active, P for passive)

A

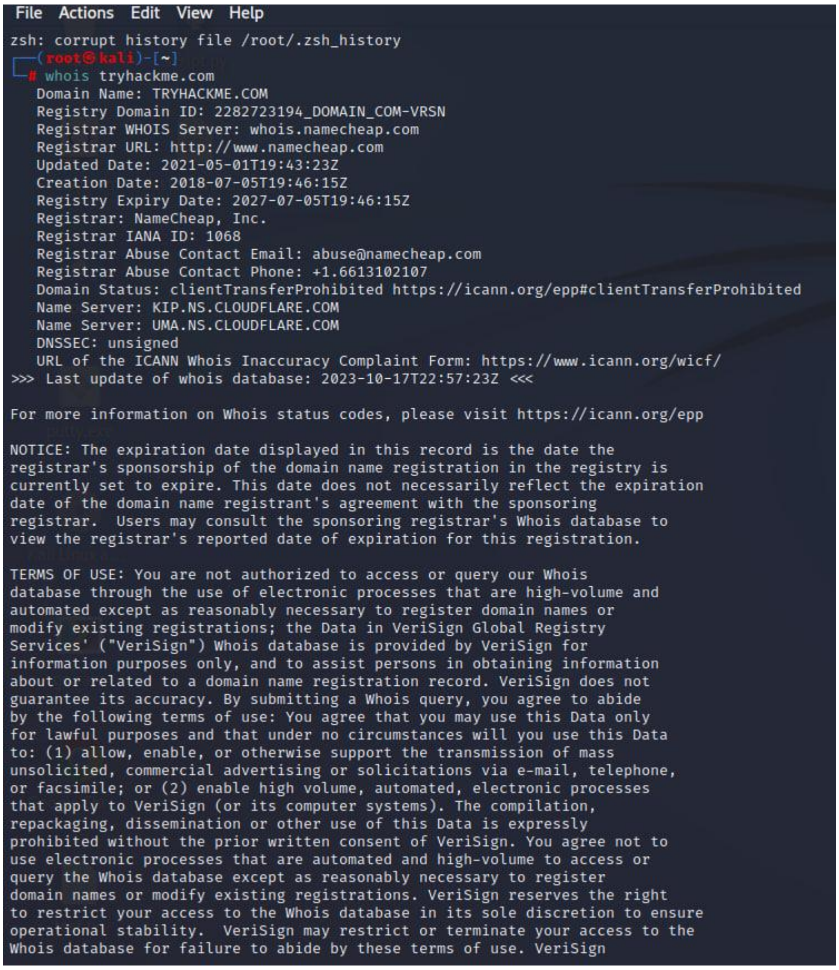
You happen to meet the IT administrator of the target company at a party. You try to use social engineering to get more information about their systems and network infrastructure. What kind of reconnaissance activity is this? (A for active, P for passive)

A

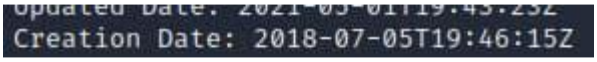
3. Whois



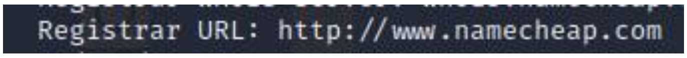
```
┌──(root㉿kali)-[~]
└─# whois tryhackme.com
```



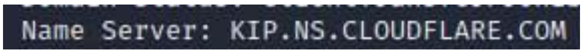
```
zsh: corrupt history file /root/.zsh_history
┌──(root㉿kali)-[~]
└─# whois tryhackme.com
   Domain Name: TRYHACKME.COM
   Registry Domain ID: 2282723194_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.namecheap.com
   Registrar URL: http://www.namecheap.com
   Updated Date: 2021-05-01T19:43:23Z
   Creation Date: 2018-07-05T19:46:15Z
   Registry Expiry Date: 2027-07-05T19:46:15Z
   Registrar: NameCheap, Inc.
   Registrar IANA ID: 1068
   Registrar Abuse Contact Email: abuse@namecheap.com
   Registrar Abuse Contact Phone: +1.6613102107
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: KIP.NS.CLOUDFLARE.COM
   Name Server: UMA.NS.CLOUDFLARE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-10-17T22:57:23Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
```



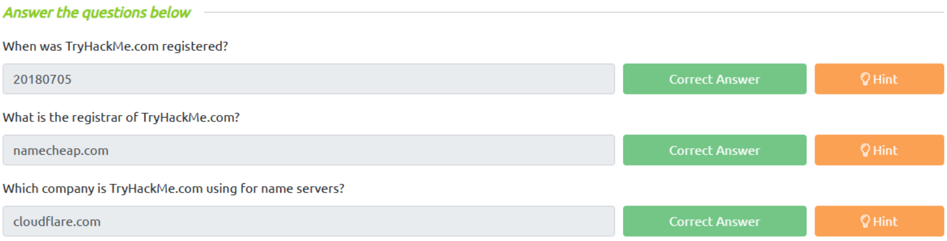
```
Creation Date: 2018-07-05T19:46:15Z
```



```
Registrar URL: http://www.namecheap.com
```



```
Name Server: KIP.NS.CLOUDFLARE.COM
```



Answer the questions below

When was TryHackMe.com registered?

20180705

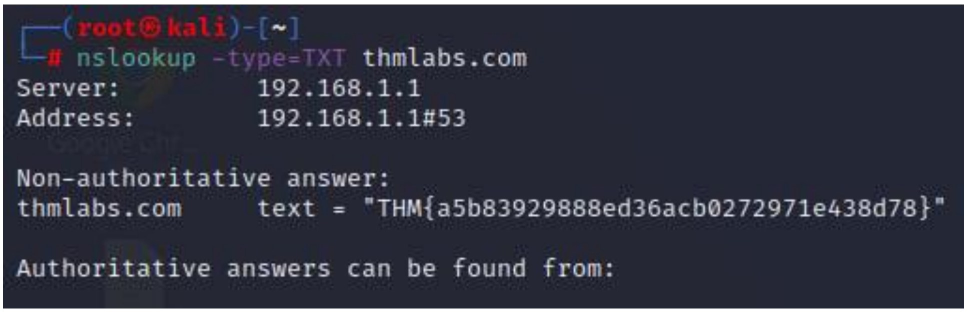
What is the registrar of TryHackMe.com?

namecheap.com

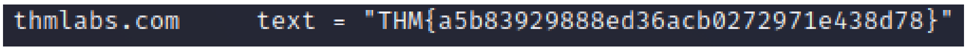
Which company is TryHackMe.com using for name servers?

cloudflare.com

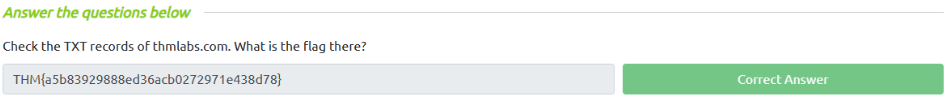
4. Nslookup and dig



```
┌──(root㉿kali)-[~]
└─# nslookup -type=TXT thmlabs.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
thmlabs.com     text = "THM{a5b83929888ed36acb0272971e438d78}"

Authoritative answers can be found from:
```



```
thmlabs.com     text = "THM{a5b83929888ed36acb0272971e438d78}"
```

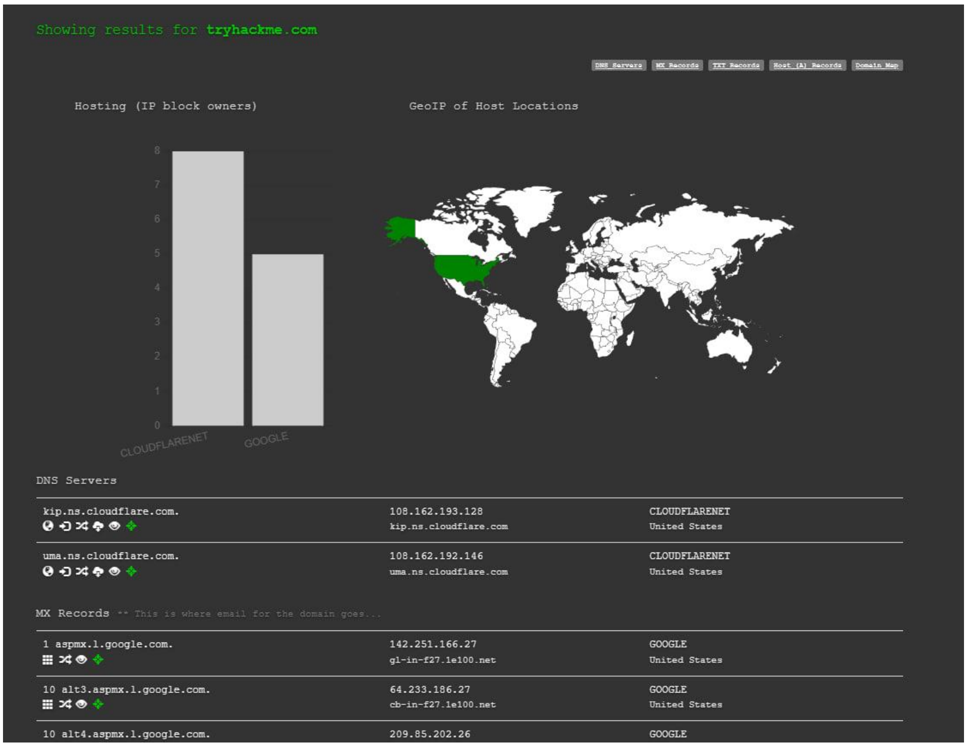


Answer the questions below

Check the TXT records of thmlabs.com. What is the flag there?

THM{a5b83929888ed36acb0272971e438d78}

5. DNSDumpster



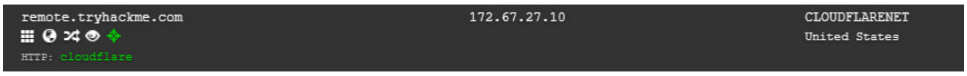
Showing results for **tryhackme.com**

DNS Servers

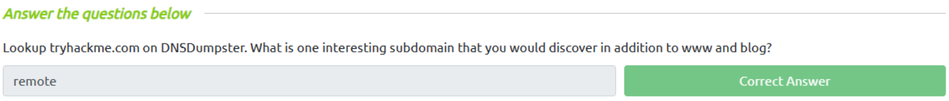
kip.ns.cloudflare.com.	108.162.193.128 kip.ns.cloudflare.com	CLOUDFLARENET United States
uma.ns.cloudflare.com.	108.162.192.146 uma.ns.cloudflare.com	CLOUDFLARENET United States

MX Records ** This is where email for the domain goes...

1 aspmx.l.google.com.	142.251.166.27 gl-in-f27.1e100.net	GOOGLE United States
10 alt3.aspmx.l.google.com.	64.233.186.27 cb-in-f27.1e100.net	GOOGLE United States
10 alt4.aspmx.l.google.com.	209.85.202.26	GOOGLE



remote.tryhackme.com HTTP: cloudflare	172.67.27.10	CLOUDFLARENET United States



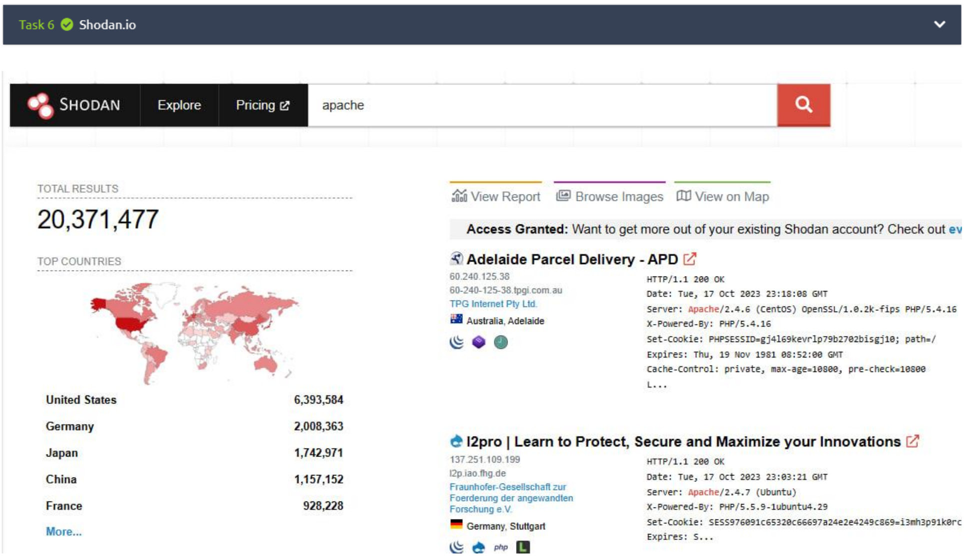
Answer the questions below

Lookup tryhackme.com on DNSDumpster. What is one interesting subdomain that you would discover in addition to www and blog?

remote

Correct Answer

6. Shodan.io



Task 6 ✓ Shodan.io

apache

TOTAL RESULTS

20,371,477

TOP COUNTRIES

United States	6,393,584
Germany	2,008,363
Japan	1,742,971
China	1,157,152
France	928,228

More...

Access Granted: Want to get more out of your existing Shodan account? Check out ev

Adelaide Parcel Delivery - APD

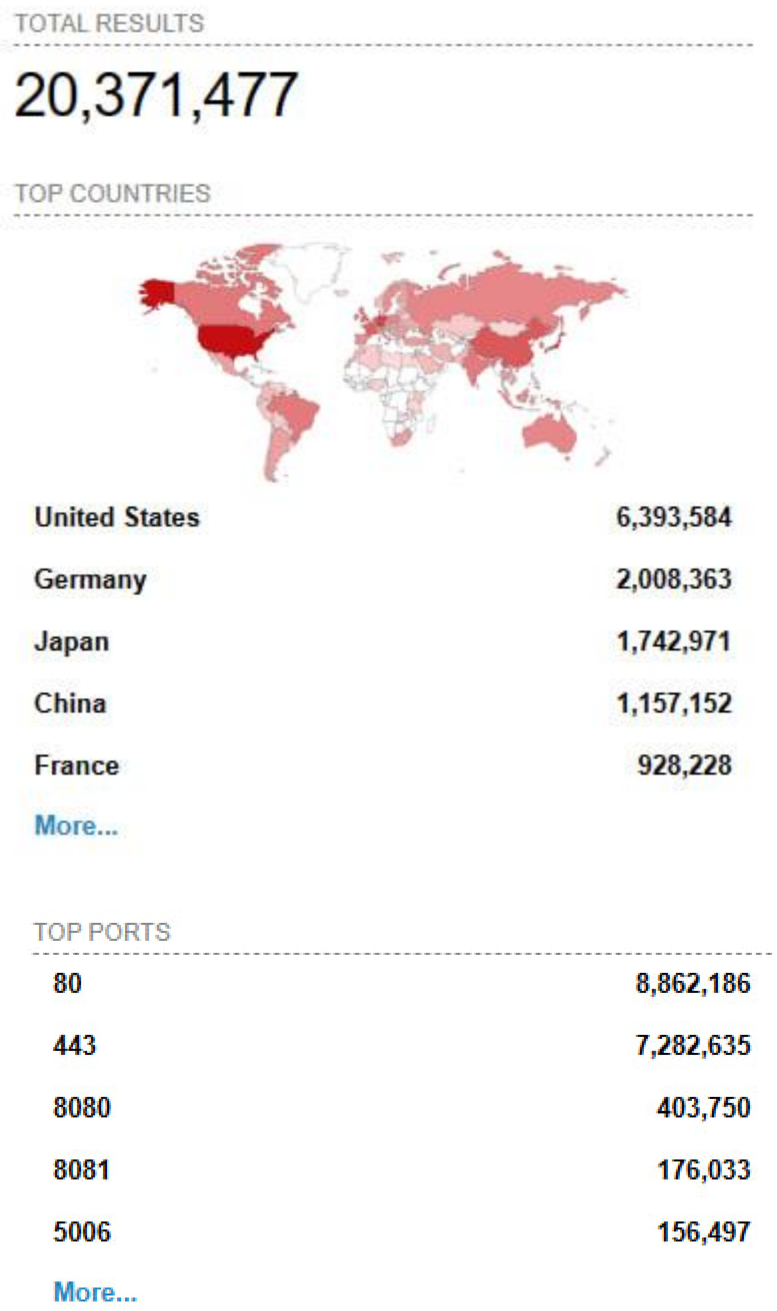
60.240.125.38
60-240-125-38.tpgi.com.au
TPG Internet Pty Ltd.
Australia, Adelaide

```
HTTP/1.1 200 OK
Date: Tue, 17 Oct 2023 23:18:08 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
X-Powered-By: PHP/5.4.16
Set-Cookie: PHPSESSID=gj4l69kevrlp79b2702bisgj10; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private, max-age=10800, pre-check=10800
L...
```

I2pro | Learn to Protect, Secure and Maximize your Innovations

137.251.109.199
l2p.iao.fhg.de
Fraunhofer-Gesellschaft zur Foerderung der angewandten Forschung e.V.
Germany, Stuttgart

```
HTTP/1.1 200 OK
Date: Tue, 17 Oct 2023 23:03:21 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Set-Cookie: SESS976091c65320c66697a24e2e4249c869=i3mh3p91k0rc
Expires: S...
```



TOTAL RESULTS

20,371,477

TOP COUNTRIES

United States	6,393,584
Germany	2,008,363
Japan	1,742,971
China	1,157,152
France	928,228

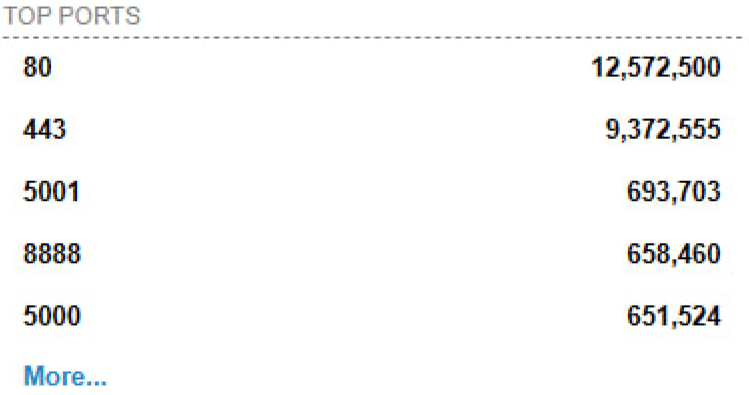
More...

TOP PORTS

80	8,862,186
443	7,282,635
8080	403,750
8081	176,033
5006	156,497

More...

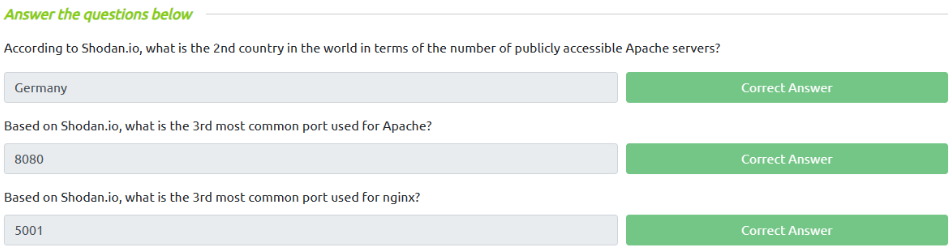
There it is based on Shodan.io, exactly the 3rd most common port used for nginx: **5001.**



TOP PORTS

80	12,572,500
443	9,372,555
5001	693,703
8888	658,460
5000	651,524

More...



