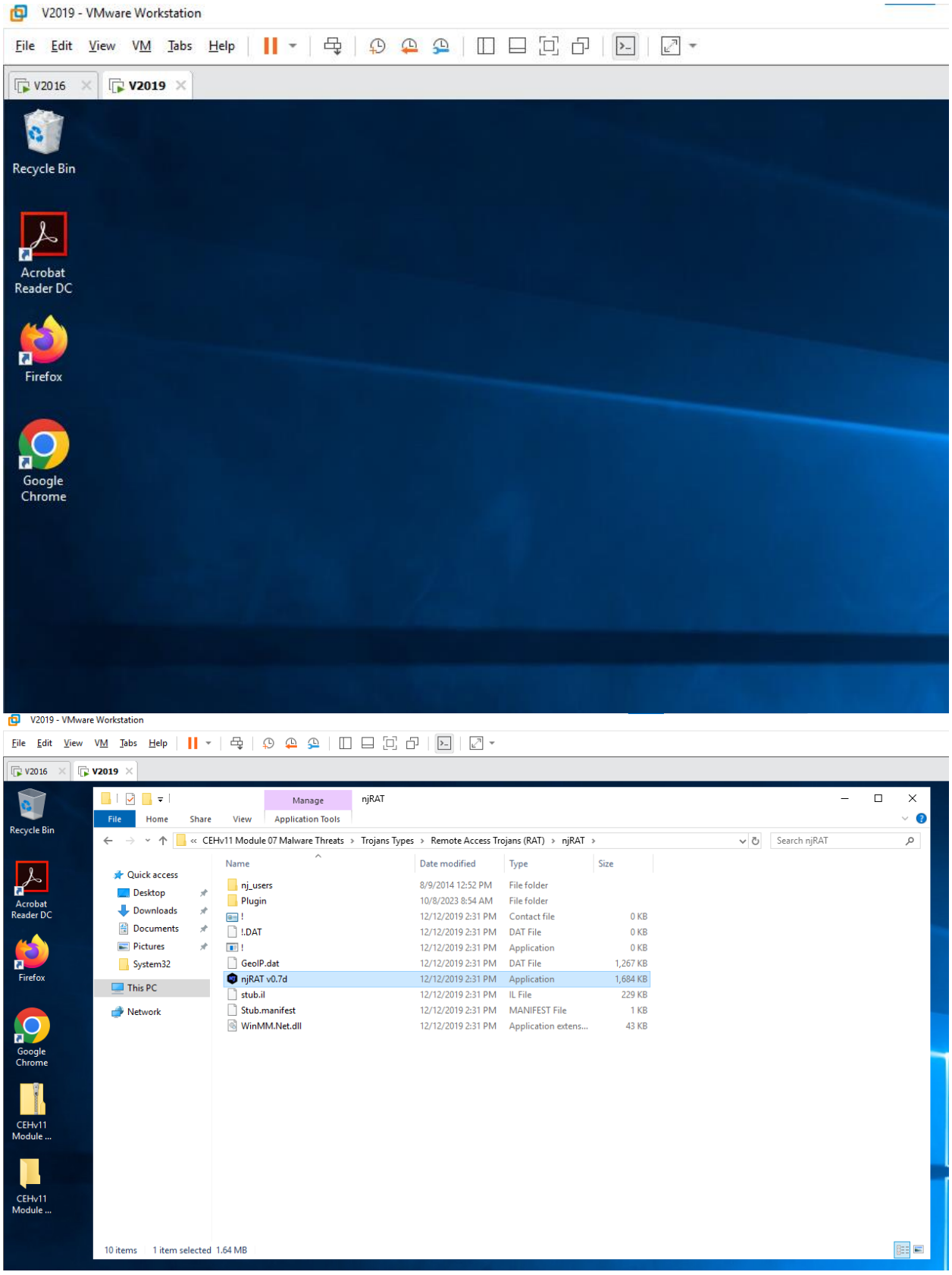
Lab 9: Malware Threats

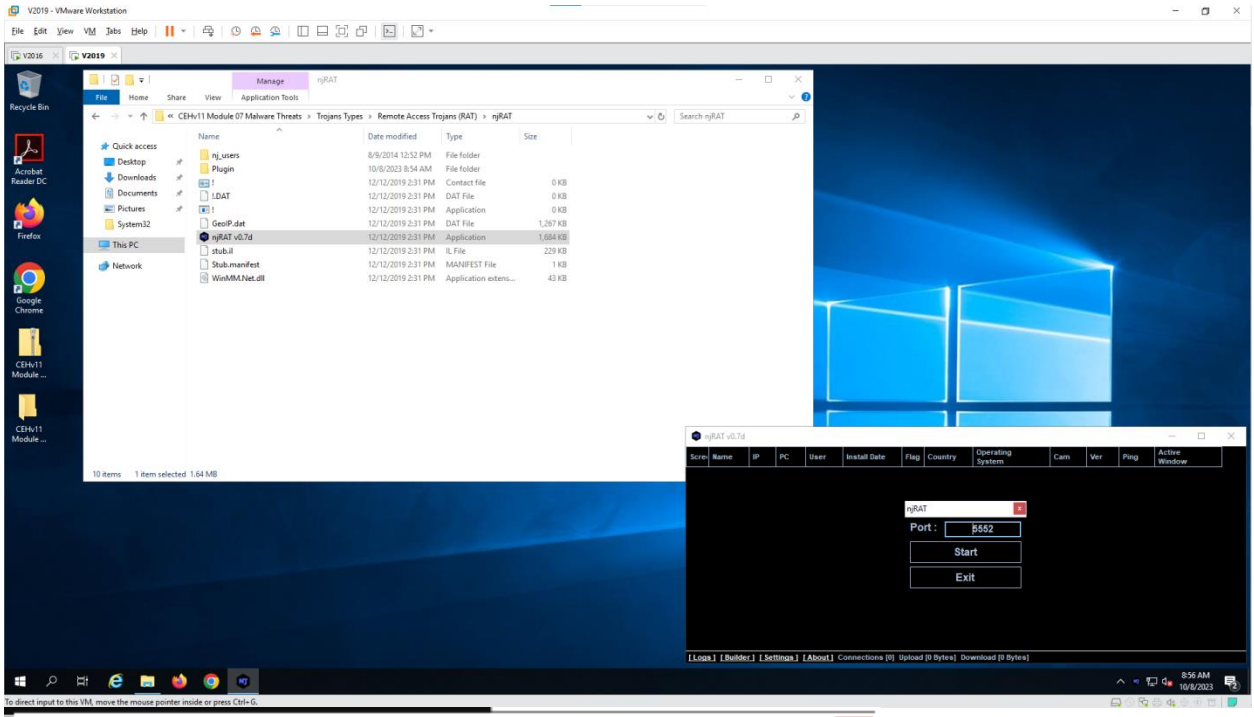
Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 07/10/2023

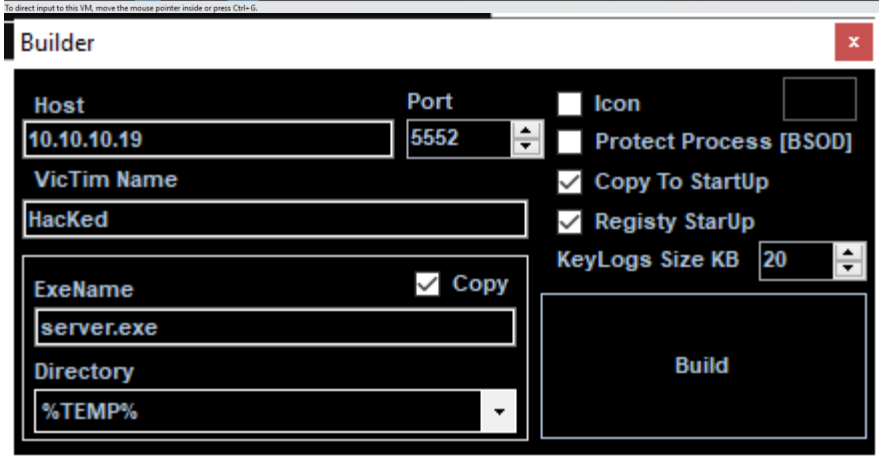
1. Gain Access to the Target System using Trojans

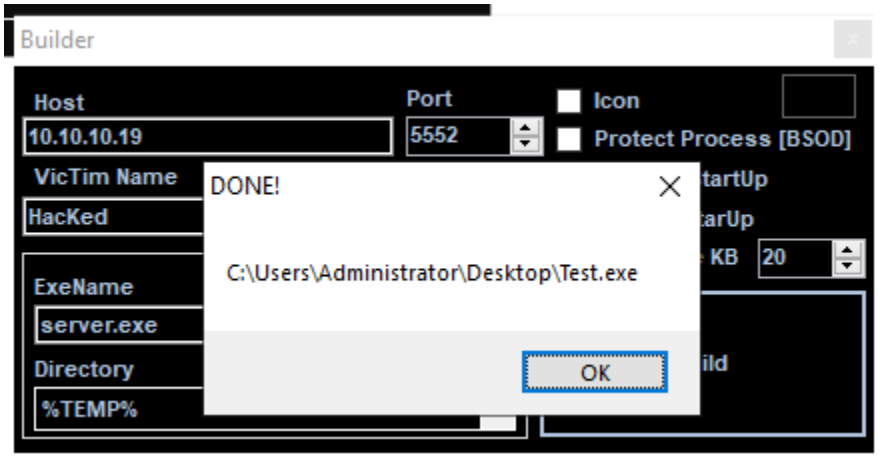
1.1 Gain Control over a Victim Machine using the njRAT RAT Trojan

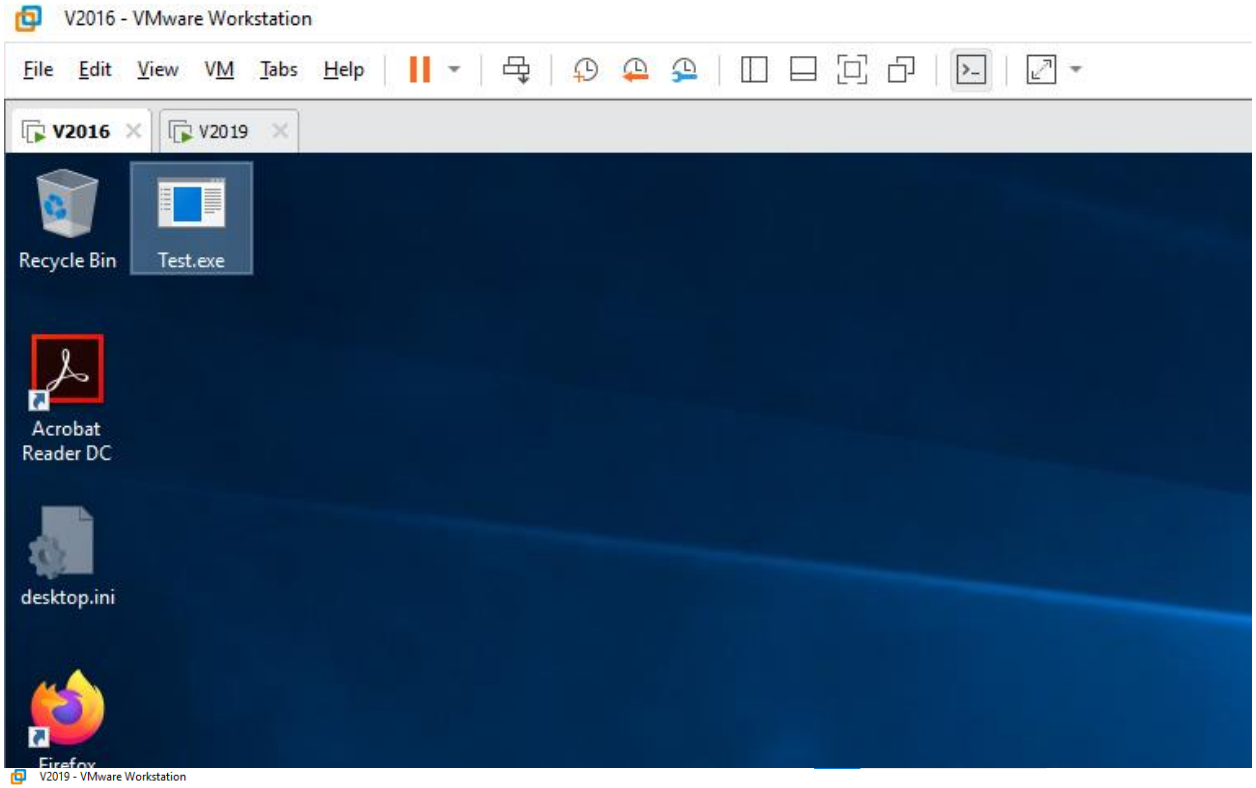
- Open Windows 10, Windows Server 2016

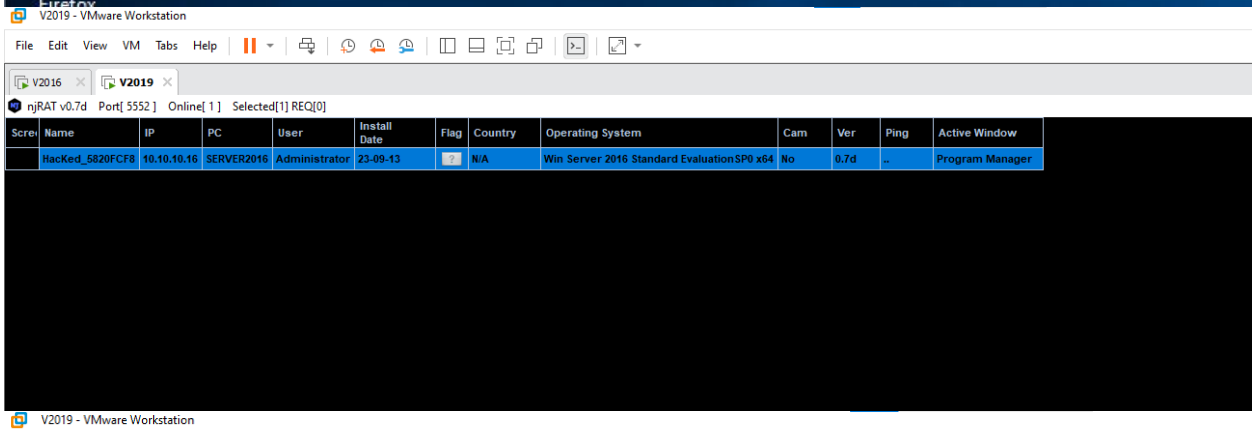

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Manage
njRAT
File Home Share View Application Tools
« CEHv11 Module 07 Malware Threats › Trojans Types › Remote Access Trojans (RAT) › njRAT ›
Search njRAT
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name Date modified Type Size
nj_users 8/9/2014 12:52 PM File folder
Plugin 10/8/2023 8:54 AM File folder
! 12/12/2019 2:31 PM Contact file 0 KB
!.DAT 12/12/2019 2:31 PM DAT File 0 KB
! 12/12/2019 2:31 PM Application 0 KB
GeoIP.dat 12/12/2019 2:31 PM DAT File 1,267 KB
njRAT v0.7d 12/12/2019 2:31 PM Application 1,684 KB
stub.il 12/12/2019 2:31 PM IL File 229 KB
Stub.manifest 12/12/2019 2:31 PM MANIFEST File 1 KB
WinMM.Net.dll 12/12/2019 2:31 PM Application extens... 43 KB
10 items 1 item selected 1.64 MB

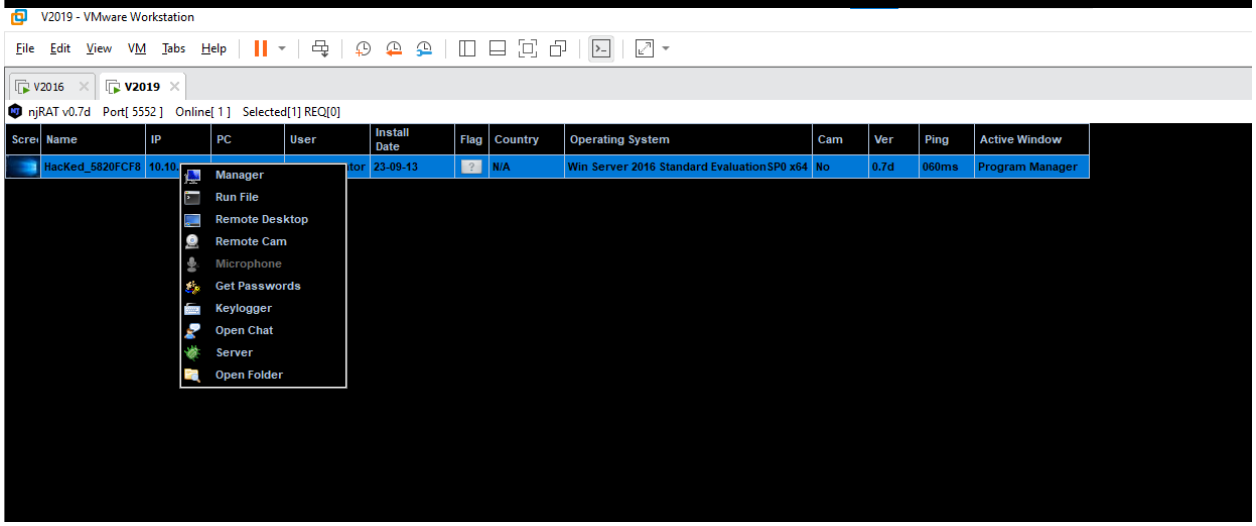

V2019 - VMware Workstation
njRAT
Port :
5552
Start
Exit

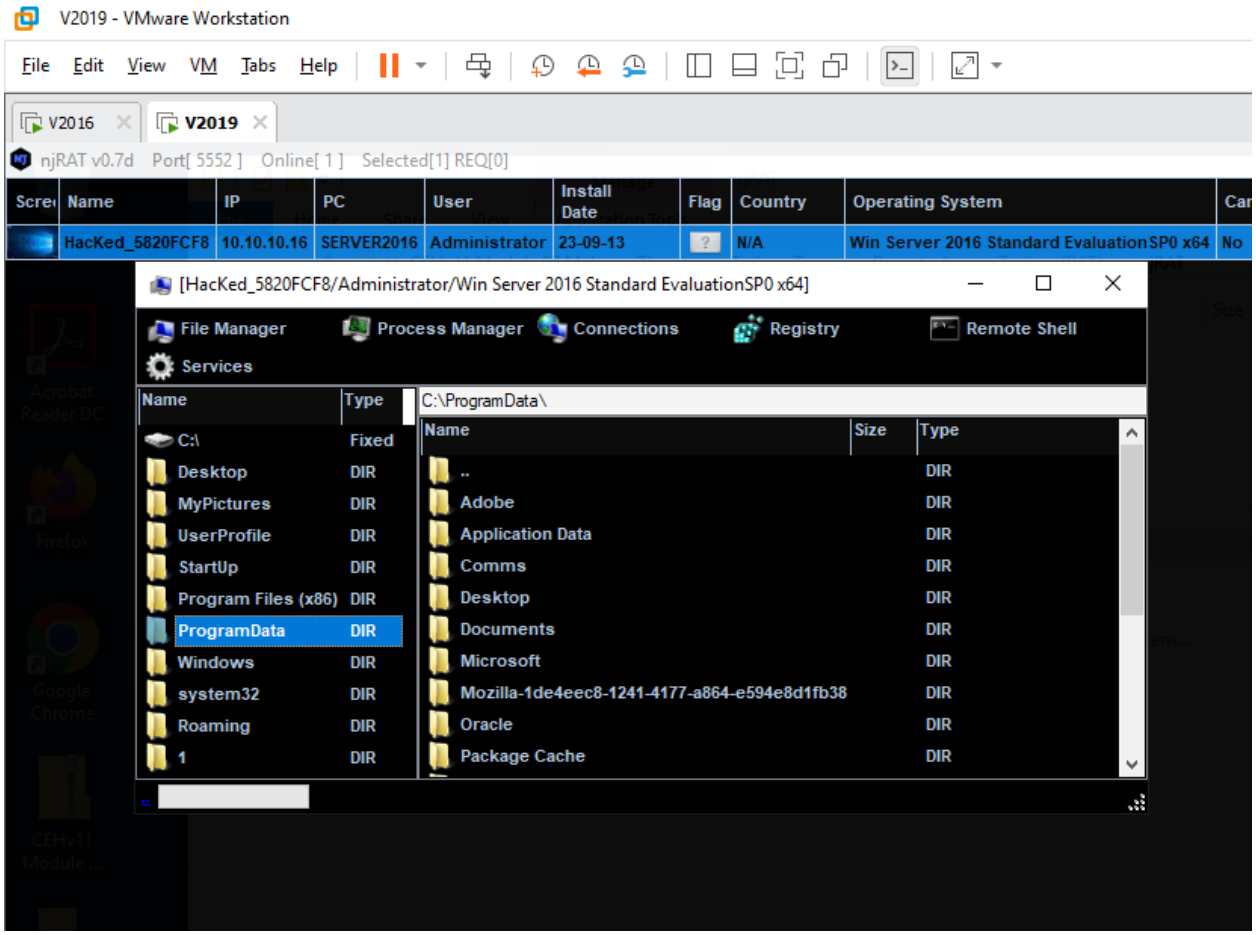

Builder
Host
10.10.10.19
Port
5552
Icon
Protect Process [BSOD]
VicTim Name
HacKed
Copy To StartUp
Registy StarUp
KeyLogs Size KB
20
ExeName
Copy
server.exe
Directory
%TEMP%
Build

