

# Linux Essentials – Final Work

Shaked Uriel Brami – 213164379

CSPP86

Instructor - Boris Frenkel

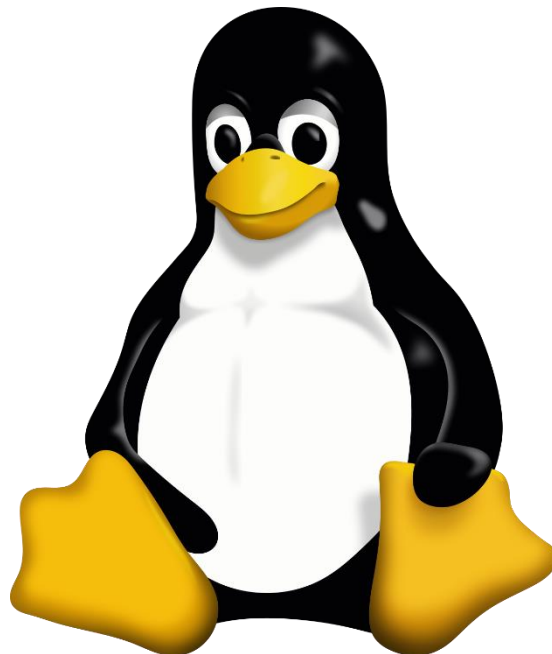
Date of Submission: 15/3/24



# Table of Contents

## Table of Contents

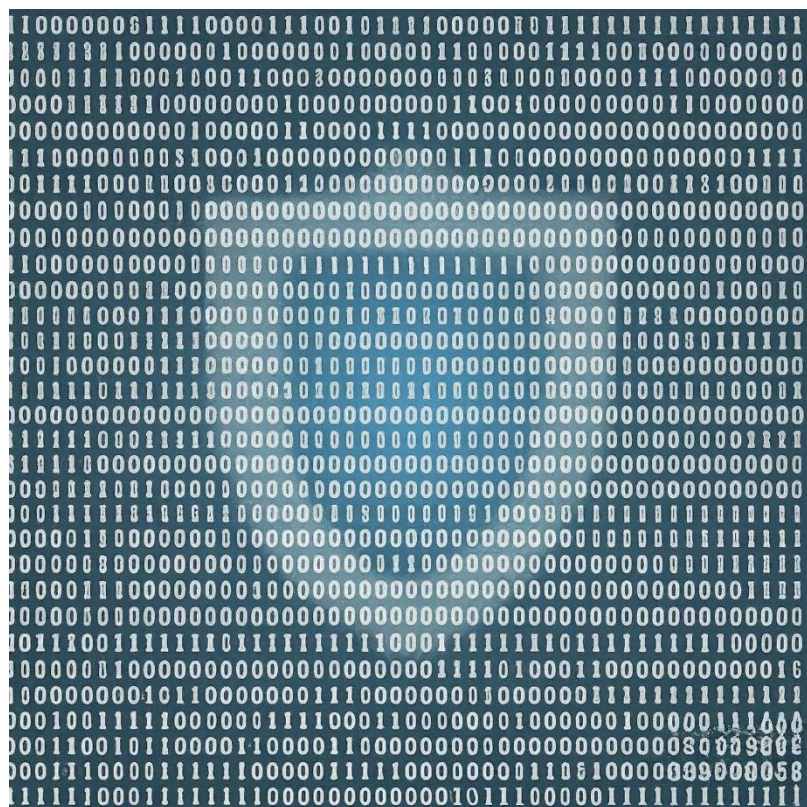
Case Scenario.....	3
Steps for the script: .....	4
Create the temporary directory which names _support in your current placement ....	4
Copy the log files to the created directory. You should copy all the *.log files which are in the directory /var/log. ....	5
Get all the relevant information about your hardware and store it in the text files. You should retrieve the info about your CPU, memory, storage, peripheral devices etc. ....	6
Get all the relevant information about your operating system and its current state: kernel version, distribution info, users list, processes etc.....	7
Get all the relevant information about your network: network interfaces, routing table, DNS information, results of the network checking by ping, traceroute etc. ....	9
Create the archive file, which will contain all the files/directories which you placed in the _support directory. The filename of the archive should be by like support- <current-date-time>.tar.gz where <current-date-time> should be provided by next format: YYYY-MM-DD_HHMMSS.....	11
Provide the final version of the script and screenshots with successful completion. ....	14



# Case Scenario

There has been suspicious activity in the system. In this case it will be necessary to create a snapshot of your system with all necessary information to send it to the technical support which can help you with the issue

You should create a script which should help you to get all the relevant information from your system, create the text files with this information, get the current log files from your system and create the archive file which contains all this data.



# Steps for the script:

For this project, we got instructions, and steps for creating the script.

We will have to break it down step-by-step.

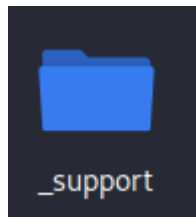
So let's start with the first step.

Create the temporary directory which names `_support` in your current placement

In order to create a folder, we will have to run "mkdir `_support`" command in the terminal.

Proof Of Work:

```
(cooluser@kali) - [~]  
$ mkdir _support
```



Copy the log files to the created directory. You should copy all the \*.log files which are in the directory /var/log.

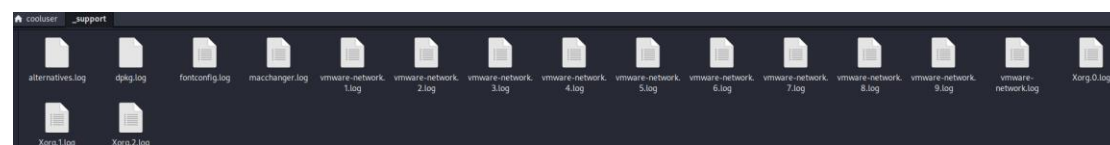
To copy all the .log files from the /var/log directory to the previously created "\_support" directory, we can use the cp command along with the wildcard (\*) to match all .log files.

This is the command which will transfer us the log files.

```
cp /var/log/*.log _support/
```

Proof Of Work:

```
(cooluser@kali)-[~]
$ cp /var/log/*.log _support/
cp: cannot open '/var/log/boot.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-root.1.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-root.2.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-root.3.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-root.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-cooluser.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-kali.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-root.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-cooluser.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-kali.log' for reading: Permission denied
```



that's our script meanwhile

```
# Create the temporary directory which names _support in your current placement
mkdir _support
# Copy the log files to the created directory.
cp /var/log/*.log _support/
```

Get all the relevant information about your hardware and store it in the text files. You should retrieve the info about your CPU, memory, storage, peripheral devices etc.

The command (lscpu && free -h && df -h && lsusb && lspci) >

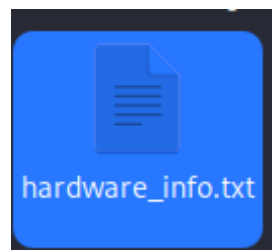
\_support/hardware\_info.txt retrieves information about the CPU, memory, storage, USB devices, and PCI devices and stores it in a file named "hardware\_info.txt" within the "\_support" directory.

