ATTACK
DEFENSE

by PentesterAcademy

Name	Cracking Private Key Passphrase
URL	https://www.attackdefense.com/challengedetails?cid=718
Type	Cracking : Protected Files

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

User should try dictionary attack using the provided dictionary file first. If the dictionary attack doesn't succeeds, then the user should go for mask based bruteforce approach according to given password policy.

Note: Some snapshots are clipped to make them readable. So, screen content will not be an exact match. However, solutions will still match.

Step 1: A passphrase protected private key file is given. Extract the crackable information from the file using John the Ripper tools and check file contents

Command: ssh2john id_rsa > hash

```
root@attackdefense:~# ssh2john id_rsa > hash
root@attackdefense:~# cat hash
id_rsa:$ssh2$2d2d2d2d2d424547494e205253412050524956415445204b45592d2d2d2d2d0a50726f632d547970653a20342c454e435259505445440a44454b2d496e666f3a20
4145532d31323832d4342432c373431314146384134314136373933453039374532443953373239353383345380a0a7366566a536446462f37442f533836532b71423138704641536
136636b6f4f4c545345794379505a45764668465277333867392f435250584a356e2b56595159650a5932732b4e4a624a474b716541463455575044447594867693069656c71314343
634d6353736867477535546417334475764d536e536c56312f6235494d57514c0a6557737551512f506a6496c75634a4a6a7856856326942696842596436c64364b4a304b6e597a305
a44484e5a5771a4f7778676586535695630785341f766c4d7964760a4773694c6d4f4f4e2b4a5356696e565775580d4231426a393545386d3867576736b716f7443526e6646e5638376e33362
36566e4e357a583173597944573759944375350a7a7276324f38306a32616471433053633343143124c5973386b6b6335734b616a68694a2f4f2f41516644387250561674b7959724
d3056477147316c5853504b470a6a6f504964156d741e5a724948677a576c50494d4979950434965a641443760d5346477639436ee77396e7a7035444d7a4b30496c4972565a474f78666369
444f713853330a75364791933756836d4d73314b6a5546462584845b5744496161516f714d396e5154305a78636c4d483574e674767357a7a4d52774b454553368b4664365271577783178d
a49346b4e6133626626e6676d47656d37565043Sb3483374772b41667434643b596e4164345534457a6d62b3045453657507434557447796154b2b4d556476383744760a544a7a504754
52756d4d4842863744897f753061663c679754945524f4670354533714467535a762f6d2f6d7558838423392b3634d59312b7537462307814738740a56376c4c4b4e634d656c33435
0686f34776577526a734e49446e6581415972314872259417792b4d6f4414176c4370736867583056a66b76553344376579617707470a732b7731733849463035384b2f446d47968
3544347a6c594756604f3065706836968486a3534736a6f6f7676784b492b396626c4d332b374f4d633S330a6a74384f394c6c6c7c703371427442683336366d774b382b575a3
5346b41573726c49745444438395052374d567359692b6d764a312F657953366534332656c58730a6d58716151594259386a6e706455522b737363767957778b6d6636062614c446f7
76797a4338694578655a45575277354e6147762f627872705874427377624e360a755a46355957523336534314d4b556c4b4c2b7a3831434d42445681517247f51434c716376534
8667a2b305355744378426d6c6c6c6c93533526c526f7362480a665a6d6a774d694c4e4a344471526b4Sa6f54427a725530524113514141723538612f72415870656b6c37499b88796
4e4835466f6f6f6504a39614234755a704a7251a52764866676f6d4d6f396c2b6768396a6e317a7363544b3596d4d5566476443563073624262704114861684572667145663054642
b5472556869395044653733410a3578704d466b14736986a31387379747979496c4f6f7a714943526553332344831b6543854305a67692b4e7567757a3234343067354947617078
5843797a616e0a52487465624a3757414a62314a6375444b794136415274383232574d665245345444294b4e7a4b30556c3957567457556c7a6a4d4a575448949651676c7379976f0
a3768565144434d6e2F5a6944359376b4a766e4776658705575266dc504c627044566366466e44463263476495a5a6965166685555767634666449646c3164451594674a4e6d4d46316146
3631455463726465577fb7447444d56627a4f441706d412b30627a6834211417e7366522a667446834677339566446447677744a58522b78764f0a552b562b45623858bf5539347
74d636696645703344b1497a7932716869333864364367457326b87344b65505449734F706735714b6673666b336f4b41520a5948364d6494427e727a48357a507a4d364c5756
396853586778445476507863685735515166326853464b9744f506e7735494367364e635433495a79686c635660a4364426f37433731527076633854305614776f6f66d5a573774a755
357536d4539774a42472f534e5777335953547745527171317a51354e3665177334224c5134326a610a6a6d5036797758476d68575034564c49666e5257726a6a584c3873a51db6f343164
6530706e6359593531532f4437a6d48724550786f53334251616d67f72974723466f0a634b7066e787151434c445526e4e4c54553848714c7a322f677252352F2f2f744533357766567643
84979506e736a54564c4a476f79624e68495374474e6583961710a2d2d2d2d2d454e442052534120505249564154454204b4559202d2d2d2d2d0a*1766*0
root@attackdefense:~#
```

Step 2: We can use John The Ripper (JTR) for this.

Launch dictionary attack using given dictionary file 1000000-password-seclists.txt

Command: john --wordlist=1000000-password-seclists.txt hash

```
root@attackdefense:~# john --wordlist=/root/wordlists/1000000-password-seclists.txt hash
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
revenge2         (id_rsa)
1g 0:00:00:00 DONE (2018-12-06 16:03) 2.127g/s 425548p/s 425548c/s 425548C/s revenge2
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@attackdefense:~#
```

Flag: revenge2

References:

1. Hashcat (https://hashcat.net)
2. Hashcat Wiki (https://hashcat.net/wiki/)
3. John the ripper jumbo (https://www.openwall.com/john/)