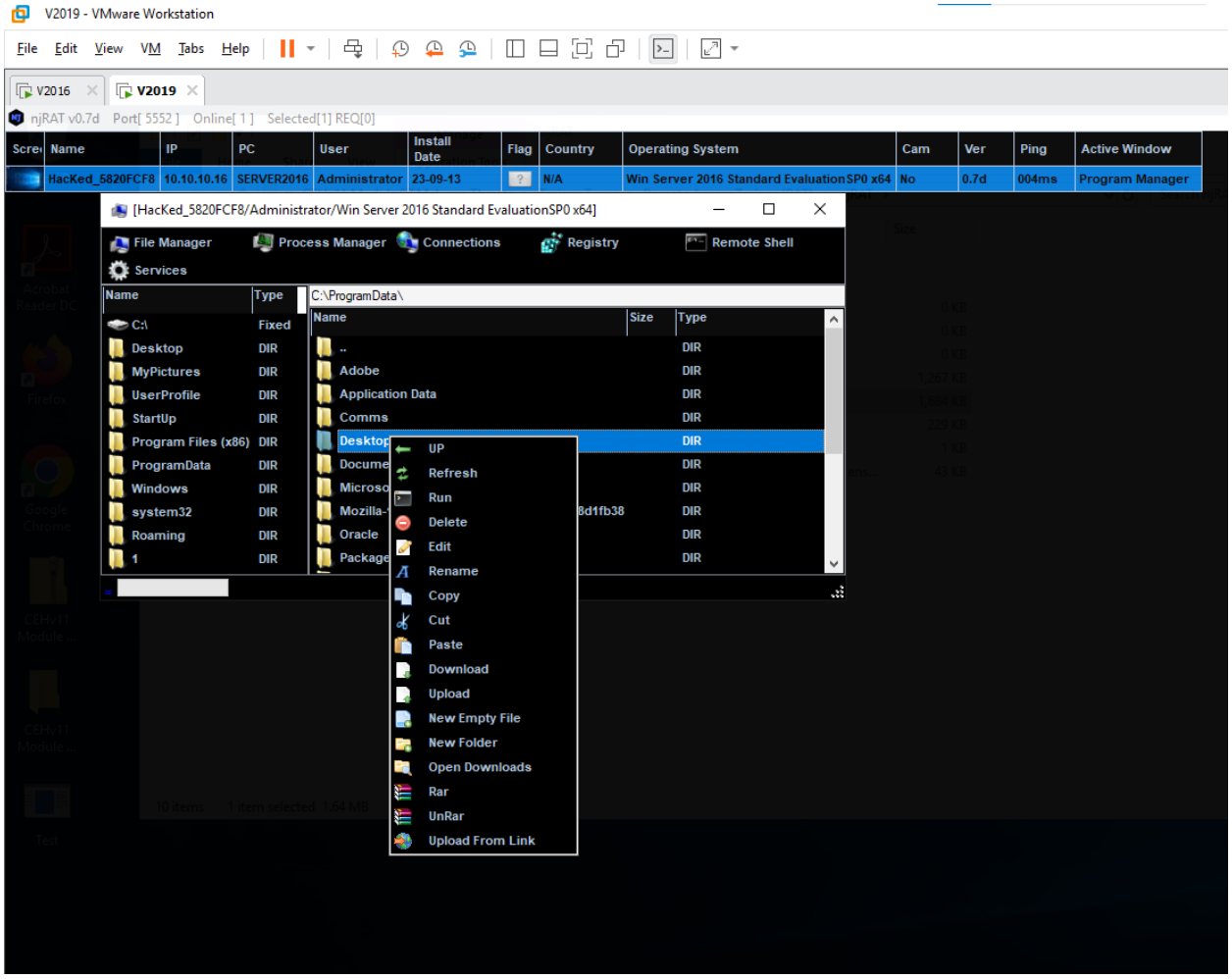

Builder
Host
10.10.10.19
Port
5552
Icon
Protect Process [BSOD]
VicTim Name
HacKed
DONE!
C:\Users\Administrator\Desktop\Test.exe
OK
ExeName
server.exe
Directory
%TEMP%

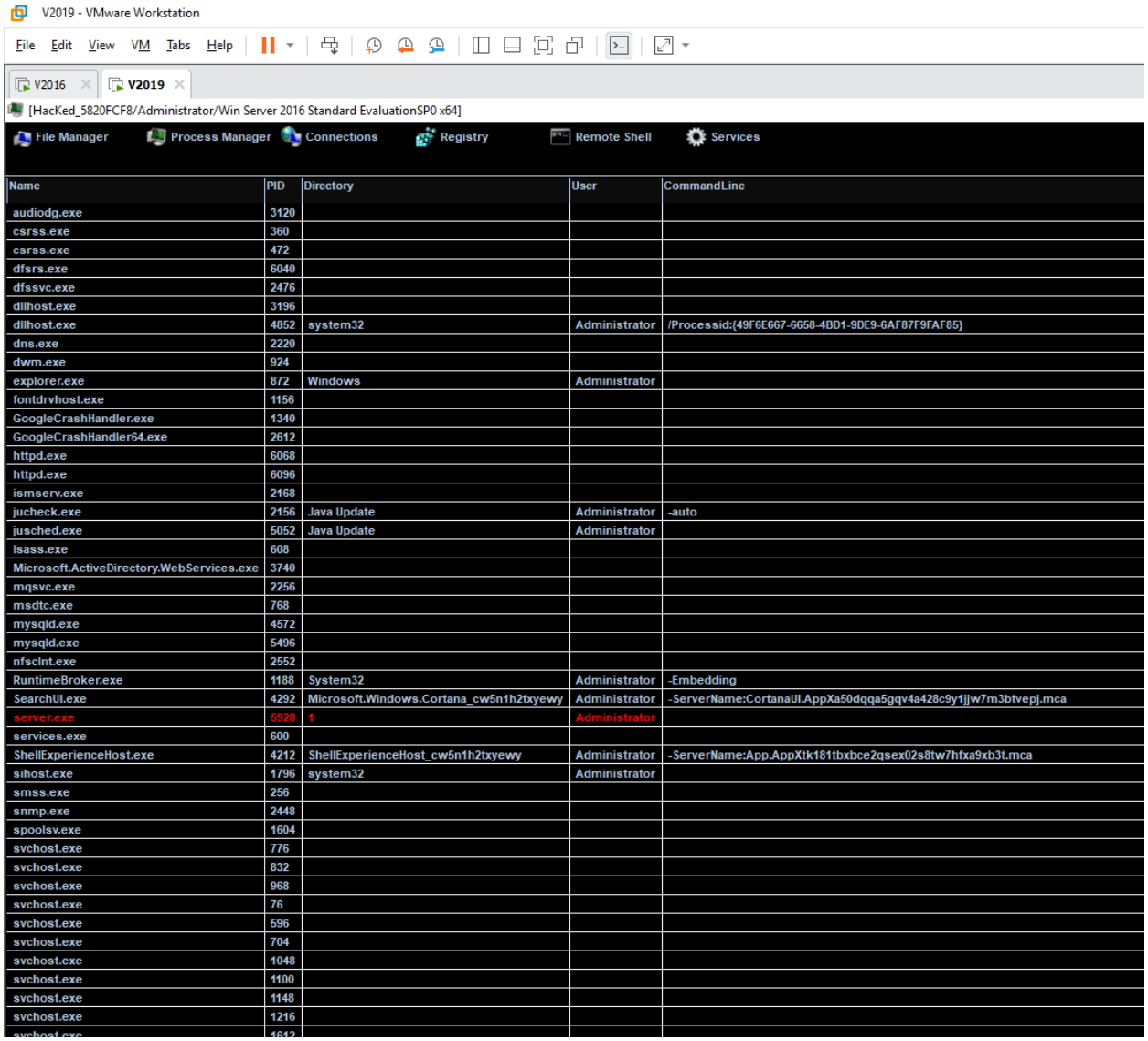

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Test.exe
Acrobat Reader DC
desktop.ini
Firefox


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scre Name IP PC User Install Date Flag Country Operating System Cam Ver Ping Active Window
HacKed_5820FCF8 10.10.10.16 SERVER2016 Administrator 23-09-13 N/A Win Server 2016 Standard Evaluation SP0 x64 No 0.7d .. Program Manager

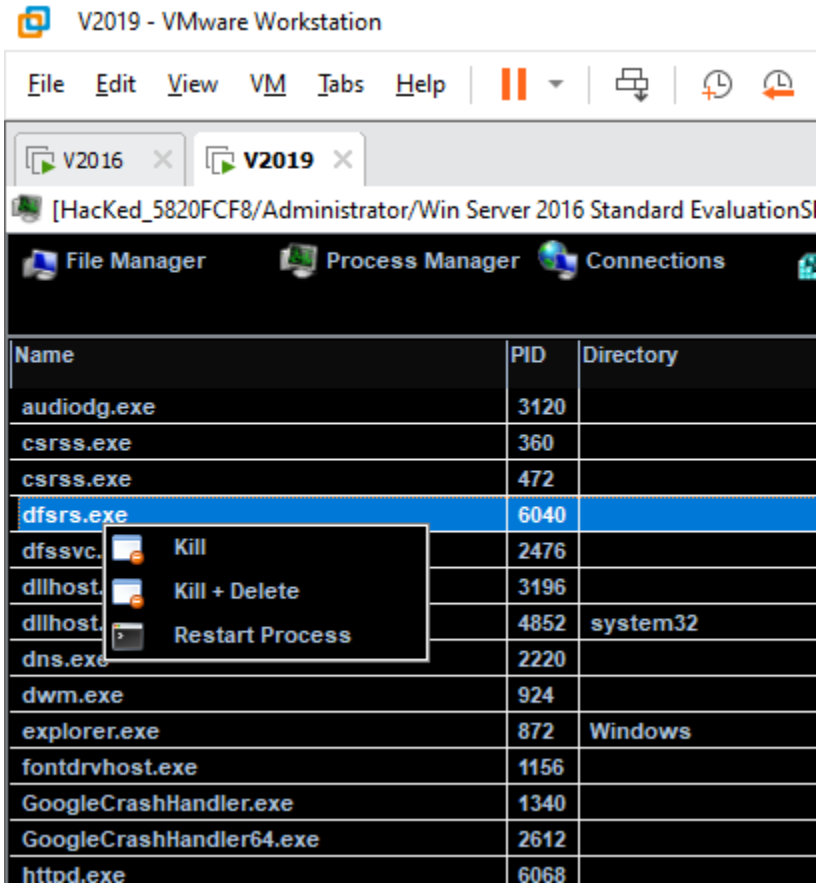

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scre Name IP PC User Install Date Flag Country Operating System Cam Ver Ping Active Window
HacKed_5820FCF8 10.10. 23-09-13 N/A Win Server 2016 Standard Evaluation SP0 x64 No 0.7d 060ms Program Manager
Manager
Run File
Remote Desktop
Remote Cam
Microphone
Get Passwords
Keylogger
Open Chat
Server
Open Folder

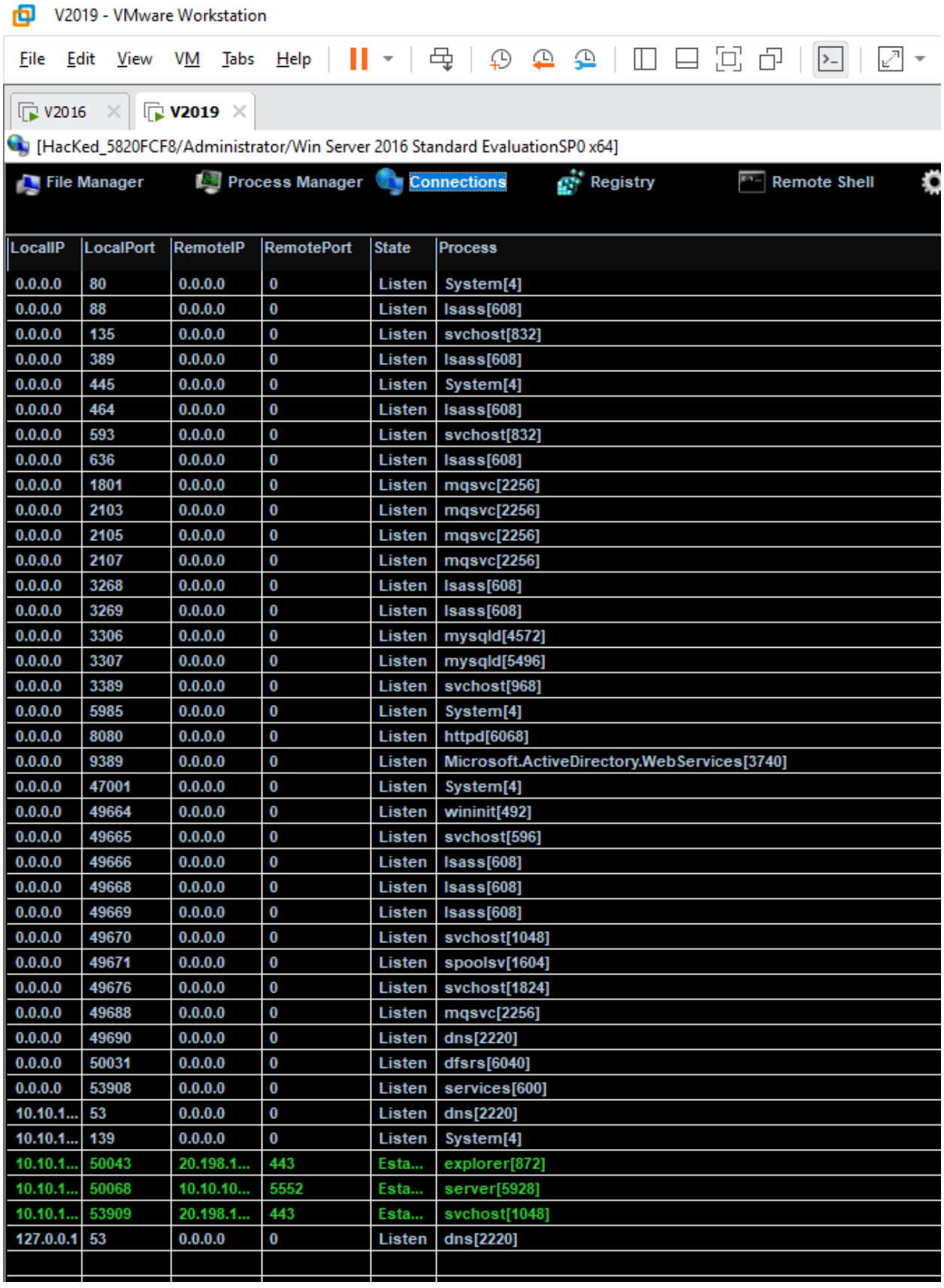

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scre Name IP PC User Install Date Flag Country Operating System Car
HacKed_5820FCF8 10.10.10.16 SERVER2016 Administrator 23-09-13 N/A Win Server 2016 Standard EvaluationSP0 x64 No
[HacKed_5820FCF8/Administrator/Win Server 2016 Standard EvaluationSP0 x64]
File Manager
Process Manager
Connections
Registry
Remote Shell
Services
Name Type
C:\ Fixed
Desktop DIR
MyPictures DIR
UserProfile DIR
StartUp DIR
Program Files (x86) DIR
ProgramData DIR
Windows DIR
system32 DIR
Roaming DIR
1 DIR
C:\ProgramData\
Name Size Type
.. DIR
Adobe DIR
Application Data DIR
Comms DIR
Desktop DIR
Documents DIR
Microsoft DIR
Mozilla-1de4eec8-1241-4177-a864-e594e8d1fb38 DIR
Oracle DIR
Package Cache DIR


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scre Name IP PC User Install Date Flag Country Operating System Cam Ver Ping Active Window
HacKed_5820FCF8 10.10.10.16 SERVER2016 Administrator 23-09-13 N/A Win Server 2016 Standard EvaluationSP0 x64 No 0.7d 004ms Program Manager
[HacKed_5820FCF8/Administrator/Win Server 2016 Standard EvaluationSP0 x64]
File Manager
Process Manager
Connections
Registry
Remote Shell
Services
Name Type
C:\ Fixed
Desktop DIR
MyPictures DIR
UserProfile DIR
StartUp DIR
Program Files (x86) DIR
ProgramData DIR
Windows DIR
system32 DIR
Roaming DIR
1 DIR
C:\ProgramData\
Name Size Type
.. DIR
Adobe DIR
Application Data DIR
Comms DIR
Desktop DIR
Docume DIR
Microso DIR
Mozilla- 8d1fb38 DIR
Oracle DIR
Package DIR
UP
Refresh
Run
Delete
Edit
Rename
Copy
Cut
Paste
Download
Upload
New Empty File
New Folder
Open Downloads
Rar
UnRar
Upload From Link

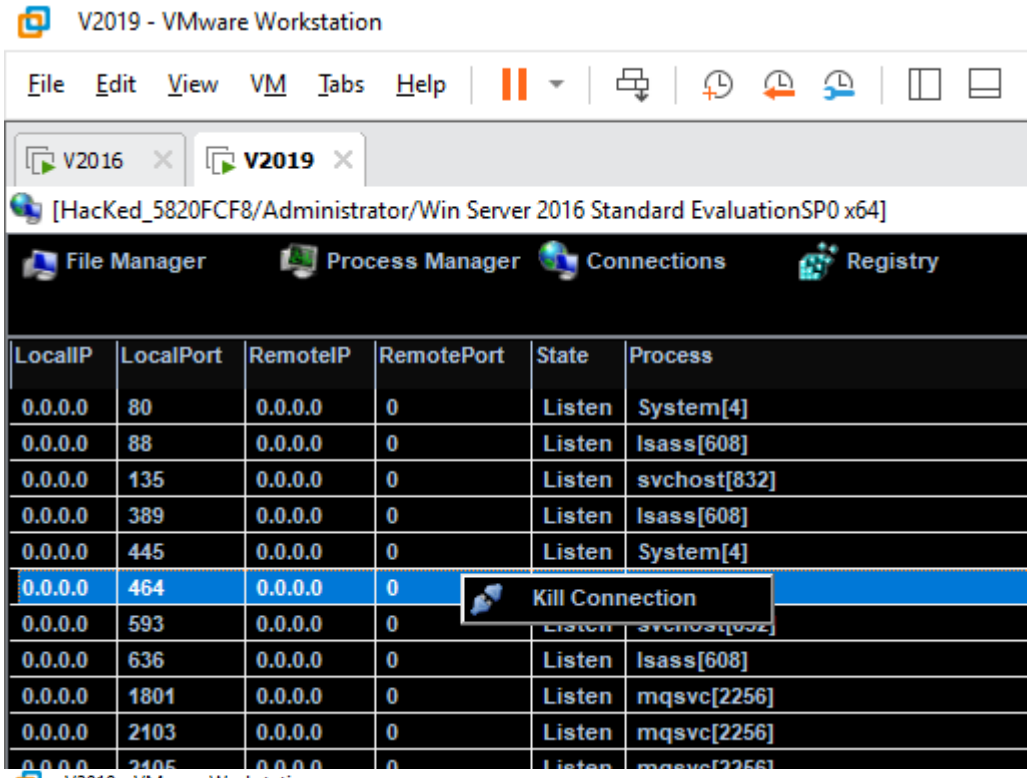


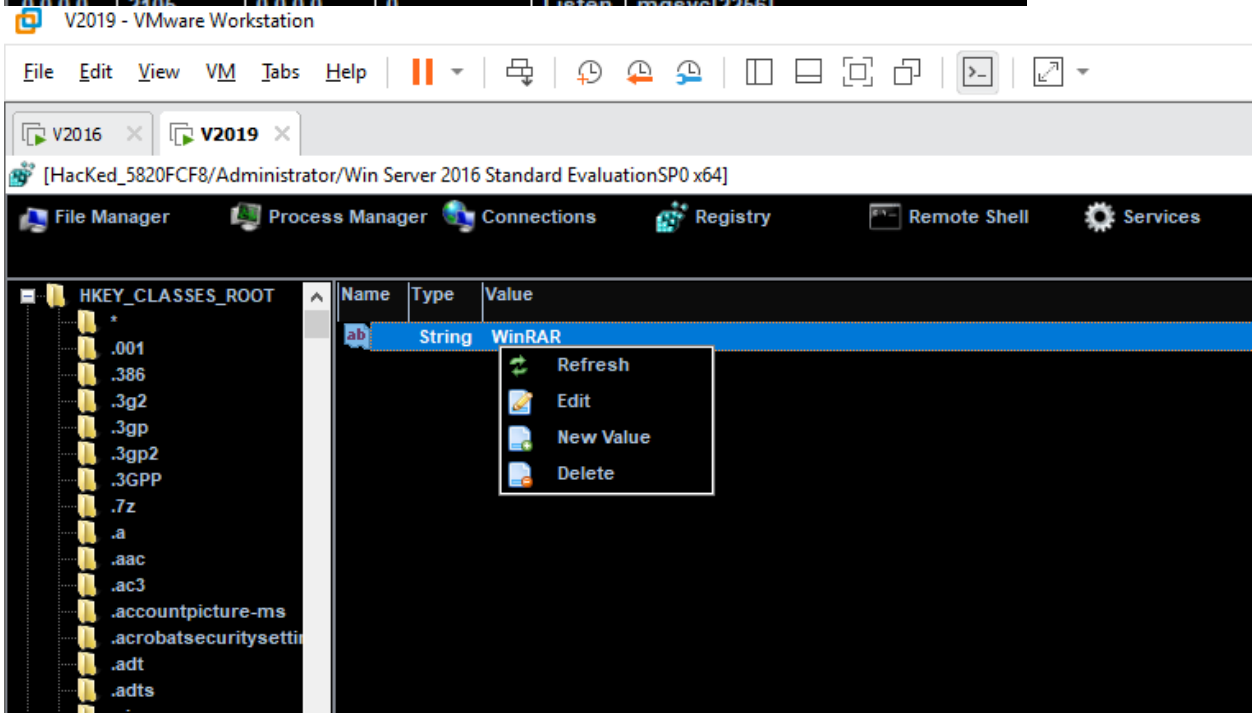
Name	PID	Directory	User	CommandLine
audiodg.exe	3120			
csrss.exe	360			
csrss.exe	472			
dfsrs.exe	6040			
dfssvc.exe	2476			
dllhost.exe	3196			
dllhost.exe	4852	system32	Administrator	/Processid:{49F6E667-6658-4BD1-9DE9-6AF87F9FAF85}
dns.exe	2220			
dwm.exe	924			
explorer.exe	872	Windows	Administrator	
fontdrvhost.exe	1156			
GoogleCrashHandler.exe	1340			
GoogleCrashHandler64.exe	2612			
httpd.exe	6068			
httpd.exe	6096			
ismserv.exe	2168			
jucheck.exe	2156	Java Update	Administrator	-auto
jusched.exe	5052	Java Update	Administrator	
lsass.exe	608			
Microsoft.ActiveDirectory.WebServices.exe	3740			
mqsvc.exe	2256			
msdtc.exe	768			
mysqld.exe	4572			
mysqld.exe	5496			
nfsclnt.exe	2552			
RuntimeBroker.exe	1188	System32	Administrator	-Embedding
SearchUI.exe	4292	Microsoft.Windows.Cortana_cw5n1h2txyewy	Administrator	-ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca
server.exe	5928	1	Administrator	
services.exe	600			
ShellExperienceHost.exe	4212	ShellExperienceHost_cw5n1h2txyewy	Administrator	-ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca
sihost.exe	1796	system32	Administrator	
smss.exe	256			
snmp.exe	2448			
spoolsv.exe	1604			
svchost.exe	776			
svchost.exe	832			
svchost.exe	968			
svchost.exe	76			
svchost.exe	596			
svchost.exe	704			
svchost.exe	1048			
svchost.exe	1100			
svchost.exe	1148			
svchost.exe	1216			
svchost.exe	1642			