So we will run this command

(lscpu && free -h && df -h && lsusb && lspci) > \_support/hardware\_info.txt

Proof Of Work

```
(cooluser@kali)-[~]  
$ (lscpu && free -h && df -h && lsusb && lspci) > _support/hardware_info.txt
```



```
File Edit Search View Document Help  
~_support/hardware_info.txt - Plaintext  
1 Architecture: x86_64  
2 CPU op mode(s): 32-bit; 64-bit  
3 Address sizes: 48 bits physical, 48 bits virtual  
4 Byte order: little endian  
5 CPU(s): 4  
6 On-line CPU(s) list: 0-3  
7 Vendor ID: GenuineIntel  
8 Model name: Intel Xeon E5-2680 v4 (Core™) 10-1580000  
9 CPU family: 6  
10 Model: 100  
11 Thread(s) per core: 1  
12 Core(s) per socket: 2  
13 Socket(s): 2  
14 Siblings: 8  
15 BogoMIPS: 4038.40  
16 Flags: fpu_eme de_pae tsc tsc_ems pae mce tsc_ems mtrr pge mca cmov pat pstate clflush mmx fxsr sse sse2 ss ht syscall nx rdtscp lahf constant_tsc arch_perfmon nopl tsc_reliable stmxr_tsc_ems pni pclmulqdq ssse3 fma cpi sse4_1 sse4_2  
17 Operating system: VMware  
18 Virtualization type: full  
19 L1d cache: 32 Kib (4 instances)  
20 L1i cache: 32 Kib (4 instances)  
21 L2 cache: 8 Kib (4 instances)  
22 L3 cache: 72 Mib (2 instances)  
23 NUMA node(s): 1  
24 NUMA node CPU(s): 0-3  
25 Vulnerability: Gather data sampling: Not affected  
26 Vulnerability: I1b multihit: KVM Mitigation: VM unsupported  
27 Vulnerability: L1TF: Mitigation: PTE Bypass  
28 Vulnerability: MDS: Vulnerable: Clear CPU buffers attempted, no microcode; SMT Host state unknown  
29 Vulnerability: Meltdown: Mitigation: PTI  
30 Vulnerability: Mithen: Unknown: No mitigations  
31 Vulnerability: Spectre v1: Not affected  
32 Vulnerability: Spectre v2: Not affected  
33 Vulnerability: Spec store bypass: Vulnerable  
34 Vulnerability: Spectre v2: Mitigation: usercopy/swapgs barriers and __user pointer sanitization  
35 Vulnerability: Spectre v2: Mitigation: Microcode, STIBP disabled, RSB filling, PBHB-v2/v3 Not affected  
36 Vulnerability: Spectre v2: Not affected  
37 Vulnerability: Spectre v2: Not affected  
38 Mem. total: 6.7GiB  
39 Mem. free: 4.2GiB  
40 Swap: 0.0GiB  
41 /dev/sda: 6.7GiB  
42 /dev/sda1: 6.7GiB  
43 /dev/sda2: 6.7GiB  
44 /dev/sda3: 6.7GiB  
45 /dev/sda4: 6.7GiB  
46 /dev/sda5: 6.7GiB  
47 /dev/sda6: 6.7GiB  
48 /dev/sda7: 6.7GiB  
49 /dev/sda8: 6.7GiB  
50 /dev/sda9: 6.7GiB  
51 /dev/sda10: 6.7GiB  
52 /dev/sda11: 6.7GiB  
53 /dev/sda12: 6.7GiB  
54 /dev/sda13: 6.7GiB  
55 /dev/sda14: 6.7GiB  
56 /dev/sda15: 6.7GiB  
57 /dev/sda16: 6.7GiB  
58 /dev/sda17: 6.7GiB  
59 /dev/sda18: 6.7GiB  
60 /dev/sda19: 6.7GiB  
61 /dev/sda20: 6.7GiB  
62 /dev/sda21: 6.7GiB  
63 /dev/sda22: 6.7GiB  
64 /dev/sda23: 6.7GiB  
65 /dev/sda24: 6.7GiB  
66 /dev/sda25: 6.7GiB  
67 /dev/sda26: 6.7GiB  
68 /dev/sda27: 6.7GiB  
69 /dev/sda28: 6.7GiB  
70 /dev/sda29: 6.7GiB  
71 /dev/sda30: 6.7GiB  
72 /dev/sda31: 6.7GiB  
73 /dev/sda32: 6.7GiB  
74 /dev/sda33: 6.7GiB  
75 /dev/sda34: 6.7GiB  
76 /dev/sda35: 6.7GiB  
77 /dev/sda36: 6.7GiB  
78 /dev/sda37: 6.7GiB  
79 /dev/sda38: 6.7GiB  
80 /dev/sda39: 6.7GiB  
81 /dev/sda40: 6.7GiB  
82 /dev/sda41: 6.7GiB  
83 /dev/sda42: 6.7GiB  
84 /dev/sda43: 6.7GiB  
85 /dev/sda44: 6.7GiB  
86 /dev/sda45: 6.7GiB  
87 /dev/sda46: 6.7GiB  
88 /dev/sda47: 6.7GiB  
89 /dev/sda48: 6.7GiB  
90 /dev/sda49: 6.7GiB  
91 /dev/sda50: 6.7GiB  
92 /dev/sda51: 6.7GiB  
93 /dev/sda52: 6.7GiB  
94 /dev/sda53: 6.7GiB  
95 /dev/sda54: 6.7GiB  
96 /dev/sda55: 6.7GiB  
97 /dev/sda56: 6.7GiB  
98 /dev/sda57: 6.7GiB  
99 /dev/sda58: 6.7GiB  
100 /dev/sda59: 6.7GiB  
101 /dev/sda60: 6.7GiB  
102 /dev/sda61: 6.7GiB  
103 /dev/sda62: 6.7GiB  
104 /dev/sda63: 6.7GiB  
105 /dev/sda64: 6.7GiB  
106 /dev/sda65: 6.7GiB  
107 /dev/sda66: 6.7GiB  
108 /dev/sda67: 6.7GiB  
109 /dev/sda68: 6.7GiB  
110 /dev/sda69: 6.7GiB  
111 /dev/sda70: 6.7GiB  
112 /dev/sda71: 6.7GiB  
113 /dev/sda72: 6.7GiB  
114 /dev/sda73: 6.7GiB  
115 /dev/sda74: 6.7GiB  
116 /dev/sda75: 6.7GiB  
117 /dev/sda76: 6.7GiB  
118 /dev/sda77: 6.7GiB  
119 /dev/sda78: 6.7GiB  
120 /dev/sda79: 6.7GiB  
121 /dev/sda80: 6.7GiB  
122 /dev/sda81: 6.7GiB  
123 /dev/sda82: 6.7GiB  
124 /dev/sda83: 6.7GiB  
125 /dev/sda84: 6.7GiB  
126 /dev/sda85: 6.7GiB  
127 /dev/sda86: 6.7GiB  
128 /dev/sda87: 6.7GiB  
129 /dev/sda88: 6.7GiB  
130 /dev/sda89: 6.7GiB  
131 /dev/sda90: 6.7GiB  
132 /dev/sda91: 6.7GiB  
133 /dev/sda92: 6.7GiB  
134 /dev/sda93: 6.7GiB  
135 /dev/sda94: 6.7GiB  
136 /dev/sda95: 6.7GiB  
137 /dev/sda96: 6.7GiB  
138 /dev/sda97: 6.7GiB  
139 /dev/sda98: 6.7GiB  
140 /dev/sda99: 6.7GiB  
141 /dev/sda100: 6.7GiB  
142 /dev/sda101: 6.7GiB  
143 /dev/sda102: 6.7GiB  
144 /dev/sda103: 6.7GiB  
145 /dev/sda104: 6.7GiB  
146 /dev/sda105: 6.7GiB  
147 /dev/sda106: 6.7GiB  
148 /dev/sda107: 6.7GiB  
149 /dev/sda108: 6.7GiB  
150 /dev/sda109: 6.7GiB  
151 /dev/sda110: 6.7GiB  
152 /dev/sda111: 6.7GiB  
153 /dev/sda112: 6.7GiB  
154 /dev/sda113: 6.7GiB  
155 /dev/sda114: 6.7GiB  
156 /dev/sda115: 6.7GiB  
157 /dev/sda116: 6.7GiB  
158 /dev/sda117: 6.7GiB  
159 /dev/sda118: 6.7GiB  
160 /dev/sda119: 6.7GiB  
161 /dev/sda120: 6.7GiB  
162 /dev/sda121: 6.7GiB  
163 /dev/sda122: 6.7GiB  
164 /dev/sda123: 6.7GiB  
165 /dev/sda124: 6.7GiB  
166 /dev/sda125: 6.7GiB  
167 /dev/sda126: 6.7GiB  
168 /dev/sda127: 6.7GiB  
169 /dev/sda128: 6.7GiB  
170 /dev/sda129: 6.7GiB  
171 /dev/sda130: 6.7GiB  
172 /dev/sda131: 6.7GiB  
173 /dev/sda132: 6.7GiB  
174 /dev/sda133: 6.7GiB  
175 /dev/sda134: 6.7GiB  
176 /dev/sda135: 6.7GiB  
177 /dev/sda136: 6.7GiB  
178 /dev/sda137: 6.7GiB  
179 /dev/sda138: 6.7GiB  
180 /dev/sda139: 6.7GiB  
181 /dev/sda140: 6.7GiB  
182 /dev/sda141: 6.7GiB  
183 /dev/sda142: 6.7GiB  
184 /dev/sda143: 6.7GiB  
185 /dev/sda144: 6.7GiB  
186 /dev/sda145: 6.7GiB  
187 /dev/sda146: 6.7GiB  
188 /dev/sda147: 6.7GiB  
189 /dev/sda148: 6.7GiB  