Answer the questions below

According to Shodan.io, what is the 2nd country in the world in terms of the number of publicly accessible Apache servers?

Germany

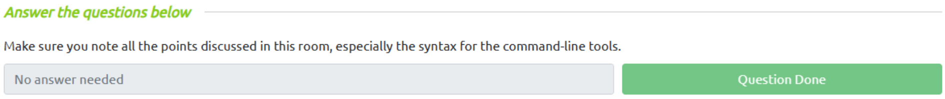
Based on Shodan.io, what is the 3rd most common port used for Apache?

8080

Based on Shodan.io, what is the 3rd most common port used for nginx?

5001

7. Summary

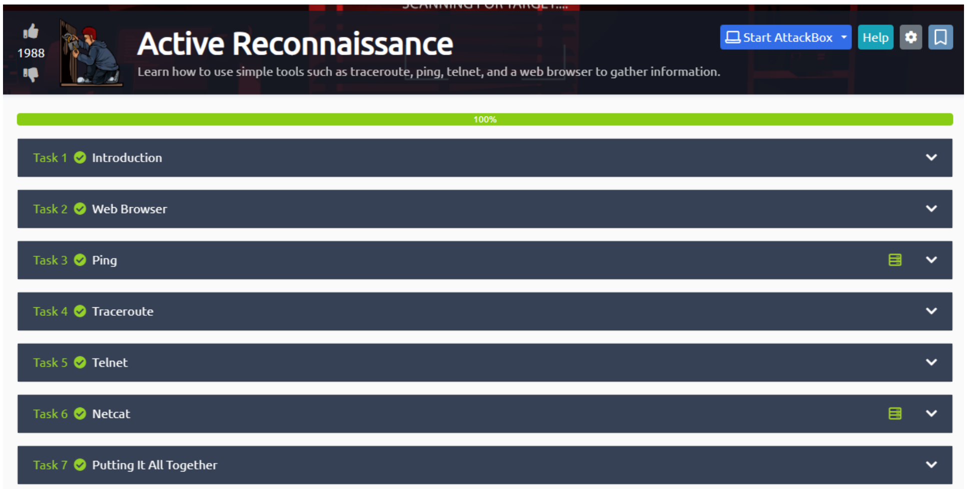


Answer the questions below

Make sure you note all the points discussed in this room, especially the syntax for the command-line tools.

No answer needed

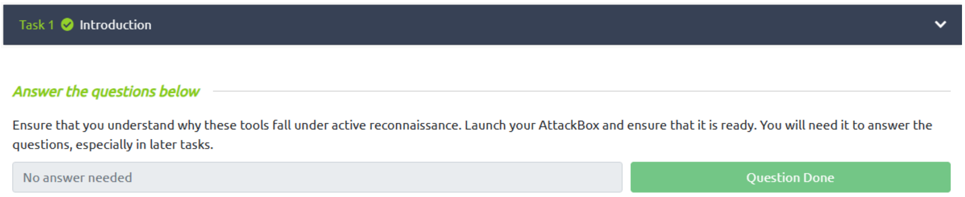
Part 2. Active Reconnaissance



Active Reconnaissance

Learn how to use simple tools such as traceroute, ping, telnet, and a web browser to gather information.

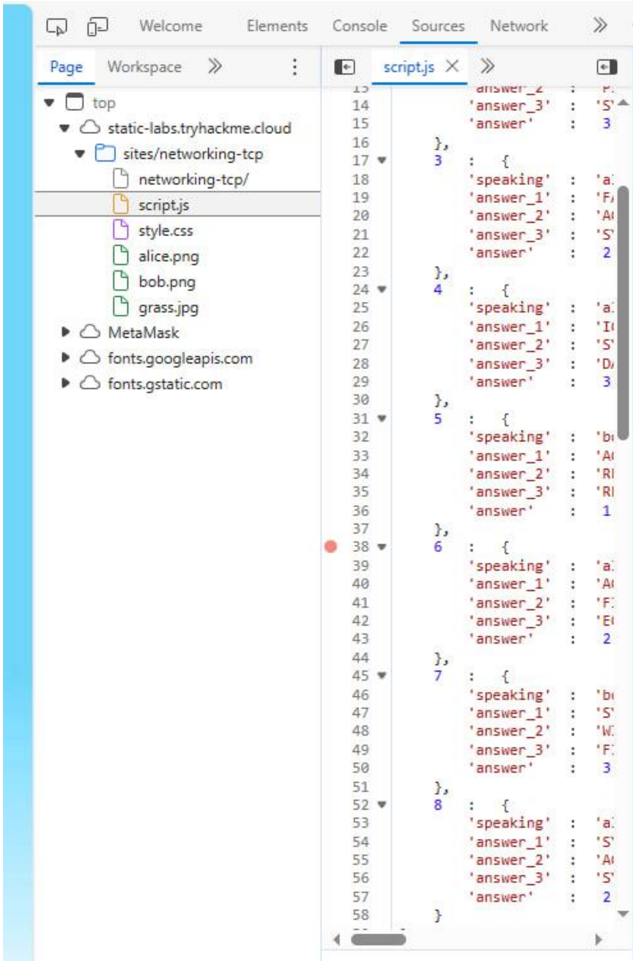
1. Introduction



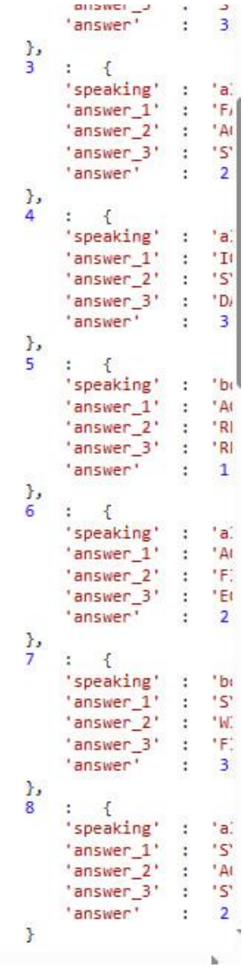
Answer the questions below

Ensure that you understand why these tools fall under active reconnaissance. Launch your AttackBox and ensure that it is ready. You will need it to answer the questions, especially in later tasks.

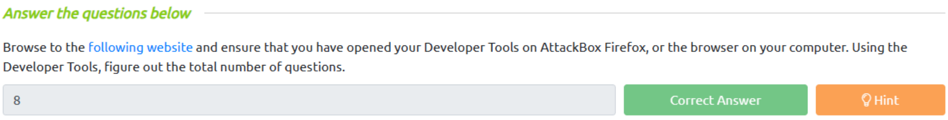
2. Web Browser



```
            'answer_2'  :  'F
            'answer_3'  :  'S
            'answer'    :  3
        },
        3   :  {
            'speaking'  :  'a
            'answer_1'  :  'F
            'answer_2'  :  'A
            'answer_3'  :  'S
            'answer'    :  2
        },
        4   :  {
            'speaking'  :  'a
            'answer_1'  :  'I
            'answer_2'  :  'S
            'answer_3'  :  'D
            'answer'    :  3
        },
        5   :  {
            'speaking'  :  'b
            'answer_1'  :  'A
            'answer_2'  :  'R
            'answer_3'  :  'R
            'answer'    :  1
        },
        6   :  {
            'speaking'  :  'a
            'answer_1'  :  'A
            'answer_2'  :  'F
            'answer_3'  :  'E
            'answer'    :  2
        },
        7   :  {
            'speaking'  :  'b
            'answer_1'  :  'S
            'answer_2'  :  'W
            'answer_3'  :  'F
            'answer'    :  3
        },
        8   :  {
            'speaking'  :  'a
            'answer_1'  :  'S
            'answer_2'  :  'A
            'answer_3'  :  'S
            'answer'    :  2
        }
```



```
        'answer_3'   :  3
        'answer'     :  3
},
3    :   {
        'speaking'   :  'a:
        'answer_1'   :  'F/
        'answer_2'   :  'A(
        'answer_3'   :  'S'
        'answer'     :  2
},
4    :   {
        'speaking'   :  'a:
        'answer_1'   :  'I(
        'answer_2'   :  'S'
        'answer_3'   :  'D/
        'answer'     :  3
},
5    :   {
        'speaking'   :  'b(
        'answer_1'   :  'A(
        'answer_2'   :  'RI
        'answer_3'   :  'RI
        'answer'     :  1
},
6    :   {
        'speaking'   :  'a:
        'answer_1'   :  'A(
        'answer_2'   :  'F:
        'answer_3'   :  'E(
        'answer'     :  2
},
7    :   {
        'speaking'   :  'b(
        'answer_1'   :  'S'
        'answer_2'   :  'W:
        'answer_3'   :  'F:
        'answer'     :  3
},
8    :   {
        'speaking'   :  'a:
        'answer_1'   :  'S'
        'answer_2'   :  'A(
        'answer_3'   :  'S'
        'answer'     :  2
}
```

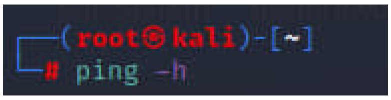


Answer the questions below

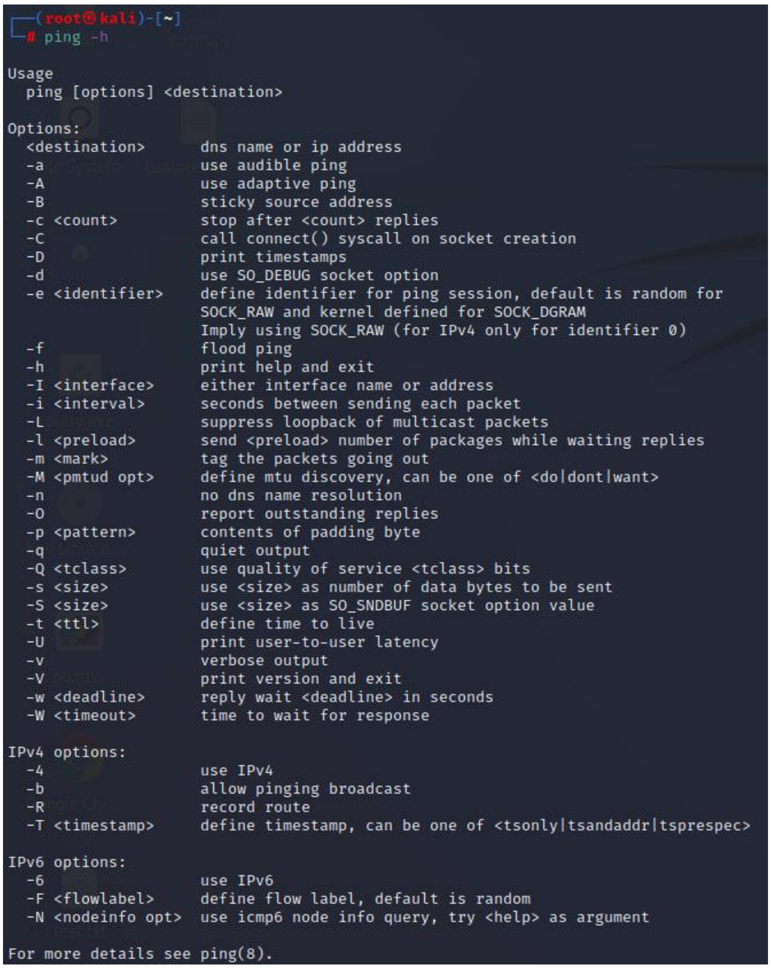
Browse to the following website and ensure that you have opened your Developer Tools on AttackBox Firefox, or the browser on your computer. Using the Developer Tools, figure out the total number of questions.

8

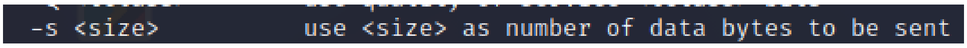
3. Ping



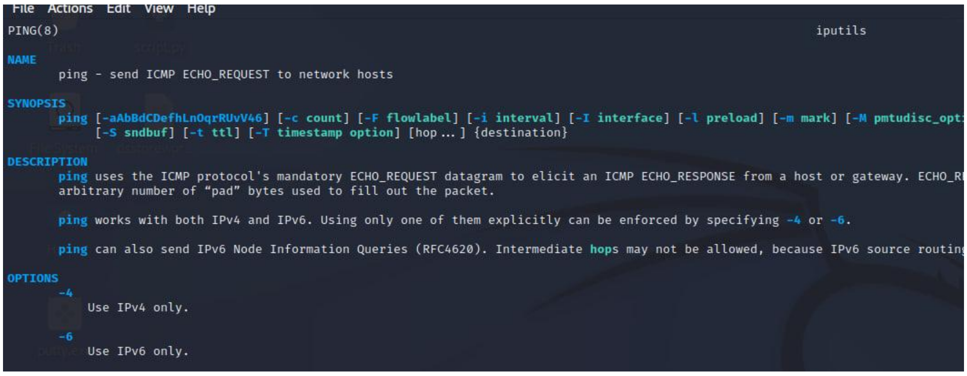
```
┌──(root㉿kali)-[~]
└─# ping -h
```



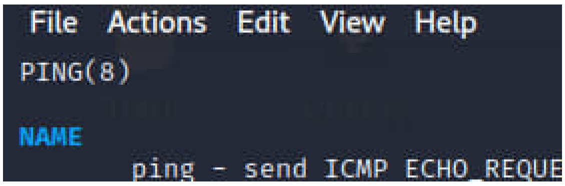
```
┌──(root㉿kali)-[~]
└─# ping -h

Usage
  ping [options] <destination>

Options:
  <destination>      dns name or ip address
  -a                 use audible ping
  -A                 use adaptive ping
  -B                 sticky source address
  -c <count>         stop after <count> replies
  -C                 call connect() syscall on socket creation
  -D                 print timestamps
  -d                 use SO_DEBUG socket option
  -e <identifier>    define identifier for ping session, default is random for
                     SOCK_RAW and kernel defined for SOCK_DGRAM
                     Imply using SOCK_RAW (for IPv4 only for identifier 0)
  -f                 flood ping
  -h                 print help and exit
  -I <interface>     either interface name or address
  -i <interval>      seconds between sending each packet
  -L                 suppress loopback of multicast packets
  -l <preload>       send <preload> number of packages while waiting replies
  -m <mark>          tag the packets going out
  -M <pmtud opt>     define mtu discovery, can be one of <do|dont|want>
  -n                 no dns name resolution
  -O                 report outstanding replies
  -p <pattern>       contents of padding byte
  -q                 quiet output
  -Q <tclass>        use quality of service <tclass> bits
  -s <size>          use <size> as number of data bytes to be sent
  -S <size>          use <size> as SO_SNDBUF socket option value
  -t <ttl>           define time to live
  -U                 print user-to-user latency
  -v                 verbose output
  -V                 print version and exit
  -w <deadline>      reply wait <deadline> in seconds
  -W <timeout>       time to wait for response

IPv4 options:
  -4                 use IPv4
  -b                 allow pinging broadcast
  -R                 record route
  -T <timestamp>     define timestamp, can be one of <tsonly|tsandaddr|tsprespec>

IPv6 options:
  -6                 use IPv6
  -F <flowlabel>     define flow label, default is random
  -N <nodeinfo opt>  use icmp6 node info query, try <help> as argument

For more details see ping(8).
```



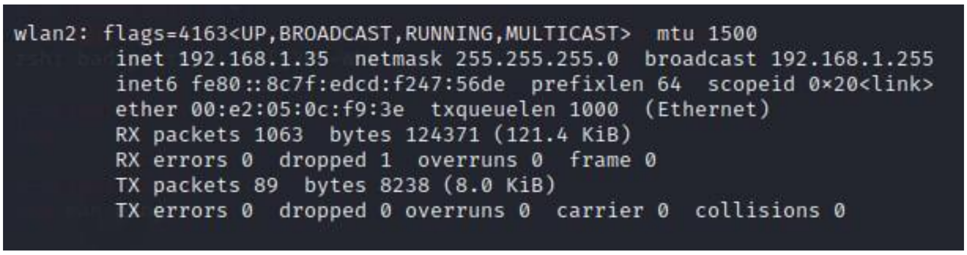
```
  -s <size>          use <size> as number of data bytes to be sent
```



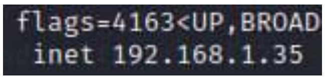
```
PING(8)                                                                  iputils

NAME
       ping - send ICMP ECHO_REQUEST to network hosts

SYNOPSIS
       ping [-aAbBdCDefhLnOqrRUvV46] [-c count] [-F flowlabel] [-i interval] [-I interface] [-l preload] [-m mark] [-M pmtudisc_opt
            [-S sndbuf] [-t ttl] [-T timestamp option] [hop ... ] {destination}

DESCRIPTION
       ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_R
       arbitrary number of “pad” bytes used to fill out the packet.

       ping works with both IPv4 and IPv6. Using only one of them explicitly can be enforced by specifying -4 or -6.

       ping can also send IPv6 Node Information Queries (RFC4620). Intermediate hops may not be allowed, because IPv6 source routing

OPTIONS
       -4
           Use IPv4 only.

       -6
           Use IPv6 only.
```



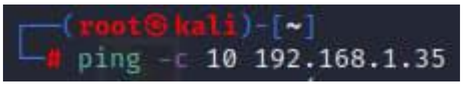
```
PING(8)

NAME
       ping - send ICMP ECHO_REQUE
```