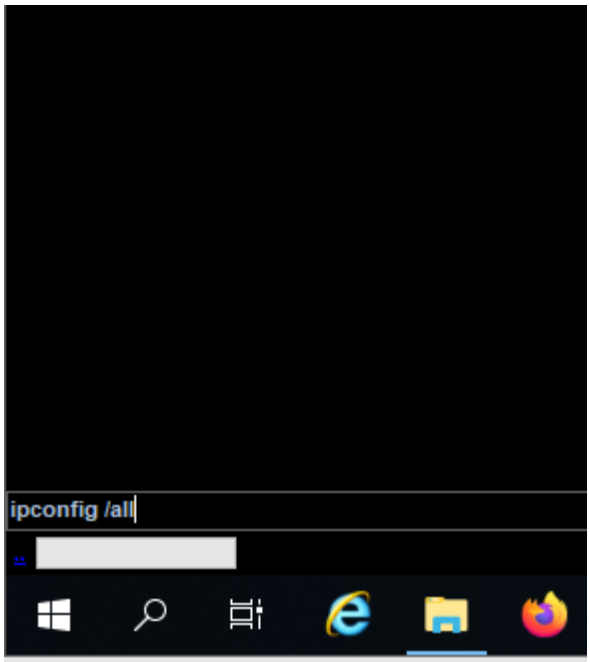

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
[HacKed_5820FCF8/Administrator/Win Server 2016 Standard EvaluationSl
File Manager
Process Manager
Connections
Name
PID
Directory
audiodg.exe 3120
csrss.exe 360
csrss.exe 472
dfsrs.exe 6040
dfssvc. 2476
dllhost. 3196
dllhost. 4852 system32
dns.exe 2220
dwm.exe 924
explorer.exe 872 Windows
fontdrvhost.exe 1156
GoogleCrashHandler.exe 1340
GoogleCrashHandler64.exe 2612
httpd.exe 6068
Kill
Kill + Delete
Restart Process

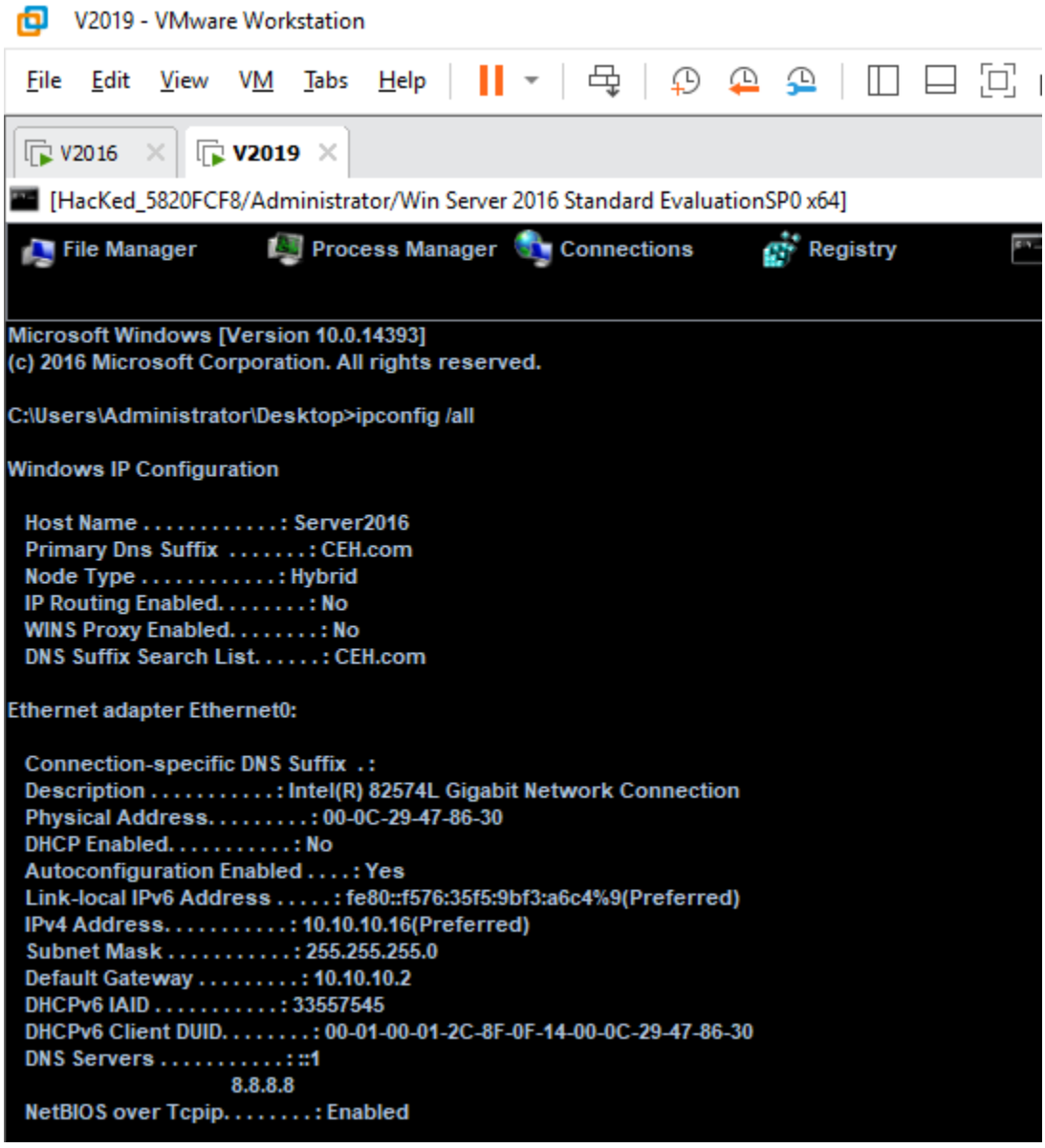


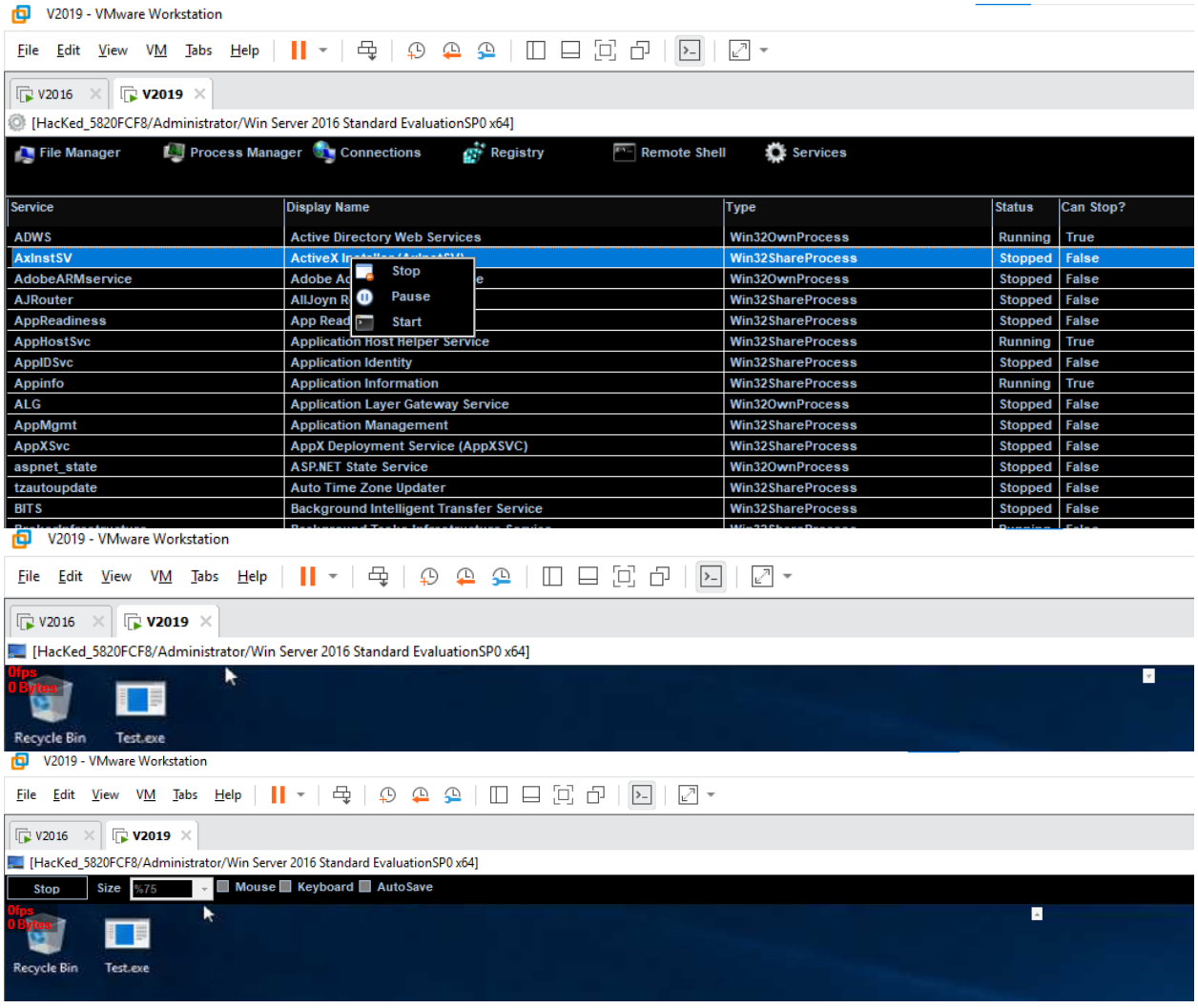
LocalIP	LocalPort	RemoteIP	RemotePort	State	Process
0.0.0.0	80	0.0.0.0	0	Listen	System[4]
0.0.0.0	88	0.0.0.0	0	Listen	lsass[608]
0.0.0.0	135	0.0.0.0	0	Listen	svchost[832]
0.0.0.0	389	0.0.0.0	0	Listen	lsass[608]
0.0.0.0	445	0.0.0.0	0	Listen	System[4]
0.0.0.0	464	0.0.0.0	0	Listen	lsass[608]
0.0.0.0	593	0.0.0.0	0	Listen	svchost[832]
0.0.0.0	636	0.0.0.0	0	Listen	lsass[608]
0.0.0.0	1801	0.0.0.0	0	Listen	mqsvc[2256]
0.0.0.0	2103	0.0.0.0	0	Listen	mqsvc[2256]
0.0.0.0	2105	0.0.0.0	0	Listen	mqsvc[2256]
0.0.0.0	2107	0.0.0.0	0	Listen	mqsvc[2256]
0.0.0.0	3268	0.0.0.0	0	Listen	lsass[608]
0.0.0.0	3269	0.0.0.0	0	Listen	lsass[608]
0.0.0.0	3306	0.0.0.0	0	Listen	mysqld[4572]
0.0.0.0	3307	0.0.0.0	0	Listen	mysqld[5496]
0.0.0.0	3389	0.0.0.0	0	Listen	svchost[968]
0.0.0.0	5985	0.0.0.0	0	Listen	System[4]
0.0.0.0	8080	0.0.0.0	0	Listen	httpd[6068]
0.0.0.0	9389	0.0.0.0	0	Listen	Microsoft.ActiveDirectory.WebServices[3740]
0.0.0.0	47001	0.0.0.0	0	Listen	System[4]
0.0.0.0	49664	0.0.0.0	0	Listen	wininit[492]
0.0.0.0	49665	0.0.0.0	0	Listen	svchost[596]
0.0.0.0	49666	0.0.0.0	0	Listen	lsass[608]
0.0.0.0	49668	0.0.0.0	0	Listen	lsass[608]
0.0.0.0	49669	0.0.0.0	0	Listen	lsass[608]
0.0.0.0	49670	0.0.0.0	0	Listen	svchost[1048]
0.0.0.0	49671	0.0.0.0	0	Listen	spoolsv[1604]
0.0.0.0	49676	0.0.0.0	0	Listen	svchost[1824]
0.0.0.0	49688	0.0.0.0	0	Listen	mqsvc[2256]
0.0.0.0	49690	0.0.0.0	0	Listen	dns[2220]
0.0.0.0	50031	0.0.0.0	0	Listen	dfsrs[6040]
0.0.0.0	53908	0.0.0.0	0	Listen	services[600]
10.10.1...	53	0.0.0.0	0	Listen	dns[2220]
10.10.1...	139	0.0.0.0	0	Listen	System[4]
10.10.1...	50043	20.198.1...	443	Esta...	explorer[872]
10.10.1...	50068	10.10.10...	5552	Esta...	server[5928]
10.10.1...	53909	20.198.1...	443	Esta...	svchost[1048]
127.0.0.1	53	0.0.0.0	0	Listen	dns[2220]


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
[HacKed_5820FCF8/Administrator/Win Server 2016 Standard EvaluationSP0 x64]
File Manager
Process Manager
Connections
Registry
LocalIP LocalPort RemoteIP RemotePort State Process
0.0.0.0 80 0.0.0.0 0 Listen System[4]
0.0.0.0 88 0.0.0.0 0 Listen lsass[608]
0.0.0.0 135 0.0.0.0 0 Listen svchost[832]
0.0.0.0 389 0.0.0.0 0 Listen lsass[608]
0.0.0.0 445 0.0.0.0 0 Listen System[4]
0.0.0.0 464 0.0.0.0 0
Kill Connection
0.0.0.0 593 0.0.0.0 0
0.0.0.0 636 0.0.0.0 0 Listen lsass[608]
0.0.0.0 1801 0.0.0.0 0 Listen mqsvc[2256]
0.0.0.0 2103 0.0.0.0 0 Listen mqsvc[2256]


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
[HacKed_5820FCF8/Administrator/Win Server 2016 Standard EvaluationSP0 x64]
File Manager
Process Manager
Connections
Registry
Remote Shell
Services
HKEY_CLASSES_ROOT
*
.001
.386
.3g2
.3gp
.3gp2
.3GPP
.7z
.a
.aac
.ac3
.accountpicture-ms
.adt
.adts
Name Type Value
String WinRAR
Refresh
Edit
New Value
Delete

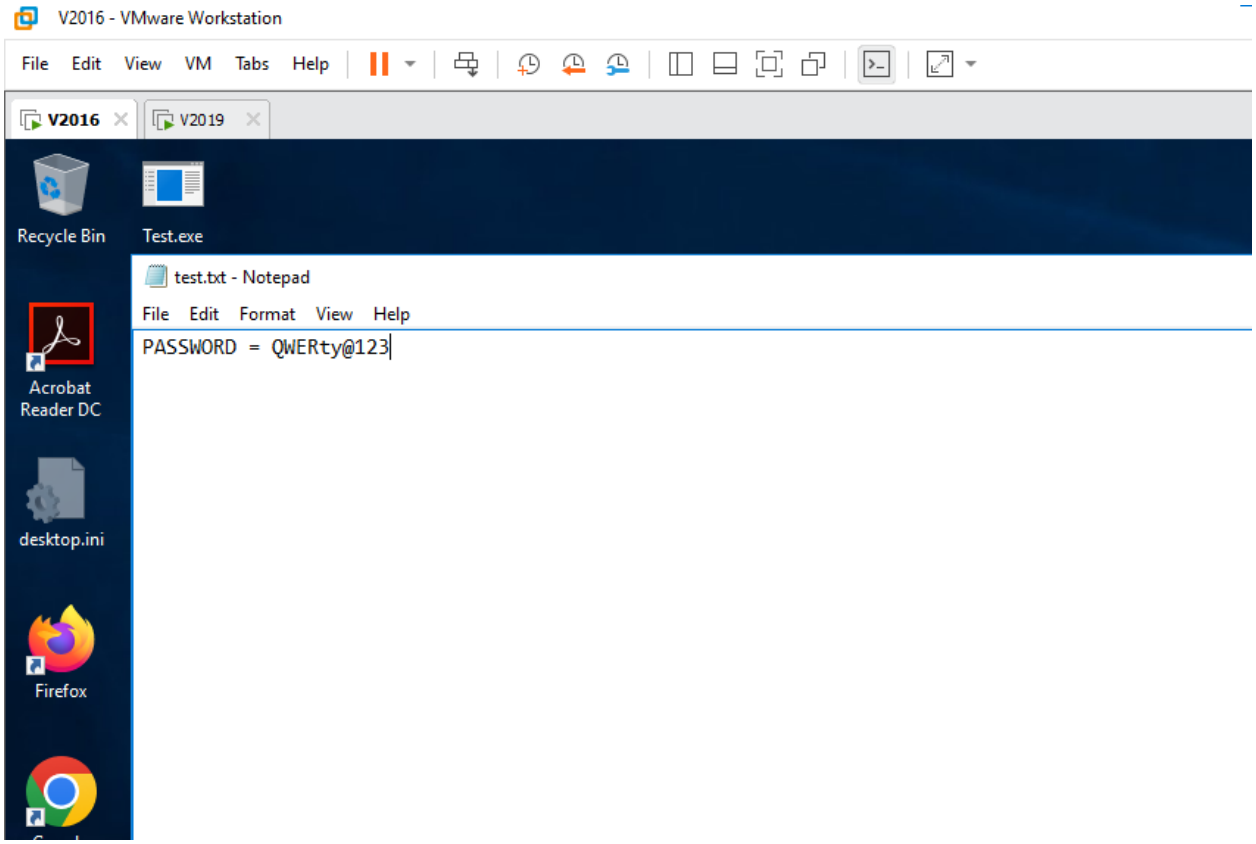

ipconfig /all
To direct input to this VM, move the mouse pointer insi

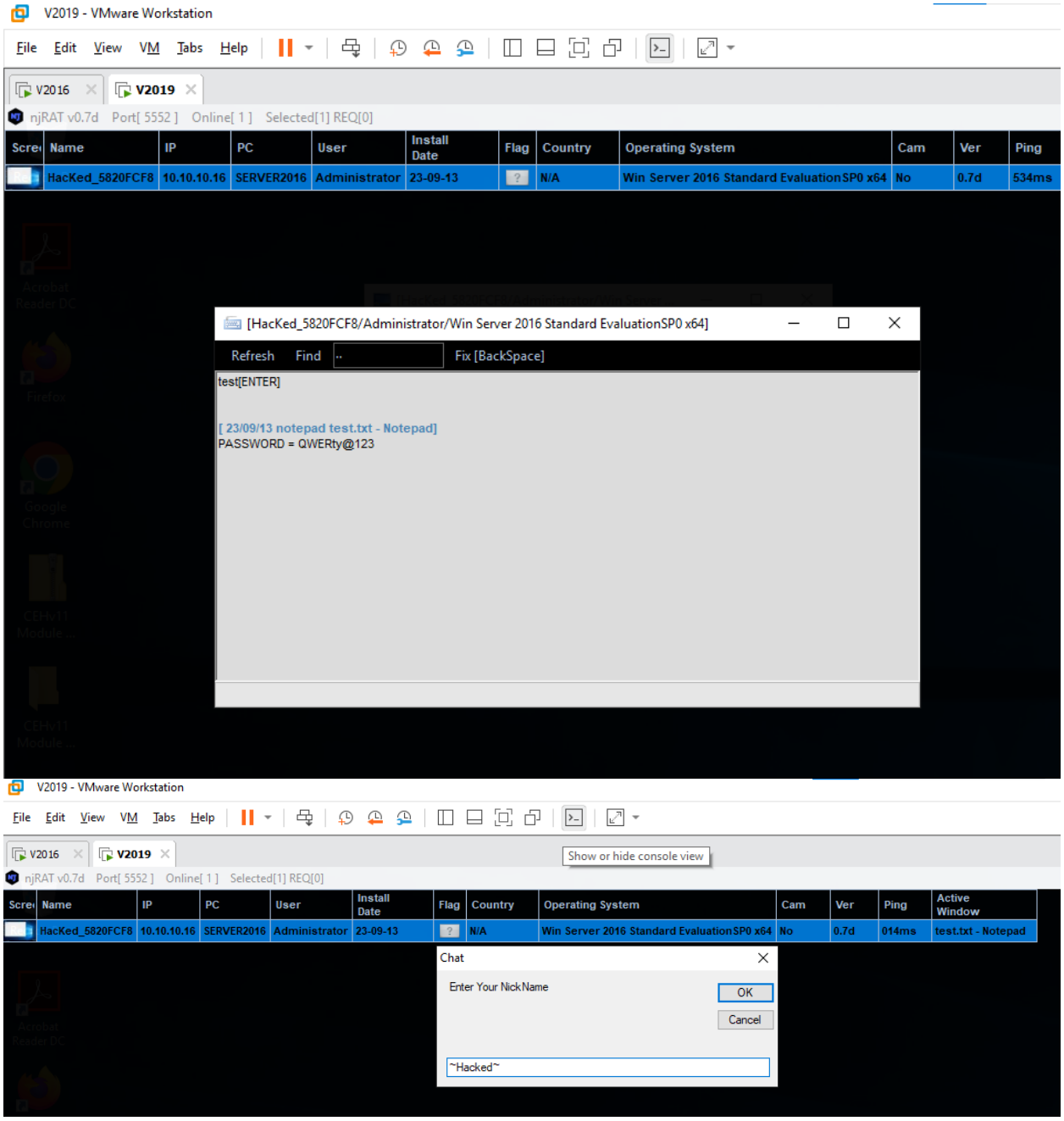

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
[HacKed_5820FCF8/Administrator/Win Server 2016 Standard EvaluationSP0 x64]
File Manager
Process Manager
Connections
Registry
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator\Desktop>ipconfig /all
Windows IP Configuration
Host Name . . . . . : Server2016
Primary Dns Suffix . . . . . : CEH.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : CEH.com
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-47-86-30
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f576:35f5:9bf3:a6c4%9(Preferred)
IPv4 Address. . . . . : 10.10.10.16(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.10.2
DHCPv6 IAID . . . . . : 33557545
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-8F-0F-14-00-0C-29-47-86-30
DNS Servers . . . . . : ::1
8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
[HacKed_5820FCF8/Administrator/Win Server 2016 Standard EvaluationSP0 x64]
File Manager
Process Manager
Connections
Registry
Remote Shell
Services
Service
Display Name
Type
Status
Can Stop?
ADWS
Active Directory Web Services
Win32OwnProcess
Running
True
AxInstSV
ActiveX Installer (AxInstSV)
Win32ShareProcess
Stopped
False
AdobeARMservice
Adobe Acrobat Update Service
Win32OwnProcess
Stopped
False
AJRouter
AllJoyn Router Service
Win32ShareProcess
Stopped
False
AppReadiness
App Readiness
Win32ShareProcess
Stopped
False
AppHostSvc
Application Host Helper Service
Win32ShareProcess
Running
True
AppIDSvc
Application Identity
Win32ShareProcess
Stopped
False
Appinfo
Application Information
Win32ShareProcess
Running
True
ALG
Application Layer Gateway Service
Win32OwnProcess
Stopped
False
AppMgmt
Application Management
Win32ShareProcess
Stopped
False
AppXSvc
AppX Deployment Service (AppXSVC)
Win32ShareProcess
Stopped
False
aspnet_state
ASP.NET State Service
Win32OwnProcess
Stopped
False
tzautoupdate
Auto Time Zone Updater
Win32ShareProcess
Stopped
False
BITS
Background Intelligent Transfer Service
Win32ShareProcess
Stopped
False
Stop
Pause
Start