190 /dev/sda149: 6.7GiB  
191 /dev/sda150: 6.7GiB  
192 /dev/sda151: 6.7GiB  
193 /dev/sda152: 6.7GiB  
194 /dev/sda153: 6.7GiB  
195 /dev/sda154: 6.7GiB  
196 /dev/sda155: 6.7GiB  
197 /dev/sda156: 6.7GiB  
198 /dev/sda157: 6.7GiB  
199 /dev/sda158: 6.7GiB  
200 /dev/sda159: 6.7GiB  
201 /dev/sda160: 6.7GiB  
202 /dev/sda161: 6.7GiB  
203 /dev/sda162: 6.7GiB  
204 /dev/sda163: 6.7GiB  
205 /dev/sda164: 6.7GiB  
206 /dev/sda165: 6.7GiB  
207 /dev/sda166: 6.7GiB  
208 /dev/sda167: 6.7GiB  
209 /dev/sda168: 6.7GiB  
210 /dev/sda169: 6.7GiB  
211 /dev/sda170: 6.7GiB  
212 /dev/sda171: 6.7GiB  
213 /dev/sda172: 6.7GiB  
214 /dev/sda173: 6.7GiB  
215 /dev/sda174: 6.7GiB  
216 /dev/sda175: 6.7GiB  
217 /dev/sda176: 6.7GiB  
218 /dev/sda177: 6.7GiB  
219 /dev/sda178: 6.7GiB  
220 /dev/sda179: 6.7GiB  
221 /dev/sda180: 6.7GiB  
222 /dev/sda181: 6.7GiB  
223 /dev/sda182: 6.7GiB  
224 /dev/sda183: 6.7GiB  
225 /dev/sda184: 6.7GiB  
226 /dev/sda185: 6.7GiB  
227 /dev/sda186: 6.7GiB  
228 /dev/sda187: 6.7GiB  
229 /dev/sda188: 6.7GiB  
230 /dev/sda189: 6.7GiB  
231 /dev/sda190: 6.7GiB  
232 /dev/sda191: 6.7GiB  
233 /dev/sda192: 6.7GiB  
234 /dev/sda193: 6.7GiB  
235 /dev/sda194: 6.7GiB  
236 /dev/sda195: 6.7GiB  
237 /dev/sda196: 6.7GiB  
238 /dev/sda197: 6.7GiB  
239 /dev/sda198: 6.7GiB  
240 /dev/sda199: 6.7GiB  
241 /dev/sda200: 6.7GiB  
242 /dev/sda201: 6.7GiB  
243 /dev/sda202: 6.7GiB  
244 /dev/sda203: 6.7GiB  
245 /dev/sda204: 6.7GiB  
246 /dev/sda205: 6.7GiB  
247 /dev/sda206: 6.7GiB  
248 /dev/sda207: 6.7GiB  
249 /dev/sda208: 6.7GiB  
250 /dev/sda209: 6.7GiB  
251 /dev/sda210: 6.7GiB  
252 /dev/sda211: 6.7GiB  
253 /dev/sda212: 6.7GiB  
254 /dev/sda213: 6.7GiB  
255 /dev/sda214: 6.7GiB  
256 /dev/sda215: 6.7GiB  
257 /dev/sda216: 6.7GiB  
258 /dev/sda217: 6.7GiB  
259 /dev/sda218: 6.7GiB  
260 /dev/sda219: 6.7GiB  
261 /dev/sda220: 6.7GiB  
262 /dev/sda221: 6.7GiB  
263 /dev/sda222: 6.7GiB  
264 /dev/sda223: 6.7GiB  
265 /dev/sda224: 6.7GiB  
266 /dev/sda225: 6.7GiB  
267 /dev/sda226: 6.7GiB  
268 /dev/sda227: 6.7GiB  
269 /dev/sda228: 6.7GiB  
270 /dev/sda229: 6.7GiB  
271 /dev/sda230: 6.7GiB  
272 /dev/sda231: 6.7GiB  
273 /dev/sda232: 6.7GiB  
274 /dev/sda233: 6.7GiB  
275 /dev/sda234: 6.7GiB  
276 /dev/sda235: 6.7GiB  
277 /dev/sda236: 6.7GiB  
278 /dev/sda237: 6.7GiB  
279 /dev/sda238: 6.7GiB  
280 /dev/sda239: 6.7GiB  
281 /dev/sda240: 6.7GiB  
282 /dev/sda241: 6.7GiB  
283 /dev/sda242: 6.7GiB  
284 /dev/sda243: 6.7GiB  
285 /dev/sda244: 6.7GiB  
286 /dev/sda245: 6.7GiB  
287 /dev/sda246: 6.7GiB  
288 /dev/sda247: 6.7GiB  
289 /dev/sda248: 6.7GiB  
290 /dev/sda249: 6.7GiB  
291 /dev/sda250: 6.7GiB  
292 /dev/sda251: 6.7GiB  
293 /dev/sda252: 6.7GiB  
294 /dev/sda253: 6.7GiB  
295 /dev/sda254: 6.7GiB  
296 /dev/sda255: 6.7GiB  
297 /dev/sda256: 6.7GiB  
298 /dev/sda257: 6.7GiB  
299 /dev/sda258: 6.7GiB  
300 /dev/sda259: 6.7GiB  
301 /dev/sda260: 6.7GiB  
302 /dev/sda261: 6.7GiB  
303 /dev/sda262: 6.7GiB  
304 /dev/sda263: 6.7GiB  
305 /dev/sda264: 6.7GiB  
306 /dev/sda265: 6.7GiB  
307 /dev/sda266: 6.7GiB  
308 /dev/sda267: 6.7GiB  
309 /dev/sda268: 6.7GiB  
310 /dev/sda269: 6.7GiB  
311 /dev/sda270: 6.7GiB  
312 /dev/sda271: 6.7GiB  
313 /dev/sda272: 6.7GiB  
314 /dev/sda273: 6.7GiB  
315 /dev/sda274: 6.7GiB  
316 /dev/sda275: 6.7GiB  
317 /dev/sda276: 6.7GiB  
318 /dev/sda277: 6.7GiB  
319 /dev/sda278: 6.7GiB  
320 /dev/sda279: 6.7GiB  
321 /dev/sda280: 6.7GiB  
322 /dev/sda281: 6.7GiB  
323 /dev/sda282: 6.7GiB  
324 /dev/sda283: 6.7GiB  
325 /dev/sda284: 6.7GiB  
326 /dev/sda285: 6.7GiB  
327 /dev/sda286: 6.7GiB  
328 /dev/sda287: 6.7GiB  
329 /dev/sda288: 6.7GiB  
330 /dev/sda289: 6.7GiB  
331 /dev/sda290: 6.7GiB  
332 /dev/sda291: 6.7GiB  
333 /dev/sda292: 6.7GiB  
334 /dev/sda293: 6.7GiB  
335 /dev/sda294: 6.7GiB  
336 /dev/sda295: 6.7GiB  
337 /dev/sda296: 6.7GiB  
338 /dev/sda297: 6.7GiB  
339 /dev/sda298: 6.7GiB  
340 /dev/sda299: 6.7GiB  
341 /dev/sda300: 6.7GiB  
342 /dev/sda301: 6.7GiB  
343 /dev/sda302: 6.7GiB  
344 /dev/sda303: 6.7GiB  
345 /dev/sda304: 6.7GiB  
346 /dev/sda305: 6.7GiB  
347 /dev/sda306: 6.7GiB  
348 /dev/sda307: 6.7GiB  
349 /dev/sda308: 6.7GiB  
350 /dev/sda309: 6.7GiB  
351 /dev/sda310: 6.7GiB  
352 /dev/sda311: 6.7GiB  
353 /dev/sda312: 6.7GiB  
354 /dev/sda313: 6.7GiB  
355 /dev/sda314: 6.7GiB  
356 /dev/sda315: 6.7GiB  
357 /dev/sda316: 6.7GiB  
358 /dev/sda317: 6.7GiB  
359 /dev/sda318: 6.7GiB  
360 /dev/sda319: 6.7GiB  
361 /dev/sda320: 6.7GiB  
362 /dev/sda321: 6.7GiB  
363 /dev/sda322: 6.7GiB  
364 /dev/sda323: 6.7GiB  
365 /dev/sda324: 6.7GiB  
366 /dev/sda325: 6.7GiB  
367 /dev/sda326: 6.7GiB  
368 /dev/sda327: 6.7GiB  
369 /dev/sda328: 6.7GiB  
370 /dev/sda329: 6.7GiB  
371 /dev/sda330: 6.7GiB  
372 /dev/sda331: 6.7GiB  
373 /dev/sda332: 6.7GiB  
374 /dev/sda333: 6.7GiB  
375 /dev/sda334: 6.7GiB  
376 /dev/sda335: 6.7GiB  
377 /dev/sda336: 6.7GiB  
378 /dev/sda337: 6.7GiB  
379 /dev/sda338: 6.7GiB  
380 /dev/sda339: 6.7GiB  
381 /dev/sda340: 6.7GiB  
382 /dev/sda341: 6.7GiB  
383 /dev/sda342: 6.7GiB  
384 /dev/sda343: 6.7GiB  
385 /dev/sda344: 6.7GiB  
386 /dev/sda345: 6.7GiB  
387 /dev/sda346: 6.7GiB  
388 /dev/sda347: 6.7GiB  
389 /dev/sda348: 6.7GiB  
390 /dev/sda349: 6.7GiB  
391 /dev/sda350: 6.7GiB  
392 /dev/sda351: 6.7GiB  
393 /dev/sda352: 6.7GiB  
394 /dev/sda353: 6.7GiB  
395 /dev/sda354: 6.7GiB  
396 /dev/sda355: 6.7GiB  
397 /dev/sda356: 6.7GiB  
398 /dev/sda357: 6.7GiB  
399 /dev/sda358: 6.7GiB  
400 /dev/sda359: 6.7GiB  
401 /dev/sda360: 6.7GiB  
402 /dev/sda361: 6.7GiB  
403 /dev/sda362: 6.7GiB  
404 /dev/sda363: 6.7GiB  
405 /dev/sda364: 6.7GiB  
406 /dev/sda365: 6.7GiB  
407 /dev/sda366: 6.7GiB  
408 /dev/sda367: 6.7GiB  
409 /dev/sda368: 6.7GiB  
410 /dev/sda369: 6.7GiB  
411 /dev/sda370: 6.7GiB  
412 /dev/sda371: 6.7GiB  
413 /dev/sda372: 6.7GiB  