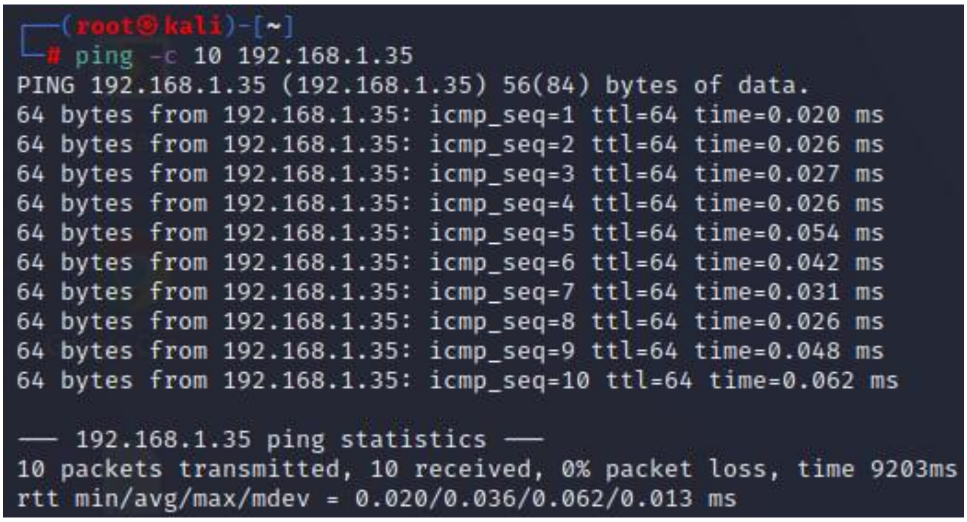
```
wlan2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.35  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::8c7f:edcd:f247:56de  prefixlen 64  scopeid 0×20<link>
        ether 00:e2:05:0c:f9:3e  txqueuelen 1000  (Ethernet)
        RX packets 1063  bytes 124371 (121.4 KiB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 89  bytes 8238 (8.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



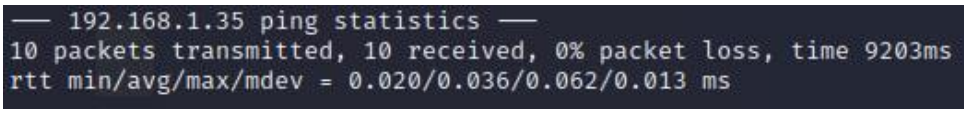
```
flags=4163<UP,BROAD
 inet 192.168.1.35
```



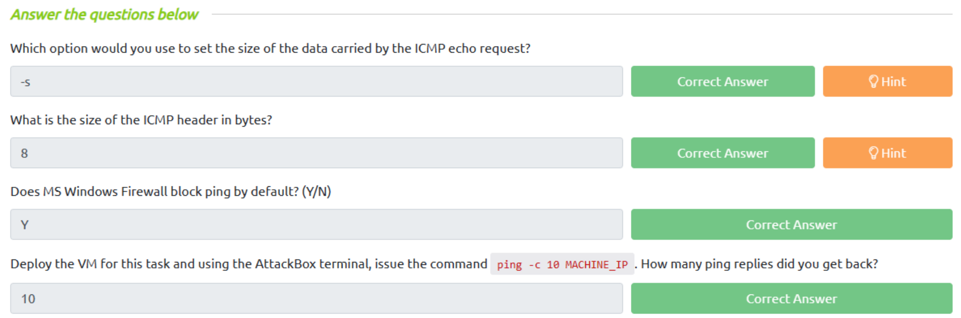
```
┌──(root㉿kali)-[~]
└─# ping -c 10 192.168.1.35
```



```
┌──(root㉿kali)-[~]
└─# ping -c 10 192.168.1.35
PING 192.168.1.35 (192.168.1.35) 56(84) bytes of data.
64 bytes from 192.168.1.35: icmp_seq=1 ttl=64 time=0.020 ms
64 bytes from 192.168.1.35: icmp_seq=2 ttl=64 time=0.026 ms
64 bytes from 192.168.1.35: icmp_seq=3 ttl=64 time=0.027 ms
64 bytes from 192.168.1.35: icmp_seq=4 ttl=64 time=0.026 ms
64 bytes from 192.168.1.35: icmp_seq=5 ttl=64 time=0.054 ms
64 bytes from 192.168.1.35: icmp_seq=6 ttl=64 time=0.042 ms
64 bytes from 192.168.1.35: icmp_seq=7 ttl=64 time=0.031 ms
64 bytes from 192.168.1.35: icmp_seq=8 ttl=64 time=0.026 ms
64 bytes from 192.168.1.35: icmp_seq=9 ttl=64 time=0.048 ms
64 bytes from 192.168.1.35: icmp_seq=10 ttl=64 time=0.062 ms

── 192.168.1.35 ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9203ms
rtt min/avg/max/mdev = 0.020/0.036/0.062/0.013 ms
```



```
── 192.168.1.35 ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9203ms
rtt min/avg/max/mdev = 0.020/0.036/0.062/0.013 ms
```



Answer the questions below

Which option would you use to set the size of the data carried by the ICMP echo request?

-s

What is the size of the ICMP header in bytes?

8

Does MS Windows Firewall block ping by default? (Y/N)

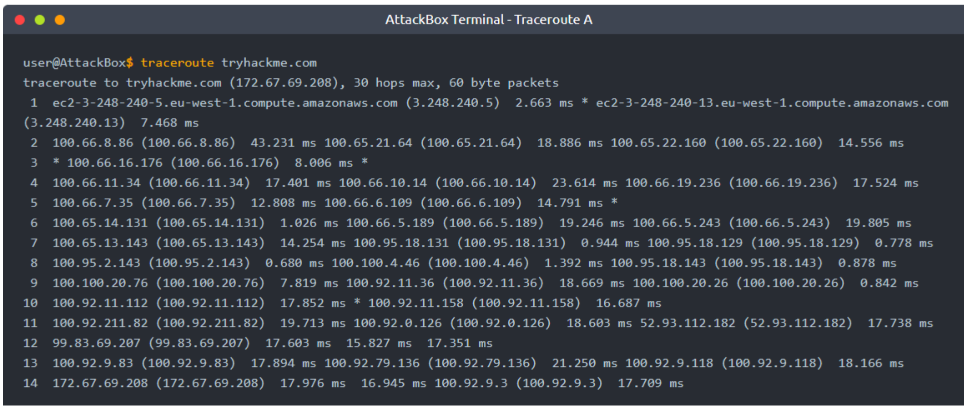
Y

Deploy the VM for this task and using the AttackBox terminal, issue the command `ping -c 10 MACHINE_IP`. How many ping replies did you get back?

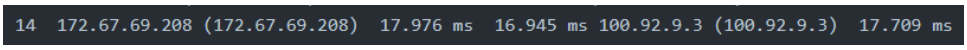
10

4. Traceroute

Task 4 ✓ Traceroute

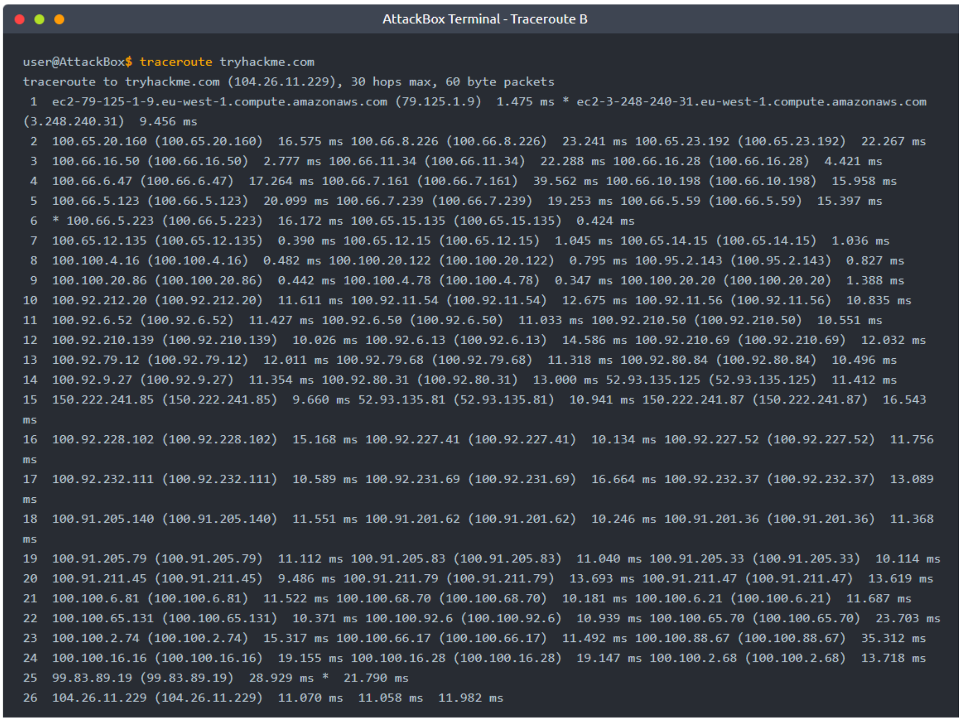


```
user@AttackBox$ traceroute tryhackme.com
traceroute to tryhackme.com (172.67.69.208), 30 hops max, 60 byte packets
 1  ec2-3-248-240-5.eu-west-1.compute.amazonaws.com (3.248.240.5)  2.663 ms * ec2-3-248-240-13.eu-west-1.compute.amazonaws.com
(3.248.240.13)  7.468 ms
 2  100.66.8.86 (100.66.8.86)  43.231 ms 100.65.21.64 (100.65.21.64)  18.886 ms 100.65.22.160 (100.65.22.160)  14.556 ms
 3  * 100.66.16.176 (100.66.16.176)  8.006 ms *
 4  100.66.11.34 (100.66.11.34)  17.401 ms 100.66.10.14 (100.66.10.14)  23.614 ms 100.66.19.236 (100.66.19.236)  17.524 ms
 5  100.66.7.35 (100.66.7.35)  12.808 ms 100.66.6.109 (100.66.6.109)  14.791 ms *
 6  100.65.14.131 (100.65.14.131)  1.026 ms 100.66.5.189 (100.66.5.189)  19.246 ms 100.66.5.243 (100.66.5.243)  19.805 ms
 7  100.65.13.143 (100.65.13.143)  14.254 ms 100.95.18.131 (100.95.18.131)  0.944 ms 100.95.18.129 (100.95.18.129)  0.778 ms
 8  100.95.2.143 (100.95.2.143)  0.680 ms 100.100.4.46 (100.100.4.46)  1.392 ms 100.95.18.143 (100.95.18.143)  0.878 ms
 9  100.100.20.76 (100.100.20.76)  7.819 ms 100.92.11.36 (100.92.11.36)  18.669 ms 100.100.20.26 (100.100.20.26)  0.842 ms
10  100.92.11.112 (100.92.11.112)  17.852 ms * 100.92.11.158 (100.92.11.158)  16.687 ms
11  100.92.211.82 (100.92.211.82)  19.713 ms 100.92.0.126 (100.92.0.126)  18.603 ms 52.93.112.182 (52.93.112.182)  17.738 ms
12  99.83.69.207 (99.83.69.207)  17.603 ms  15.827 ms  17.351 ms
13  100.92.9.83 (100.92.9.83)  17.894 ms 100.92.79.136 (100.92.79.136)  21.250 ms 100.92.9.118 (100.92.9.118)  18.166 ms
14  172.67.69.208 (172.67.69.208)  17.976 ms  16.945 ms 100.92.9.3 (100.92.9.3)  17.709 ms
```

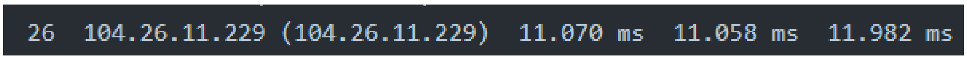


```
14  172.67.69.208 (172.67.69.208)  17.976 ms  16.945 ms 100.92.9.3 (100.92.9.3)  17.709 ms
```

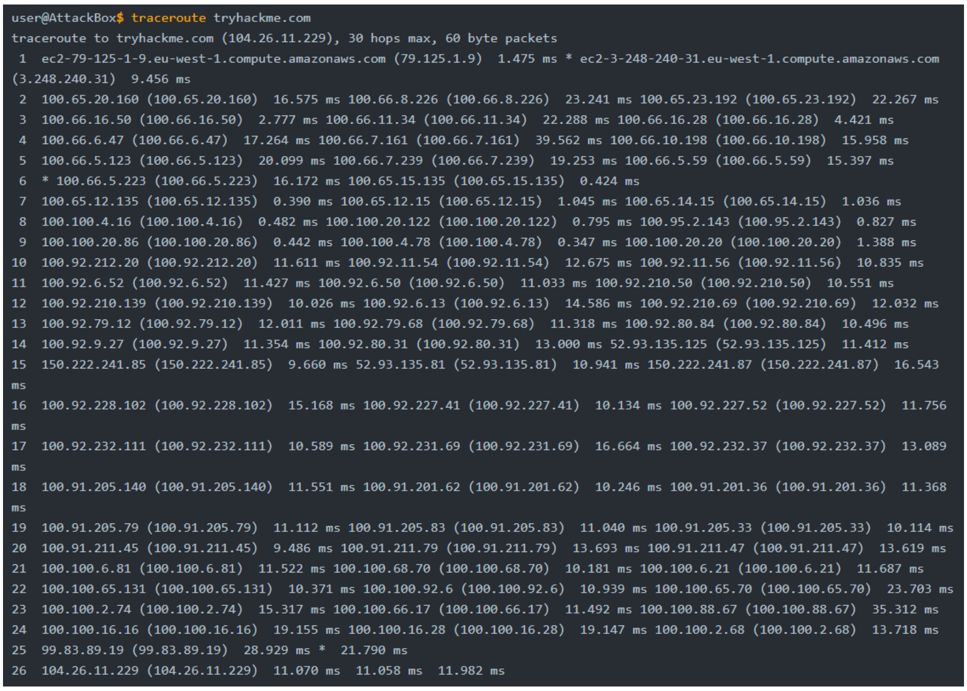
Traceroute B



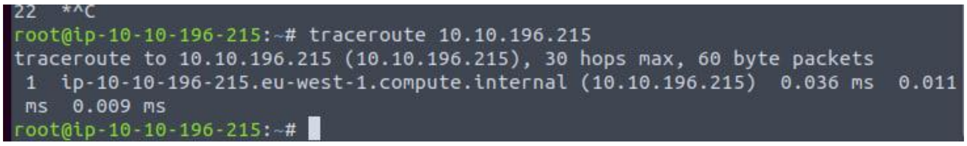
```
user@AttackBox$ traceroute tryhackme.com
traceroute to tryhackme.com (104.26.11.229), 30 hops max, 60 byte packets
 1  ec2-79-125-1-9.eu-west-1.compute.amazonaws.com (79.125.1.9)  1.475 ms * ec2-3-248-240-31.eu-west-1.compute.amazonaws.com
(3.248.240.31)  9.456 ms
 2  100.65.20.160 (100.65.20.160)  16.575 ms 100.66.8.226 (100.66.8.226)  23.241 ms 100.65.23.192 (100.65.23.192)  22.267 ms
 3  100.66.16.50 (100.66.16.50)  2.777 ms 100.66.11.34 (100.66.11.34)  22.288 ms 100.66.16.28 (100.66.16.28)  4.421 ms
 4  100.66.6.47 (100.66.6.47)  17.264 ms 100.66.7.161 (100.66.7.161)  39.562 ms 100.66.10.198 (100.66.10.198)  15.958 ms
 5  100.66.5.123 (100.66.5.123)  20.099 ms 100.66.7.239 (100.66.7.239)  19.253 ms 100.66.5.59 (100.66.5.59)  15.397 ms
 6  * 100.66.5.223 (100.66.5.223)  16.172 ms 100.65.15.135 (100.65.15.135)  0.424 ms
 7  100.65.12.135 (100.65.12.135)  0.390 ms 100.65.12.15 (100.65.12.15)  1.045 ms 100.65.14.15 (100.65.14.15)  1.036 ms
 8  100.100.4.16 (100.100.4.16)  0.482 ms 100.100.20.122 (100.100.20.122)  0.795 ms 100.95.2.143 (100.95.2.143)  0.827 ms
 9  100.100.20.86 (100.100.20.86)  0.442 ms 100.100.4.78 (100.100.4.78)  0.347 ms 100.100.20.20 (100.100.20.20)  1.388 ms
10  100.92.212.20 (100.92.212.20)  11.611 ms 100.92.11.54 (100.92.11.54)  12.675 ms 100.92.11.56 (100.92.11.56)  10.835 ms
11  100.92.6.52 (100.92.6.52)  11.427 ms 100.92.6.50 (100.92.6.50)  11.033 ms 100.92.210.50 (100.92.210.50)  10.551 ms
12  100.92.210.139 (100.92.210.139)  10.026 ms 100.92.6.13 (100.92.6.13)  14.586 ms 100.92.210.69 (100.92.210.69)  12.032 ms
13  100.92.79.12 (100.92.79.12)  12.011 ms 100.92.79.68 (100.92.79.68)  11.318 ms 100.92.80.84 (100.92.80.84)  10.496 ms
14  100.92.9.27 (100.92.9.27)  11.354 ms 100.92.80.31 (100.92.80.31)  13.000 ms 52.93.135.125 (52.93.135.125)  11.412 ms
15  150.222.241.85 (150.222.241.85)  9.660 ms 52.93.135.81 (52.93.135.81)  10.941 ms 150.222.241.87 (150.222.241.87)  16.543
ms
16  100.92.228.102 (100.92.228.102)  15.168 ms 100.92.227.41 (100.92.227.41)  10.134 ms 100.92.227.52 (100.92.227.52)  11.756
ms
17  100.92.232.111 (100.92.232.111)  10.589 ms 100.92.231.69 (100.92.231.69)  16.664 ms 100.92.232.37 (100.92.232.37)  13.089
ms
18  100.91.205.140 (100.91.205.140)  11.551 ms 100.91.201.62 (100.91.201.62)  10.246 ms 100.91.201.36 (100.91.201.36)  11.368
ms
19  100.91.205.79 (100.91.205.79)  11.112 ms 100.91.205.83 (100.91.205.83)  11.040 ms 100.91.205.33 (100.91.205.33)  10.114 ms
20  100.91.211.45 (100.91.211.45)  9.486 ms 100.91.211.79 (100.91.211.79)  13.693 ms 100.91.211.47 (100.91.211.47)  13.619 ms
21  100.100.6.81 (100.100.6.81)  11.522 ms 100.100.68.70 (100.100.68.70)  10.181 ms 100.100.6.21 (100.100.6.21)  11.687 ms
22  100.100.65.131 (100.100.65.131)  10.371 ms 100.100.92.6 (100.100.92.6)  10.939 ms 100.100.65.70 (100.100.65.70)  23.703 ms
23  100.100.2.74 (100.100.2.74)  15.317 ms 100.100.66.17 (100.100.66.17)  11.492 ms 100.100.88.67 (100.100.88.67)  35.312 ms
24  100.100.16.16 (100.100.16.16)  19.155 ms 100.100.16.28 (100.100.16.28)  19.147 ms 100.100.2.68 (100.100.2.68)  13.718 ms
25  99.83.89.19 (99.83.89.19)  28.929 ms *  21.790 ms
26  104.26.11.229 (104.26.11.229)  11.070 ms  11.058 ms  11.982 ms
```



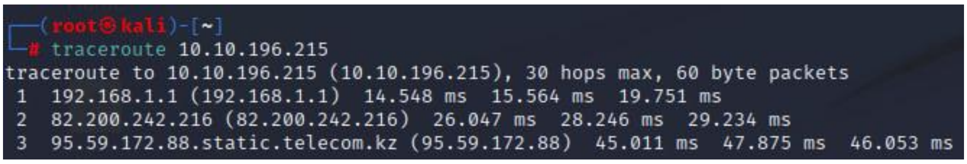
```
26  104.26.11.229 (104.26.11.229)  11.070 ms  11.058 ms  11.982 ms
```



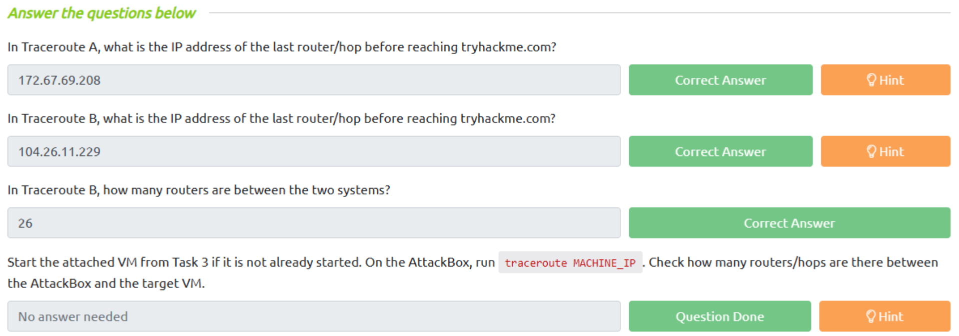
```
user@AttackBox$ traceroute tryhackme.com
traceroute to tryhackme.com (104.26.11.229), 30 hops max, 60 byte packets
 1  ec2-79-125-1-9.eu-west-1.compute.amazonaws.com (79.125.1.9)  1.475 ms * ec2-3-248-240-31.eu-west-1.compute.amazonaws.com
(3.248.240.31)  9.456 ms
 2  100.65.20.160 (100.65.20.160)  16.575 ms 100.66.8.226 (100.66.8.226)  23.241 ms 100.65.23.192 (100.65.23.192)  22.267 ms
 3  100.66.16.50 (100.66.16.50)  2.777 ms 100.66.11.34 (100.66.11.34)  22.288 ms 100.66.16.28 (100.66.16.28)  4.421 ms
 4  100.66.6.47 (100.66.6.47)  17.264 ms 100.66.7.161 (100.66.7.161)  39.562 ms 100.66.10.198 (100.66.10.198)  15.958 ms
 5  100.66.5.123 (100.66.5.123)  20.099 ms 100.66.7.239 (100.66.7.239)  19.253 ms 100.66.5.59 (100.66.5.59)  15.397 ms
 6  * 100.66.5.223 (100.66.5.223)  16.172 ms 100.65.15.135 (100.65.15.135)  0.424 ms
 7  100.65.12.135 (100.65.12.135)  0.390 ms 100.65.12.15 (100.65.12.15)  1.045 ms 100.65.14.15 (100.65.14.15)  1.036 ms
 8  100.100.4.16 (100.100.4.16)  0.482 ms 100.100.20.122 (100.100.20.122)  0.795 ms 100.95.2.143 (100.95.2.143)  0.827 ms
 9  100.100.20.86 (100.100.20.86)  0.442 ms 100.100.4.78 (100.100.4.78)  0.347 ms 100.100.20.20 (100.100.20.20)  1.388 ms
10  100.92.212.20 (100.92.212.20)  11.611 ms 100.92.11.54 (100.92.11.54)  12.675 ms 100.92.11.56 (100.92.11.56)  10.835 ms
11  100.92.6.52 (100.92.6.52)  11.427 ms 100.92.6.50 (100.92.6.50)  11.033 ms 100.92.210.50 (100.92.210.50)  10.551 ms
12  100.92.210.139 (100.92.210.139)  10.026 ms 100.92.6.13 (100.92.6.13)  14.586 ms 100.92.210.69 (100.92.210.69)  12.032 ms
13  100.92.79.12 (100.92.79.12)  12.011 ms 100.92.79.68 (100.92.79.68)  11.318 ms 100.92.80.84 (100.92.80.84)  10.496 ms
14  100.92.9.27 (100.92.9.27)  11.354 ms 100.92.80.31 (100.92.80.31)  13.000 ms 52.93.135.125 (52.93.135.125)  11.412 ms
15  150.222.241.85 (150.222.241.85)  9.660 ms 52.93.135.81 (52.93.135.81)  10.941 ms 150.222.241.87 (150.222.241.87)  16.543
ms
16  100.92.228.102 (100.92.228.102)  15.168 ms 100.92.227.41 (100.92.227.41)  10.134 ms 100.92.227.52 (100.92.227.52)  11.756
ms
17  100.92.232.111 (100.92.232.111)  10.589 ms 100.92.231.69 (100.92.231.69)  16.664 ms 100.92.232.37 (100.92.232.37)  13.089
ms
18  100.91.205.140 (100.91.205.140)  11.551 ms 100.91.201.62 (100.91.201.62)  10.246 ms 100.91.201.36 (100.91.201.36)  11.368
ms
19  100.91.205.79 (100.91.205.79)  11.112 ms 100.91.205.83 (100.91.205.83)  11.040 ms 100.91.205.33 (100.91.205.33)  10.114 ms
20  100.91.211.45 (100.91.211.45)  9.486 ms 100.91.211.79 (100.91.211.79)  13.693 ms 100.91.211.47 (100.91.211.47)  13.619 ms
21  100.100.6.81 (100.100.6.81)  11.522 ms 100.100.68.70 (100.100.68.70)  10.181 ms 100.100.6.21 (100.100.6.21)  11.687 ms
22  100.100.65.131 (100.100.65.131)  10.371 ms 100.100.92.6 (100.100.92.6)  10.939 ms 100.100.65.70 (100.100.65.70)  23.703 ms
23  100.100.2.74 (100.100.2.74)  15.317 ms 100.100.66.17 (100.100.66.17)  11.492 ms 100.100.88.67 (100.100.88.67)  35.312 ms
24  100.100.16.16 (100.100.16.16)  19.155 ms 100.100.16.28 (100.100.16.28)  19.147 ms 100.100.2.68 (100.100.2.68)  13.718 ms
25  99.83.89.19 (99.83.89.19)  28.929 ms *  21.790 ms
26  104.26.11.229 (104.26.11.229)  11.070 ms  11.058 ms  11.982 ms
```