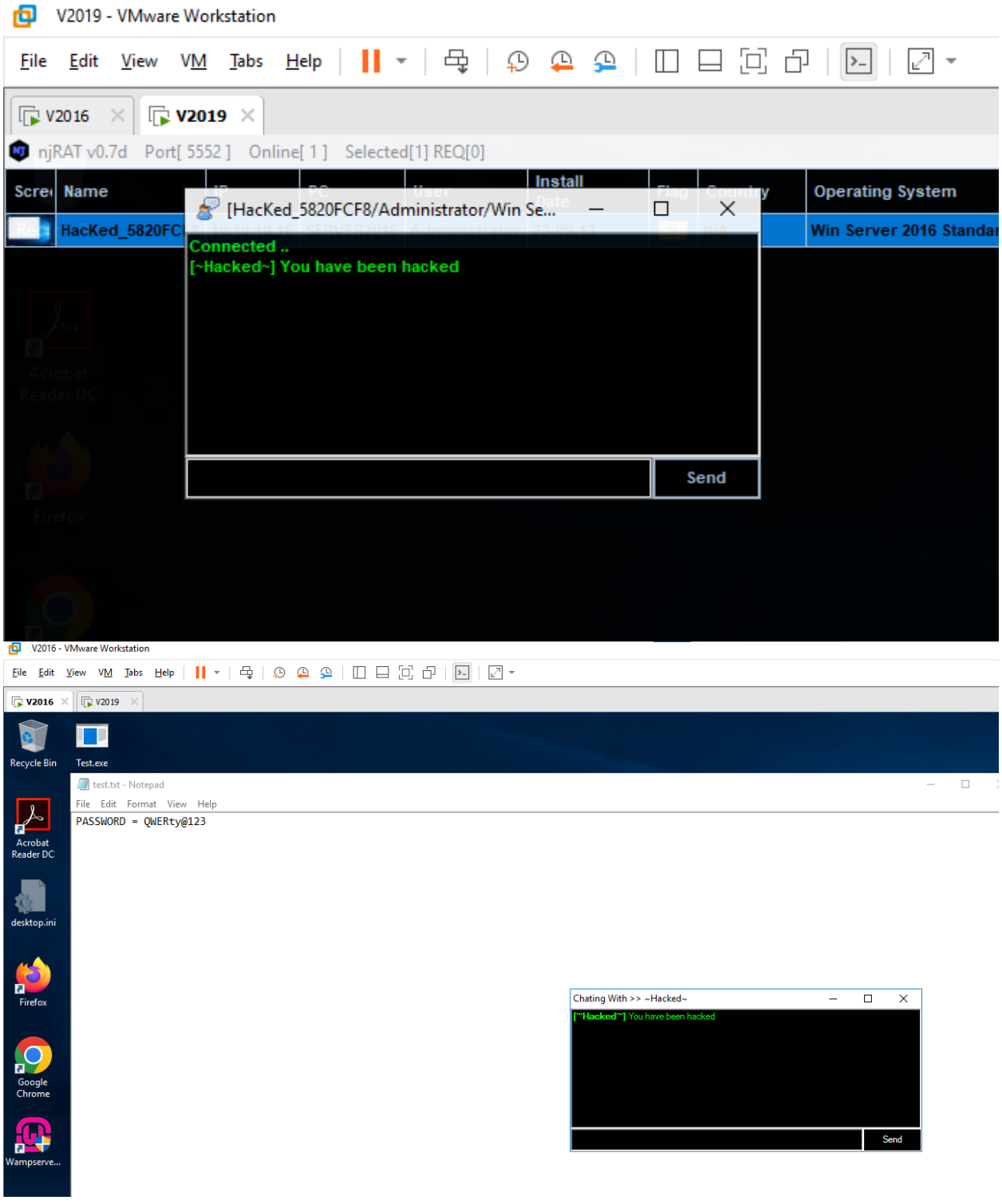
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
[HacKed_5820FCF8/Administrator/Win Server 2016 Standard EvaluationSP0 x64]
0fps
0 Bytes
Recycle Bin
Test.exe

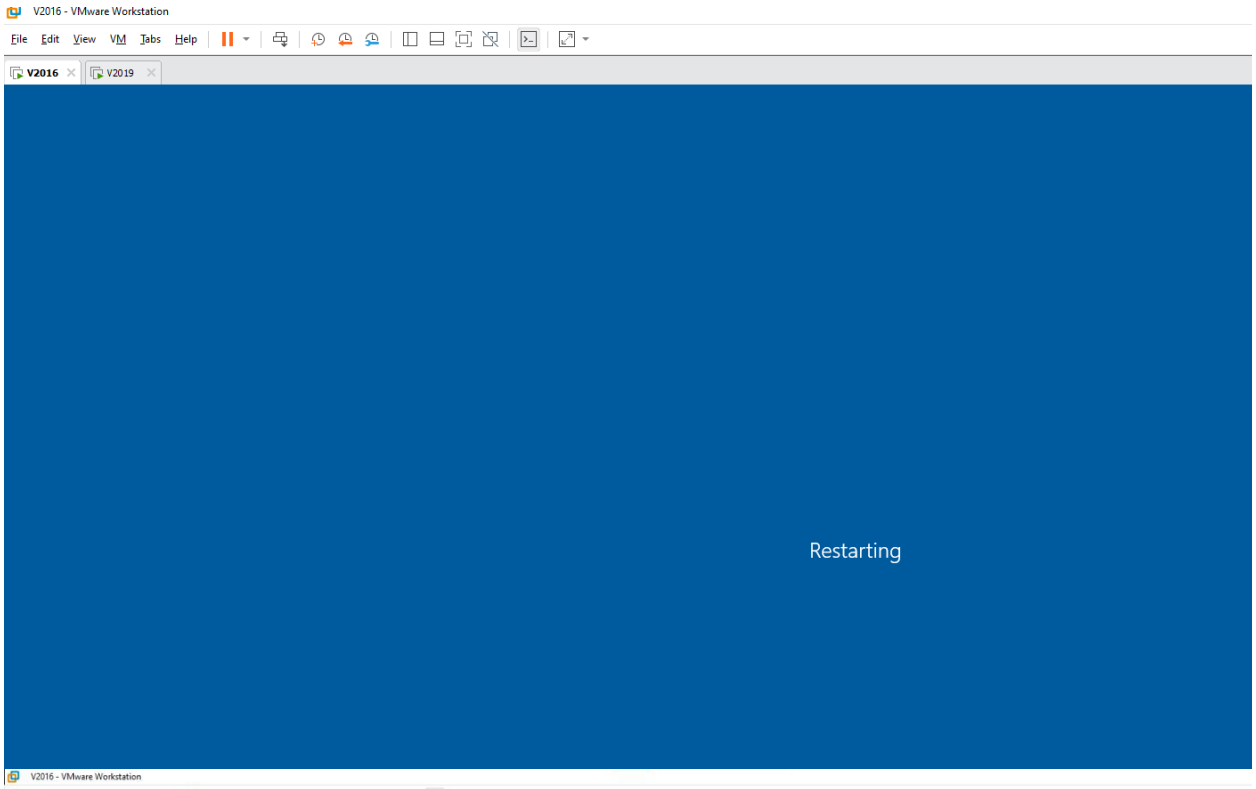
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
[HacKed_5820FCF8/Administrator/Win Server 2016 Standard EvaluationSP0 x64]
Stop
Size
%75
Mouse
Keyboard
AutoSave
0fps
0 Bytes
Recycle Bin
Test.exe

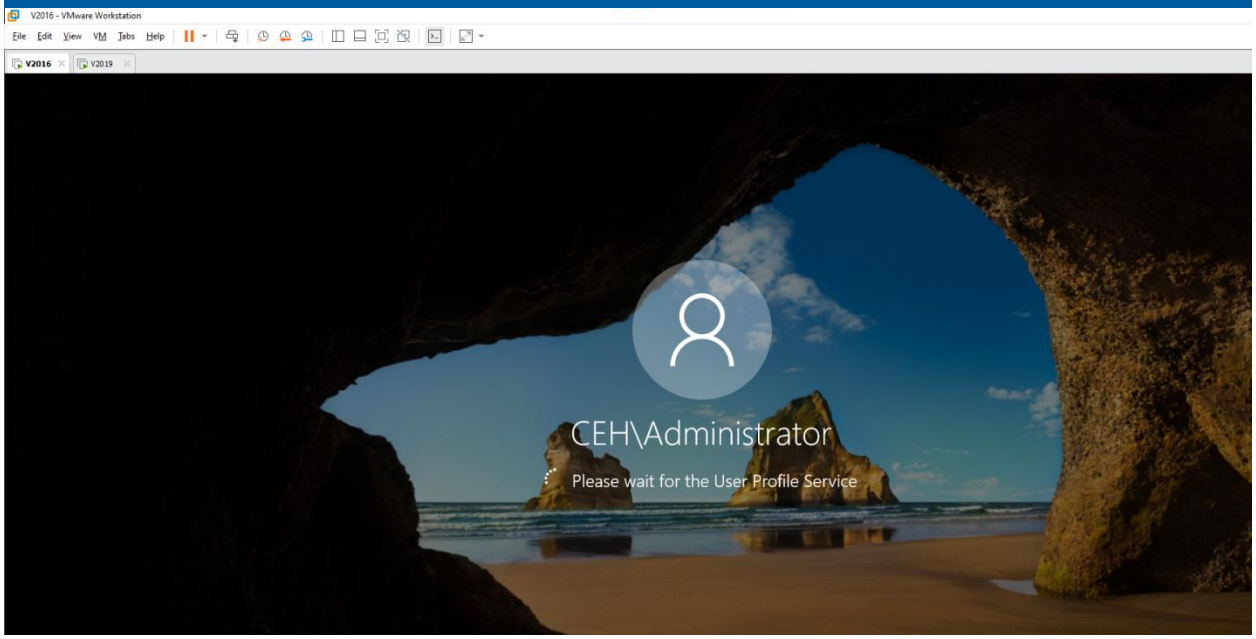

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Test.exe
test.txt - Notepad
File Edit Format View Help
PASSWORD = QWERty@123
Acrobat Reader DC
desktop.ini
Firefox

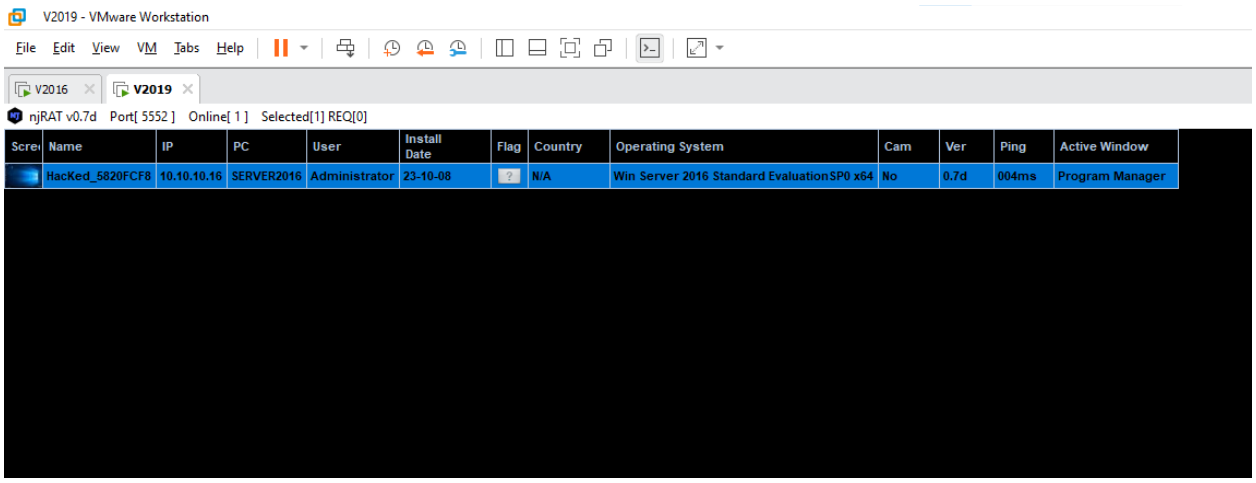

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scre Name IP PC User Install Date Flag Country Operating System Cam Ver Ping
HacKed_5820FCF8 10.10.10.16 SERVER2016 Administrator 23-09-13 N/A Win Server 2016 Standard EvaluationSP0 x64 No 0.7d 534ms
[HacKed_5820FCF8/Administrator/Win Server 2016 Standard EvaluationSP0 x64]
Refresh Find .. Fix [BackSpace]
test[ENTER]
[23/09/13 notepad test.txt - Notepad]
PASSWORD = QWERty@123

V2019 - VMware Workstation
File Edit View VM Tabs Help
Show or hide console view
V2016
V2019
njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Scre Name IP PC User Install Date Flag Country Operating System Cam Ver Ping Active Window
HacKed_5820FCF8 10.10.10.16 SERVER2016 Administrator 23-09-13 N/A Win Server 2016 Standard EvaluationSP0 x64 No 0.7d 014ms test.txt - Notepad
Chat
Enter Your NickName
OK
Cancel
~Hacked~


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
njRAT v0.7d Port[5552] Online[1] Selected[1] REQ[0]
Name
Install
Operating System
HacKed_5820FC
Win Server 2016 Standar
[HacKed_5820FCF8/Administrator/Win Se...
Connected ..
[~Hacked~] You have been hacked
Send
Acrobat Reader DC
Firefox
V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Test.exe
test.txt - Notepad
File Edit Format View Help
PASSWORD = QWERty@123
Acrobat Reader DC
desktop.ini
Firefox
Google Chrome
Wampserve...
Chating With >> ~Hacked~
[~Hacked~] You have been hacked
Send

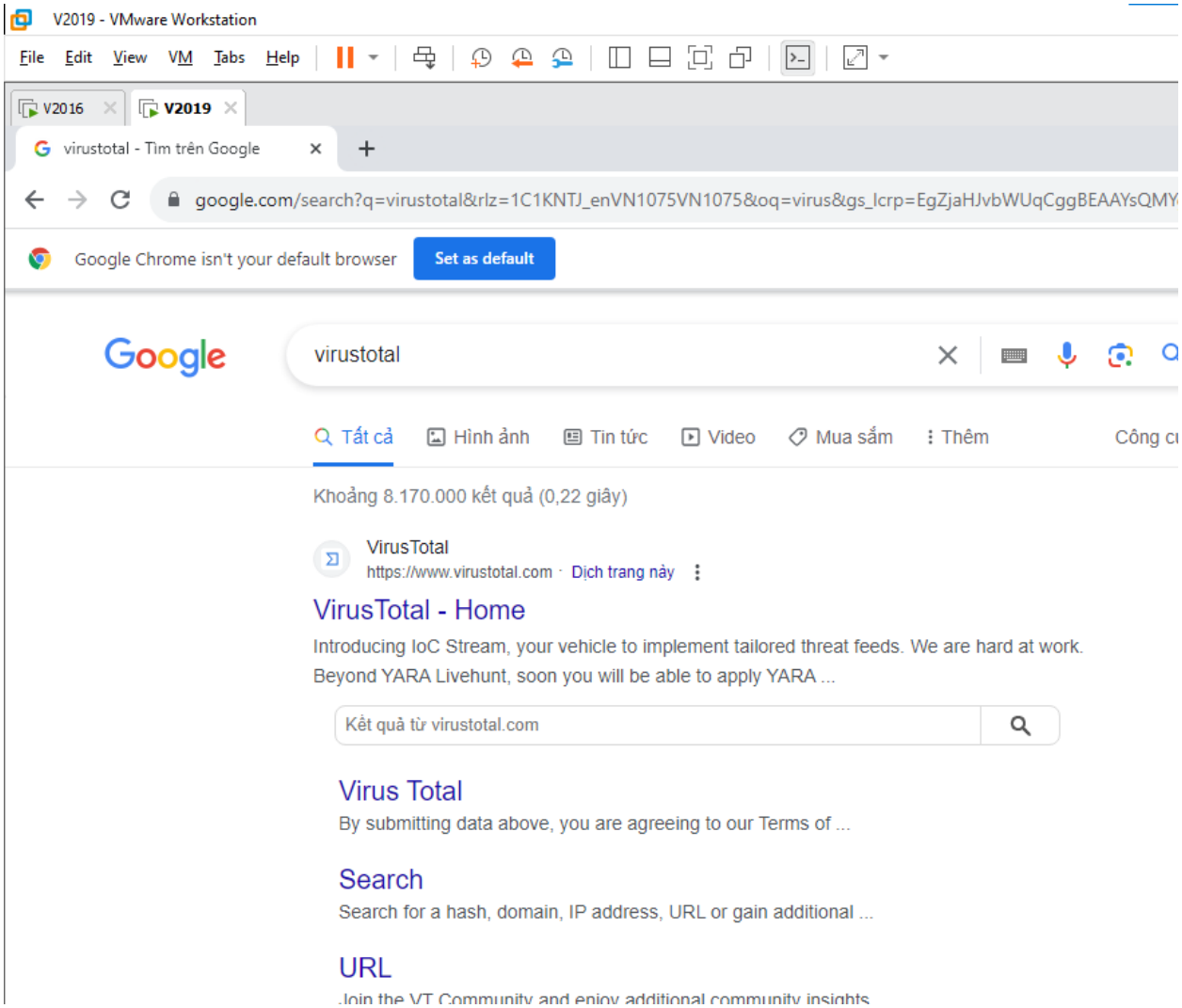

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Restarting

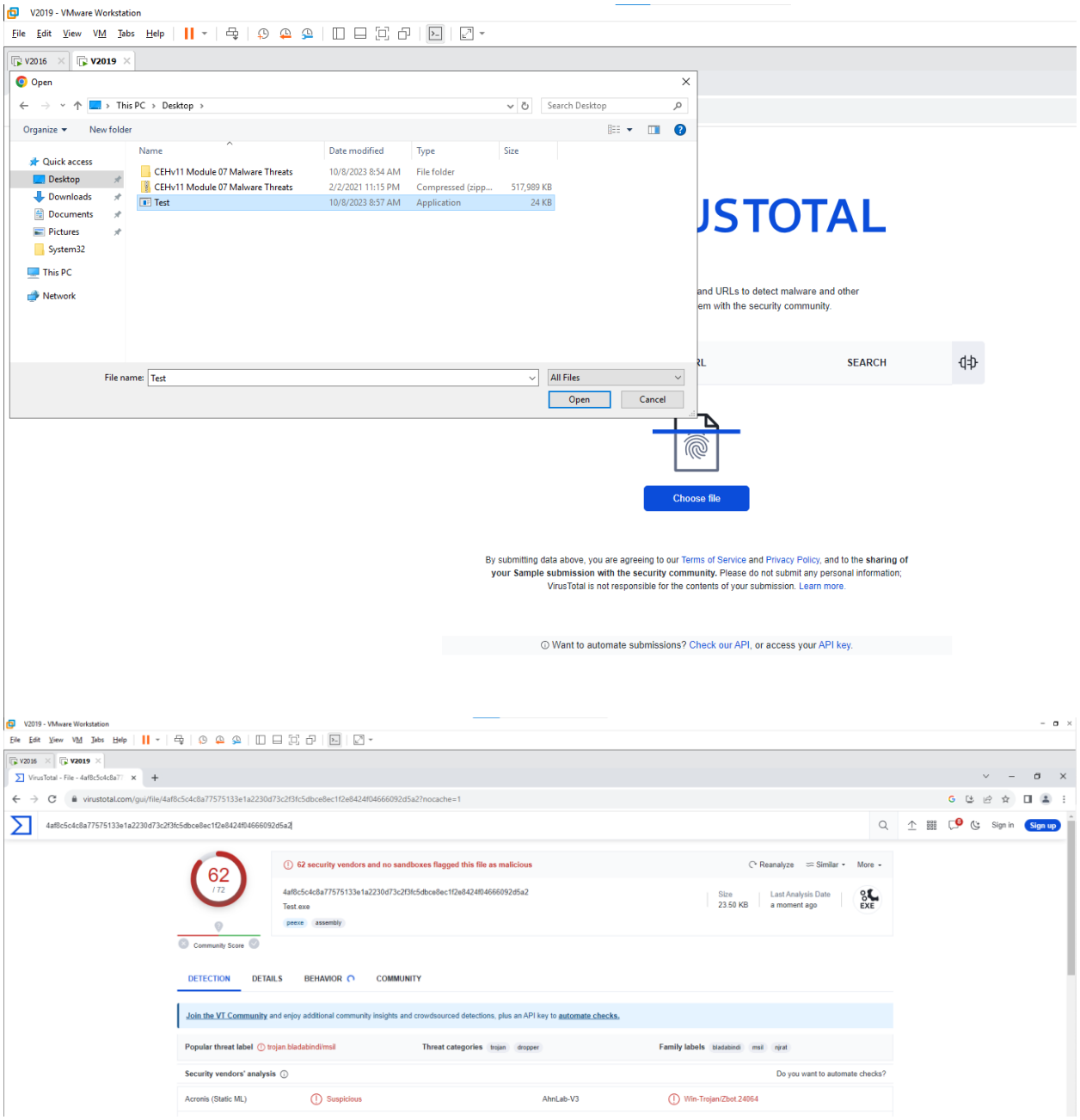

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
CEH\Administrator
Please wait for the User Profile Service



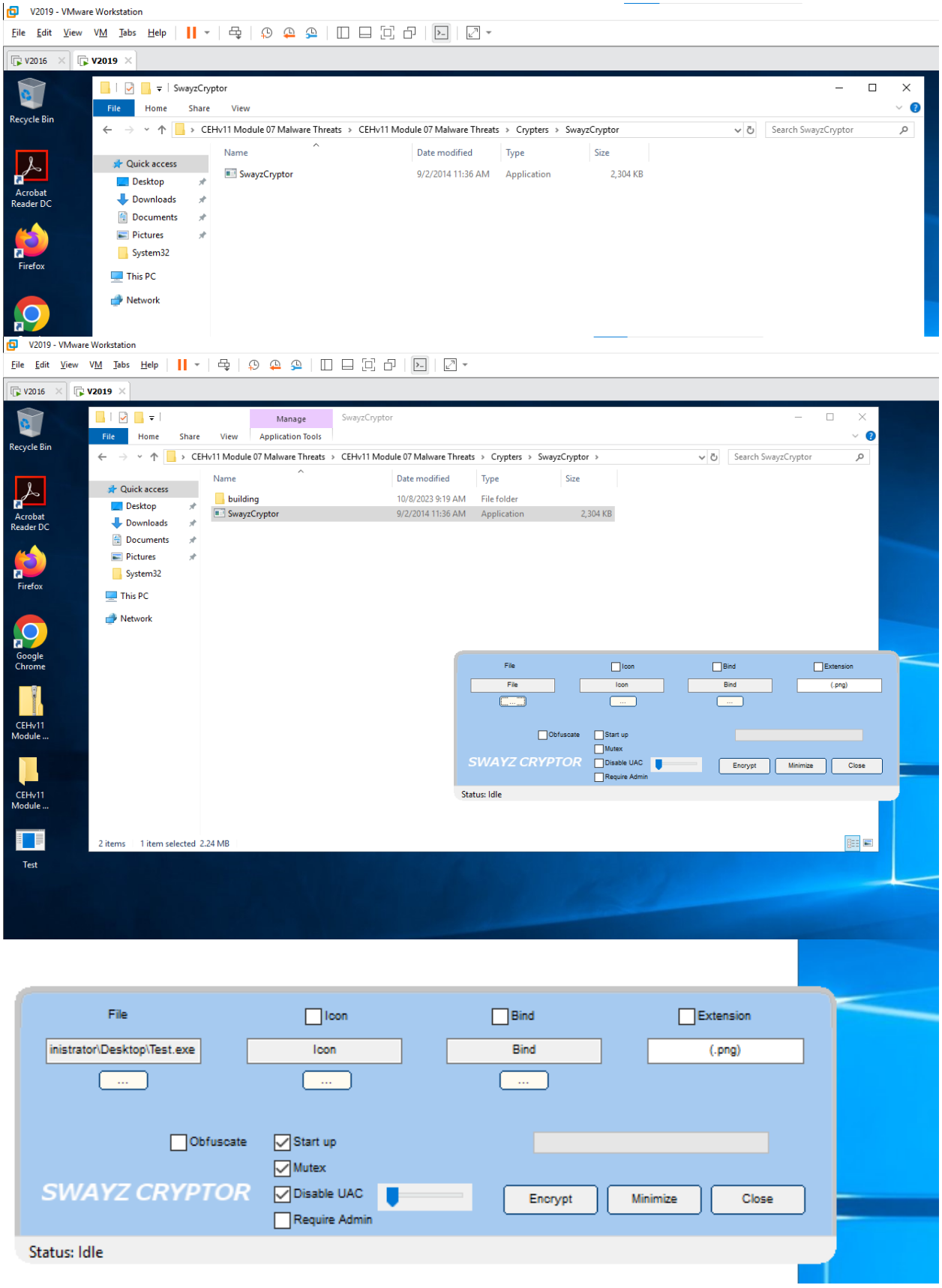
1.2 Hide a Trojan using SwayzCryptor and Make it Undetectable to Various Anti-Virus Programs