414 /dev/sda373: 6.7GiB  
415 /dev/sda374: 6.7GiB  
416 /dev/sda375: 6.7GiB  
417 /dev/sda376: 6.7GiB  
418 /dev/sda377: 6.7GiB  
419 /dev/sda378: 6.7GiB  
420 /dev/sda379: 6.7GiB  
421 /dev/sda380: 6.7GiB  
422 /dev/sda381: 6.7GiB  
423 /dev/sda382: 6.7GiB  
424 /dev/sda383: 6.7GiB  
425 /dev/sda384: 6.7GiB  
426 /dev/sda385: 6.7GiB  
427 /dev/sda386: 6.7GiB  
428 /dev/sda387: 6.7GiB  
429 /dev/sda388: 6.7GiB  
430 /dev/sda389: 6.7GiB  
431 /dev/sda390: 6.7GiB  
432 /dev/sda391: 6.7GiB  
433 /dev/sda392: 6.7GiB  
434 /dev/sda393: 6.7GiB  
435 /dev/sda394: 6.7GiB  
436 /dev/sda395: 6.7GiB  
437 /dev/sda396: 6.7GiB  
438 /dev/sda397: 6.7GiB  
439 /dev/sda398: 6.7GiB  
440 /dev/sda399: 6.7GiB  
441 /dev/sda400: 6.7GiB  
442 /dev/sda401: 6.7GiB  
443 /dev/sda402: 6.7GiB  
444 /dev/sda403: 6.7GiB  
445 /dev/sda404: 6.7GiB  
446 /dev/sda405: 6.7GiB  
447 /dev/sda406: 6.7GiB  
448 /dev/sda407: 6.7GiB  
449 /dev/sda408: 6.7GiB  
450 /dev/sda409: 6.7GiB  
451 /dev/sda410: 6.7GiB  
452 /dev/sda411: 6.7GiB  
453 /dev/sda412: 6.7GiB  
454 /dev/sda413: 6.7GiB  
455 /dev/sda414: 6.7GiB  
456 /dev/sda415: 6.7GiB  
457 /dev/sda416: 6.7GiB  
458 /dev/sda417: 6.7GiB  
459 /dev/sda418: 6.7GiB  
460 /dev/sda419: 6.7GiB  
461 /dev/sda420: 6.7GiB  
462 /dev/sda421: 6.7GiB  
463 /dev/sda422: 6.7GiB  
464 /dev/sda423: 6.7GiB  
465 /dev/sda424: 6.7GiB  
466 /dev/sda425: 6.7GiB  
467 /dev/sda426: 6.7GiB  
468 /dev/sda427: 6.7GiB  
469 /dev/sda428: 6.7GiB  
470 /dev/sda429: 6.7GiB  
471 /dev/sda430: 6.7GiB  
472 /dev/sda431: 6.7GiB  
473 /dev/sda432: 6.7GiB  
474 /dev/sda433: 6.7GiB  
475 /dev/sda434: 6.7GiB  
476 /dev/sda435: 6.7GiB  
477 /dev/sda436: 6.7GiB  
478 /dev/sda437: 6.7GiB  
479 /dev/sda438: 6.7GiB  
480 /dev/sda439: 6.7GiB  
481 /dev/sda440: 6.7GiB  
482 /dev/sda441: 6.7GiB  
483 /dev/sda442: 6.7GiB  
484 /dev/sda443: 6.7GiB  
485 /dev/sda444: 6.7GiB  
486 /dev/sda445: 6.7GiB  
487 /dev/sda446: 6.7GiB  
488 /dev/sda447: 6.7GiB  
489 /dev/sda448: 6.7GiB  
490 /dev/sda449: 6.7GiB  
491 /dev/sda450: 6.7GiB  
492 /dev/sda451: 6.7GiB  
493 /dev/sda452: 6.7GiB  
494 /dev/sda453: 6.7GiB  
495 /dev/sda454: 6.7GiB  
496 /dev/sda455: 6.7GiB  
497 /dev/sda456: 6.7GiB  
498 /dev/sda457: 6.7GiB  
499 /dev/sda458: 6.7GiB  
500 /dev/sda459: 6.7GiB  
501 /dev/sda460: 6.7GiB  
502 /dev/sda461: 6.7GiB  
503 /dev/sda462: 6.7GiB  
504 /dev/sda463: 6.7GiB  
505 /dev/sda464: 6.7GiB  
506 /dev/sda465: 6.7GiB  
507 /dev/sda466: 6.7GiB  
508 /dev/sda467: 6.7GiB  
509 /dev/sda468: 6.7GiB  
510 /dev/sda469: 6.7GiB  
511 /dev/sda470: 6.7GiB  
512 /dev/sda471: 6.7GiB  
513 /dev/sda472: 6.7GiB  
514 /dev/sda473: 6.7GiB  
515 /dev/sda474: 6.7GiB  
516 /dev/sda475: 6.7GiB  
517 /dev/sda476: 6.7GiB  
518 /dev/sda477: 6.7GiB  
519 /dev/sda478: 6.7GiB  
520 /dev/sda479: 6.7GiB  
521 /dev/sda480: 6.7GiB  
522 /dev/sda481: 6.7GiB  
523 /dev/sda482: 6.7GiB  
524 /dev/sda483: 6.7GiB  
525 /dev/sda484: 6.7GiB  
526 /dev/sda485: 6.7GiB  
527 /dev/sda486: 6.7GiB  
528 /dev/sda487: 6.7GiB  
529 /dev/sda488: 6.7GiB  
530 /dev/sda489: 6.7GiB  
531 /dev/sda490: 6.7GiB  
532 /dev/sda491: 6.7GiB  
533 /dev/sda492: 6.7GiB  
534 /dev/sda493: 6.7GiB  
535 /dev/sda494: 6.7GiB  
536 /dev/sda495: 6.7GiB  
537 /dev/sda496: 6.7GiB  
538 /dev/sda497: 6.7GiB  
539 /dev/sda498: 6.7GiB  
540 /dev/sda499: 6.7GiB  
541 /dev/sda500: 6.7GiB  
542 /dev/sda501: 6.7GiB  
543 /dev/sda502: 6.7GiB  
544 /dev/sda503: 6.7GiB  
545 /dev/sda504: 6.7GiB  
546 /dev/sda505: 6.7GiB  
547 /dev/sda506: 6.7GiB  
548 /dev/sda507: 6.7GiB  
549 /dev/sda508: 6.7GiB  
550 /dev/sda509: 6.7GiB  
551 /dev/sda510: 6.7GiB  
552 /dev/sda511: 6.7GiB  
553 /dev/sda512: 6.7GiB  
554 /dev/sda513: 6.7GiB  
555 /dev/sda514: 6.7GiB  
556 /dev/sda515: 6.7GiB  
557 /dev/sda516: 6.7GiB  
558 /dev/sda517: 6.7GiB  
559 /dev/sda518: 6.7GiB  
560 /dev/sda519: 6.7GiB  
561 /dev/sda520: 6.7GiB  
562 /dev/sda521: 6.7GiB  
563 /dev/sda522: 6.7GiB  
564 /dev/sda523: 6.7GiB  
565 /dev/sda524: 6.7GiB  
566 /dev/sda525: 6.7GiB  
567 /dev/sda526: 6.7GiB  
568 /dev/sda527: 6.7GiB  
569 /dev/sda528: 6.7GiB  
570 /dev/sda529: 6.7GiB  
571 /dev/sda530: 6.7GiB  
572 /dev/sda531: 6.7GiB  
573 /dev/sda532: 6.7GiB  
574 /dev/sda533: 6.7GiB  
575 /dev/sda534: 6.7GiB  
576 /dev/sda535: 6.7GiB  
577 /dev/sda536: 6.7GiB  
578 /dev/sda537: 6.7GiB  
579 /dev/sda538: 6.7GiB  
580 /dev/sda539: 6.7GiB  
581 /dev/sda540: 6.7GiB  
582 /dev/sda541: 6.7GiB  
583 /dev/sda542: 6.7GiB  
584 /dev/sda543: 6.7GiB  
585 /dev/sda544: 6.7GiB  
586 /dev/sda545: 6.7GiB  
587 /dev/sda546: 6.7GiB  
588 /dev/sda547: 6.7GiB  
589 /dev/sda548: 6.7GiB  
590 /dev/sda549: 6.7GiB  
591 /dev/sda550: 6.7GiB  
592 /dev/sda551: 6.7GiB  
593 /dev/sda552: 6.7GiB  
594 /dev/sda553: 6.7GiB  
595 /dev/sda554: 6.7GiB  
596 /dev/sda555: 6.7GiB  
597 /dev/sda556: 6.7GiB  
598 /dev/sda557: 6.7GiB  
599 /dev/sda558: 6.7GiB  
600 /dev/sda559: 6.7GiB  
601 /dev/sda560: 6.7GiB  
602 /dev/sda561: 6.7GiB  
603 /dev/sda562: 6.7GiB  
604 /dev/sda563: 6.7GiB  
605 /dev/sda564: 6.7GiB  
606 /dev/sda565: 6.7GiB  
607 /dev/sda566: 6.7GiB  
608 /dev/sda567: 6.7GiB  
609 /dev/sda568: 6.7GiB  
610 /dev/sda569: 6.7GiB  
611 /dev/sda570: 6.7GiB  
612 /dev/sda571: 6.7GiB  
613 /dev/sda572: 6.7GiB  
614 /dev/sda573: 6.7GiB  
615 /dev/sda574: 6.7GiB  
616 /dev/sda575: 6.7GiB  
617 /dev/sda576: 6.7GiB  
618 /dev/sda577: 6.7GiB  
619 /dev/sda578: 6.7GiB  
620 /dev/sda579: 6.7GiB  
621 /dev/sda580: 6.7GiB  
622 /dev/sda581: 6.7GiB  
623 /dev/sda582: 6.7GiB  
624 /dev/sda583: 6.7GiB  
625 /dev/sda584: 6.7GiB  
626 /dev/sda585: 6.7GiB  
627 /dev/sda586: 6.7GiB  
628 /dev/sda587: 6.7GiB  
629 /dev/sda588: 6.7GiB  
630 /dev/sda589: 6.7GiB  
631 /dev/sda590: 6.7GiB  
632 /dev/sda591: 6.7GiB  
633 /dev/sda592: 6.7GiB  
634 /dev/sda593: 6.7GiB  
635 /dev/sda594: 6.7GiB  
636 /dev/sda595: 6.7GiB
```