```
22  **^C
root@ip-10-10-196-215:~# traceroute 10.10.196.215
traceroute to 10.10.196.215 (10.10.196.215), 30 hops max, 60 byte packets
 1  ip-10-10-196-215.eu-west-1.compute.internal (10.10.196.215)  0.036 ms  0.011
 ms  0.009 ms
root@ip-10-10-196-215:~# 
```



```
┌──(root㉿kali)-[~]
└─# traceroute 10.10.196.215
traceroute to 10.10.196.215 (10.10.196.215), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  14.548 ms  15.564 ms  19.751 ms
 2  82.200.242.216 (82.200.242.216)  26.047 ms  28.246 ms  29.234 ms
 3  95.59.172.88.static.telecom.kz (95.59.172.88)  45.011 ms  47.875 ms  46.053 ms
```



Answer the questions below

In Traceroute A, what is the IP address of the last router/hop before reaching tryhackme.com?

172.67.69.208

In Traceroute B, what is the IP address of the last router/hop before reaching tryhackme.com?

104.26.11.229

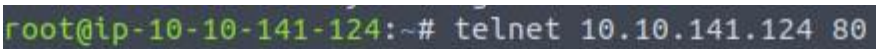
In Traceroute B, how many routers are between the two systems?

26

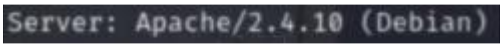
Start the attached VM from Task 3 if it is not already started. On the AttackBox, run `traceroute MACHINE_IP`. Check how many routers/hops are there between the AttackBox and the target VM.

No answer needed

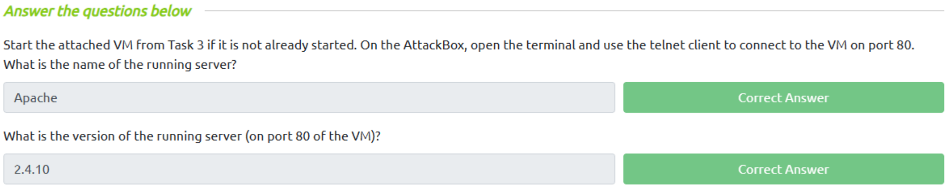
5. Telnet



```
root@ip-10-10-141-124:~# telnet 10.10.141.124 80
```



```
Server: Apache/2.4.10 (Debian)
```



Answer the questions below

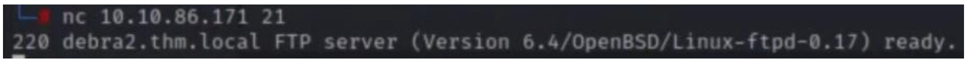
Start the attached VM from Task 3 if it is not already started. On the AttackBox, open the terminal and use the telnet client to connect to the VM on port 80. What is the name of the running server?

Apache

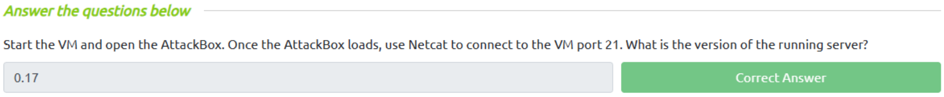
What is the version of the running server (on port 80 of the VM)?

2.4.10

6. Netcat



```
└─ nc 10.10.86.171 21
220 debra2.thm.local FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
```

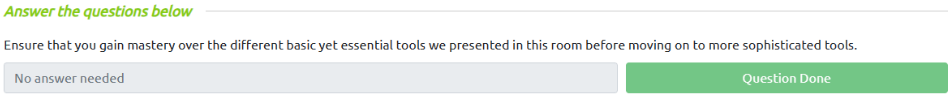


Answer the questions below

Start the VM and open the AttackBox. Once the AttackBox loads, use Netcat to connect to the VM port 21. What is the version of the running server?

0.17

7. Putting It All Together

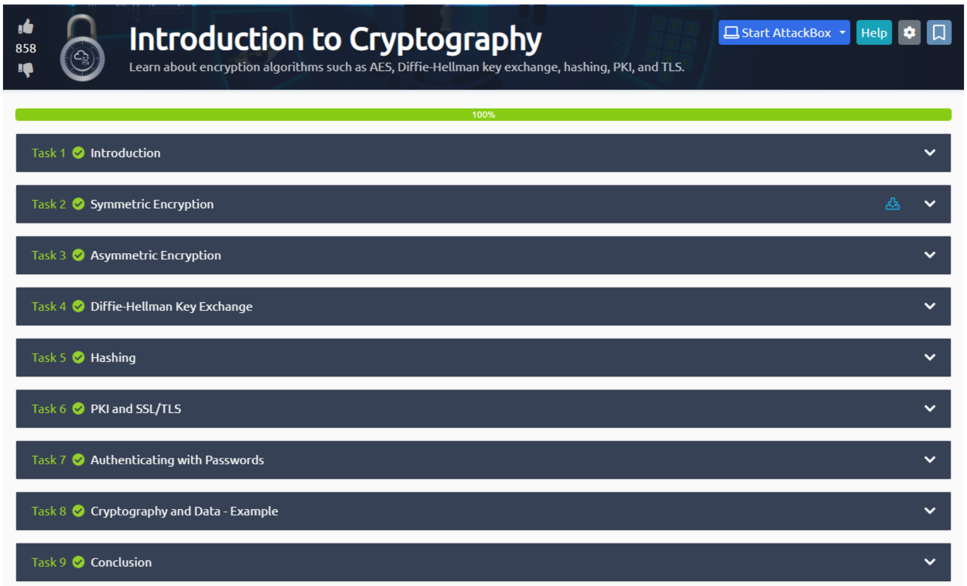


Answer the questions below

Ensure that you gain mastery over the different basic yet essential tools we presented in this room before moving on to more sophisticated tools.

No answer needed

Part 3. Introduction to Cryptography

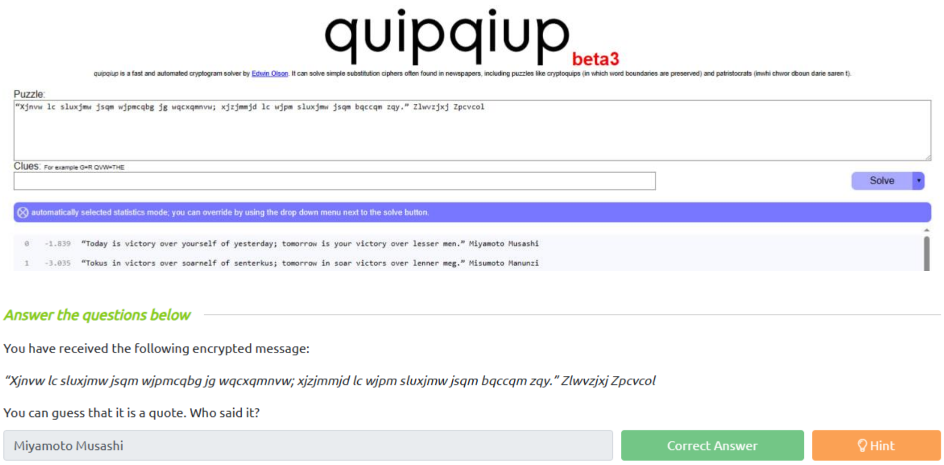


Introduction to Cryptography

Learn about encryption algorithms such as AES, Diffie-Hellman key exchange, hashing, PKI, and TLS.

- Task 1 Introduction
- Task 2 Symmetric Encryption
- Task 3 Asymmetric Encryption
- Task 4 Diffie-Hellman Key Exchange
- Task 5 Hashing
- Task 6 PKI and SSL/TLS
- Task 7 Authenticating with Passwords
- Task 8 Cryptography and Data - Example
- Task 9 Conclusion

1. Introduction



quipqiup beta3

quipqiup is a fast and automated cryptogram solver by Edwin Olson. It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

```
“Xjnvw lc sluxjmw jsqm wjpmcqbg jg wqcxqmnvw; xjzjmmjd lc wjpm sluxjmw jsqm bqccqm zqy.” Zlwvzjxj Zpcvcol
```

Clues: For example G=R QVW=THE

automatically selected statistics mode; you can override by using the drop down menu next to the solve button.

```
0   -1.839   “Today is victory over yourself of yesterday; tomorrow is your victory over lesser men.” Miyamoto Musashi
1   -3.035   “Tokus in victors over soarnelf of senterkus; tomorrow in soar victors over lenner meg.” Misumoto Manunzi
```

Answer the questions below

You have received the following encrypted message:

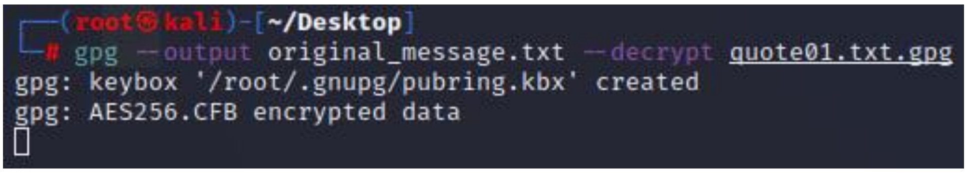
“Xjnvw lc sluxjmw jsqm wjpmcqbg jg wqcxqmnvw; xjzjmmjd lc wjpm sluxjmw jsqm bqccqm zqy.” Zlwvzjxj Zpcvcol

You can guess that it is a quote. Who said it?

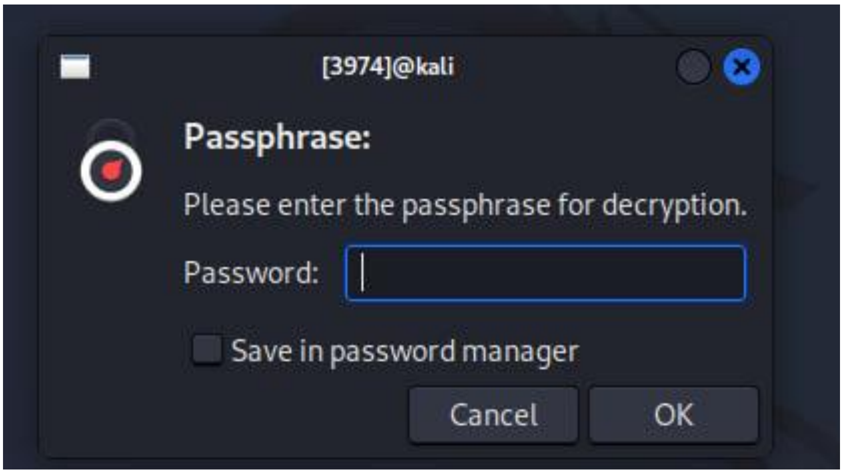
Miyamoto Musashi

2. Symmetric Encryption

Task 2 Symmetric Encryption



```
┌──(root㉿kali)-[~/Desktop]
└─# gpg --output original_message.txt --decrypt quote01.txt.gpg
gpg: keybox '/root/.gnupg/pubring.kbx' created
gpg: AES256.CFB encrypted data
```



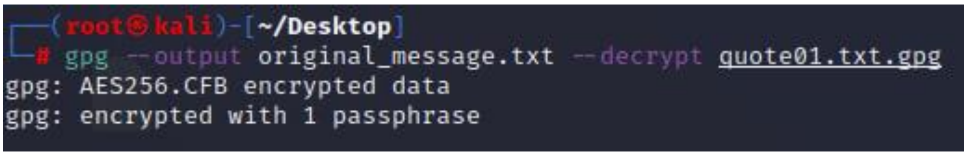
[3974]@kali

Passphrase:

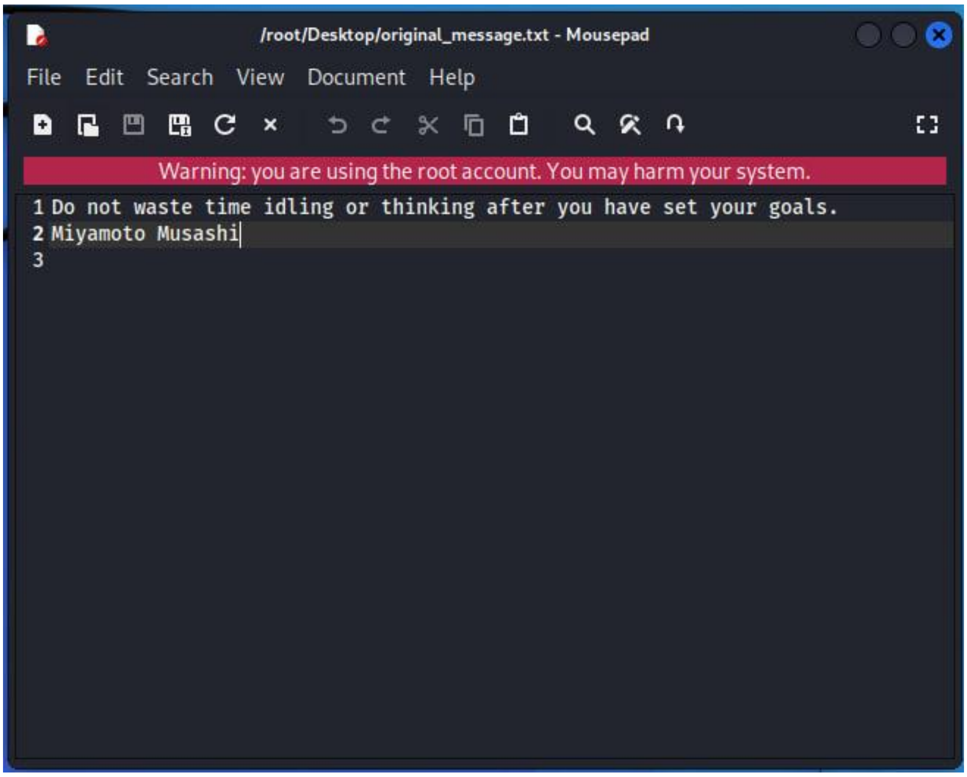
Please enter the passphrase for decryption.

Password:

□ Save in password manager



```
┌──(root㉿kali)-[~/Desktop]
└─# gpg --output original_message.txt --decrypt quote01.txt.gpg
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
```

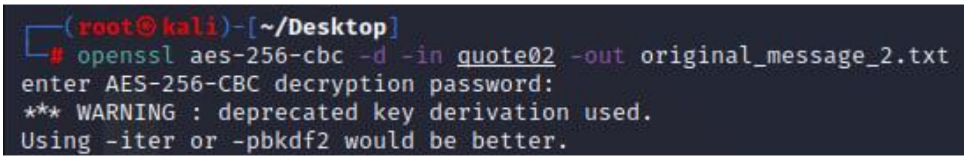


/root/Desktop/original_message.txt - Mousepad
File Edit Search View Document Help

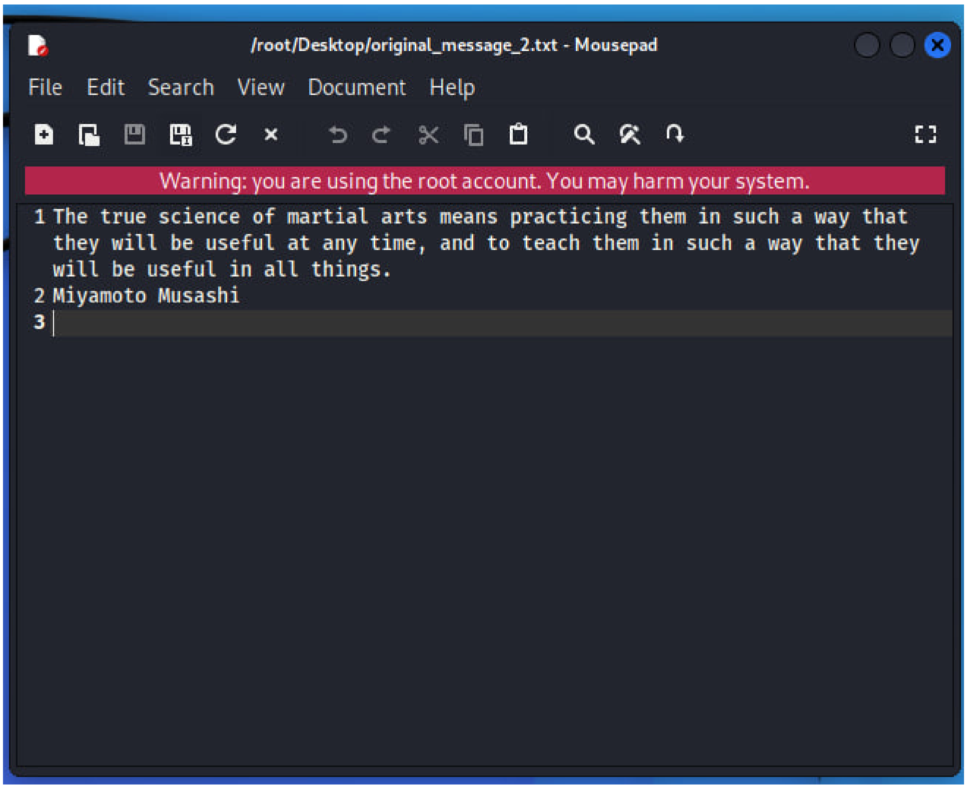
Warning: you are using the root account. You may harm your system.