- Open Windows 10

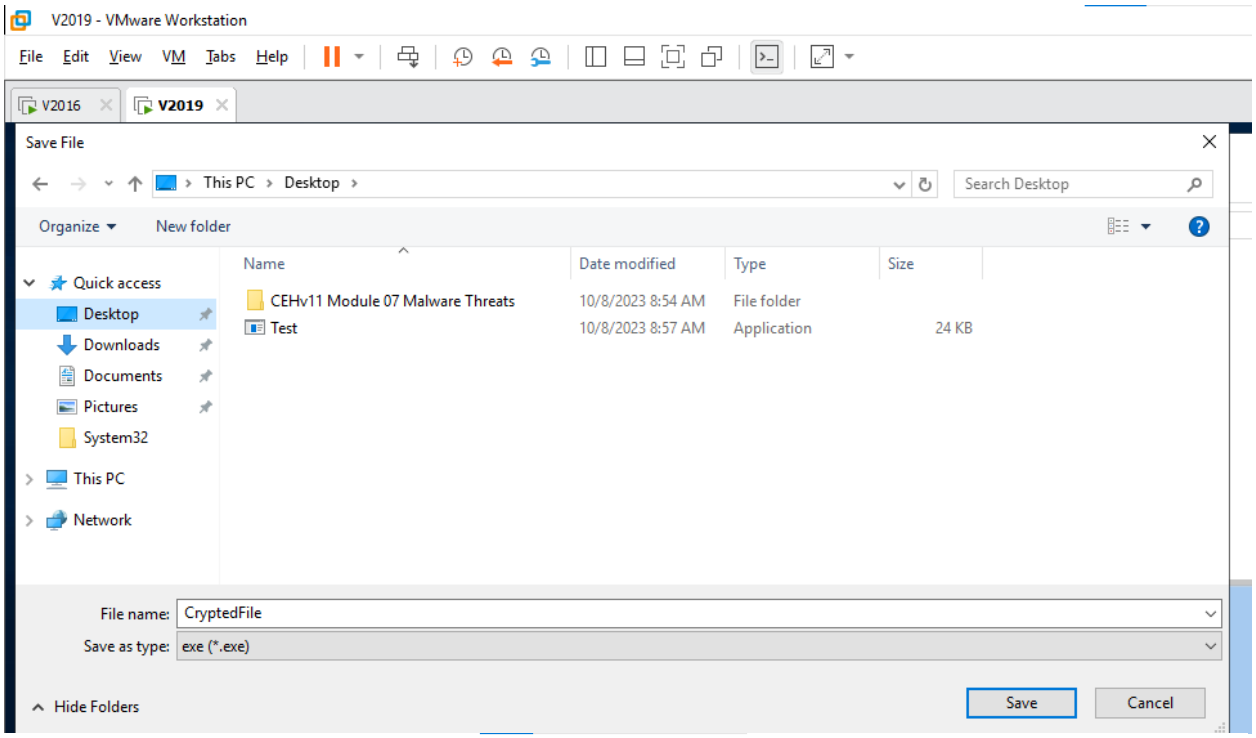

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
virustotal - Tìm trên Google
google.com/search?q=virustotal&rlz=1C1KNTJ_enVN1075VN1075&oq=virus&gs_lcrp=EgZjaHJvbWUqCggBEAAYsQMY
Google Chrome isn't your default browser
Set as default
Google
virustotal
Tất cả
Hình ảnh
Tin tức
Video
Mua sắm
Thêm
Công cụ
Khoảng 8.170.000 kết quả (0,22 giây)
VirusTotal
https://www.virustotal.com · Dịch trang này
VirusTotal - Home
Introducing IoC Stream, your vehicle to implement tailored threat feeds. We are hard at work.
Beyond YARA Livehunt, soon you will be able to apply YARA ...
Kết quả từ virustotal.com
Virus Total
By submitting data above, you are agreeing to our Terms of ...
Search
Search for a hash, domain, IP address, URL or gain additional ...
URL
Join the VT Community and enjoy additional community insights

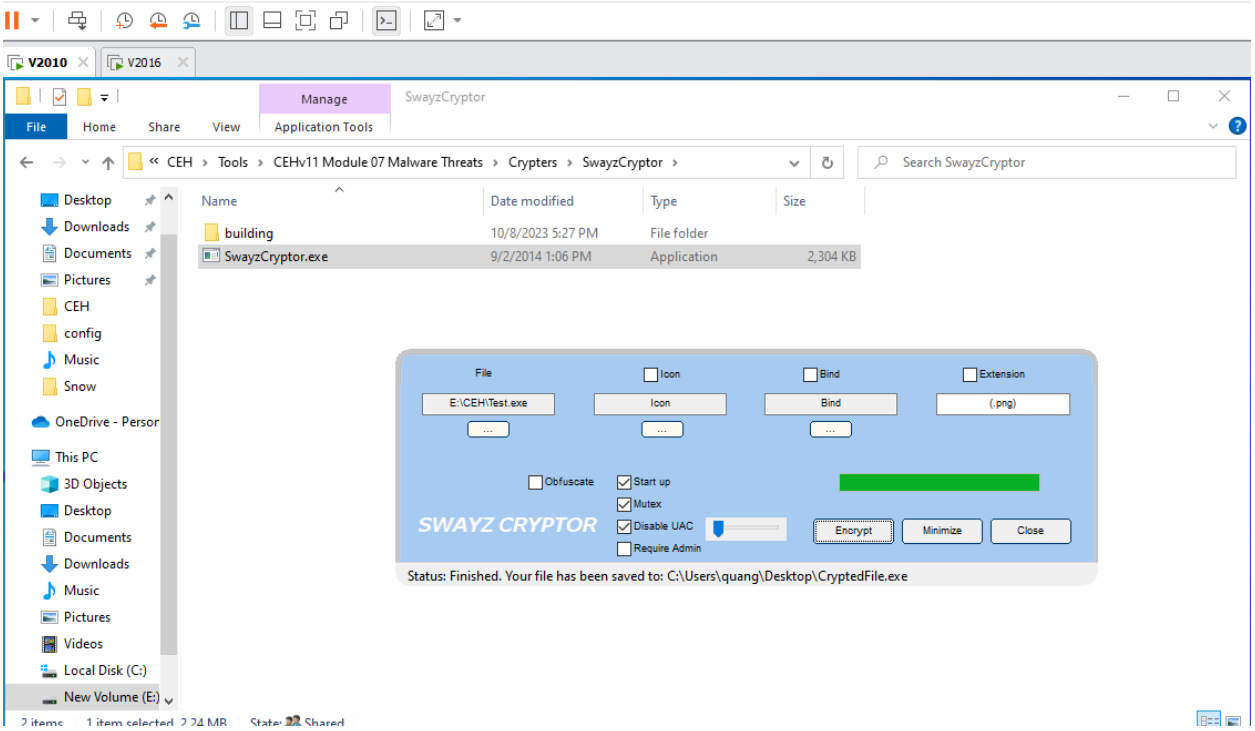

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Open
This PC › Desktop ›
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
CEHv11 Module 07 Malware Threats
10/8/2023 8:54 AM
File folder
CEHv11 Module 07 Malware Threats
2/2/2021 11:15 PM
Compressed (zipp...
517,989 KB
Test
10/8/2023 8:57 AM
Application
24 KB
File name: Test
All Files
Open
Cancel
USTOTAL
and URLs to detect malware and other
em with the security community.
SEARCH
Choose file
By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the sharing of your Sample submission with the security community. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.
Want to automate submissions? Check our API, or access your API key.

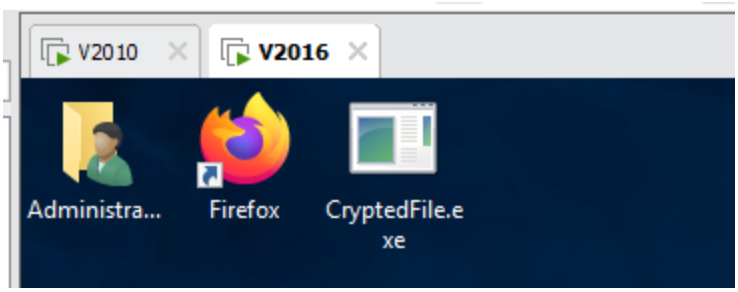
V2019 - VMware Workstation
V2016
V2019
VirusTotal - File - 4af8c5c4c8a7
virustotal.com/gui/file/4af8c5c4c8a77575133e1a2230d73c2f3fc5dbce8ec1f2e8424f04666092d5a2?nocache=1
4af8c5c4c8a77575133e1a2230d73c2f3fc5dbce8ec1f2e8424f04666092d5a2
Sign in
Sign up
62
/ 72
Community Score
62 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
4af8c5c4c8a77575133e1a2230d73c2f3fc5dbce8ec1f2e8424f04666092d5a2
Test.exe
peexe
assembly
Size
23.50 KB
Last Analysis Date
a moment ago
EXE
DETECTION
DETAILS
BEHAVIOR
COMMUNITY
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label
trojan.bladabindi/msil
Threat categories
trojan
dropper
Family labels
bladabindi
msil
njrat
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML)
Suspicious
AhnLab-V3
Win-Trojan/Zbot.24064

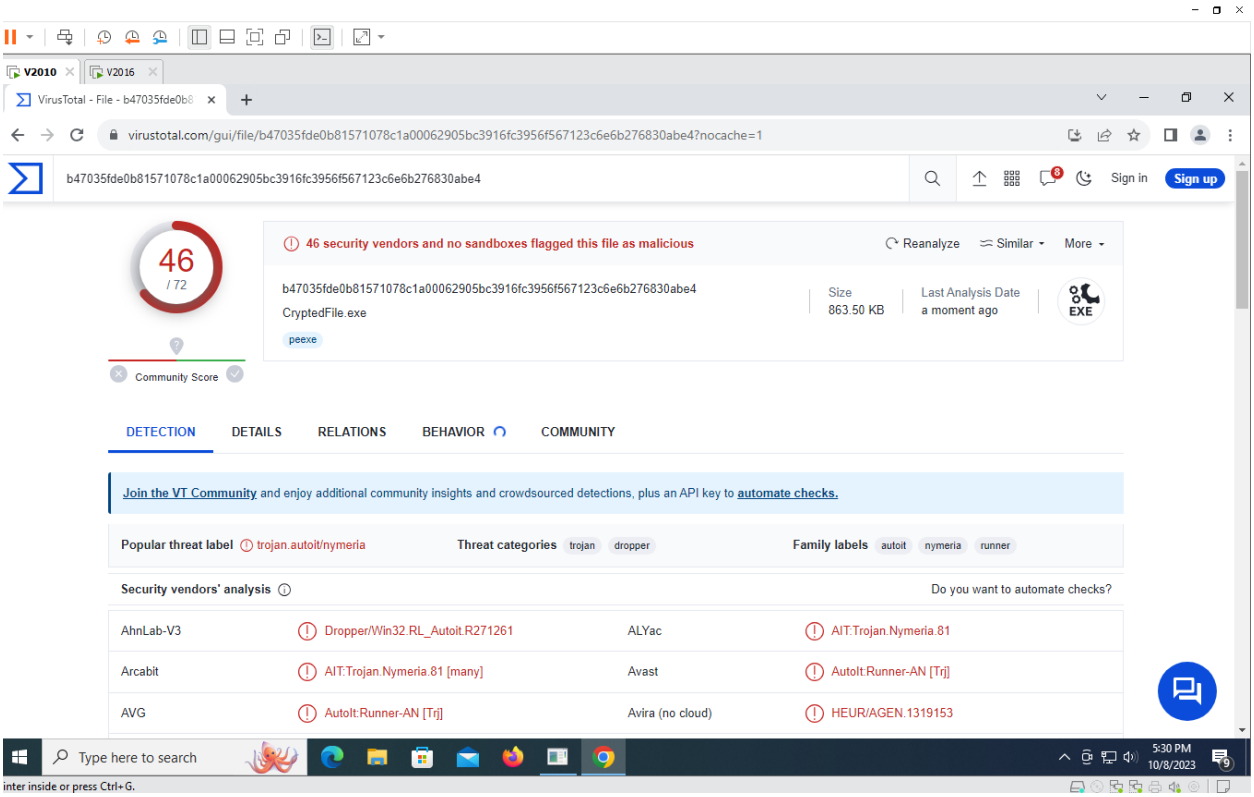

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
SwayzCryptor
File Home Share View
CEHv11 Module 07 Malware Threats › CEHv11 Module 07 Malware Threats › Crypters › SwayzCryptor
Search SwayzCryptor
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
SwayzCryptor
9/2/2014 11:36 AM
Application
2,304 KB
Manage
Application Tools
building
10/8/2023 9:19 AM
File folder
2 items
1 item selected 2.24 MB
File
Icon
Bind
Extension
(.png)
Obfuscate
Start up
Mutex
Disable UAC
Require Admin
SWAYZ CRYPTOR
Encrypt
Minimize
Close
Status: Idle

File
Icon
Bind
Extension
inistrator\Desktop\Test.exe
Icon
Bind
(.png)
...
Obfuscate
Start up
Mutex
Disable UAC
Require Admin
SWAYZ CRYPTOR
Encrypt
Minimize
Close
Status: Idle


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Save File
This PC › Desktop ›
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
CEHv11 Module 07 Malware Threats
10/8/2023 8:54 AM
File folder
Test
10/8/2023 8:57 AM
Application
24 KB
File name:
CryptedFile
Save as type:
exe (*.exe)
Hide Folders
Save
Cancel

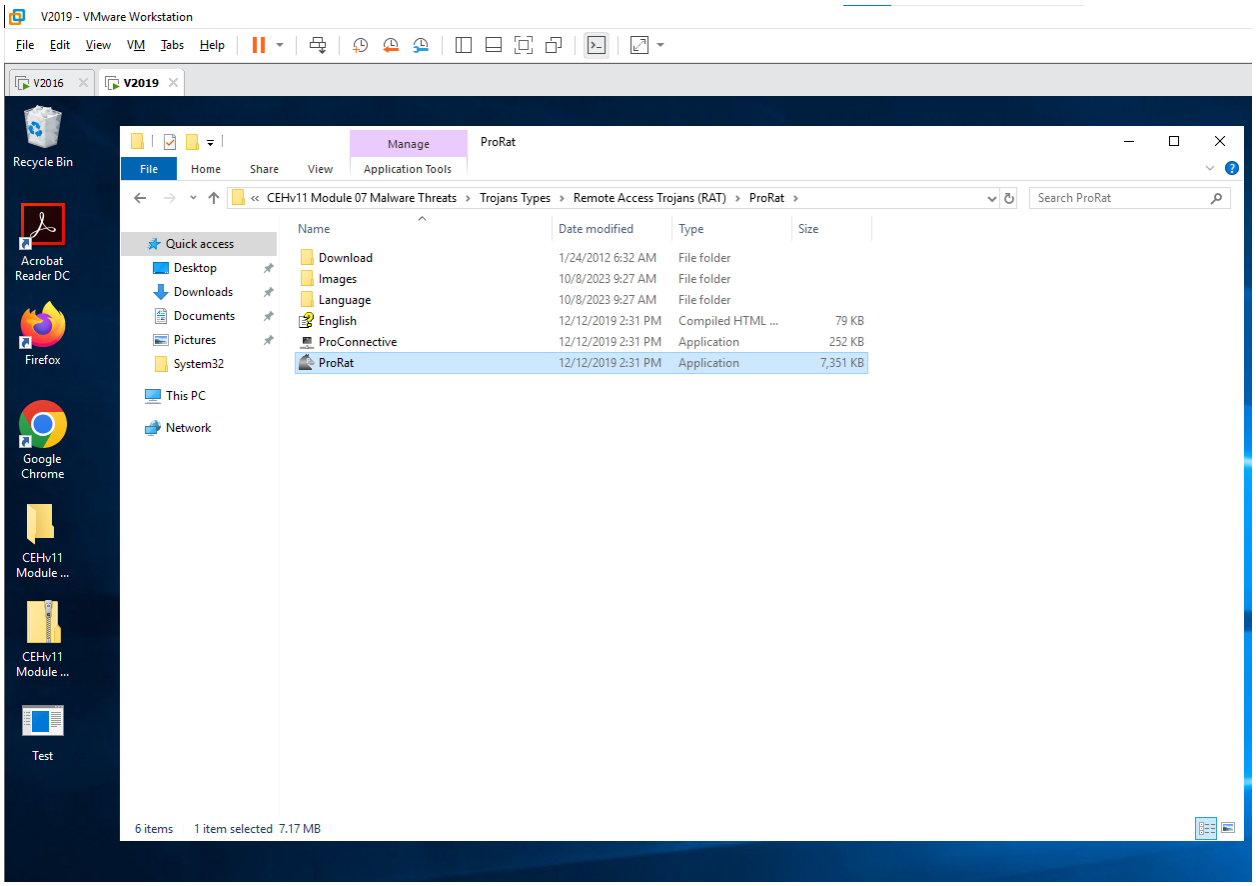

V2010
V2016
Manage
SwayzCryptor
File
Home
Share
View
Application Tools
« CEH › Tools › CEHv11 Module 07 Malware Threats › Crypters › SwayzCryptor ›
Search SwayzCryptor
Desktop
Downloads
Documents
Pictures
CEH
config
Music
Snow
OneDrive - Persor
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (E:)
Name
Date modified
Type
Size
building
10/8/2023 5:27 PM
File folder
SwayzCryptor.exe
9/2/2014 1:06 PM
Application
2,304 KB
File
Icon
Bind
Extension
E:\CEH\Test.exe
Icon
Bind
(.png)
Obfuscate
Start up
Mutex
Disable UAC
Require Admin
SWAYZ CRYPTOR
Encrypt
Minimize
Close
Status: Finished. Your file has been saved to: C:\Users\quang\Desktop\CryptedFile.exe