## Get all the relevant information about your operating system and its current state: kernel version, distribution info, users list, processes etc.

To gather information about the operating system and its current state, including kernel version, distribution info, users list, processes, etc., and save it in the same folder, we can use the following command:

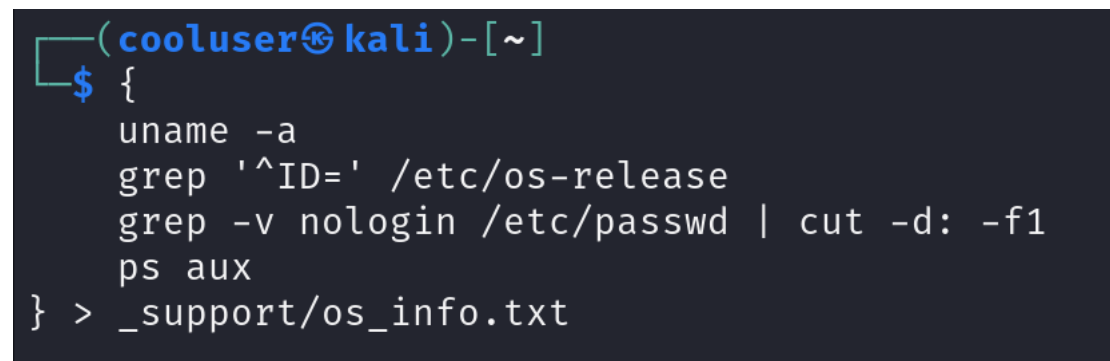
```
{  
    uname -a  
    grep '^ID=' /etc/os-release  
    grep -v nologin /etc/passwd | cut -d: -f1  
    ps aux  
}> _support/os_info.txt
```

uname -a: Displays system information, including the kernel version.

ps aux: Provides a snapshot of the current processes running on the system.

> \_support/os\_info.txt: Redirects the combined output of all the commands to a file named "os\_info.txt" within the "\_support" directory.

Proof of work:

A terminal window with a dark background. The prompt is (cooluser@kali)-[~]. The user has entered a block of commands enclosed in curly braces, followed by a redirection to \_support/os\_info.txt. The commands are: uname -a, grep '^ID=' /etc/os-release, grep -v nologin /etc/passwd | cut -d: -f1, and ps aux.

```
(cooluser@kali)-[~]  
$ {  
    uname -a  
    grep '^ID=' /etc/os-release  
    grep -v nologin /etc/passwd | cut -d: -f1  
    ps aux  
} > _support/os_info.txt
```



```
File Edit Search View Document Help
~/support/os_info.txt - Mousetrap

1 Linux Kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.0-1kali1 (2023-10-09) x86_64 GNU/Linux
2 PRETTY_NAME="Kali GNU/Linux Rolling"
3 NAME="Kali GNU/Linux"
4 VERSION_ID="2023.4"
5 VERSION="2023.4"
6 VERSION_CODENAME=kali-rolling
7 ID=kali
8 ID_LIKE=debian
9 HOME_URL="https://www.kali.org/"
10 SUPPORT_URL="https://forums.kali.org/"
11 BUG_REPORT_URL="https://bugs.kali.org/"
12 ANSI_COLOR="1;31"
13 cooluser tty/ 2023-03-14 17:46 (10)
14 USER PID CPU MEM VSZ RSS TTY STAT START TIME COMMAND
15 root 1 0.0 0.1 21040 12540 ? Ss 16:14 0:03 /sbin/init splash
16 root 2 0.0 0.0 0 0 ? S 16:14 0:00 [kthreadd]
17 root 3 0.0 0.0 0 0 ? Ic 16:14 0:00 [rcu_gp]
18 root 4 0.0 0.0 0 0 ? Ic 16:14 0:00 [rcu_par_gp]
19 root 5 0.0 0.0 0 0 ? Ic 16:14 0:00 [slub_flushwq]
20 root 6 0.0 0.0 0 0 ? Ic 16:14 0:00 [netns]
21 root 11 0.0 0.0 0 0 ? Ic 16:14 0:00 [mm_percpu_wq]
22 root 12 0.0 0.0 0 0 ? I 16:14 0:00 [rcu_tasks_kthread]
23 root 13 0.0 0.0 0 0 ? I 16:14 0:00 [rcu_tasks_rude_kthread]
24 root 14 0.0 0.0 0 0 ? I 16:14 0:00 [rcu_tasks_trace_kthread]
25 root 15 0.0 0.0 0 0 ? S 16:14 0:00 [ksoftirqd/0]
26 root 16 0.1 0.0 0 0 ? I 16:14 0:10 [rcu_preempt]
27 root 17 0.0 0.0 0 0 ? S 16:14 0:00 [migration/0]
28 root 18 0.0 0.0 0 0 ? S 16:14 0:00 [idle_inject/0]
29 root 19 0.0 0.0 0 0 ? S 16:14 0:00 [cpuhp/0]
30 root 20 0.0 0.0 0 0 ? S 16:14 0:00 [cpuhp/1]
31 root 21 0.0 0.0 0 0 ? S 16:14 0:00 [idle_inject/1]
32 root 22 0.0 0.0 0 0 ? S 16:14 0:01 [migration/1]
33 root 23 0.0 0.0 0 0 ? S 16:14 0:00 [ksoftirqd/1]
34 root 26 0.0 0.0 0 0 ? S 16:14 0:00 [cpuhp/2]
35 root 27 0.0 0.0 0 0 ? S 16:14 0:00 [idle_inject/2]
36 root 28 0.0 0.0 0 0 ? S 16:14 0:01 [migration/2]
37 root 29 0.0 0.0 0 0 ? S 16:14 0:00 [ksoftirqd/2]
38 root 31 0.0 0.0 0 0 ? Ic 16:14 0:00 [kworker/2:0H-kblockd]
39 root 32 0.0 0.0 0 0 ? S 16:14 0:00 [cpuhp/3]
40 root 33 0.0 0.0 0 0 ? S 16:14 0:00 [idle_inject/3]
41 root 34 0.0 0.0 0 0 ? S 16:14 0:01 [migration/3]
42 root 35 0.0 0.0 0 0 ? S 16:14 0:00 [ksoftirqd/3]
43 root 37 0.0 0.0 0 0 ? Ic 16:14 0:00 [kworker/3:0H-events_highpri]
44 root 42 0.0 0.0 0 0 ? S 16:14 0:00 [kdevtmpfs]
45 root 43 0.0 0.0 0 0 ? Ic 16:14 0:00 [inet_frag_wq]
46 root 44 0.0 0.0 0 0 ? S 16:14 0:00 [kauditd]
47 root 46 0.0 0.0 0 0 ? S 16:14 0:00 [khungtaskd]
48 root 47 0.0 0.0 0 0 ? S 16:14 0:00 [oom_reaper]
49 root 48 0.0 0.0 0 0 ? Ic 16:14 0:00 [writeback]
50 root 49 0.0 0.0 0 0 ? S 16:14 0:00 [kcompactd0]
51 root 50 0.0 0.0 0 0 ? SN 16:14 0:00 [ksmd]
52 root 51 0.0 0.0 0 0 ? SN 16:14 0:01 [khugepaged]
53 root 52 0.0 0.0 0 0 ? Ic 16:14 0:00 [kintegrityd]
54 root 53 0.0 0.0 0 0 ? Ic 16:14 0:00 [kblockd]
55 root 54 0.0 0.0 0 0 ? Ic 16:14 0:00 [blkcg_punt_bio]
56 root 57 0.0 0.0 0 0 ? Ic 16:14 0:00 [tpm_dev_wq]
57 root 58 0.0 0.0 0 0 ? Ic 16:14 0:00 [edac-poller]
58 root 59 0.0 0.0 0 0 ? Ic 16:14 0:00 [devfreq_wq]
59 root 61 0.0 0.0 0 0 ? Ic 16:14 0:00 [kworker/2:1n]
60 root 62 0.0 0.0 0 0 ? S 16:14 0:00 [ksmadd]
61 root 68 0.0 0.0 0 0 ? Ic 16:14 0:00 [kthrotld]
62 root 70 0.0 0.0 0 0 ? S 16:14 0:00 [irq/24-pciehp]
63 root 71 0.0 0.0 0 0 ? S 16:14 0:00 [irq/25-pciehp]
64 root 72 0.0 0.0 0 0 ? S 16:14 0:00 [irq/26-pciehp]
65 root 73 0.0 0.0 0 0 ? S 16:14 0:00 [irq/27-pciehp]
66 root 74 0.0 0.0 0 0 ? S 16:14 0:00 [irq/28-pciehp]
67 root 75 0.0 0.0 0 0 ? S 16:14 0:00 [irq/29-pciehp]
68 root 76 0.0 0.0 0 0 ? S 16:14 0:00 [irq/30-pciehp]
69 root 77 0.0 0.0 0 0 ? S 16:14 0:00 [irq/31-pciehp]
70 root 78 0.0 0.0 0 0 ? S 16:14 0:00 [irq/32-pciehp]
```

So that's our script now

```
# Create the temporary directory which names _support in your current placement
mkdir _support
# Copy the log files to the created directory.
cp /var/log/*.log _support/
# Get all the relevant information about your hardware
(lscpu && free -h && df -h && lsusb && lspci) > _support/hardware_info.txt
# Get all the relevant information about your operating system and its current state
{
    uname -a
    grep '^ID=' /etc/os-release
    grep -v nologin /etc/passwd | cut -d: -f1
    ps aux
} > _support/os_info.txt
```



## Get all the relevant information about your network: network interfaces, routing table, DNS information, results of the network checking by ping, traceroute etc.

To gather information about the network, including network interfaces, routing table, DNS information, results of network checking by ping, traceroute, etc., and save it in the same folder, we can use the following command:

```
{  
  ip addr  
  
  ip route  
  
  cat /etc/resolv.conf  
  
  ping -c 5 www.google.com  
  
  traceroute -n www.google.com  
}> _support/network_info.txt
```

**ip addr:** This command displays information about network interfaces, including IP addresses assigned to them.

**ip route:** This command displays the kernel routing table, which shows how packets will be forwarded based on their destination IP addresses.