```
Do not waste time idling or thinking after you have set your goals.
Miyamoto Musashi
```

```
1 Do not waste
```

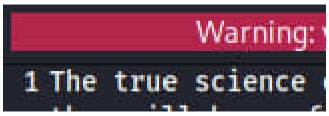


```
┌──(root㉿kali)-[~/Desktop]
└─# openssl aes-256-cbc -d -in quote02 -out original_message_2.txt
enter AES-256-CBC decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
```


/root/Desktop/original_message_2.txt - Mousepad
File Edit Search View Document Help

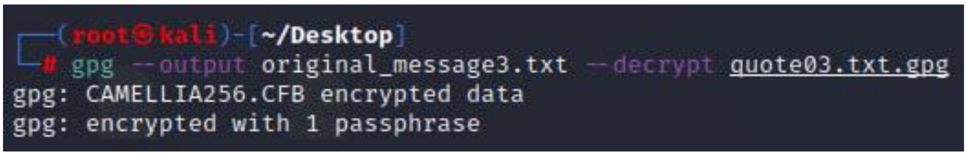
Warning: you are using the root account. You may harm your system.

```
The true science of martial arts means practicing them in such a way that they will be useful at any time, and to teach them in such a way that they will be useful in all things.
Miyamoto Musashi
```

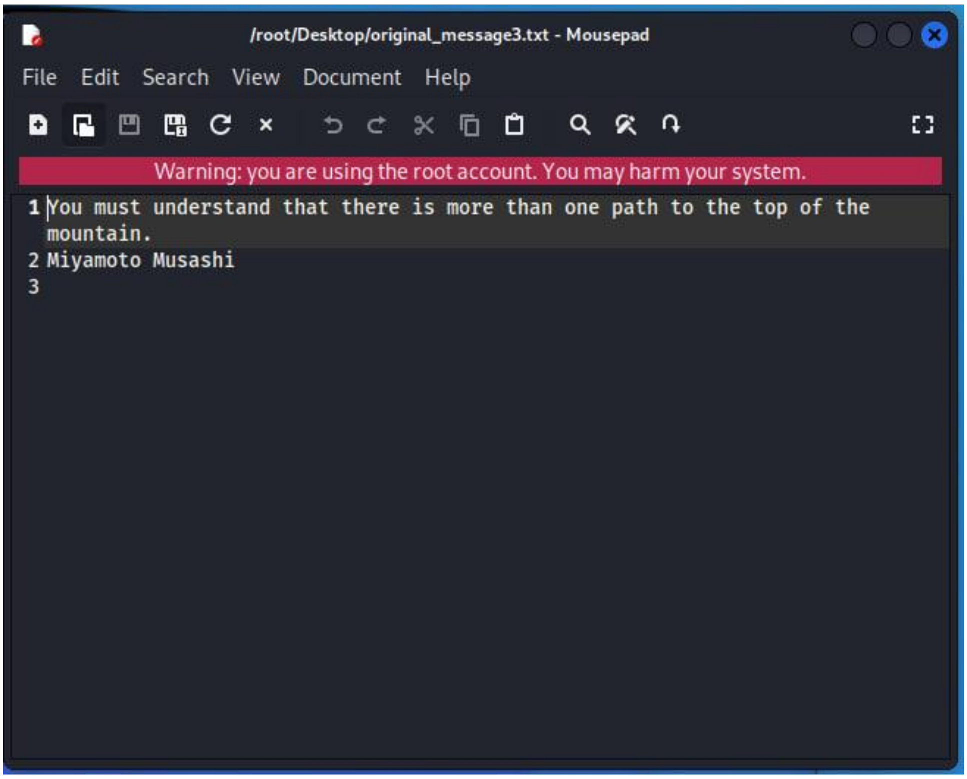


Warning:

1 The true science

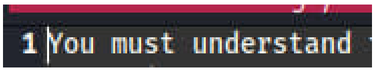


```
┌──(root㉿kali)-[~/Desktop]
└─# gpg --output original_message3.txt --decrypt quote03.txt.gpg
gpg: CAMELLIA256.CFB encrypted data
gpg: encrypted with 1 passphrase
```

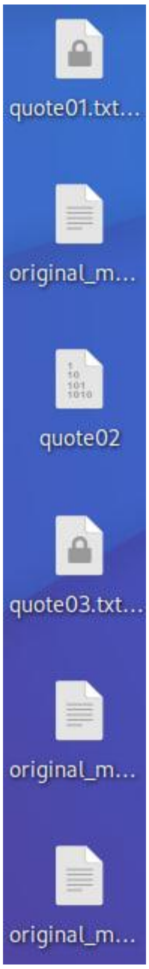


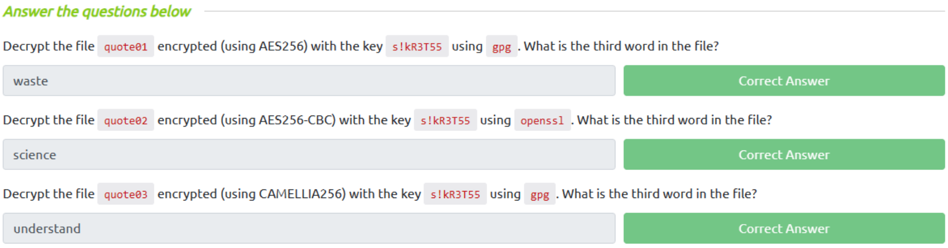
Warning: you are using the root account. You may harm your system.

```
You must understand that there is more than one path to the top of the
mountain.
Miyamoto Musashi
```



```
You must understand
```





Answer the questions below

Decrypt the file `quote01` encrypted (using AES256) with the key `s!kR3T55` using `gpg`. What is the third word in the file?

waste

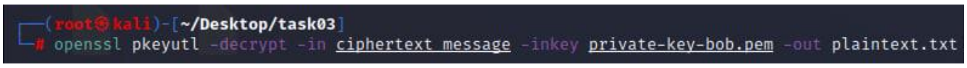
Decrypt the file `quote02` encrypted (using AES256-CBC) with the key `s!kR3T55` using `openssl`. What is the third word in the file?

science

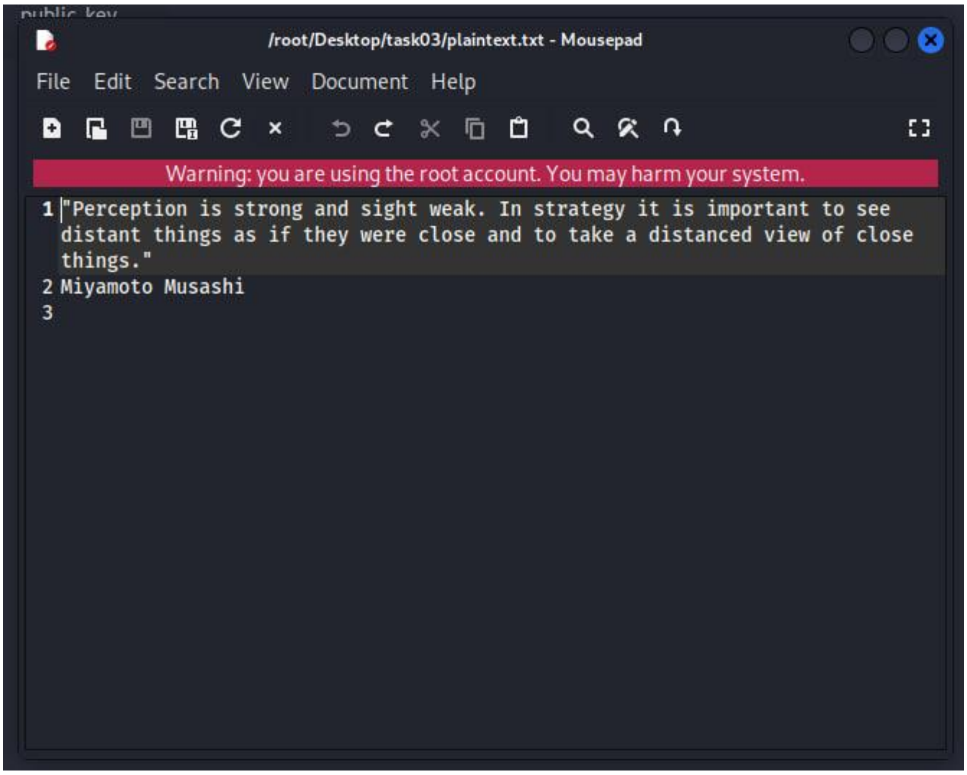
Decrypt the file `quote03` encrypted (using CAMELLIA256) with the key `s!kR3T55` using `gpg`. What is the third word in the file?

understand

3. Assymmetric Encryption

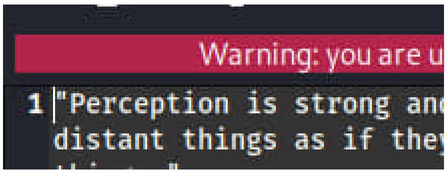


```
┌──(root㉿kali)-[~/Desktop/task03]
└─# openssl pkeyutl -decrypt -in ciphertext_message -inkey private-key-bob.pem -out plaintext.txt
```



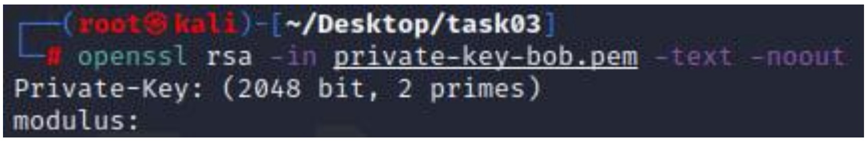
Warning: you are using the root account. You may harm your system.

```
"Perception is strong and sight weak. In strategy it is important to see distant things as if they were close and to take a distanced view of close things."
Miyamoto Musashi

```

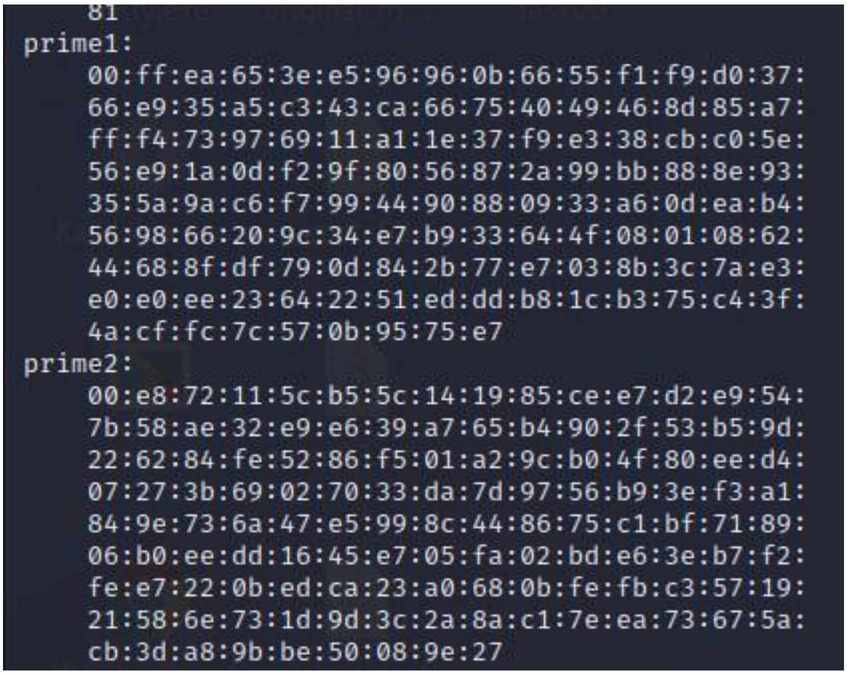


Warning: you are u

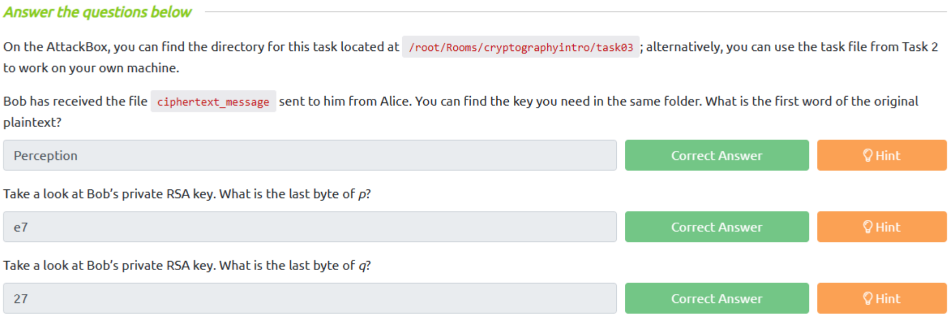
```
"Perception is strong and
distant things as if they
```



```
┌──(root㉿kali)-[~/Desktop/task03]
└─# openssl rsa -in private-key-bob.pem -text -noout
Private-Key: (2048 bit, 2 primes)
modulus:
```



```
    81
prime1:
    00:ff:ea:65:3e:e5:96:96:0b:66:55:f1:f9:d0:37:
    66:e9:35:a5:c3:43:ca:66:75:40:49:46:8d:85:a7:
    ff:f4:73:97:69:11:a1:1e:37:f9:e3:38:cb:c0:5e:
    56:e9:1a:0d:f2:9f:80:56:87:2a:99:bb:88:8e:93:
    35:5a:9a:c6:f7:99:44:90:88:09:33:a6:0d:ea:b4:
    56:98:66:20:9c:34:e7:b9:33:64:4f:08:01:08:62:
    44:68:8f:df:79:0d:84:2b:77:e7:03:8b:3c:7a:e3:
    e0:e0:ee:23:64:22:51:ed:dd:b8:1c:b3:75:c4:3f:
    4a:cf:fc:7c:57:0b:95:75:e7
prime2:
    00:e8:72:11:5c:b5:5c:14:19:85:ce:e7:d2:e9:54:
    7b:58:ae:32:e9:e6:39:a7:65:b4:90:2f:53:b5:9d:
    22:62:84:fe:52:86:f5:01:a2:9c:b0:4f:80:ee:d4:
    07:27:3b:69:02:70:33:da:7d:97:56:b9:3e:f3:a1:
    84:9e:73:6a:47:e5:99:8c:44:86:75:c1:bf:71:89:
    06:b0:ee:dd:16:45:e7:05:fa:02:bd:e6:3e:b7:f2:
    fe:e7:22:0b:ed:ca:23:a0:68:0b:fe:fb:c3:57:19:
    21:58:6e:73:1d:9d:3c:2a:8a:c1:7e:ea:73:67:5a:
    cb:3d:a8:9b:be:50:08:9e:27
```



Answer the questions below

On the AttackBox, you can find the directory for this task located at `/root/Rooms/cryptographyintro/task03`; alternatively, you can use the task file from Task 2 to work on your own machine.

Bob has received the file `ciphertext_message` sent to him from Alice. You can find the key you need in the same folder. What is the first word of the original plaintext?

Perception

Take a look at Bob's private RSA key. What is the last byte of *p*?

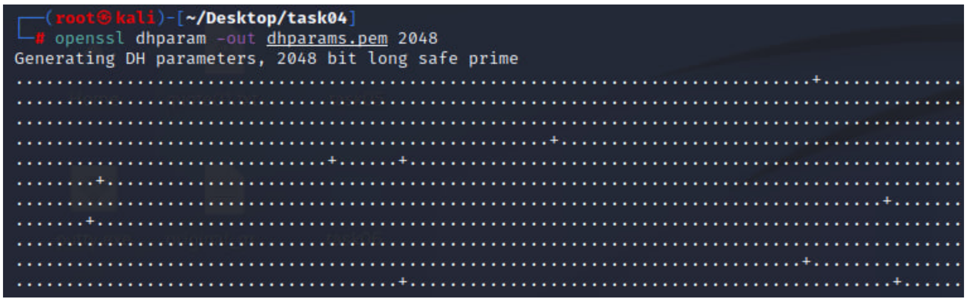
e7

Take a look at Bob's private RSA key. What is the last byte of *q*?

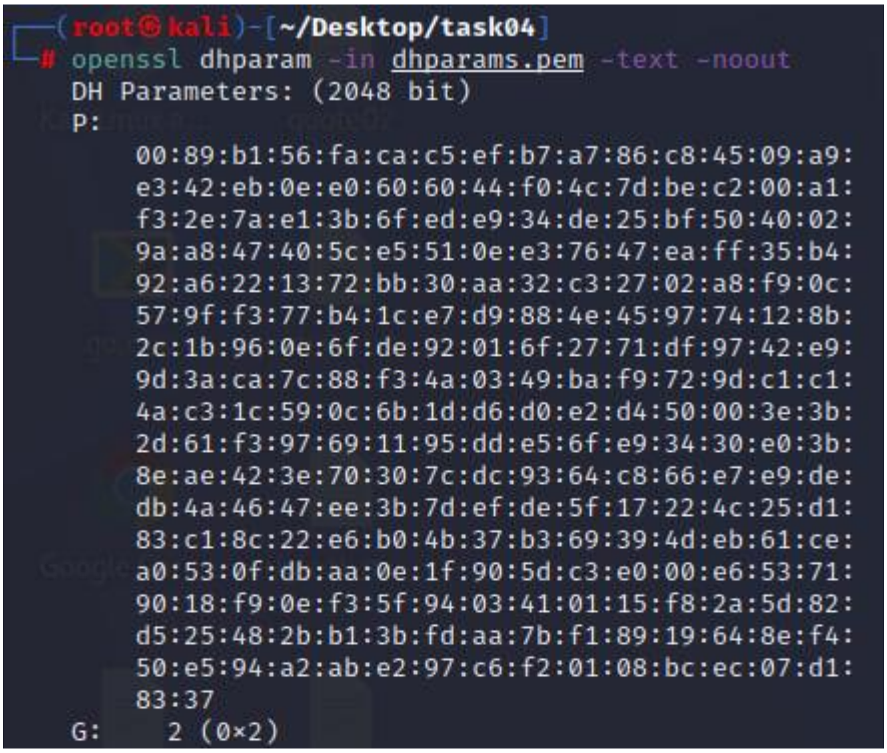
27

4. Diffie-Hellman Key Exchange

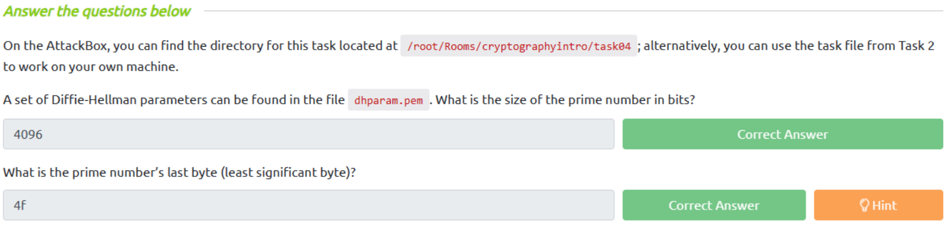
Task 4 ✓ Diffie-Hellman Key Exchange