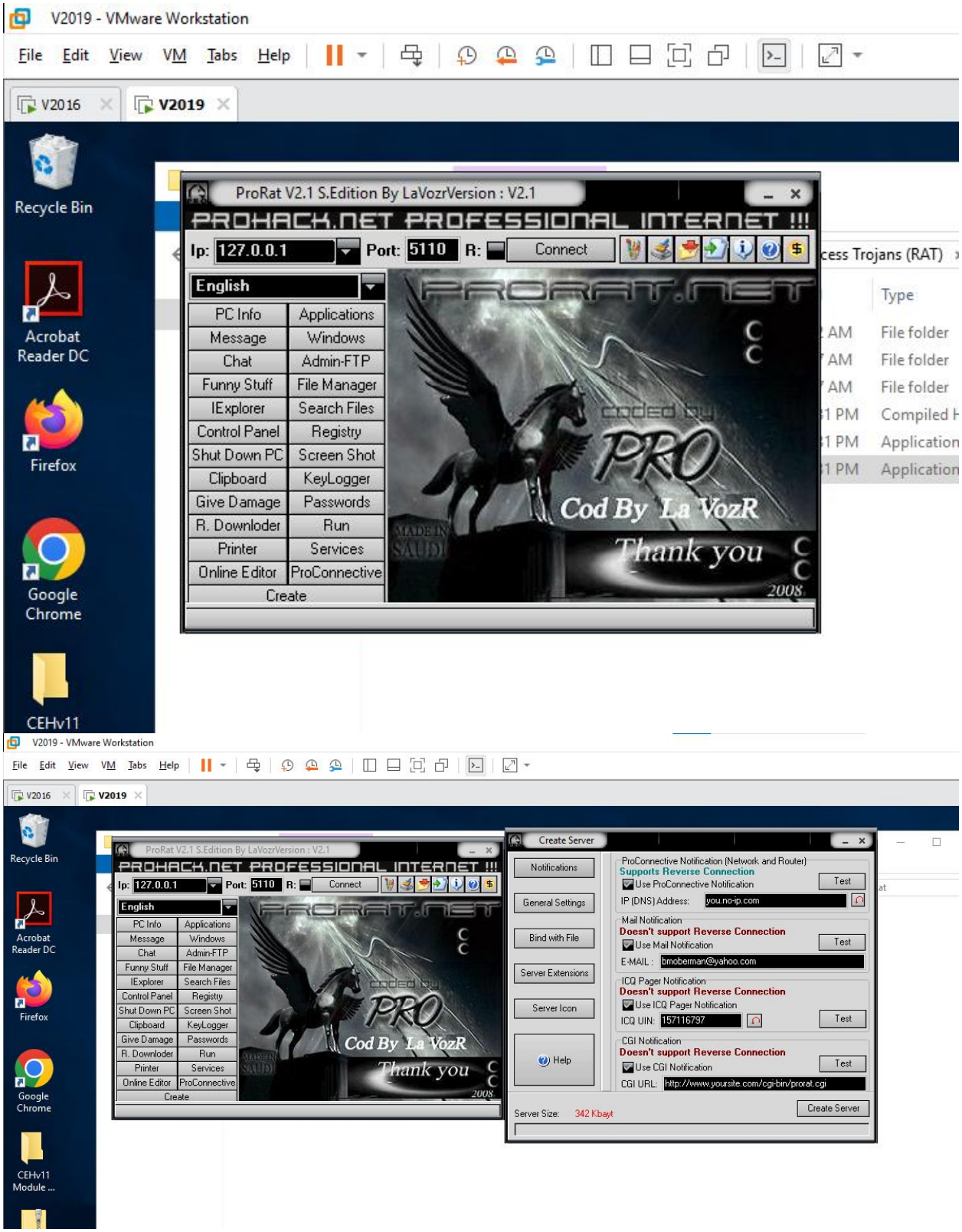


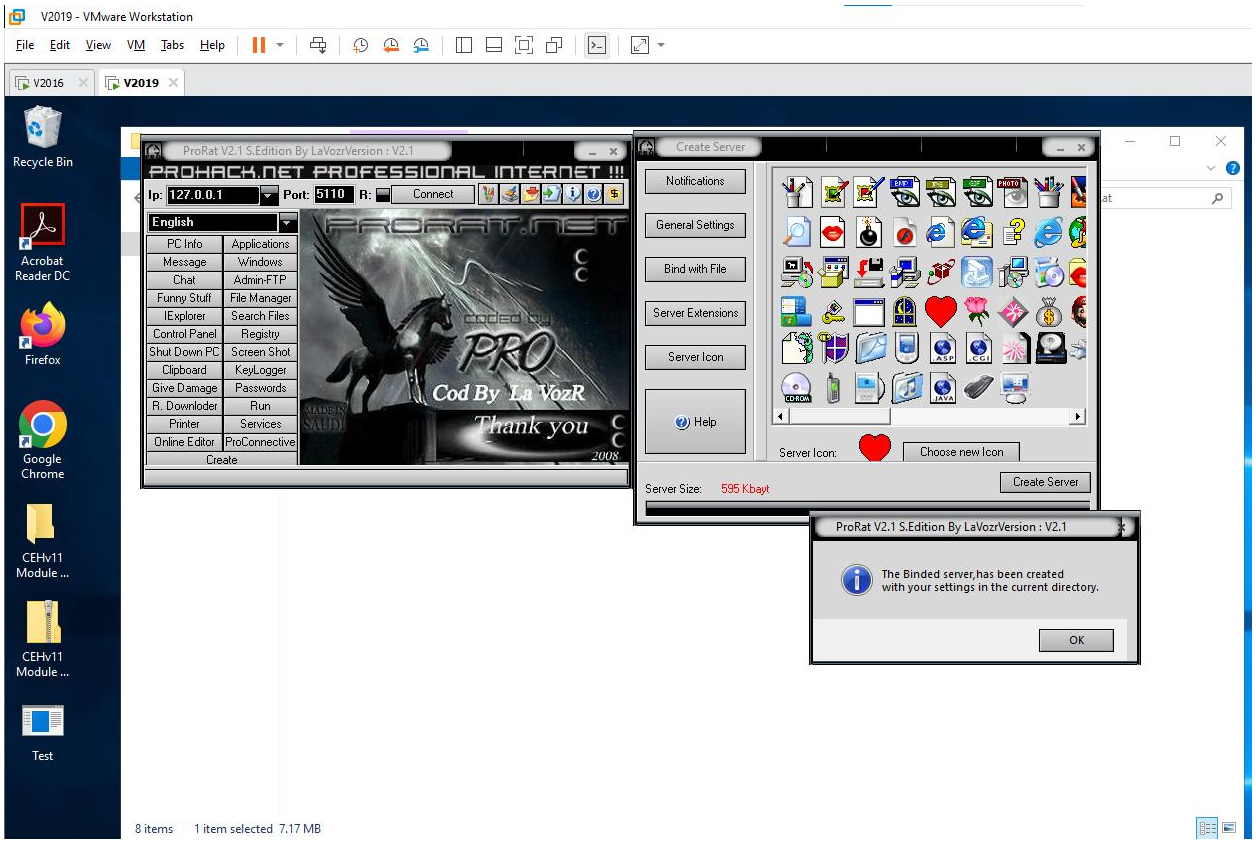


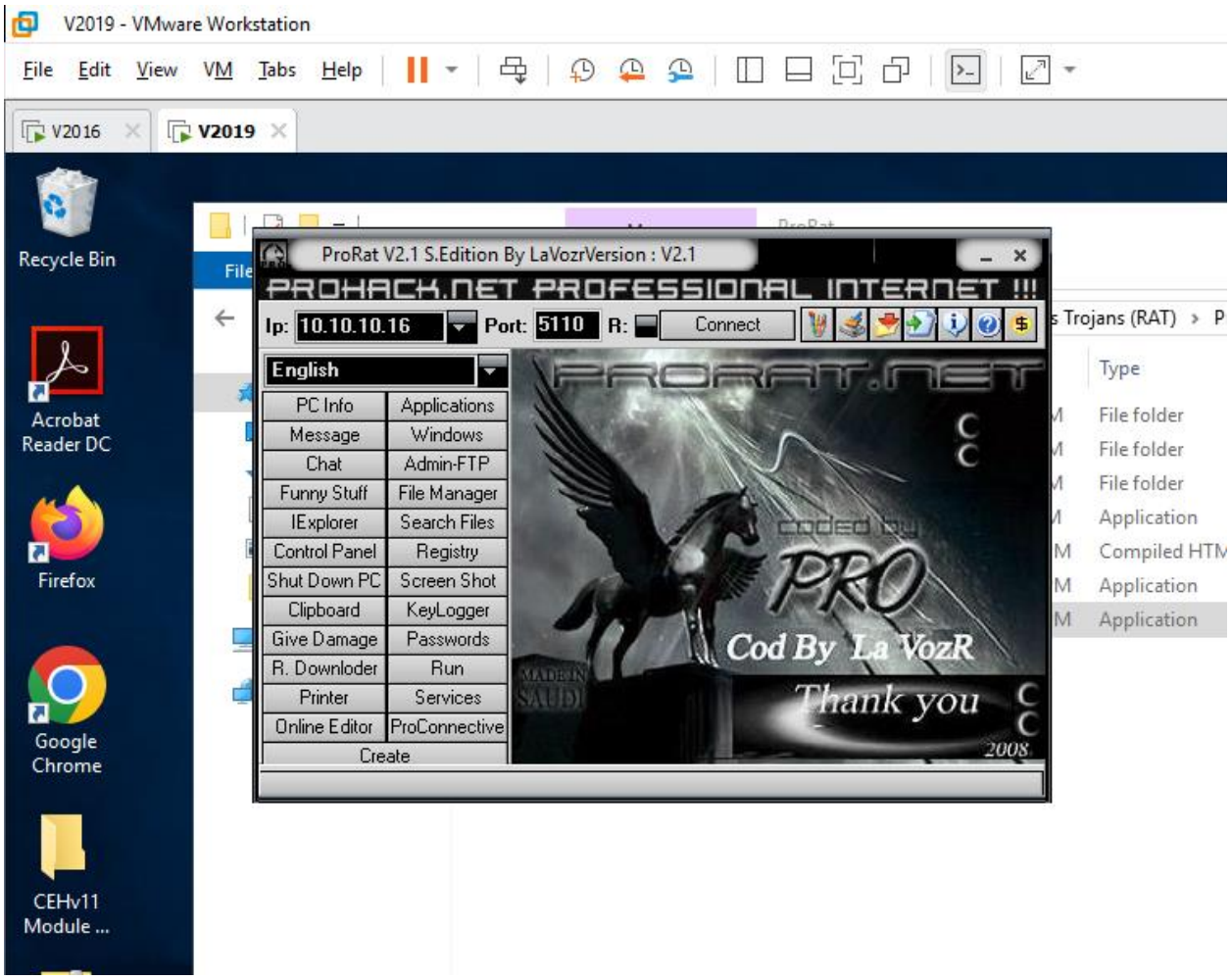
1.3 Create a Server using ProRat Tool

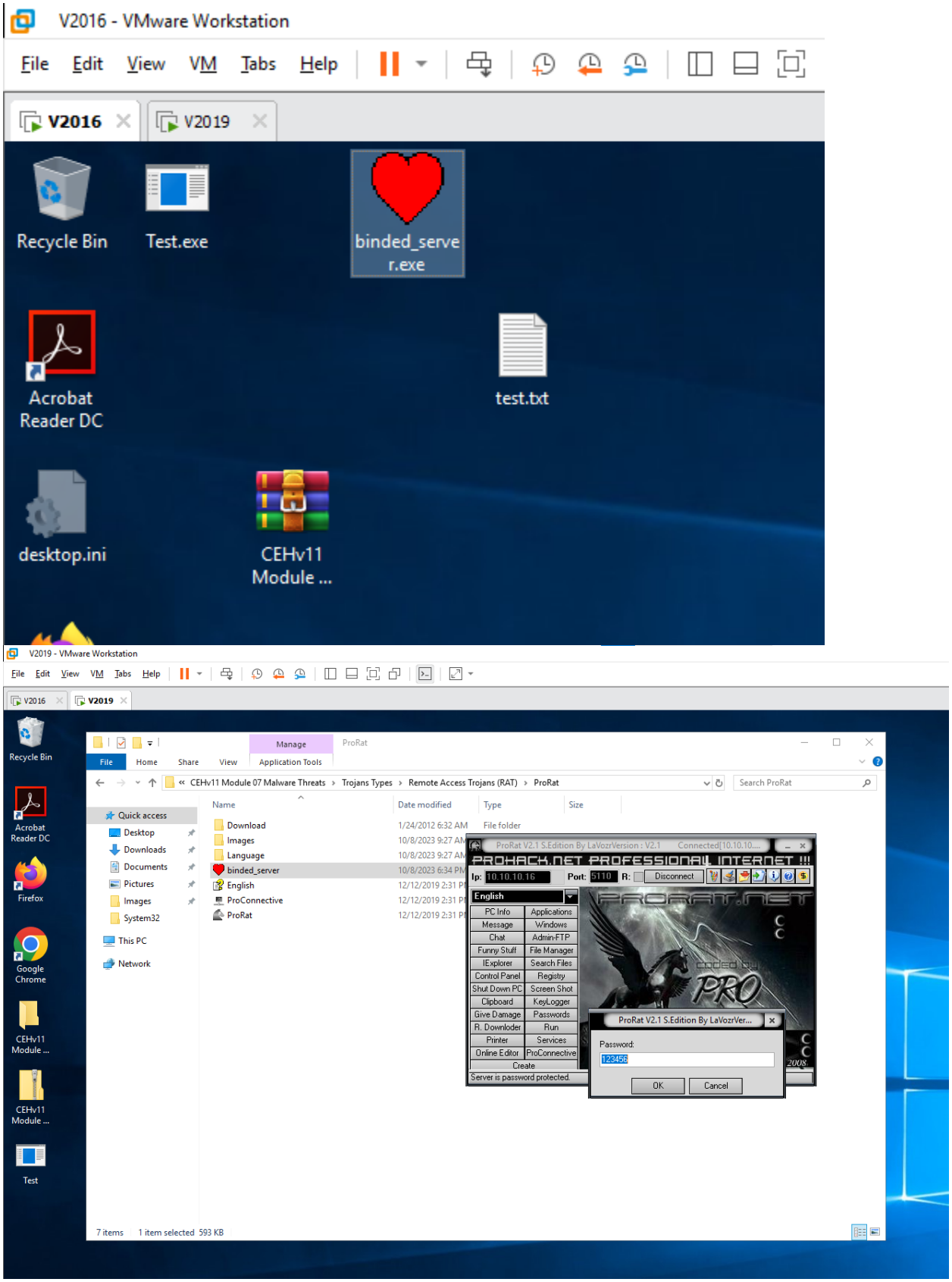
- Open Windows 10

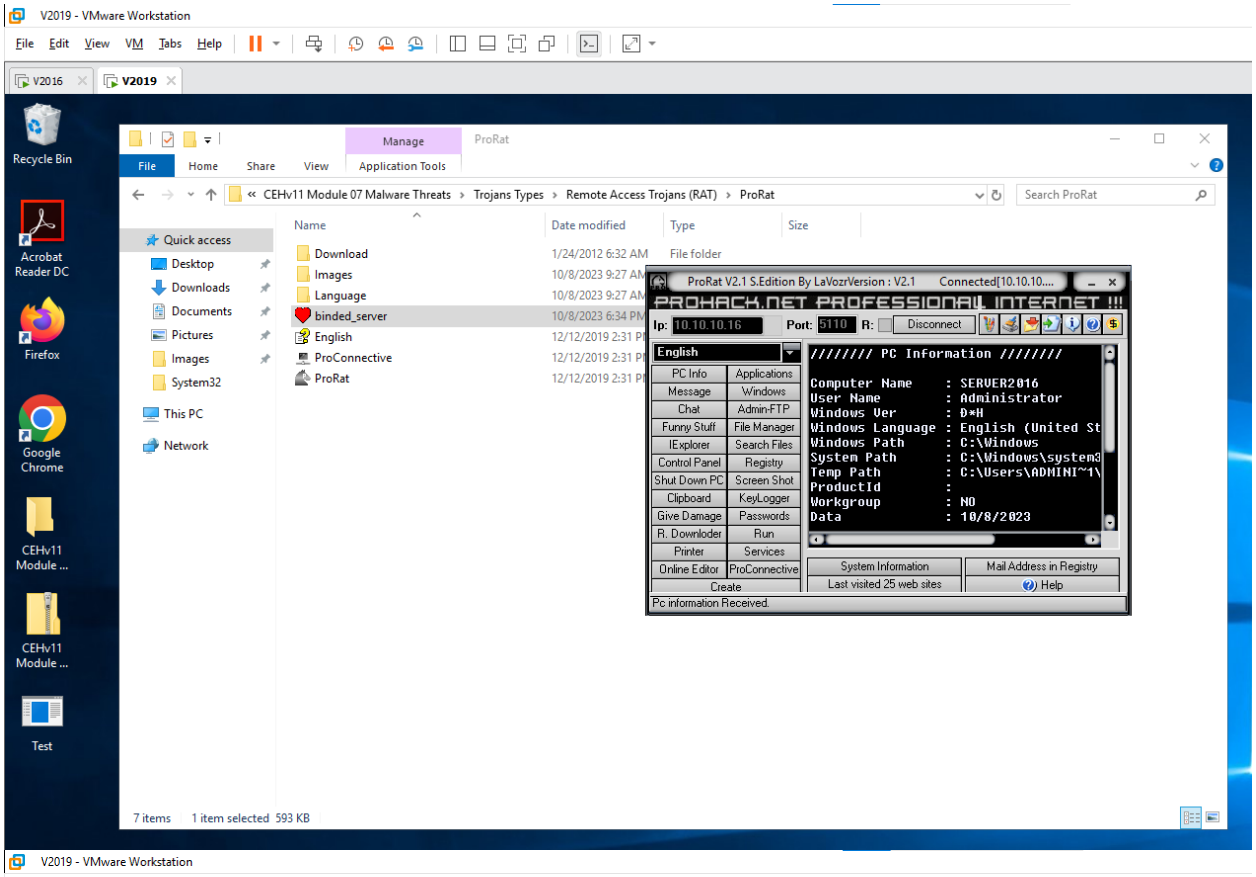

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
Manage
ProRat
File Home Share View Application Tools
« CEHv11 Module 07 Malware Threats › Trojans Types › Remote Access Trojans (RAT) › ProRat ›
Search ProRat
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name Date modified Type Size
Download 1/24/2012 6:32 AM File folder
Images 10/8/2023 9:27 AM File folder
Language 10/8/2023 9:27 AM File folder
English 12/12/2019 2:31 PM Compiled HTML ... 79 KB
ProConnective 12/12/2019 2:31 PM Application 252 KB
ProRat 12/12/2019 2:31 PM Application 7,351 KB
6 items 1 item selected 7.17 MB

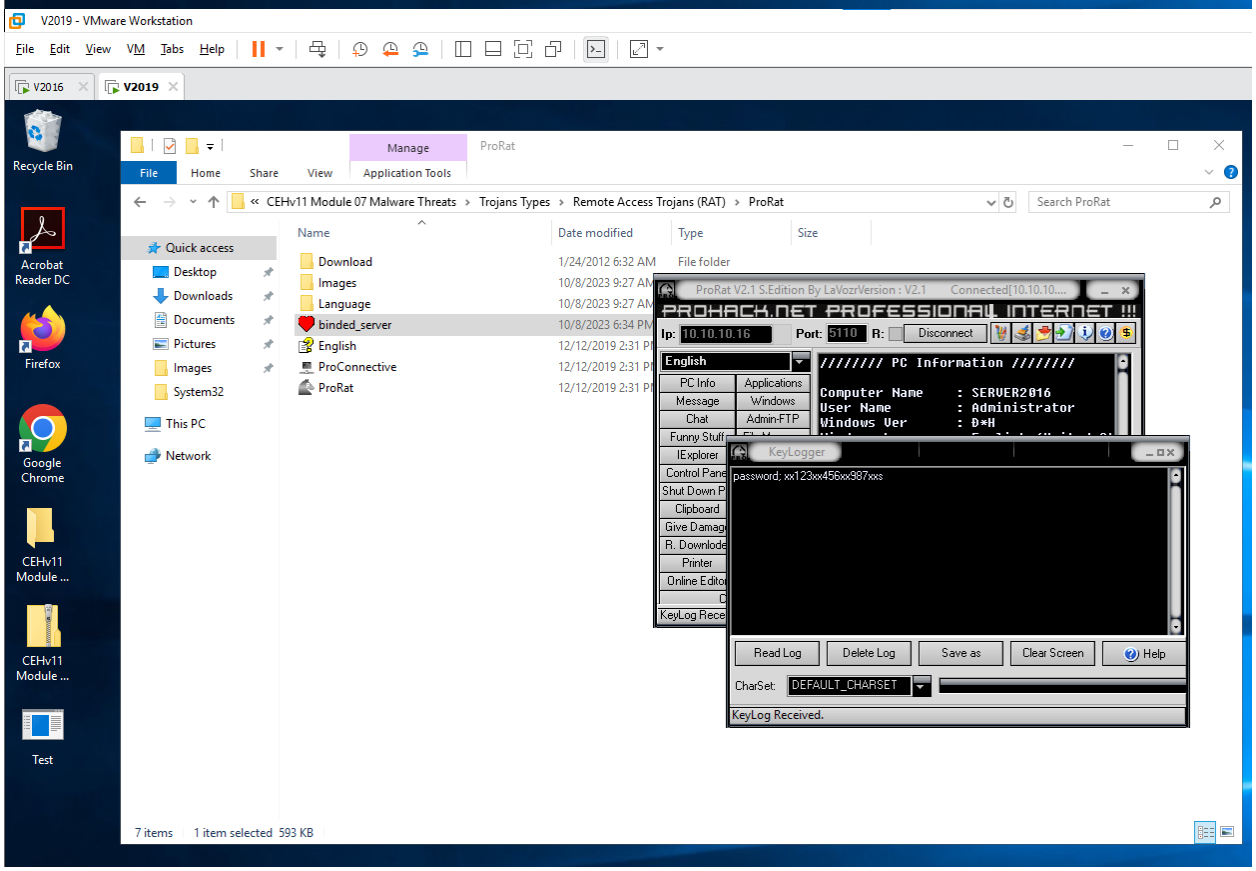

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11
ProRat V2.1 S.Edition By LaVozrVersion : V2.1
PROHACK.NET PROFESSIONAL INTERNET !!!
Ip: 127.0.0.1
Port: 5110
R:
Connect
English
PC Info
Applications
Message
Windows
Chat
Admin-FTP
Funny Stuff
File Manager
IExplorer
Search Files
Control Panel
Registry
Shut Down PC
Screen Shot
Clipboard
KeyLogger
Give Damage
Passwords
R. Downloder
Run
Printer
Services
Online Editor
ProConnective
Create
PRORAT.NET
coded by
PRO
Cod By La VozR
Thank you
2008
Type
File folder
Compiled H
Application
Create Server
Notifications
General Settings
Bind with File
Server Extensions
Server Icon
Help
ProConnective Notification (Network and Router)
Supports Reverse Connection
Use ProConnective Notification
Test
IP (DNS) Address:
you.no-ip.com
Mail Notification
Doesn't support Reverse Connection
Use Mail Notification
E-MAIL :
bmoberman@yahoo.com
ICQ Pager Notification
Use ICQ Pager Notification
ICQ UIN:
157116797
CGI Notification
Use CGI Notification
CGI URL:
http://www.yoursite.com/cgi-bin/prorat.cgi
Server Size:
342 Kbayt
Create Server

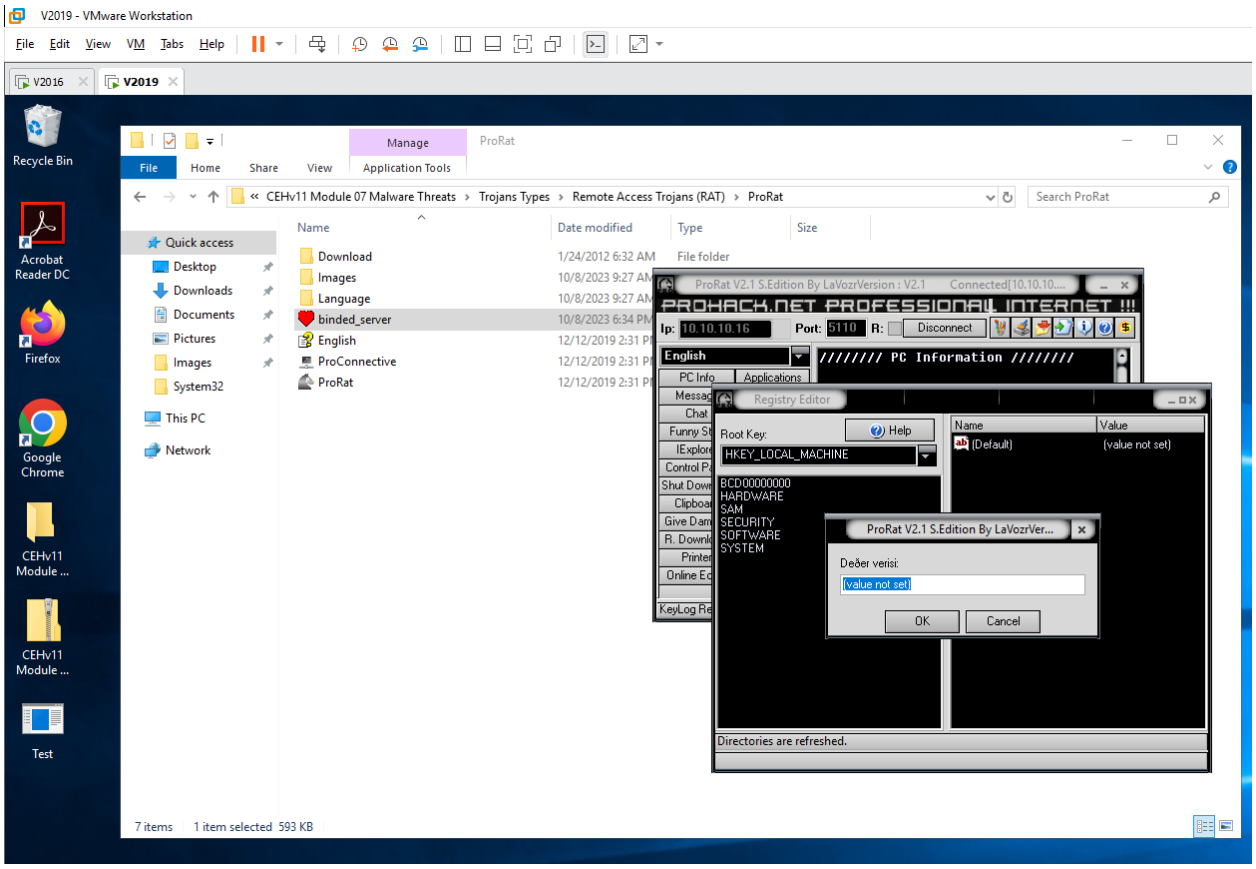

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
ProRat V2.1 S.Edition By LaVozrVersion : V2.1
PROHACK.NET PROFESSIONAL INTERNET !!!
Ip: 127.0.0.1
Port: 5110
R:
Connect
English
PC Info
Applications
Message
Windows
Chat
Admin-FTP
Funny Stuff
File Manager
IExplorer
Search Files
Control Panel
Registry
Shut Down PC
Screen Shot
Clipboard
KeyLogger
Give Damage
Passwords
R. Downloder
Run
Printer
Services
Online Editor
ProConnective
Create
PRORAT.NET
coded by
PRO
Cod By La VozR
Thank you
2008
Create Server
Notifications
General Settings
Bind with File
Server Extensions
Server Icon
Help
Server Icon:
Choose new Icon
Server Size:
595 Kbayt
Create Server
ProRat V2.1 S.Edition By LaVozrVersion : V2.1
The Binded server,has been created
with your settings in the current directory.
OK
8 items
1 item selected 7.17 MB