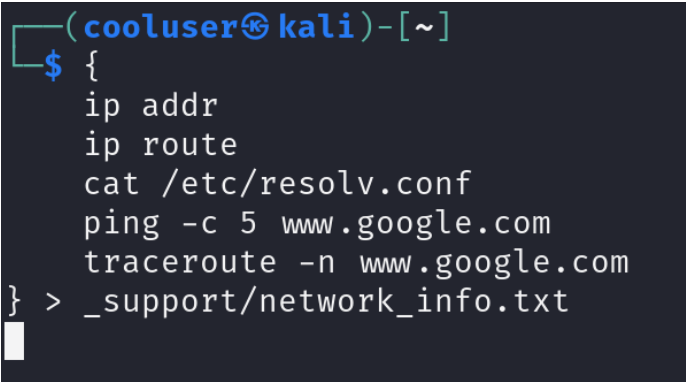
**cat /etc/resolv.conf:** This command displays the DNS resolver configuration file, which contains information about the DNS servers used by the system.

**ping -c 5 www.google.com:** This command sends ICMP echo requests to the specified host (www.google.com) and waits for responses. It sends 5 packets in total.

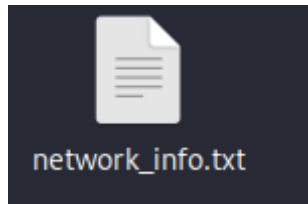
**traceroute -n www.google.com:** This command traces the route that packets take from the local machine to the specified host (www.google.com) by sending packets with increasing TTL values and recording the IP addresses of the routers along the way.

**> \_support/network\_info.txt:** Redirects the combined output of all the commands to a file named "network\_info.txt" within the "\_support" directory.

Proof Of Work:



```
(cooluser@kali)-[~]  
$ {  
  ip addr  
  ip route  
  cat /etc/resolv.conf  
  ping -c 5 www.google.com  
  traceroute -n www.google.com  
}> _support/network_info.txt
```



```
File Edit Search View Document Help
network_info.txt
1:11 lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
2:   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
3:   inet 127.0.0.1/8 scope host lo
4:     valid_lft forever preferred_lft forever
5:   inet6 ::1/128 scope host noprefixroute
6:     valid_lft forever preferred_lft forever
7:2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
8:   link/ether 8a:2b:4c:7c:8d:1a/48 brd ff:ff:ff:ff:ff:ff
9:   inet 192.168.88.20/24 brd 192.168.88.255 scope global dynamic noprefixroute eth0
10:     valid_lft 1128sec preferred_lft 1128sec
11:   inet6 fe80::8a2b4c7c8d1a/48 scope link noprefixroute
12:     valid_lft forever preferred_lft forever
13: default via 192.168.88.2 dev eth0 proto dhcp src 192.168.88.20 metric 100
14: 192.168.88.2 dev eth0 proto kernel scope link src 192.168.88.20 metric 100
15: # Generated by NetworkManager
16: search localdomain
17: nameserver 192.168.88.2
18: PMW www.google.com (172.217.22.4) 56(84) bytes of data.
19: 0A bytes from fr33idc1a-in-f4.1e100.net (172.217.22.4): icmp_seq=1 ttl=128 time=6.73 ms
20: 0A bytes from fr33idc1a-in-f4.1e100.net (172.217.22.4): icmp_seq=2 ttl=128 time=13.8 ms
21: 0A bytes from fr33idc1a-in-f4.1e100.net (172.217.22.4): icmp_seq=3 ttl=128 time=6.49 ms
22: 0A bytes from fr33idc1a-in-f4.1e100.net (172.217.22.4): icmp_seq=4 ttl=128 time=6.24 ms
23: 0A bytes from fr33idc1a-in-f4.1e100.net (172.217.22.4): icmp_seq=5 ttl=128 time=6.78 ms
24:
25: --- www.google.com ping statistics ---
26: 5 packets transmitted, 5 received, 0% packet loss, time 4807ms
27: rtt min/avg/max/mdev = 6.865/7.916/13.767/2.937 ms
28: traceroute to www.google.com (172.217.22.4), 30 hops max, 60 byte packets
29: 1 192.168.88.2 0.236 ms 0.203 ms 0.135 ms
30: 2 * * *
31: 3 * * *
32: 4 * * *
33: 5 * * *
34: 6 * * *
35: 7 * * *
36: 8 * * *
37: 9 * * *
38: 10 * * *
39: 11 * * *
40: 12 * * *
41: 13 * * *
42: 14 * * *
43: 15 * * *
44: 16 * * *
45: 17 * * *
46: 18 * * *
47: 19 * * *
48: 20 * * *
49: 21 * * *
50: 22 * * *
51: 23 * * *
52: 24 * * *
53: 25 * * *
54: 26 * * *
55: 27 * * *
56: 28 * * *
57: 29 * * *
58: 30 * * *
59:
60:
```

So that's our script now:

```
# Create the temporary directory which names _support in your current placement
mkdir _support
# Copy the log files to the created directory.
cp /var/log/*.log _support/
# Get all the relevant information about your hardware
(lscpu && free -h && df -h && lsusb && lspci) > _support/hardware_info.txt
# Get all the relevant information about your operating system and its current state
{
    uname -a
    grep '^ID=' /etc/os-release
    grep -v nologin /etc/passwd | cut -d: -f1
    ps aux
} > _support/os_info.txt
# Get all the relevant information about your network
{
    ip addr
    ip route
    cat /etc/resolv.conf
    ping -c 5 www.google.com
    traceroute -n www.google.com
} > _support/network_info.txt
```

Create the archive file, which will contain all the files/directories which you placed in the `_support` directory. The filename of the archive should be by like `support-<current-date-time>.tar.gz` where `<current-date-time>` should be provided by next format: `YYYY-MM-DD_HHMMSS`.

We can create the archive file containing all the files and directories in the "`_support`" directory using the following command:

```
tar -czvf "support-$(date +%Y-%m-%d_%H%M%S').tar.gz" _support
```

Explanation:

`tar`: This command is used to manipulate archives.

`-czvf`: Options used for creating a compressed archive:

`c`: Create a new archive.

`z`: Compress the archive using gzip.

`v`: Verbose mode to display the files being archived.

`f`: Specifies the filename of the archive.

`"support-$(date +%Y-%m-%d_%H%M%S').tar.gz"`: This constructs the filename of the archive using the current date and time in the specified format. `$(date +%Y-%m-%d_%H%M%S')` is a command substitution that inserts the current date and time formatted as `YYYY-MM-DD_HHMMSS`.

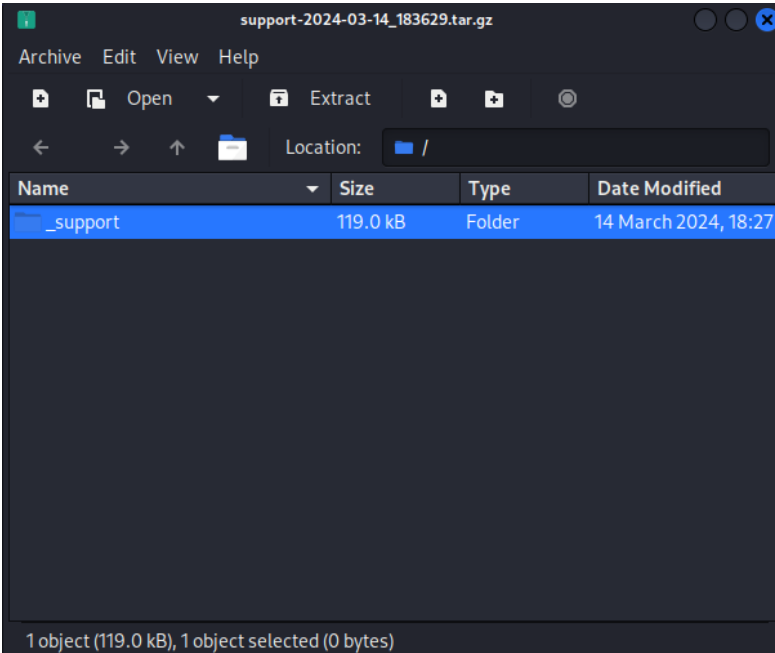
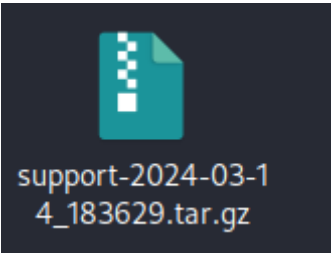
`_support`: Specifies the directory to be archived.