```
┌──(root㉿kali)-[~/Desktop/task04]
└─# openssl dhparam -out dhparams.pem 2048
Generating DH parameters, 2048 bit long safe prime
..............................................................................+.............
............................................................................................
............................................................................................
....................................................+.......................................
...............................+......+.....................................................
........+...................................................................................
.....................................................................................+......
.......+....................................................................................
............................................................................................
.............................................................................+..............
.....................................+................................................+.....
```



```
┌──(root㉿kali)-[~/Desktop/task04]
└─# openssl dhparam -in dhparams.pem -text -noout
    DH Parameters: (2048 bit)
    P:
        00:89:b1:56:fa:ca:c5:ef:b7:a7:86:c8:45:09:a9:
        e3:42:eb:0e:e0:60:60:44:f0:4c:7d:be:c2:00:a1:
        f3:2e:7a:e1:3b:6f:ed:e9:34:de:25:bf:50:40:02:
        9a:a8:47:40:5c:e5:51:0e:e3:76:47:ea:ff:35:b4:
        92:a6:22:13:72:bb:30:aa:32:c3:27:02:a8:f9:0c:
        57:9f:f3:77:b4:1c:e7:d9:88:4e:45:97:74:12:8b:
        2c:1b:96:0e:6f:de:92:01:6f:27:71:df:97:42:e9:
        9d:3a:ca:7c:88:f3:4a:03:49:ba:f9:72:9d:c1:c1:
        4a:c3:1c:59:0c:6b:1d:d6:d0:e2:d4:50:00:3e:3b:
        2d:61:f3:97:69:11:95:dd:e5:6f:e9:34:30:e0:3b:
        8e:ae:42:3e:70:30:7c:dc:93:64:c8:66:e7:e9:de:
        db:4a:46:47:ee:3b:7d:ef:de:5f:17:22:4c:25:d1:
        83:c1:8c:22:e6:b0:4b:37:b3:69:39:4d:eb:61:ce:
        a0:53:0f:db:aa:0e:1f:90:5d:c3:e0:00:e6:53:71:
        90:18:f9:0e:f3:5f:94:03:41:01:15:f8:2a:5d:82:
        d5:25:48:2b:b1:3b:fd:aa:7b:f1:89:19:64:8e:f4:
        50:e5:94:a2:ab:e2:97:c6:f2:01:08:bc:ec:07:d1:
        83:37
    G:    2 (0×2)
```



Answer the questions below

On the AttackBox, you can find the directory for this task located at `/root/Rooms/cryptographyintro/task04`; alternatively, you can use the task file from Task 2 to work on your own machine.

A set of Diffie-Hellman parameters can be found in the file `dhparam.pem`. What is the size of the prime number in bits?

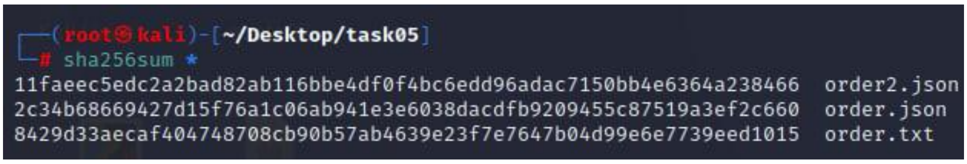
4096

What is the prime number's last byte (least significant byte)?

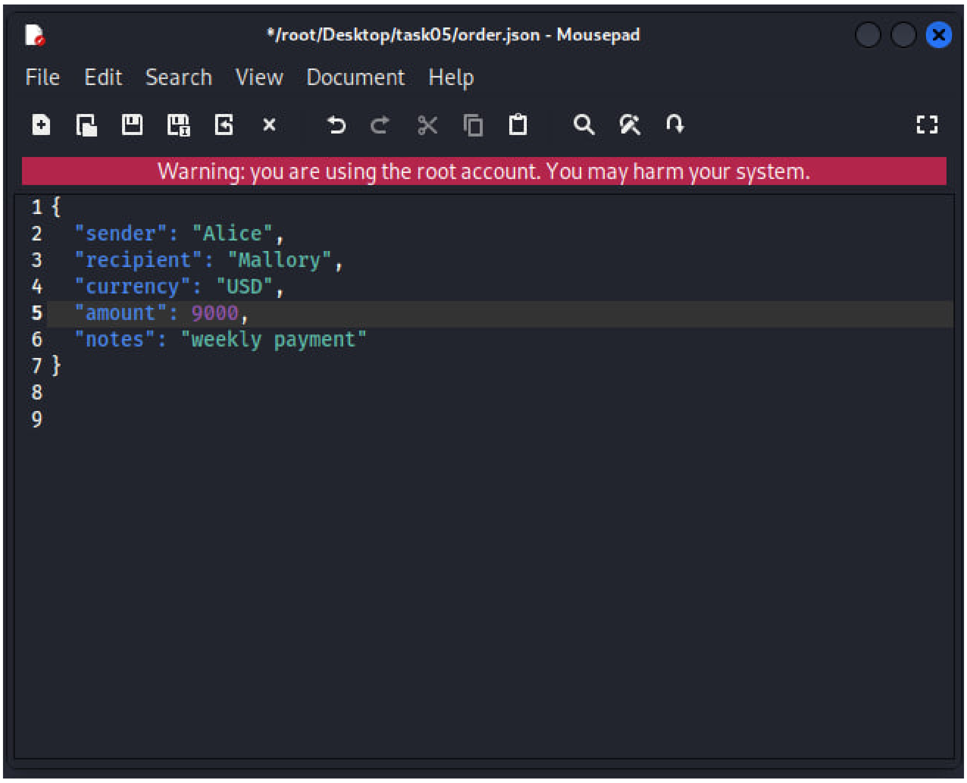
4f

5. Hashing

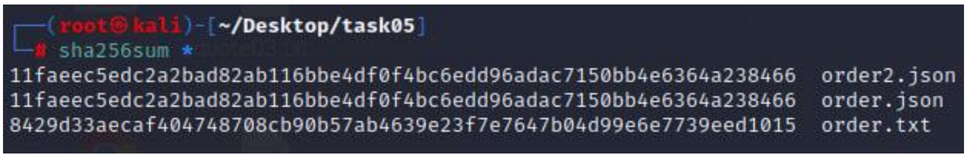
Task 5 ✓ Hashing



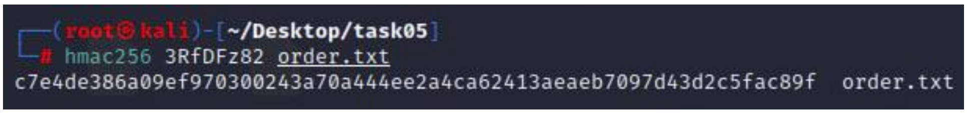
```
┌──(root㉿kali)-[~/Desktop/task05]
└─# sha256sum *
11faeec5edc2a2bad82ab116bbe4df0f4bc6edd96adac7150bb4e6364a238466  order2.json
2c34b68669427d15f76a1c06ab941e3e6038dacdfb9209455c87519a3ef2c660  order.json
8429d33aecaf404748708cb90b57ab4639e23f7e7647b04d99e6e7739eed1015  order.txt
```


*/root/Desktop/task05/order.json - Mousepad
File
Edit
Search
View
Document
Help
Warning: you are using the root account. You may harm your system.

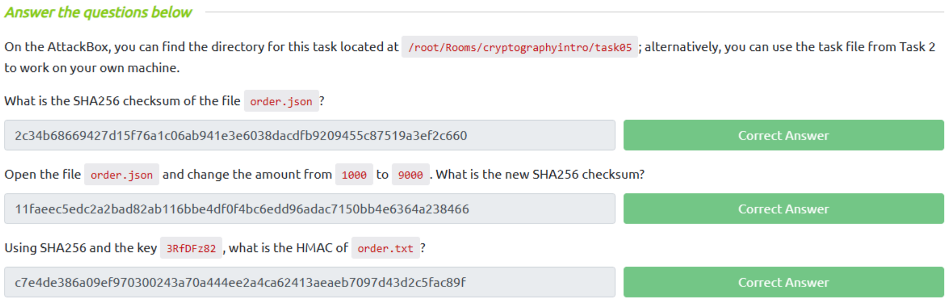
```
{
  "sender": "Alice",
  "recipient": "Mallory",
  "currency": "USD",
  "amount": 9000,
  "notes": "weekly payment"
}
```



```
┌──(root㉿kali)-[~/Desktop/task05]
└─# sha256sum *
11faeec5edc2a2bad82ab116bbe4df0f4bc6edd96adac7150bb4e6364a238466  order2.json
11faeec5edc2a2bad82ab116bbe4df0f4bc6edd96adac7150bb4e6364a238466  order.json
8429d33aecaf404748708cb90b57ab4639e23f7e7647b04d99e6e7739eed1015  order.txt
```



```
┌──(root㉿kali)-[~/Desktop/task05]
└─# hmac256 3RfDFz82 order.txt
c7e4de386a09ef970300243a70a444ee2a4ca62413aeaeb7097d43d2c5fac89f  order.txt
```



Answer the questions below

On the AttackBox, you can find the directory for this task located at `/root/Rooms/cryptographyintro/task05`; alternatively, you can use the task file from Task 2 to work on your own machine.

What is the SHA256 checksum of the file `order.json`?

2c34b68669427d15f76a1c06ab941e3e6038dacdfb9209455c87519a3ef2c660 | Correct Answer

Open the file `order.json` and change the amount from `1000` to `9000`. What is the new SHA256 checksum?

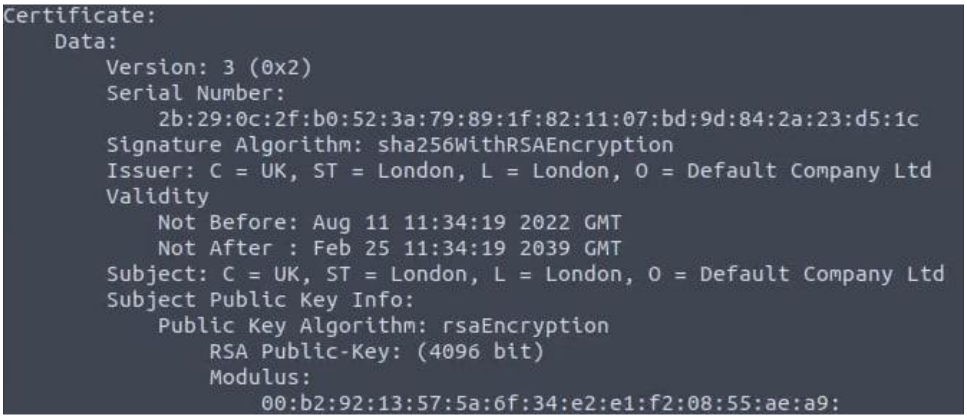
11faeec5edc2a2bad82ab116bbe4df0f4bc6edd96adac7150bb4e6364a238466 | Correct Answer

Using SHA256 and the key `3RfDFz82`, what is the HMAC of `order.txt`?

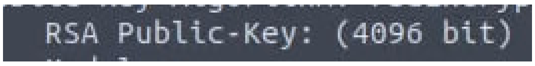
c7e4de386a09ef970300243a70a444ee2a4ca62413aeaeb7097d43d2c5fac89f | Correct Answer

6. PKI and SSL/TLS

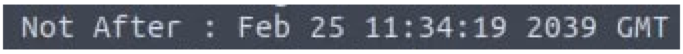
Task 6 ✓ PKI and SSL/TLS



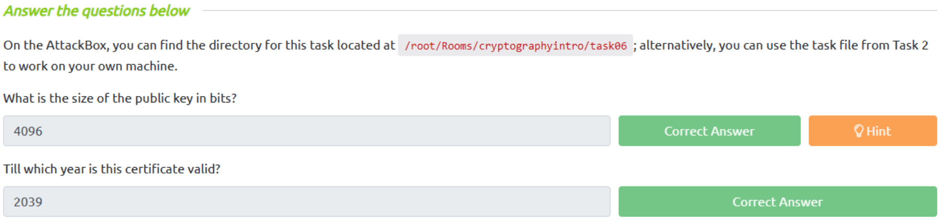
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2b:29:0c:2f:b0:52:3a:79:89:1f:82:11:07:bd:9d:84:2a:23:d5:1c
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = UK, ST = London, L = London, O = Default Company Ltd
        Validity
            Not Before: Aug 11 11:34:19 2022 GMT
            Not After : Feb 25 11:34:19 2039 GMT
        Subject: C = UK, ST = London, L = London, O = Default Company Ltd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:b2:92:13:57:5a:6f:34:e2:e1:f2:08:55:ae:a9:
```



```
RSA Public-Key: (4096 bit)
```



```
Not After : Feb 25 11:34:19 2039 GMT
```



Answer the questions below

On the AttackBox, you can find the directory for this task located at `/root/Rooms/cryptographyintro/task06` ; alternatively, you can use the task file from Task 2 to work on your own machine.

What is the size of the public key in bits?

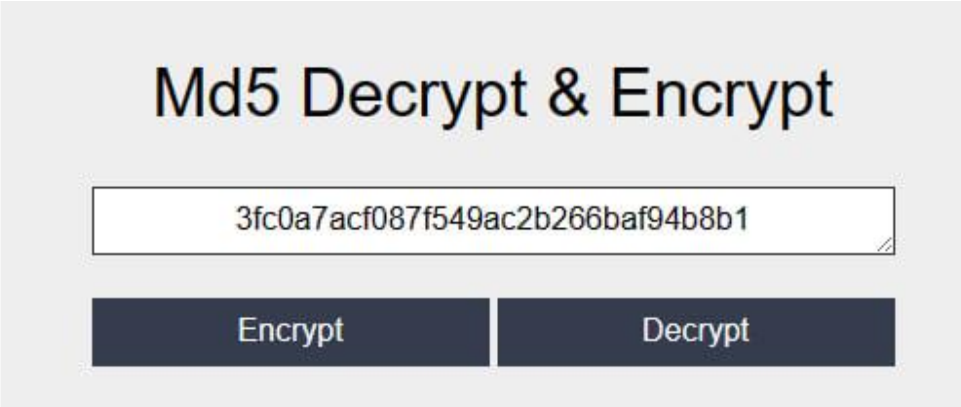
4096 | Correct Answer | Hint

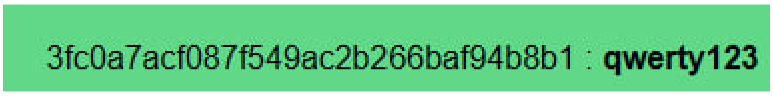
Till which year is this certificate valid?

2039 | Correct Answer

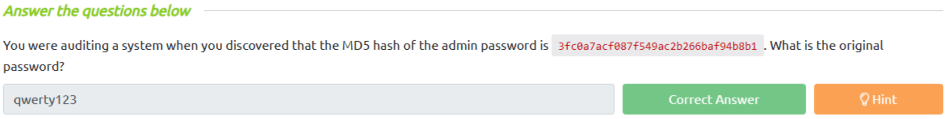
7. Authenticating with Passwords

Task 7 ✓ Authenticating with Passwords





3fc0a7acf087f549ac2b266baf94b8b1 : **qwerty123**

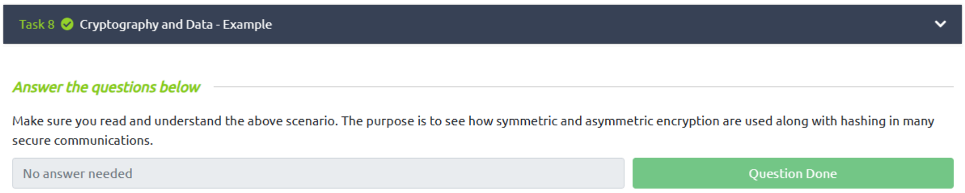


Answer the questions below

You were auditing a system when you discovered that the MD5 hash of the admin password is `3fc0a7acf087f549ac2b266baf94b8b1` . What is the original password?

qwerty123 | Correct Answer | Hint

8. Cryptography and Data – Example



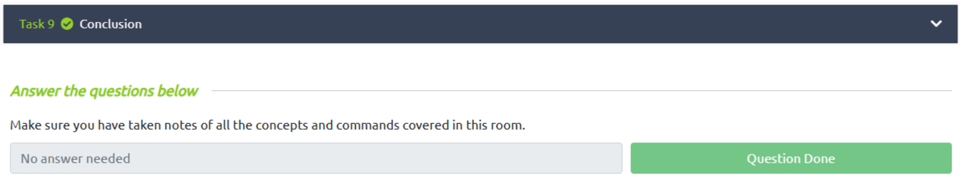
Task 8 Cryptography and Data - Example

Answer the questions below

Make sure you read and understand the above scenario. The purpose is to see how symmetric and asymmetric encryption are used along with hashing in many secure communications.