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
ProRat V2.1 S.Edition By LaVozrVersion : V2.1
PROHACK.NET PROFESSIONAL INTERNET !!!
Ip: 10.10.10.16
Port: 5110
R:
Connect
English
PC Info
Applications
Message
Windows
Chat
Admin-FTP
Funny Stuff
File Manager
IExplorer
Search Files
Control Panel
Registry
Shut Down PC
Screen Shot
Clipboard
KeyLogger
Give Damage
Passwords
R. Downloder
Run
Printer
Services
Online Editor
ProConnective
Create
PRORAT.NET
coded by
PRO
Cod By La VozR
Thank you
2008
Type
File folder
File folder
File folder
Application
Compiled HTM
Application
Application


V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Test.exe
binded_server.exe
Acrobat Reader DC
test.txt
desktop.ini
CEHv11 Module ...
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
Manage
ProRat
File Home Share View Application Tools
CEHv11 Module 07 Malware Threats › Trojans Types › Remote Access Trojans (RAT) › ProRat
Search ProRat
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
Download 1/24/2012 6:32 AM File folder
Images 10/8/2023 9:27 AM
Language 10/8/2023 9:27 AM
binded_server 10/8/2023 6:34 PM
English 12/12/2019 2:31 PM
ProConnective 12/12/2019 2:31 PM
ProRat 12/12/2019 2:31 PM
7 items 1 item selected 593 KB
ProRat V2.1 S.Edition By LaVozrVersion : V2.1 Connected[10.10.10....
PROHACK.NET PROFESSIONAL INTERNET !!!
Ip: 10.10.10.16 Port: 5110 R: Disconnect
English
PC Info Applications
Message Windows
Chat Admin-FTP
Funny Stuff File Manager
IExplorer Search Files
Control Panel Registry
Shut Down PC Screen Shot
Clipboard KeyLogger
Give Damage Passwords
R. Downloader Run
Printer Services
Online Editor ProConnective
Create
Server is password protected.
PRORAT.NET
coded by
PRO
ProRat V2.1 S.Edition By LaVozrVer...
Password:
123456
OK
Cancel

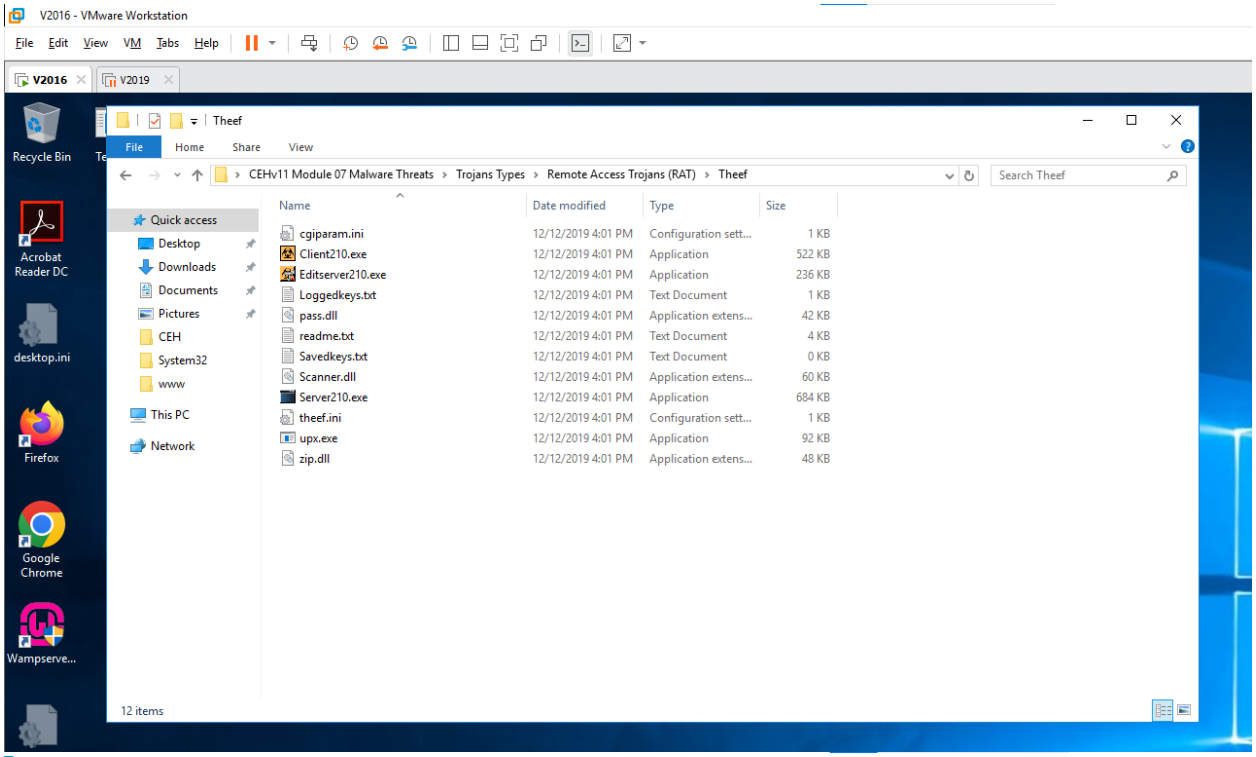

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
Manage
ProRat
File Home Share View Application Tools
« CEHv11 Module 07 Malware Threats › Trojans Types › Remote Access Trojans (RAT) › ProRat
Search ProRat
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
Download 1/24/2012 6:32 AM File folder
Images 10/8/2023 9:27 AM
Language 10/8/2023 9:27 AM
binded_server 10/8/2023 6:34 PM
English 12/12/2019 2:31 PM
ProConnective 12/12/2019 2:31 PM
ProRat 12/12/2019 2:31 PM
ProRat V2.1 S.Edition By LaVozrVersion : V2.1 Connected[10.10.10....
PROHACK.NET PROFESSIONAL INTERNET !!!
Ip: 10.10.10.16 Port: 5110 R: Disconnect
English
PC Info Applications
Message Windows
Chat Admin-FTP
Funny Stuff File Manager
IExplorer Search Files
Control Panel Registry
Shut Down PC Screen Shot
Clipboard KeyLogger
Give Damage Passwords
R. Downloder Run
Printer Services
Online Editor ProConnective
Create
//////// PC Information ////////
Computer Name : SERVER2016
User Name : Administrator
Windows Ver : Ð*H
Windows Language : English (United St
Windows Path : C:\Windows
System Path : C:\Windows\system3
Temp Path : C:\Users\ADMINI~1\
ProductId :
Workgroup : NO
Data : 10/8/2023
System Information
Mail Address in Registry
Last visited 25 web sites
Help
Pc information Received.
7 items 1 item selected 593 KB

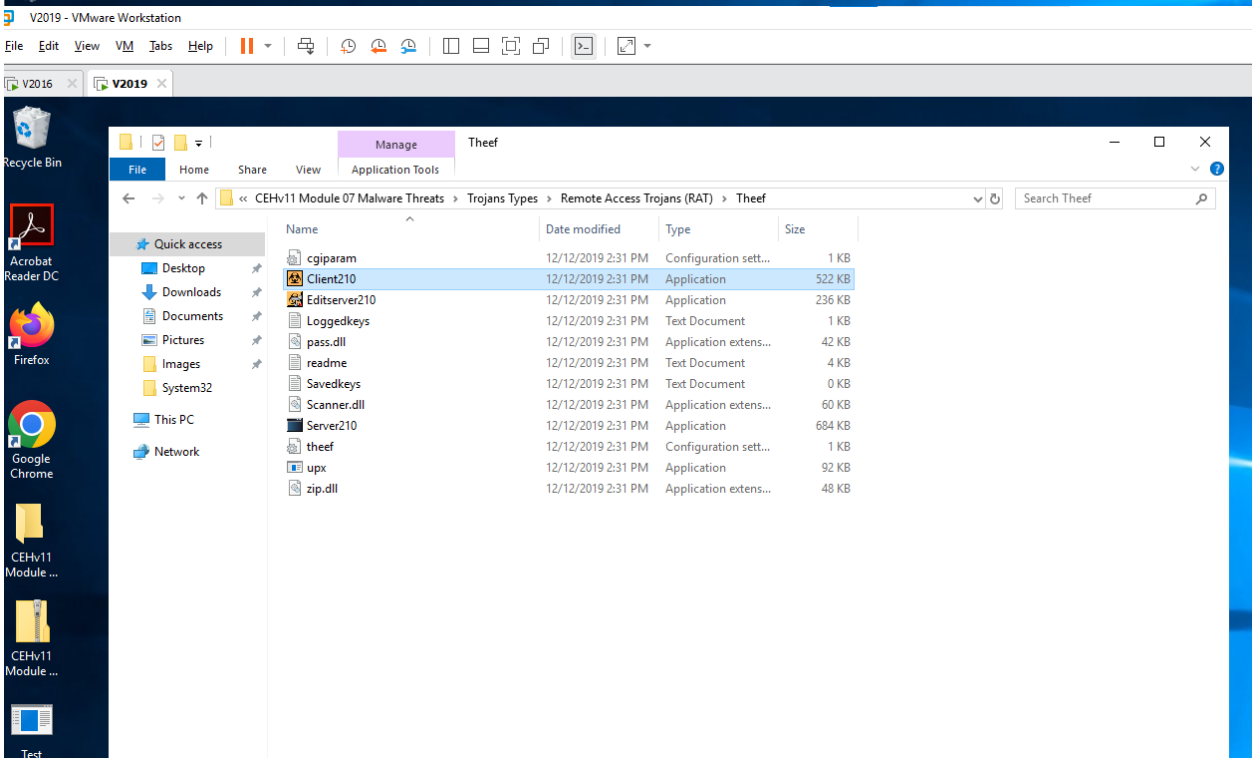

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
Manage
ProRat
File Home Share View Application Tools
« CEHv11 Module 07 Malware Threats › Trojans Types › Remote Access Trojans (RAT) › ProRat
Search ProRat
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
Download 1/24/2012 6:32 AM File folder
Images 10/8/2023 9:27 AM
Language 10/8/2023 9:27 AM
binded_server 10/8/2023 6:34 PM
English 12/12/2019 2:31 PM
ProConnective 12/12/2019 2:31 PM
ProRat 12/12/2019 2:31 PM
ProRat V2.1 S.Edition By LaVozrVersion : V2.1 Connected[10.10.10....
PROHACK.NET PROFESSIONAL INTERNET !!!
Ip: 10.10.10.16 Port: 5110 R: Disconnect
English
PC Info Applications
Message Windows
Chat Admin-FTP
//////// PC Information ////////
Computer Name : SERVER2016
User Name : Administrator
Windows Ver : Ð*H
KeyLogger
password: xx123xx456xx987xxs
Read Log
Delete Log
Save as
Clear Screen
Help
CharSet: DEFAULT_CHARSET
KeyLog Received.
7 items 1 item selected 593 KB

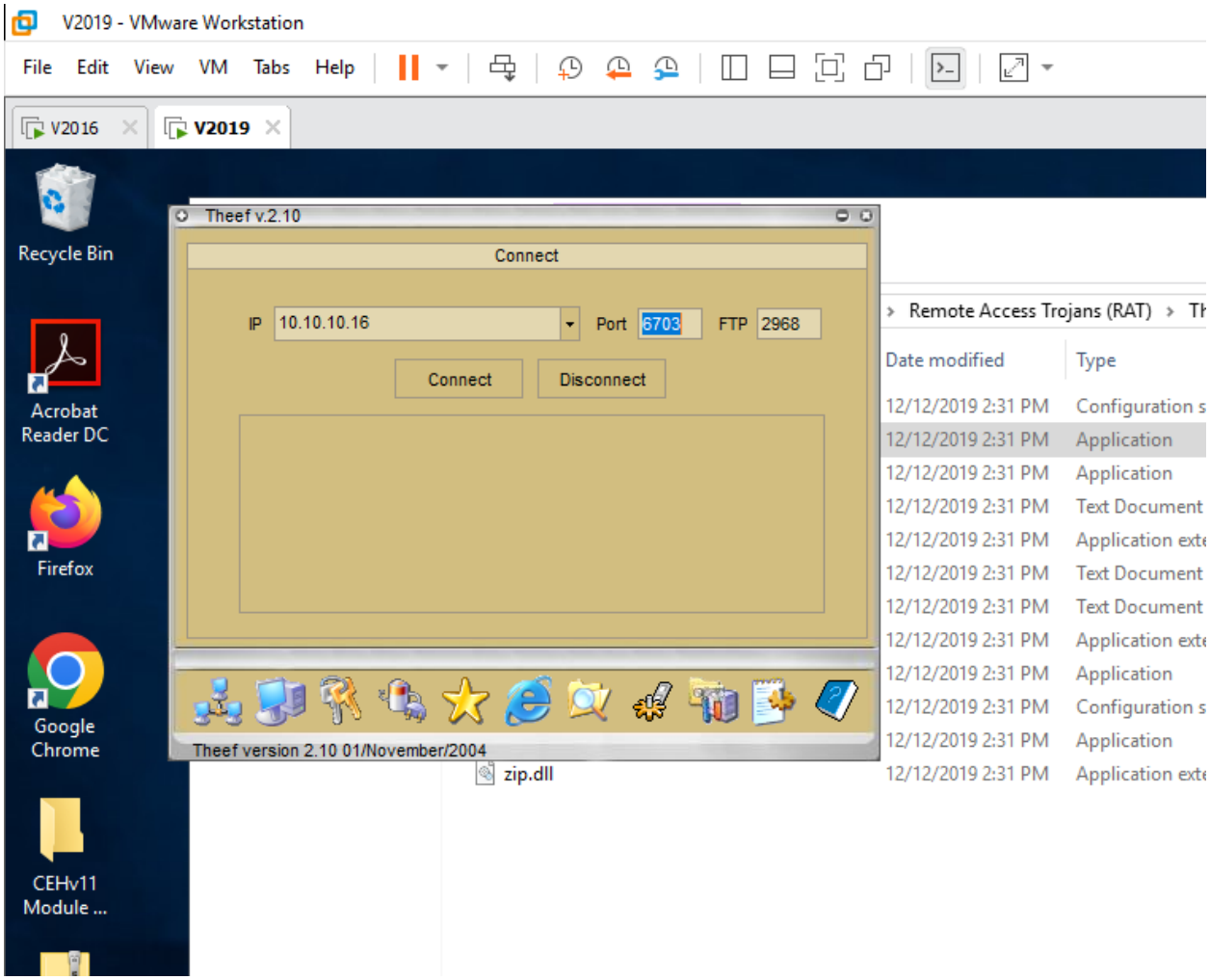


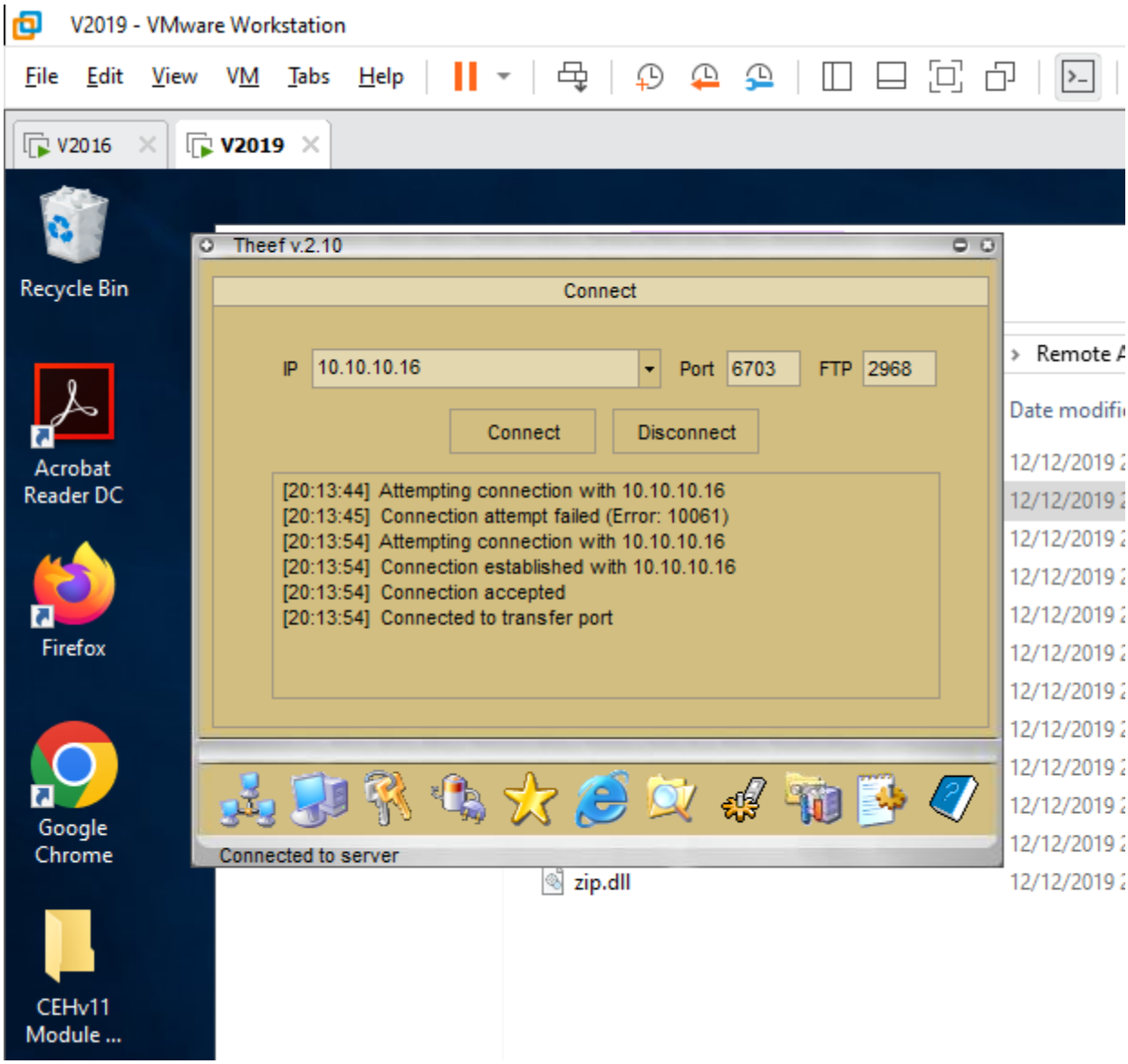
1.4 Create a Trojan Server using Theef RAT Trojan