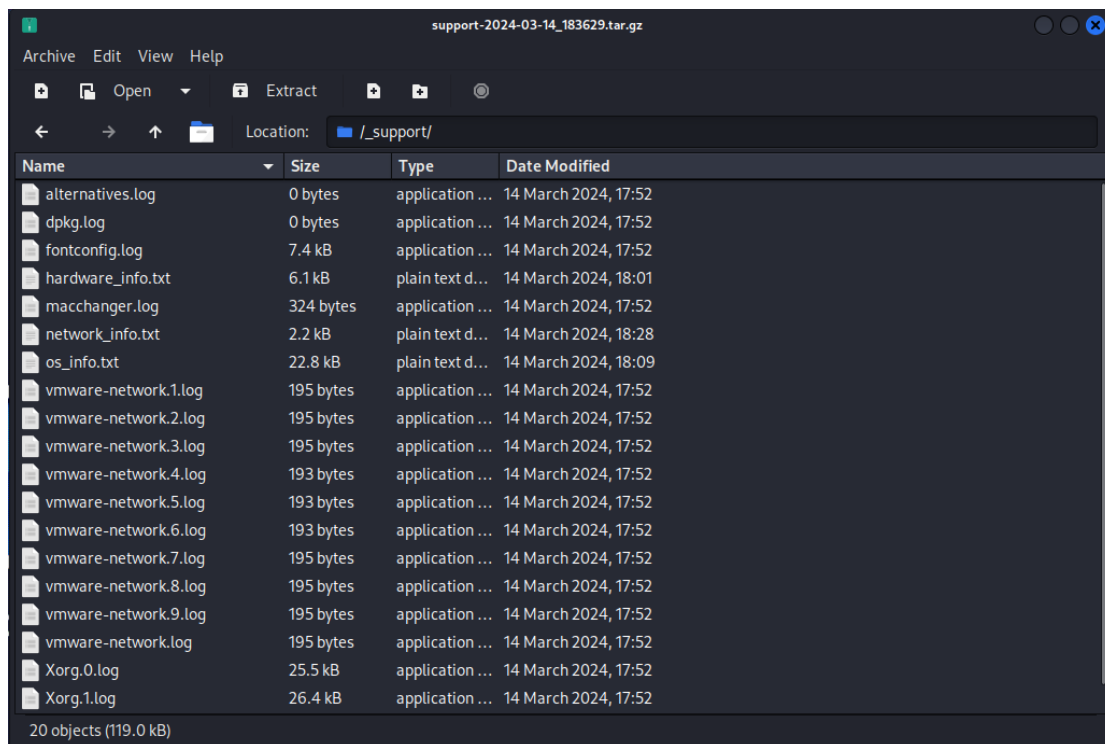
So that's our script now:

```
# Create the temporary directory which names _support in your current placement
mkdir _support
# Copy the log files to the created directory.
cp /var/log/*.log _support/
# Get all the relevant information about your hardware
(lscpu && free -h && df -h && lsusb && lspci) > _support/hardware_info.txt
# Get all the relevant information about your operating system and its current state
{
    uname -a
    grep '^ID=' /etc/os-release
    grep -v nologin /etc/passwd | cut -d: -f1
    ps aux
} > _support/os_info.txt
# Get all the relevant information about your network
{
    ip addr
    ip route
    cat /etc/resolv.conf
    ping -c 5 www.google.com
    traceroute -n www.google.com
} > _support/network_info.txt
# Create the archive file
tar -czvf "support-$(date +%Y-%m-%d_%H%M%S').tar.gz" _support
```

Proof Of Work:

```
(cooluser@kali)-[~]
$ tar -czvf "support-$(date +%Y-%m-%d_%H%M%S').tar.gz" _support
_support/
_support/Xorg.1.log
_support/macchanger.log
_support/vmware-network.4.log
_support/os_info.txt
_support/hardware_info.txt
_support/fontconfig.log
_support/vmware-network.6.log
_support/vmware-network.3.log
_support/vmware-network.8.log
_support/vmware-network.7.log
_support/vmware-network.2.log
_support/vmware-network.5.log
_support/alternatives.log
_support/vmware-network.log
_support/network_info.txt
_support/vmware-network.9.log
_support/Xorg.2.log
_support/vmware-network.1.log
_support/dpkg.log
_support/Xorg.0.log
```





## Provide the final version of the script and screenshots with successful completion.

After we did everything successfully, we will take everything into one script, and we will try it as one script.

That's my ready script:

```
# Create the temporary directory which names _support in your current placement
```

```
mkdir _support
```

```
# Copy the log files to the created directory.
```

```
cp /var/log/*.log _support/
```

```
# Get all the relevant information about your hardware
```

```
(lscpu && free -h && df -h && lsusb && lspci) > _support/hardware_info.txt
```

```
# Get all the relevant information about your operating system and its current state
```

```
{
```

```
    uname -a
```

```
    grep '^ID=' /etc/os-release
```

```
    grep -v nologin /etc/passwd | cut -d: -f1
```

```
    ps aux
```

```
# Get all the relevant information about your network
```

```
{
```

```
    ip addr
```

```
    ip route
```

```
    cat /etc/resolv.conf
```

```
    ping -c 5 www.google.com
```

```
    traceroute -n www.google.com
```

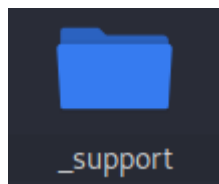
```
# Create the archive file
```

```
tar -czvf "support-$(date +%Y-%m-%d_%H%M%S').tar.gz" _support
```

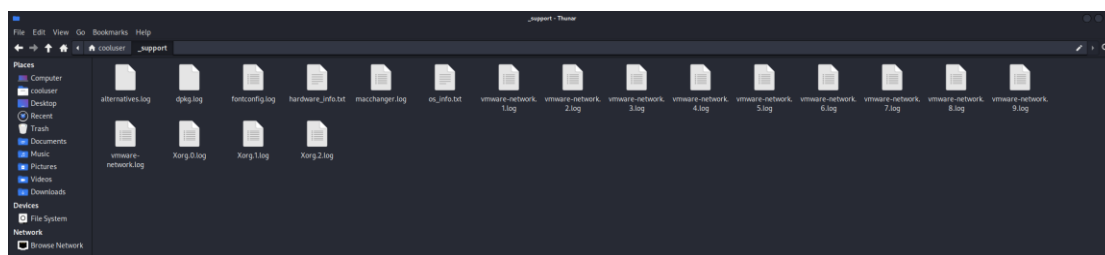
now I will run this on my terminal

```
File Actions Edit View Help
cooluser@kali ~
$ # Create the temporary directory which names _support in your current placement
mkdir _support
# Copy the log files to the created directory.
cp /var/log/*.log _support/
# Get all the relevant information about your hardware
(lscpu && free -h && df -h && lsusb && lspci) > _support/hardware_info.txt
# Get all the relevant information about your operating system and its current state
{
    uname -a
    grep '^ID=' /etc/os-release
    grep -v nologin /etc/passwd | cut -d: -f1
    ps aux
} > _support/os_info.txt
# Get all the relevant information about your network
{
    ip addr
    ip route
    cat /etc/resolv.conf
    ping -c 5 www.google.com
    traceroute -n www.google.com
} > _support/network_info.txt
# Create the archive file
tar -czvf "support-$(date +%Y-%m-%d_%H%M%S').tar.gz" _support
cp: cannot open '/var/log/boot.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-root.1.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-root.2.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-root.3.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-root.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-cooluser.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-kali.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-root.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-cooluser.log' for reading: Permission denied
cp: cannot open '/var/log/vmware-vmtoolsd-kali.log' for reading: Permission denied
```

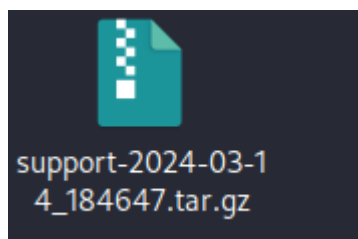
we will check that we have the \_support folder:



We will check the files there:

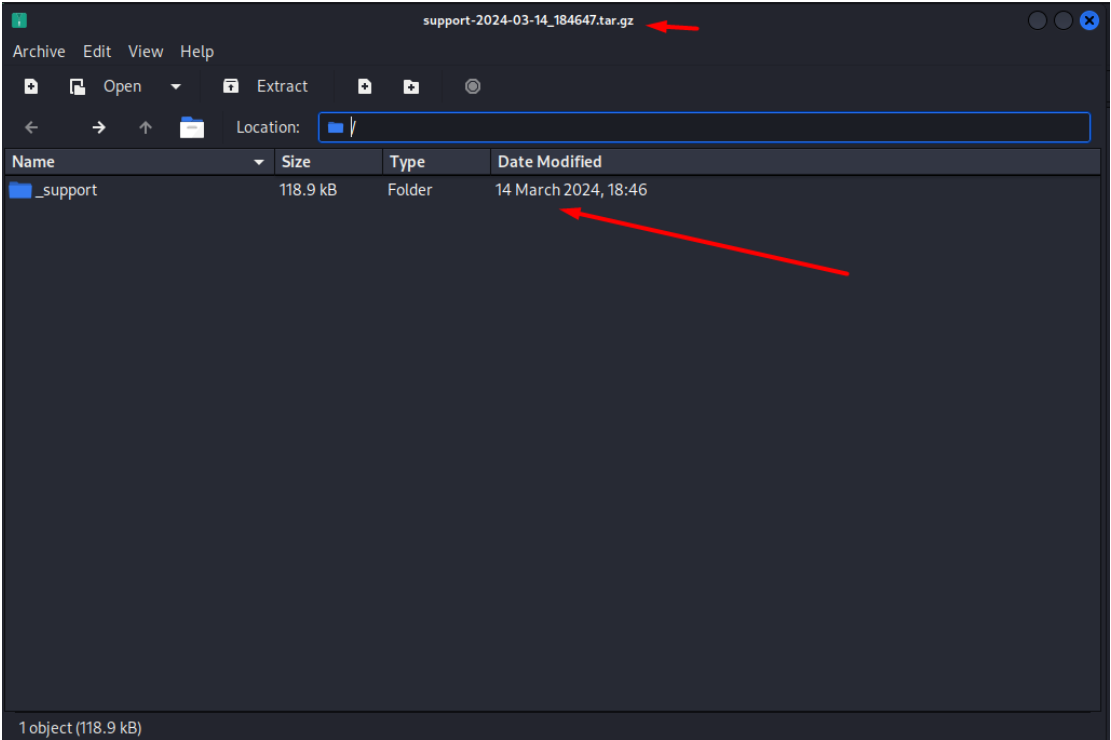


Now we will check if the .tar.gz file has been created:






Now we will check the files there too:



We would like to create a script file, that could be easily opened.