No answer needed | Question Done

9. Conclusion



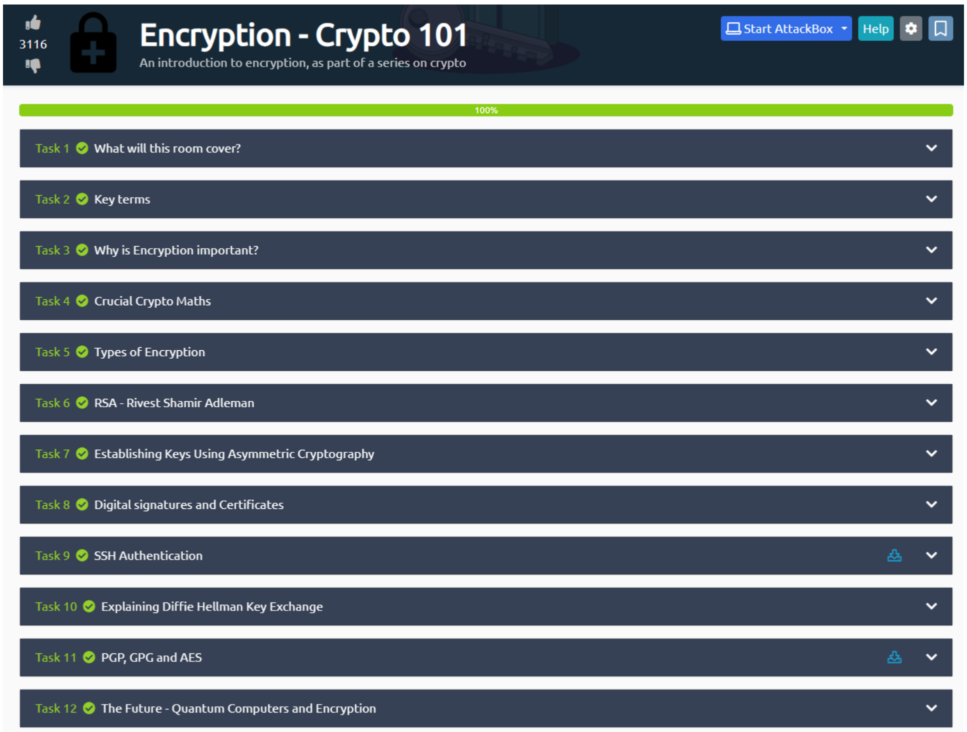
Task 9 Conclusion

Answer the questions below

Make sure you have taken notes of all the concepts and commands covered in this room.

No answer needed | Question Done

Part 4. Encryption – Crypto 101



Encryption - Crypto 101

An introduction to encryption, as part of a series on crypto

Task 1 What will this room cover?

Task 2 Key terms

Task 3 Why is Encryption important?

Task 4 Crucial Crypto Maths

Task 5 Types of Encryption

Task 6 RSA - Rivest Shamir Adleman

Task 7 Establishing Keys Using Asymmetric Cryptography

Task 8 Digital signatures and Certificates

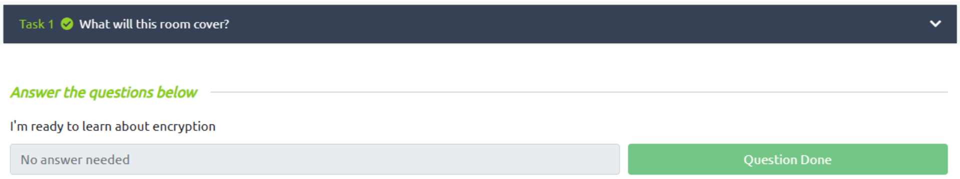
Task 9 SSH Authentication

Task 10 Explaining Diffie Hellman Key Exchange

Task 11 PGP, GPG and AES

Task 12 The Future - Quantum Computers and Encryption

1. What will this room cover?



Task 1 What will this room cover?

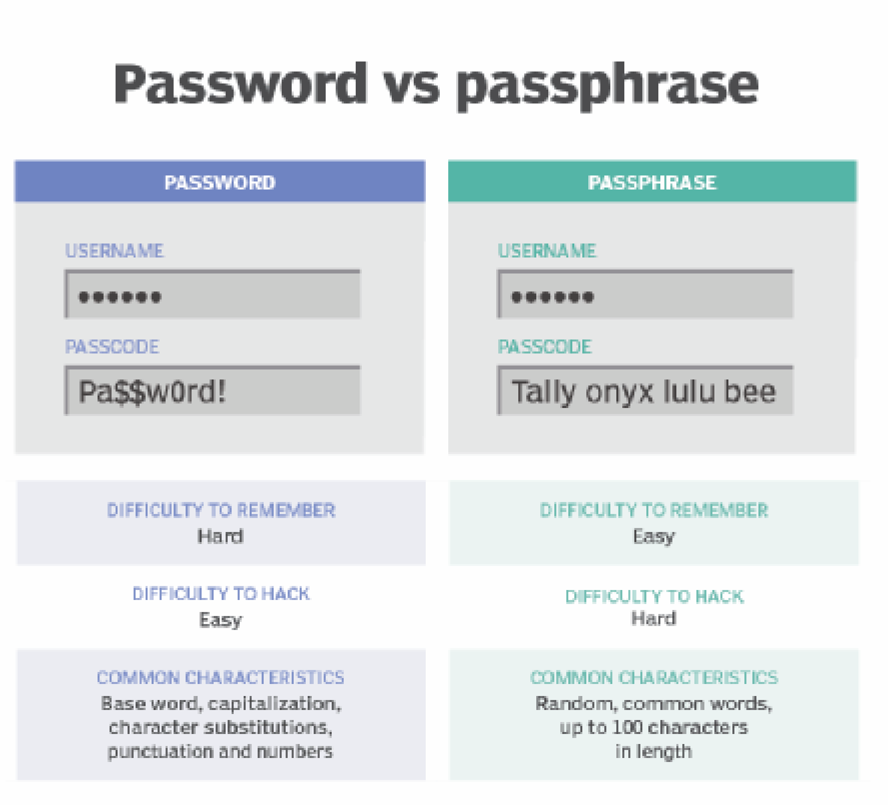
Answer the questions below

I'm ready to learn about encryption

No answer needed | Question Done

2. Key terms

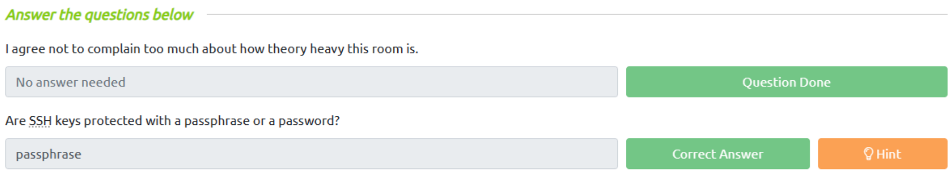
Task 2 Key terms



Password vs passphrase

PASSWORD	PASSPHRASE
USERNAME ●●●●●● PASSCODE Pa$$w0rd!	USERNAME ●●●●●● PASSCODE Tally onyx lulu bee
DIFFICULTY TO REMEMBER Hard	DIFFICULTY TO REMEMBER Easy
DIFFICULTY TO HACK Easy	DIFFICULTY TO HACK Hard
COMMON CHARACTERISTICS Base word, capitalization, character substitutions, punctuation and numbers	COMMON CHARACTERISTICS Random, common words, up to 100 characters in length

Therefore, an answer is **passphrase**.



Answer the questions below

I agree not to complain too much about how theory heavy this room is.

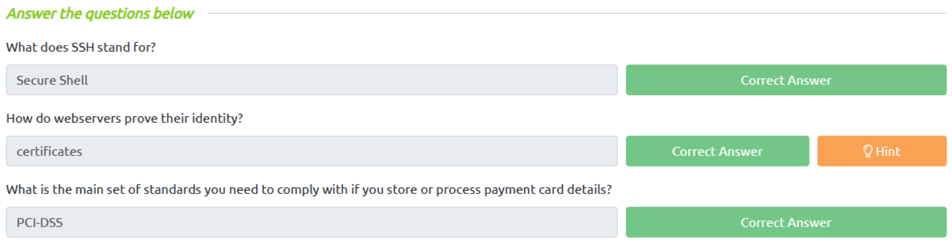
No answer needed

Are SSH keys protected with a passphrase or a password?

passphrase

3. Why is Encryption important?

- SSH (Secure Shell)
- By certificates webservers prove their identity
- Payment Card Industry Data Security Standard (PCI-DSS) is needed for store or process our payment card details



Answer the questions below

What does SSH stand for?

Secure Shell

How do webservers prove their identity?

certificates

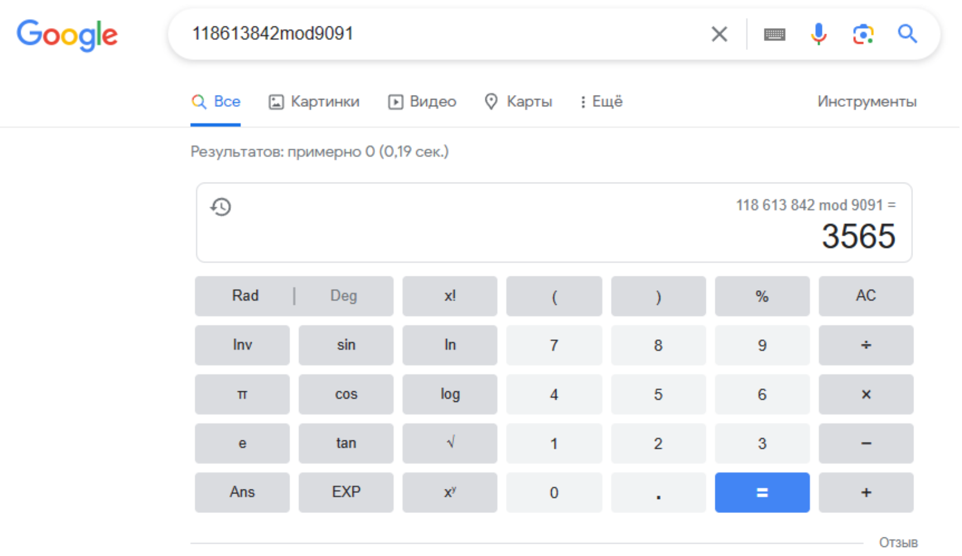
What is the main set of standards you need to comply with if you store or process payment card details?

PCI-DSS

4. Crucial Crypto Maths

Task 4 Crucial Crypto Maths

- 30 % 5 is look like to 30mod5, by simply covering explanation 30 / 5 = 6, without any remainder, therefore it is **0**.
- 25 % 7 is look like to 25mod7, but it has remainder 4 comes from 25 / 7 = 3 with remainder **4**.
- 118613842 % 9091 is look like to 118613842mod9091, but it has remainder 3565 that comes from 118613842 / 9091 = 13047 with remainder **3565**.

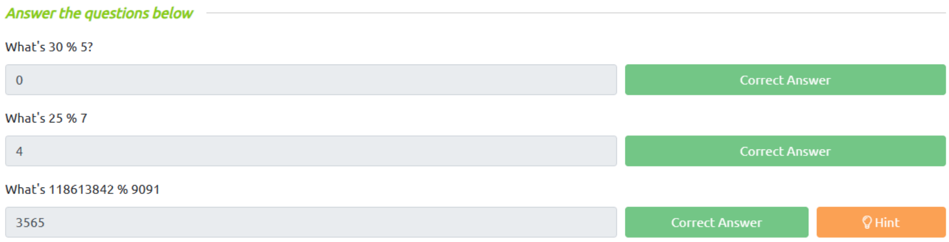


118613842mod9091

Результатов: примерно 0 (0,19 сек.)

118 613 842 mod 9091 =

3565



Answer the questions below

What's 30 % 5?

0

What's 25 % 7

4

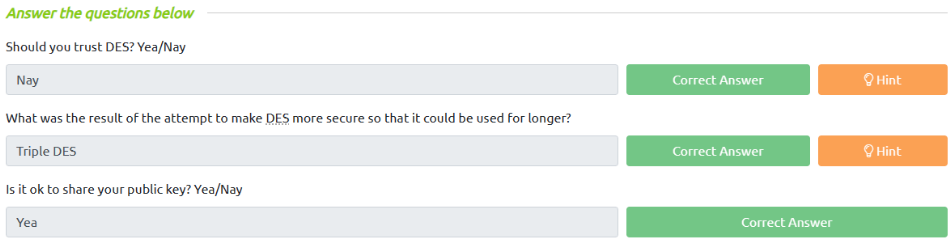
What's 118613842 % 9091

3565

5. Types of Encryption

Task 5 Types of Encryption

- We shouldn't trust DES, because it is a symmetric encryption with the key size of 56 bits, being insecure.
- By researches, in order to make DES more secure it has developed to Triple DES.
- We can share our public key, beause it is a public than a private key which is a secret and can't be shared.



Answer the questions below

Should you trust DES? Yea/Nay

Nay

What was the result of the attempt to make DES more secure so that it could be used for longer?

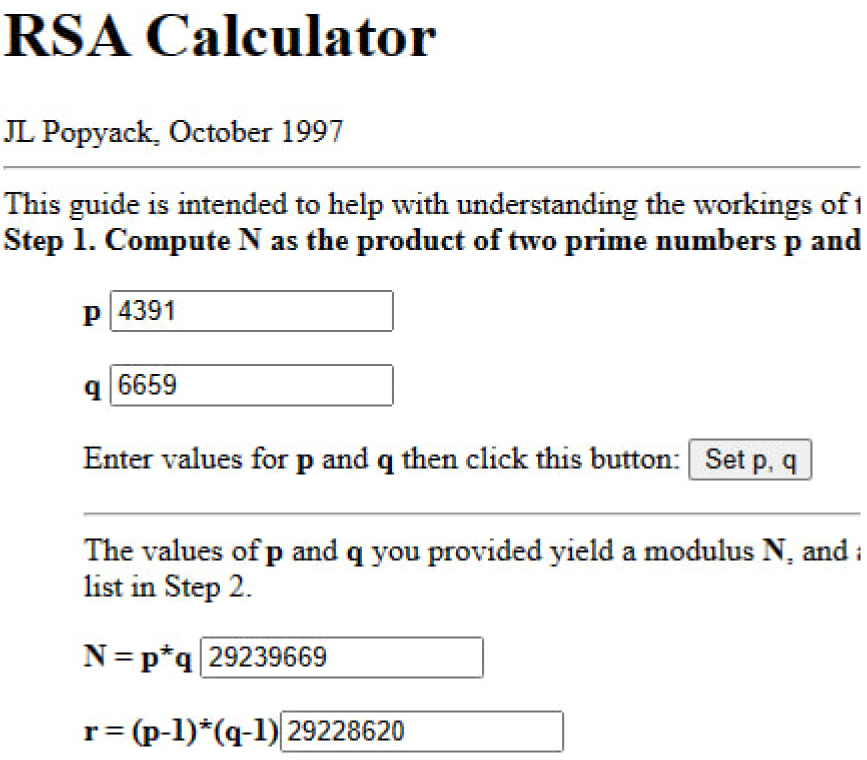
Triple DES

Is it ok to share your public key? Yea/Nay

Yea

6. RSA Rivest Shamir Adleman

Task 6 RSA - Rivest Shamir Adleman



RSA Calculator

JL Popyack, October 1997

This guide is intended to help with understanding the workings of t

Step 1. Compute N as the product of two prime numbers p and

p 4391

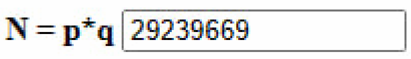
q 6659

Enter values for **p** and **q** then click this button:

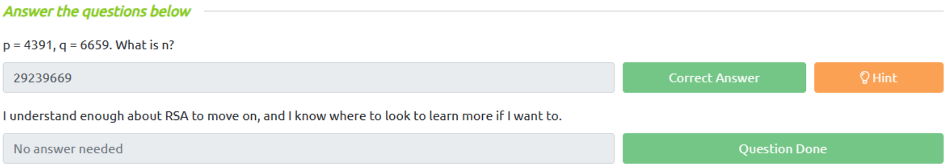
The values of **p** and **q** you provided yield a modulus **N**, and a list in Step 2.

N = p*q 29239669

r = (p-1)*(q-1) 29228620



N = p*q 29239669



Answer the questions below

p = 4391, q = 6659. What is n?

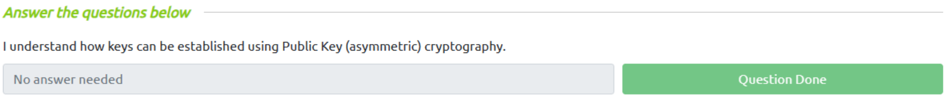
29239669

I understand enough about RSA to move on, and I know where to look to learn more if I want to.

No answer needed

7. Establishing Keys Using Assymmetric Cryptography

Task 7 Establishing Keys Using Asymmetric Cryptography



Answer the questions below

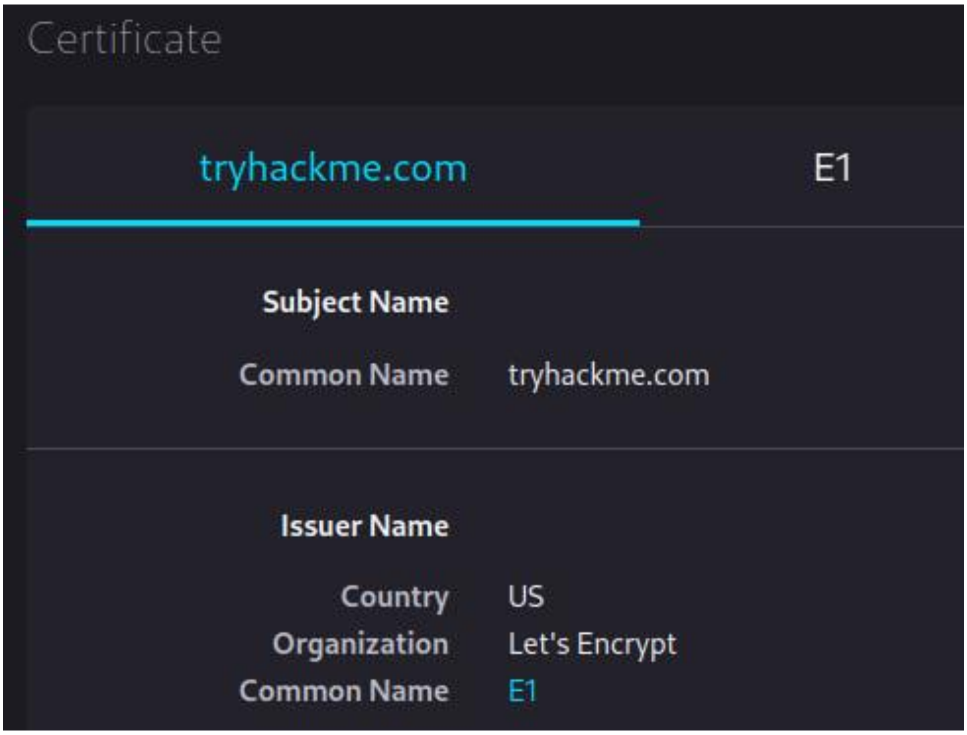
I understand how keys can be established using Public Key (asymmetric) cryptography.

No answer needed

Question Done

8. Digital signatures and Certificates

Task 8 ✓ Digital signatures and Certificates



Certificate

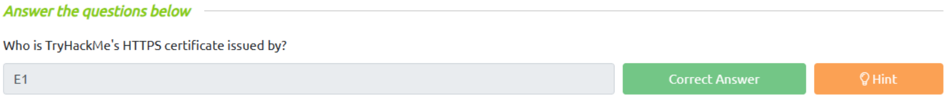
tryhackme.com | E1

Subject Name

Common Name	tryhackme.com

Issuer Name

Country	US
Organization	Let's Encrypt
Common Name	E1



Answer the questions below

Who is TryHackMe's HTTPS certificate issued by?

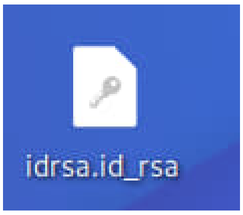
E1

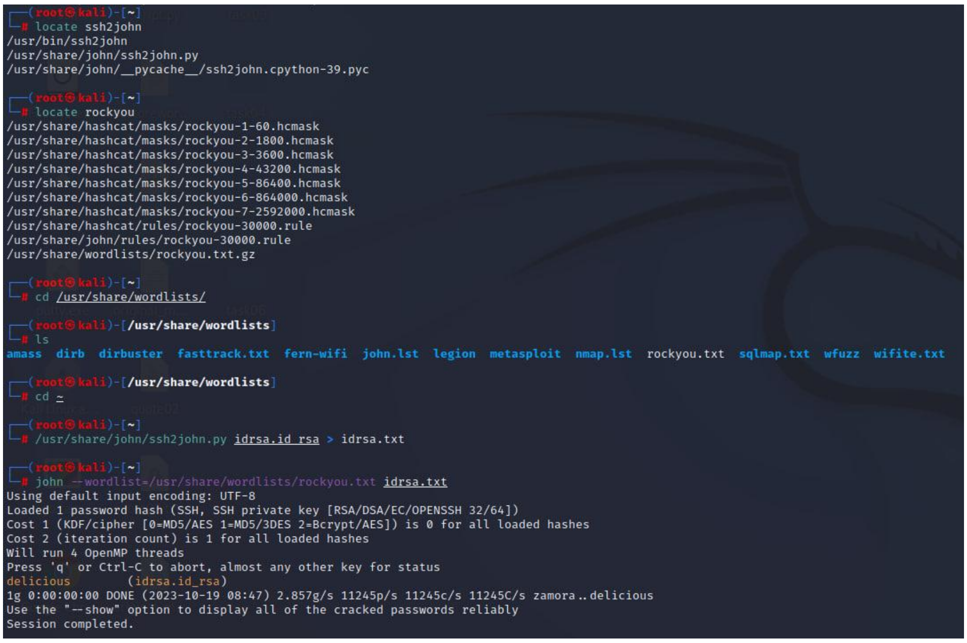
Correct Answer

Hint

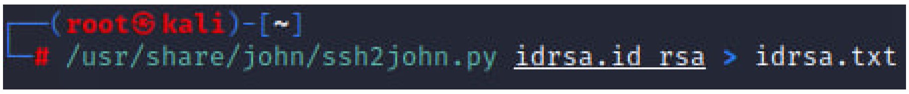
9. SSH Authentication

Task 9 ✓ SSH Authentication

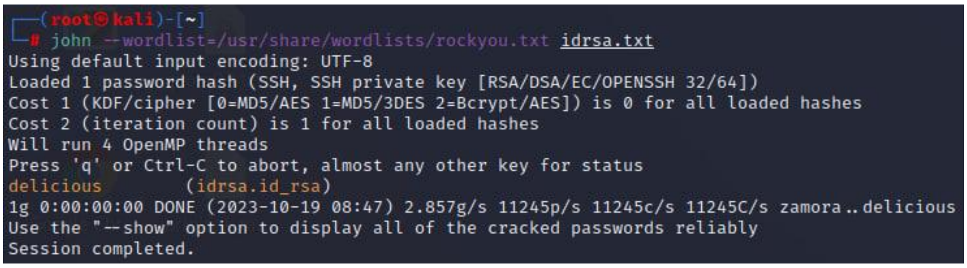




```
┌──(root㉿kali)-[~]
└─# locate ssh2john
/usr/bin/ssh2john
/usr/share/john/ssh2john.py
/usr/share/john/__pycache__/ssh2john.cpython-39.pyc

┌──(root㉿kali)-[~]
└─# locate rockyou
/usr/share/hashcat/masks/rockyou-1-60.hcmask
/usr/share/hashcat/masks/rockyou-2-1800.hcmask
/usr/share/hashcat/masks/rockyou-3-3600.hcmask
/usr/share/hashcat/masks/rockyou-4-43200.hcmask
/usr/share/hashcat/masks/rockyou-5-86400.hcmask
/usr/share/hashcat/masks/rockyou-6-864000.hcmask
/usr/share/hashcat/masks/rockyou-7-2592000.hcmask
/usr/share/hashcat/rules/rockyou-30000.rule
/usr/share/john/rules/rockyou-30000.rule
/usr/share/wordlists/rockyou.txt.gz

┌──(root㉿kali)-[~]
└─# cd /usr/share/wordlists/

┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass  dirb  dirbuster  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt

┌──(root㉿kali)-[/usr/share/wordlists]
└─# cd ~

┌──(root㉿kali)-[~]
└─# /usr/share/john/ssh2john.py idrsa.id_rsa > idrsa.txt

┌──(root㉿kali)-[~]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt idrsa.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
delicious        (idrsa.id_rsa)
1g 0:00:00:00 DONE (2023-10-19 08:47) 2.857g/s 11245p/s 11245c/s 11245C/s zamora..delicious
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

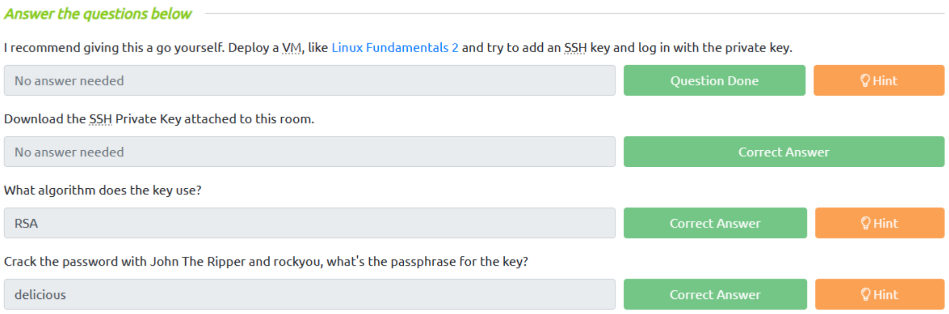


```
┌──(root㉿kali)-[~]
└─# /usr/share/john/ssh2john.py idrsa.id_rsa > idrsa.txt
```



```
┌──(root㉿kali)-[~]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt idrsa.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
delicious        (idrsa.id_rsa)
1g 0:00:00:00 DONE (2023-10-19 08:47) 2.857g/s 11245p/s 11245c/s 11245C/s zamora..delicious
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
delicious        (idrsa.id_rsa)
```



Answer the questions below

I recommend giving this a go yourself. Deploy a VM, like Linux Fundamentals 2 and try to add an SSH key and log in with the private key.

No answer needed

Download the SSH Private Key attached to this room.

No answer needed

What algorithm does the key use?

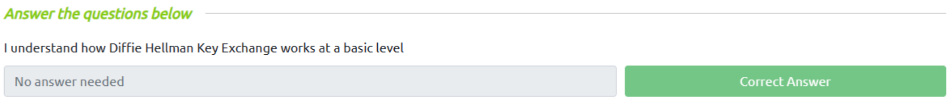
RSA

Crack the password with John The Ripper and rockyou, what's the passphrase for the key?

delicious

10. Explaining Diffie Hellman Key Exchange

Task 10 ✓ Explaining Diffie Hellman Key Exchange



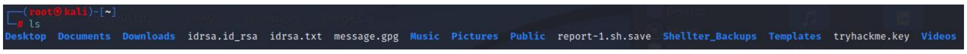
Answer the questions below

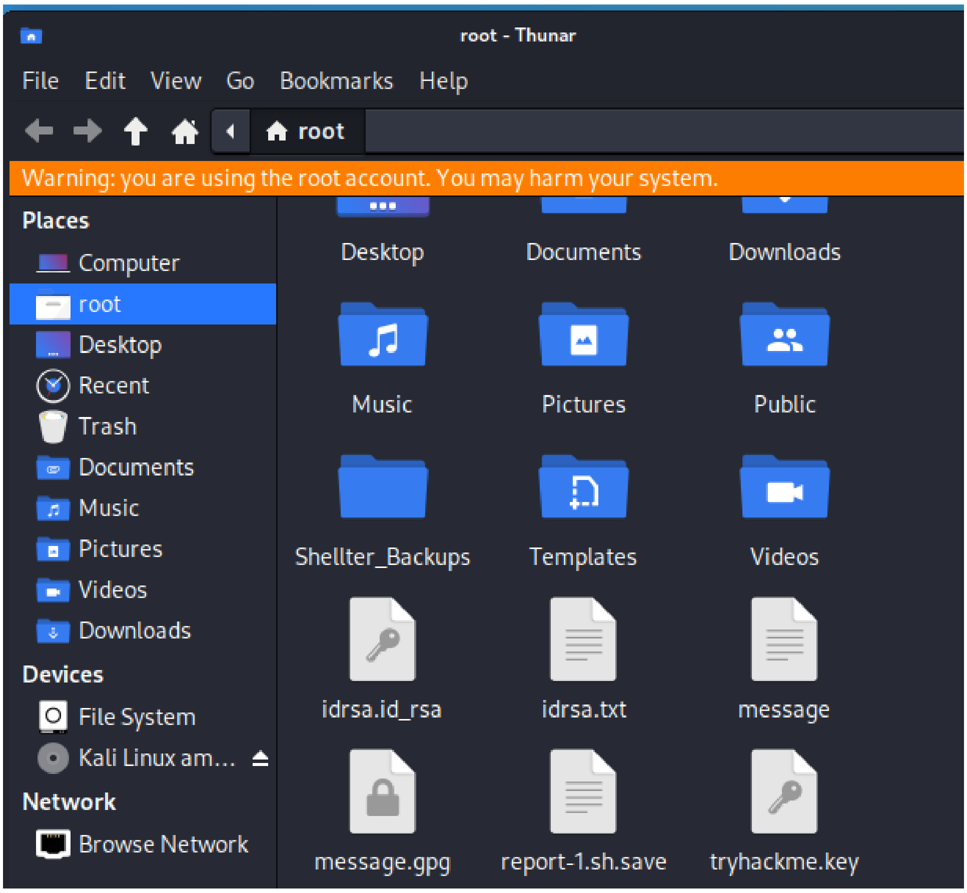
I understand how Diffie Hellman Key Exchange works at a basic level

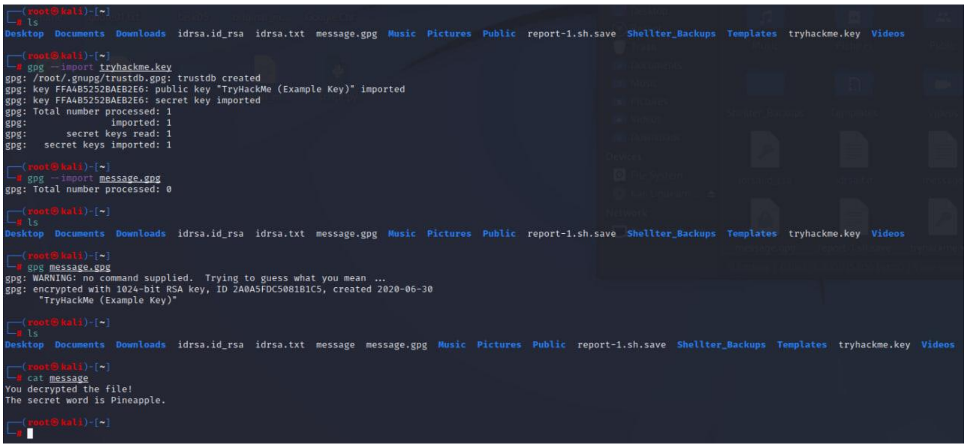
No answer needed

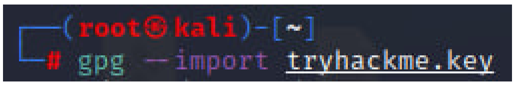
11. PGP, GPG and AES

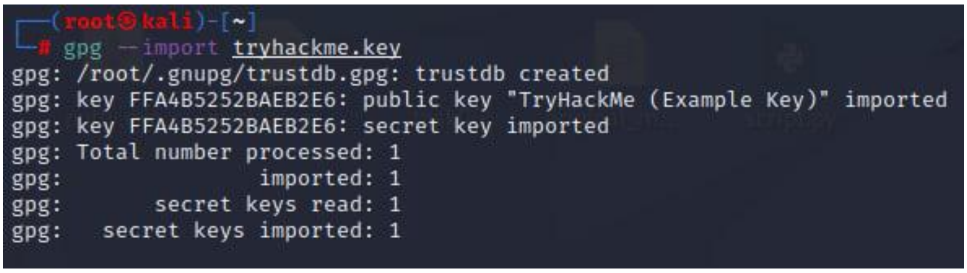
Task 11 PGP, GPG and AES


```
┌──(root㉿kali)-[~]
└─# ls
Desktop  Documents  Downloads  idrsa.id_rsa  idrsa.txt  message.gpg  Music  Pictures  Public  report-1.sh.save  Shellter_Backups  Templates  tryhackme.key  Videos
```

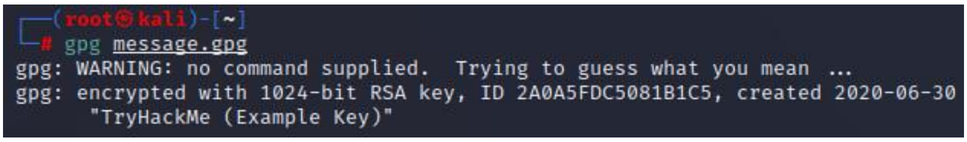



```
┌──(root㉿kali)-[~]
└─# ls
Desktop  Documents  Downloads  idrsa.id_rsa  idrsa.txt  message.gpg  Music  Pictures  Public  report-1.sh.save  Shellter_Backups  Templates  tryhackme.key  Videos

┌──(root㉿kali)-[~]
└─# gpg --import tryhackme.key
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key FFA4B5252BAEB2E6: public key "TryHackMe (Example Key)" imported
gpg: key FFA4B5252BAEB2E6: secret key imported
gpg: Total number processed: 1
gpg:               imported: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1

┌──(root㉿kali)-[~]
└─# gpg --import message.gpg
gpg: Total number processed: 0

┌──(root㉿kali)-[~]
└─# ls
Desktop  Documents  Downloads  idrsa.id_rsa  idrsa.txt  message.gpg  Music  Pictures  Public  report-1.sh.save  Shellter_Backups  Templates  tryhackme.key  Videos

┌──(root㉿kali)-[~]
└─# gpg message.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: encrypted with 1024-bit RSA key, ID 2A0A5FDC5081B1C5, created 2020-06-30
      "TryHackMe (Example Key)"

┌──(root㉿kali)-[~]
└─# ls
Desktop  Documents  Downloads  idrsa.id_rsa  idrsa.txt  message  message.gpg  Music  Pictures  Public  report-1.sh.save  Shellter_Backups  Templates  tryhackme.key  Videos

┌──(root㉿kali)-[~]
└─# cat message
You decrypted the file!
The secret word is Pineapple.

┌──(root㉿kali)-[~]
└─# 
```

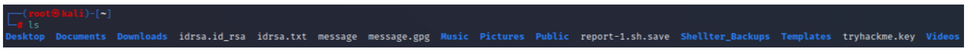

```
┌──(root㉿kali)-[~]
└─# gpg --import tryhackme.key
```



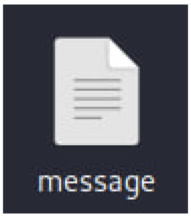
```
┌──(root㉿kali)-[~]
└─# gpg --import tryhackme.key
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key FFA4B5252BAEB2E6: public key "TryHackMe (Example Key)" imported
gpg: key FFA4B5252BAEB2E6: secret key imported
gpg: Total number processed: 1
gpg:               imported: 1
gpg:       secret keys read: 1
gpg:   secret keys imported: 1
```

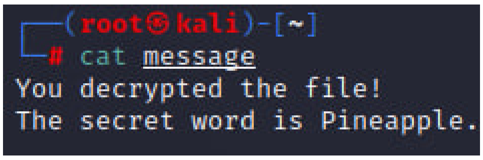


```
┌──(root㉿kali)-[~]
└─# gpg message.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: encrypted with 1024-bit RSA key, ID 2A0A5FDC5081B1C5, created 2020-06-30
      "TryHackMe (Example Key)"
```

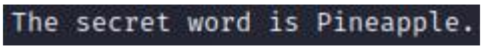


```
┌──(root㉿kali)-[~]
└─# ls
Desktop  Documents  Downloads  idrsa.id_rsa  idrsa.txt  message  message.gpg  Music  Pictures  Public  report-1.sh.save  Shellter_Backups  Templates  tryhackme.key  Videos
```

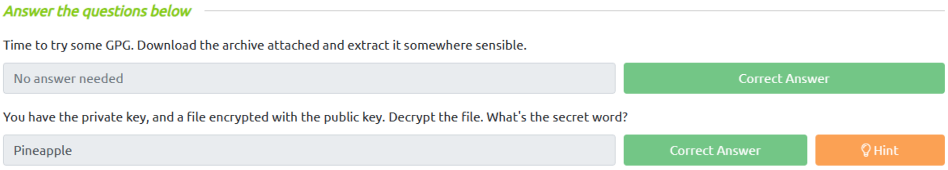




```
┌──(root㉿kali)-[~]
└─# cat message
You decrypted the file!
The secret word is Pineapple.
```



```
The secret word is Pineapple.
```



Answer the questions below

Time to try some GPG. Download the archive attached and extract it somewhere sensible.

No answer needed

Correct Answer

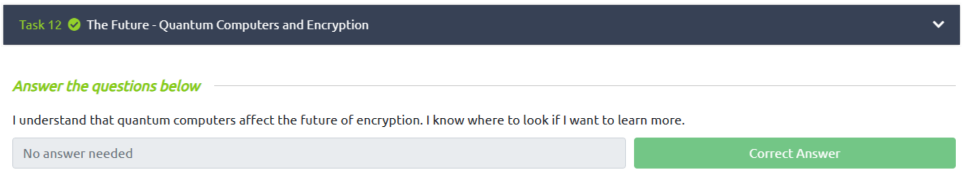
You have the private key, and a file encrypted with the public key. Decrypt the file. What's the secret word?

Pineapple

Correct Answer

Hint

12. The Future – Quantum Computers and Encryption



Task 12 ✓ The Future - Quantum Computers and Encryption

Answer the questions below

I understand that quantum computers affect the future of encryption. I know where to look if I want to learn more.

No answer needed

Correct Answer