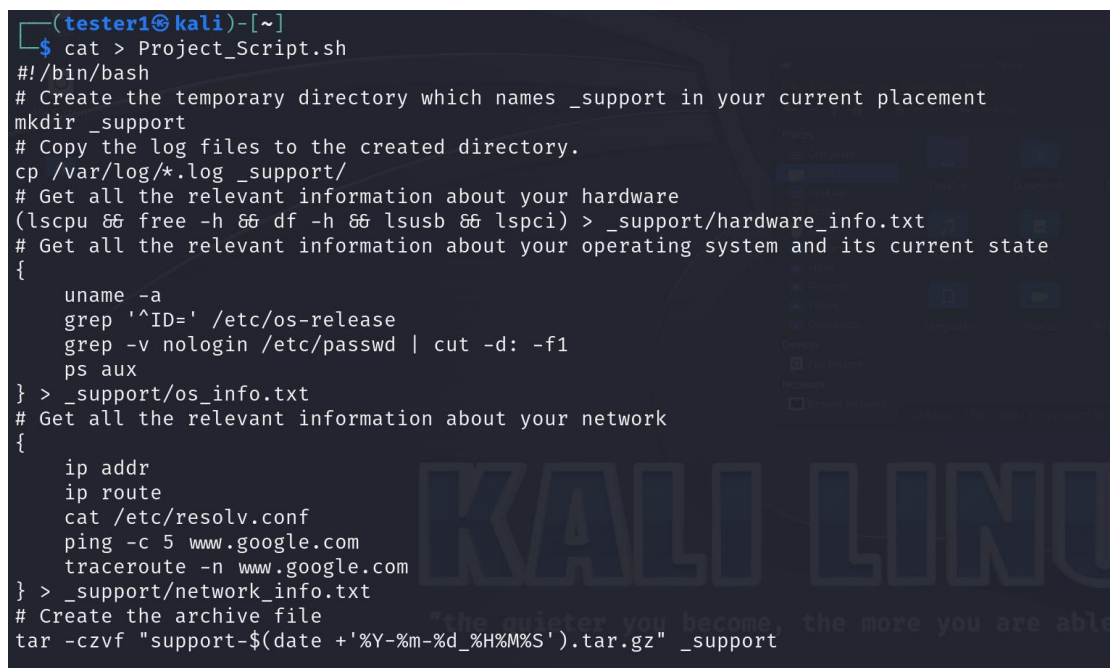
To create a script file we would need to write this command

cat > Project\_Script.sh



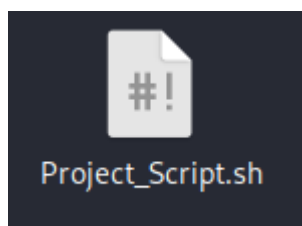
```
(tester1@kali)-[~]  
$ cat > Project_Script.sh
```

After we will enter this command, it will give us a blank space, which there we will need to insert our script.



```
(tester1@kali)-[~]  
$ cat > Project_Script.sh  
#!/bin/bash  
# Create the temporary directory which names _support in your current placement  
mkdir _support  
# Copy the log files to the created directory.  
cp /var/log/*.log _support/  
# Get all the relevant information about your hardware  
(lscpu && free -h && df -h && lsusb && lspci) > _support/hardware_info.txt  
# Get all the relevant information about your operating system and its current state  
{  
    uname -a  
    grep '^ID=' /etc/os-release  
    grep -v nologin /etc/passwd | cut -d: -f1  
    ps aux  
}> _support/os_info.txt  
# Get all the relevant information about your network  
{  
    ip addr  
    ip route  
    cat /etc/resolv.conf  
    ping -c 5 www.google.com  
    traceroute -n www.google.com  
}> _support/network_info.txt  
# Create the archive file  
tar -czvf "support-$(date +%Y-%m-%d_%H%M%S').tar.gz" _support
```

After we inserted our script to there, we will get out new file.



In order to run it, we will need to open this file for executing for everyone.

We will run this command

```
chmod +x Project_Script.sh
```

```
(tester1@kali)-[~]  
$ chmod +x Project_Script.sh
```

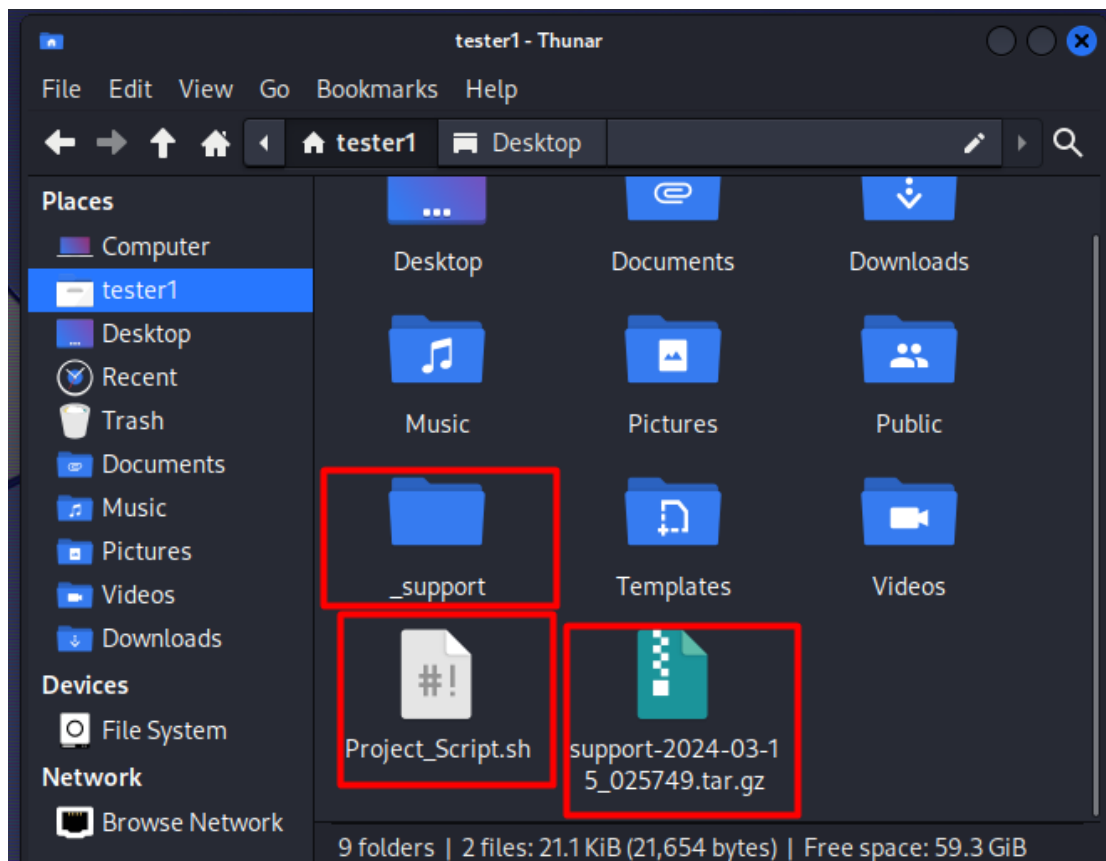
Now to run the script we will need to run this command

```
./Project_Script.sh
```

```
(tester1@kali)-[~]  
$ ./Project_Script.sh
```

And we can see its working

```
(tester1@kali)-[~]  
$ ./Project_Script.sh  
cp: cannot open '/var/log/boot.log' for reading: Permission denied  
cp: cannot open '/var/log/vmware-vmtoolsd-root.1.log' for reading: Permission denied  
cp: cannot open '/var/log/vmware-vmtoolsd-root.2.log' for reading: Permission denied  
cp: cannot open '/var/log/vmware-vmtoolsd-root.3.log' for reading: Permission denied  
cp: cannot open '/var/log/vmware-vmtoolsd-root.log' for reading: Permission denied  
cp: cannot open '/var/log/vmware-vmtoolsd-cooluser.log' for reading: Permission denied  
cp: cannot open '/var/log/vmware-vmtoolsd-kali.log' for reading: Permission denied  
cp: cannot open '/var/log/vmware-vmtoolsd-root.log' for reading: Permission denied  
cp: cannot open '/var/log/vmware-vmtoolsd-tester1.log' for reading: Permission denied  
cp: cannot open '/var/log/vmware-vmtoolsd-cooluser.log' for reading: Permission denied  
cp: cannot open '/var/log/vmware-vmtoolsd-kali.log' for reading: Permission denied  
cp: cannot open '/var/log/vmware-vmtoolsd-tester1.log' for reading: Permission denied  
_support/  
_support/Xorg.1.log  
_support/macchanger.log  
_support/vmware-network.4.log  
_support/os_info.txt  
_support/hardware_info.txt  
_support/fontconfig.log  
_support/vmware-network.6.log  
_support/vmware-network.3.log  
_support/vmware-network.8.log  
_support/vmware-network.7.log  
_support/vmware-network.2.log  
_support/vmware-network.5.log  
_support/alternatives.log  
_support/vmware-network.log  
_support/network_info.txt  
_support/vmware-network.9.log  
_support/Xorg.2.log  
_support/vmware-network.1.log  
_support/dpkg.log  
_support/Xorg.0.log
```



The script file will be available in the teams assignment too