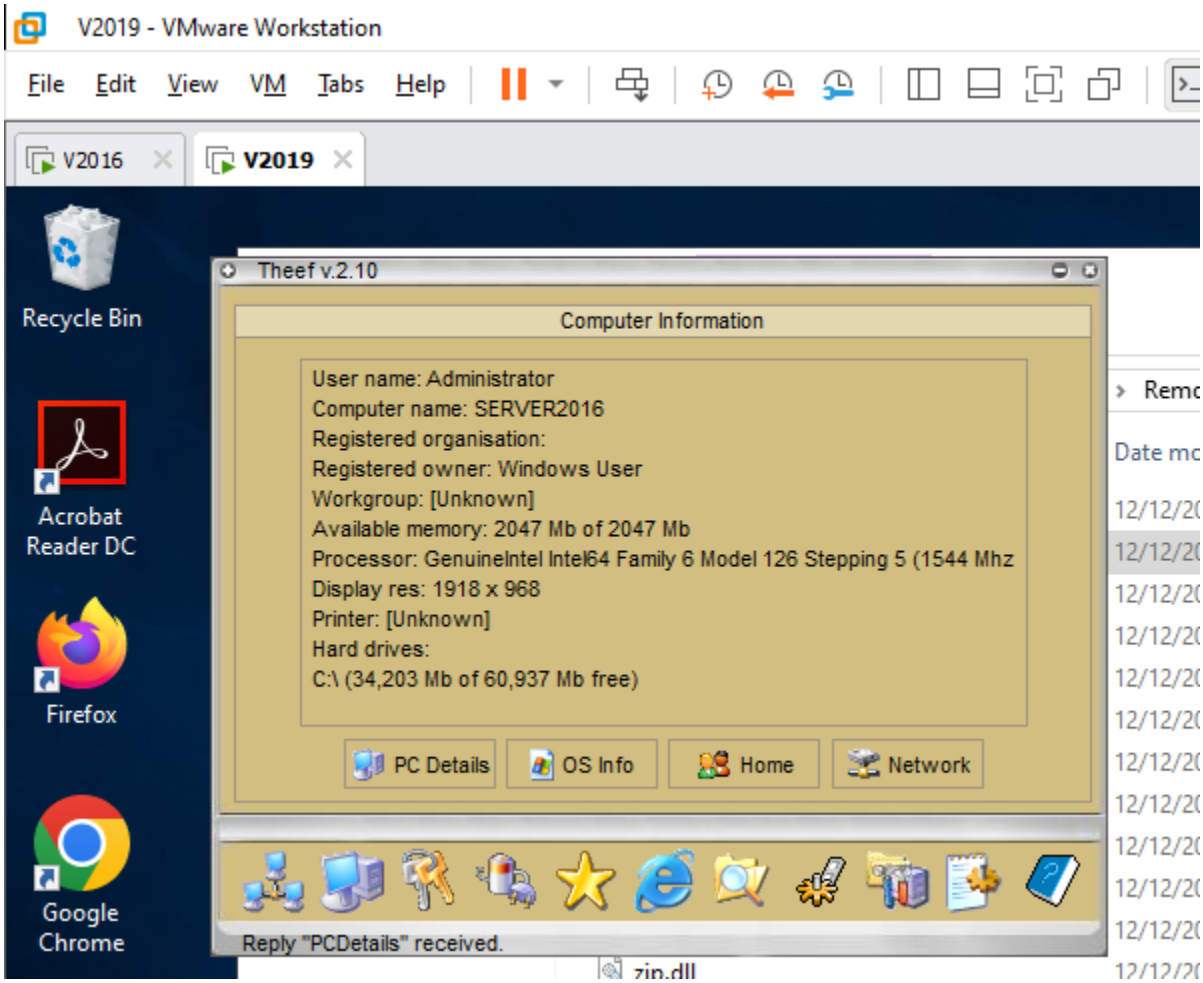
- Open Windows 10, Windows Server 2016

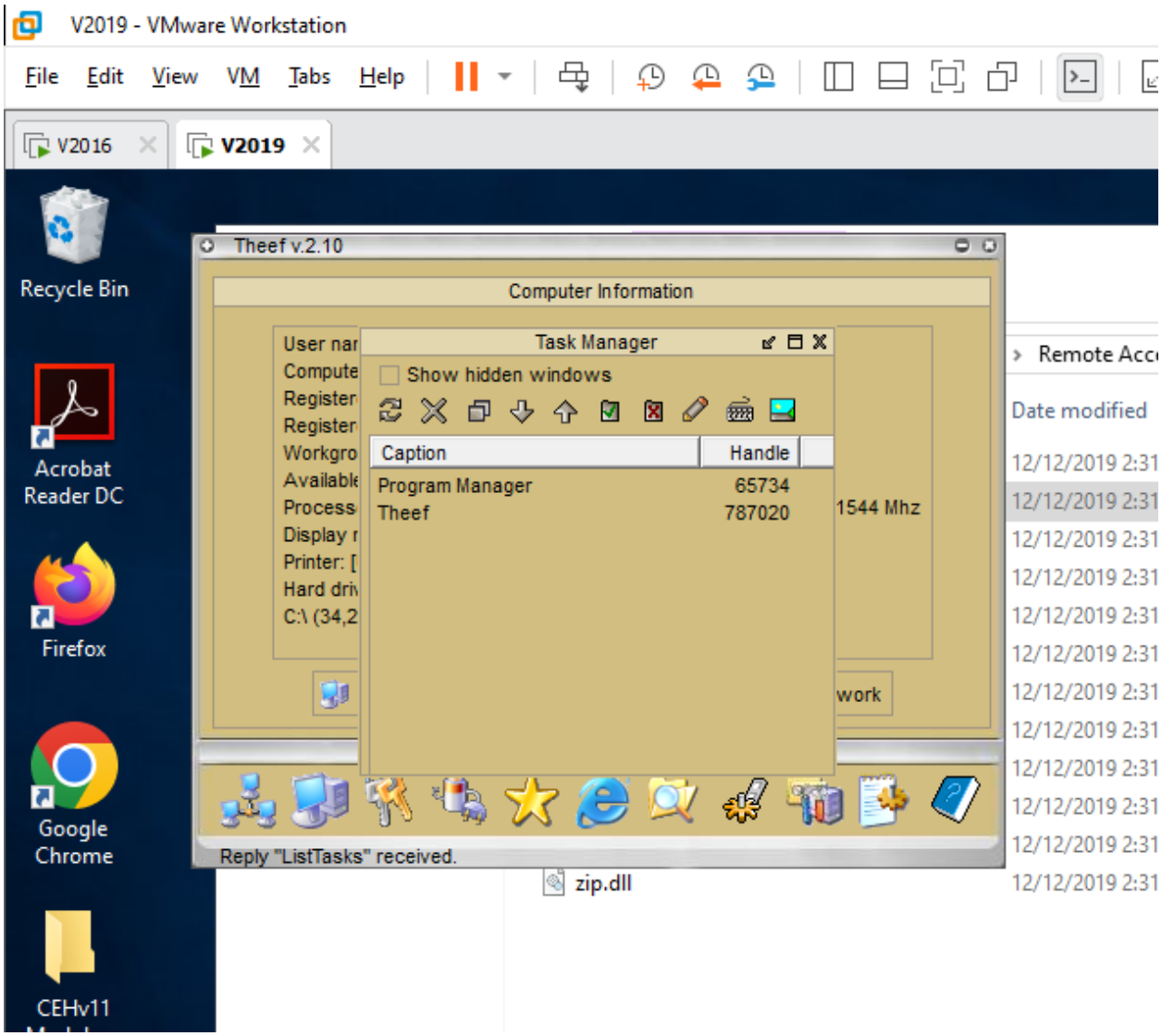

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Theef
File Home Share View
CEHv11 Module 07 Malware Threats › Trojans Types › Remote Access Trojans (RAT) › Theef
Search Theef
Quick access
Desktop
Downloads
Documents
Pictures
CEH
System32
www
This PC
Network
Name
Date modified
Type
Size
cgiparam.ini 12/12/2019 4:01 PM Configuration sett... 1 KB
Client210.exe 12/12/2019 4:01 PM Application 522 KB
Editserver210.exe 12/12/2019 4:01 PM Application 236 KB
Loggedkeys.txt 12/12/2019 4:01 PM Text Document 1 KB
pass.dll 12/12/2019 4:01 PM Application extens... 42 KB
readme.txt 12/12/2019 4:01 PM Text Document 4 KB
Savedkeys.txt 12/12/2019 4:01 PM Text Document 0 KB
Scanner.dll 12/12/2019 4:01 PM Application extens... 60 KB
Server210.exe 12/12/2019 4:01 PM Application 684 KB
theef.ini 12/12/2019 4:01 PM Configuration sett... 1 KB
upx.exe 12/12/2019 4:01 PM Application 92 KB
zip.dll 12/12/2019 4:01 PM Application extens... 48 KB
12 items
Recycle Bin
Acrobat Reader DC
desktop.ini
Firefox
Google Chrome
Wampserve...

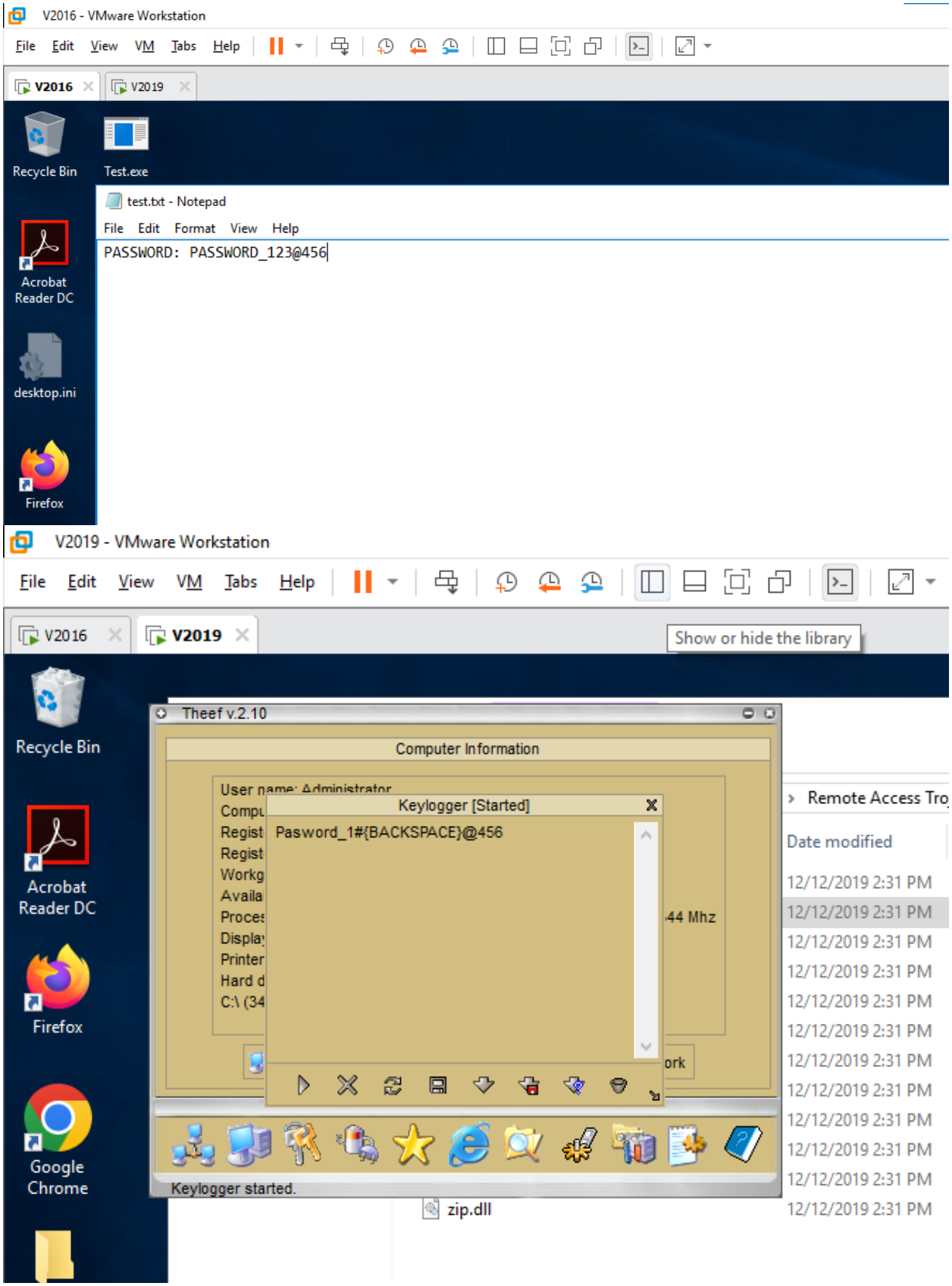

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Manage
Theef
File Home Share View Application Tools
« CEHv11 Module 07 Malware Threats › Trojans Types › Remote Access Trojans (RAT) › Theef
Search Theef
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
cgiparam 12/12/2019 2:31 PM Configuration sett... 1 KB
Client210 12/12/2019 2:31 PM Application 522 KB
Editserver210 12/12/2019 2:31 PM Application 236 KB
Loggedkeys 12/12/2019 2:31 PM Text Document 1 KB
pass.dll 12/12/2019 2:31 PM Application extens... 42 KB
readme 12/12/2019 2:31 PM Text Document 4 KB
Savedkeys 12/12/2019 2:31 PM Text Document 0 KB
Scanner.dll 12/12/2019 2:31 PM Application extens... 60 KB
Server210 12/12/2019 2:31 PM Application 684 KB
theef 12/12/2019 2:31 PM Configuration sett... 1 KB
upx 12/12/2019 2:31 PM Application 92 KB
zip.dll 12/12/2019 2:31 PM Application extens... 48 KB
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
Theef v.2.10
Connect
IP 10.10.10.16
Port 6703
FTP 2968
Connect
Disconnect
Theef version 2.10 01/November/2004
Remote Access Trojans (RAT)
Date modified
Type
12/12/2019 2:31 PM Configuration s
12/12/2019 2:31 PM Application
12/12/2019 2:31 PM Application
12/12/2019 2:31 PM Text Document
12/12/2019 2:31 PM Application exte
12/12/2019 2:31 PM Text Document
12/12/2019 2:31 PM Text Document
12/12/2019 2:31 PM Application exte
12/12/2019 2:31 PM Application
12/12/2019 2:31 PM Configuration s
12/12/2019 2:31 PM Application
12/12/2019 2:31 PM Application exte
zip.dll


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
Theef v.2.10
Connect
IP 10.10.10.16
Port 6703
FTP 2968
Connect
Disconnect
[20:13:44] Attempting connection with 10.10.10.16
[20:13:45] Connection attempt failed (Error: 10061)
[20:13:54] Attempting connection with 10.10.10.16
[20:13:54] Connection established with 10.10.10.16
[20:13:54] Connection accepted
[20:13:54] Connected to transfer port
Connected to server
Remote A
Date modifi
12/12/2019
zip.dll

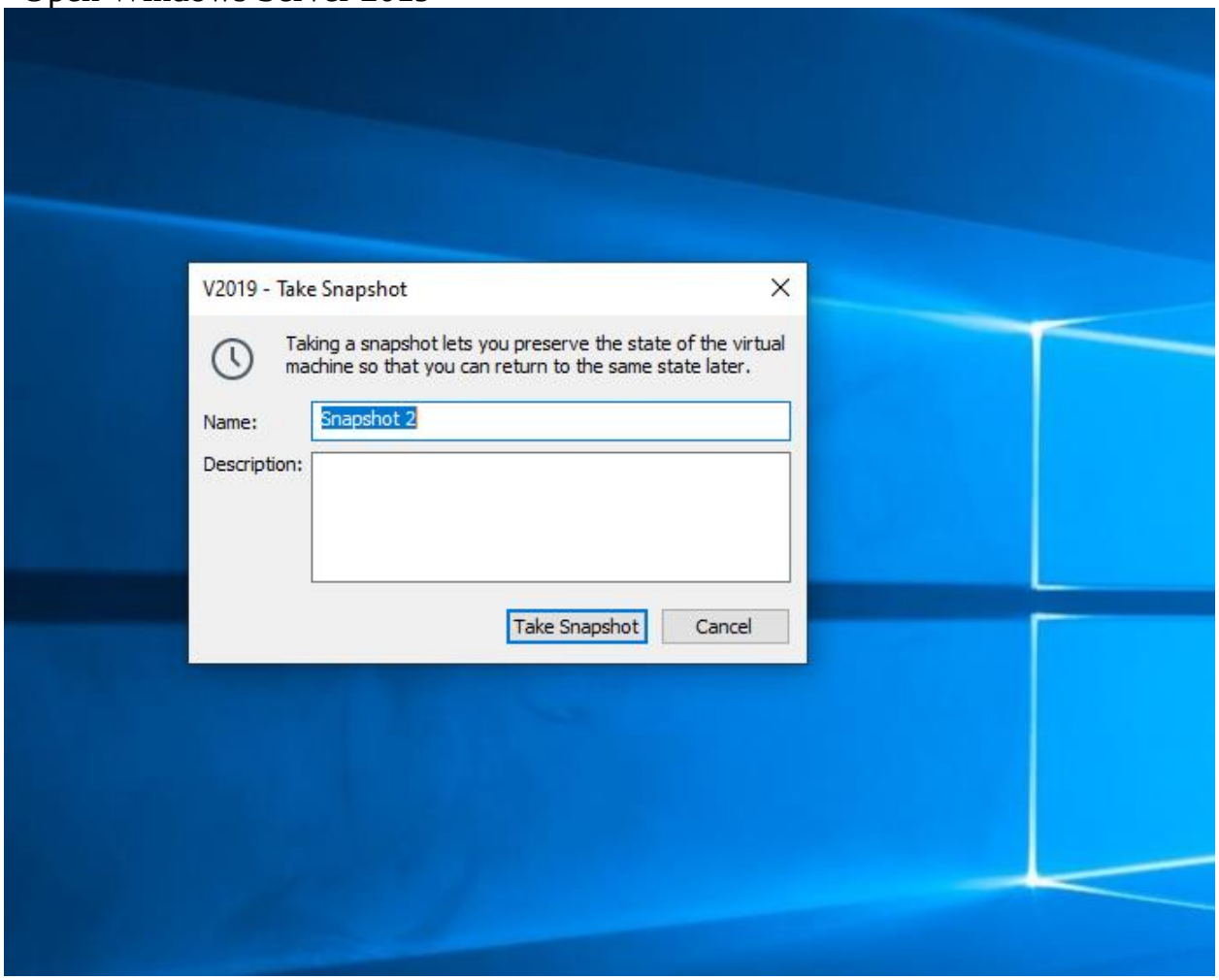

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
Theef v.2.10
Computer Information
User name: Administrator
Computer name: SERVER2016
Registered organisation:
Registered owner: Windows User
Workgroup: [Unknown]
Available memory: 2047 Mb of 2047 Mb
Processor: GenuineIntel Intel64 Family 6 Model 126 Stepping 5 (1544 Mhz
Display res: 1918 x 968
Printer: [Unknown]
Hard drives:
C:\ (34,203 Mb of 60,937 Mb free)
PC Details
OS Info
Home
Network
Reply "PCDetails" received.
zip.dll

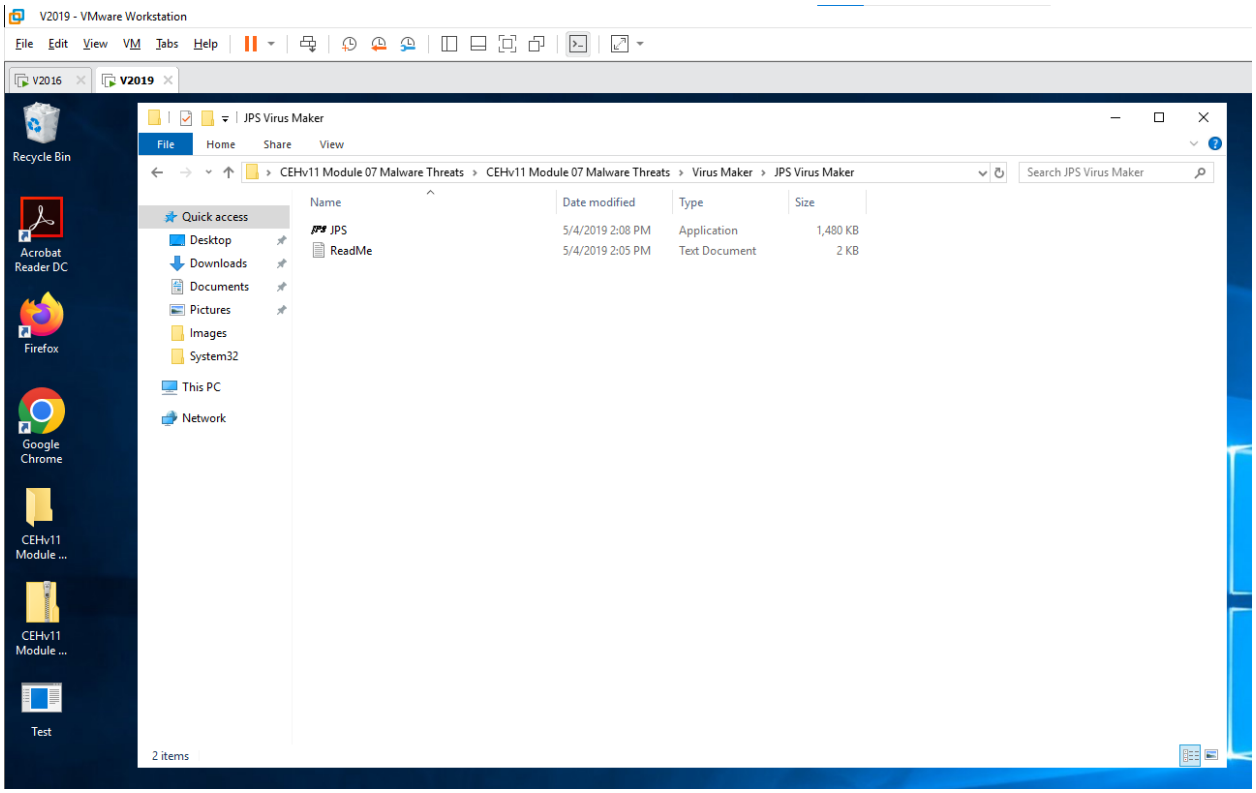

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11
Theef v.2.10
Computer Information
Task Manager
Show hidden windows
Caption
Handle
Program Manager 65734
Theef 787020
1544 Mhz
Reply "ListTasks" received.
Remote Acc
Date modified
12/12/2019 2:31
zip.dll

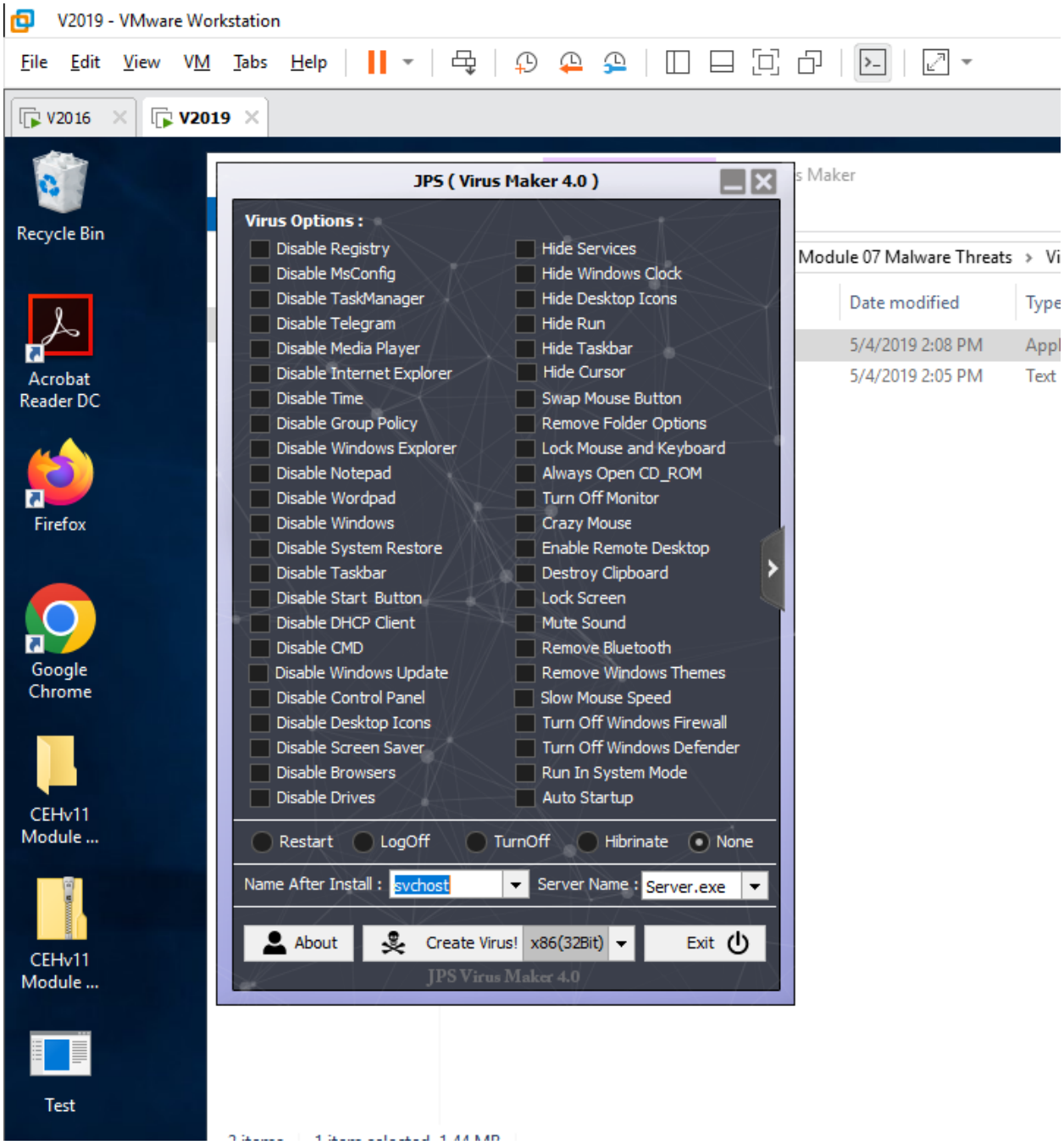

V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Test.exe
test.txt - Notepad
File Edit Format View Help
PASSWORD: PASSWORD_123@456
Acrobat Reader DC
desktop.ini
Firefox
V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Show or hide the library
Recycle Bin
Theef v.2.10
Computer Information
Keylogger [Started]
Pasword_1#{BACKSPACE}@456
Acrobat Reader DC
Firefox
Google Chrome
Keylogger started.
Remote Access Tro
Date modified
12/12/2019 2:31 PM
zip.dll

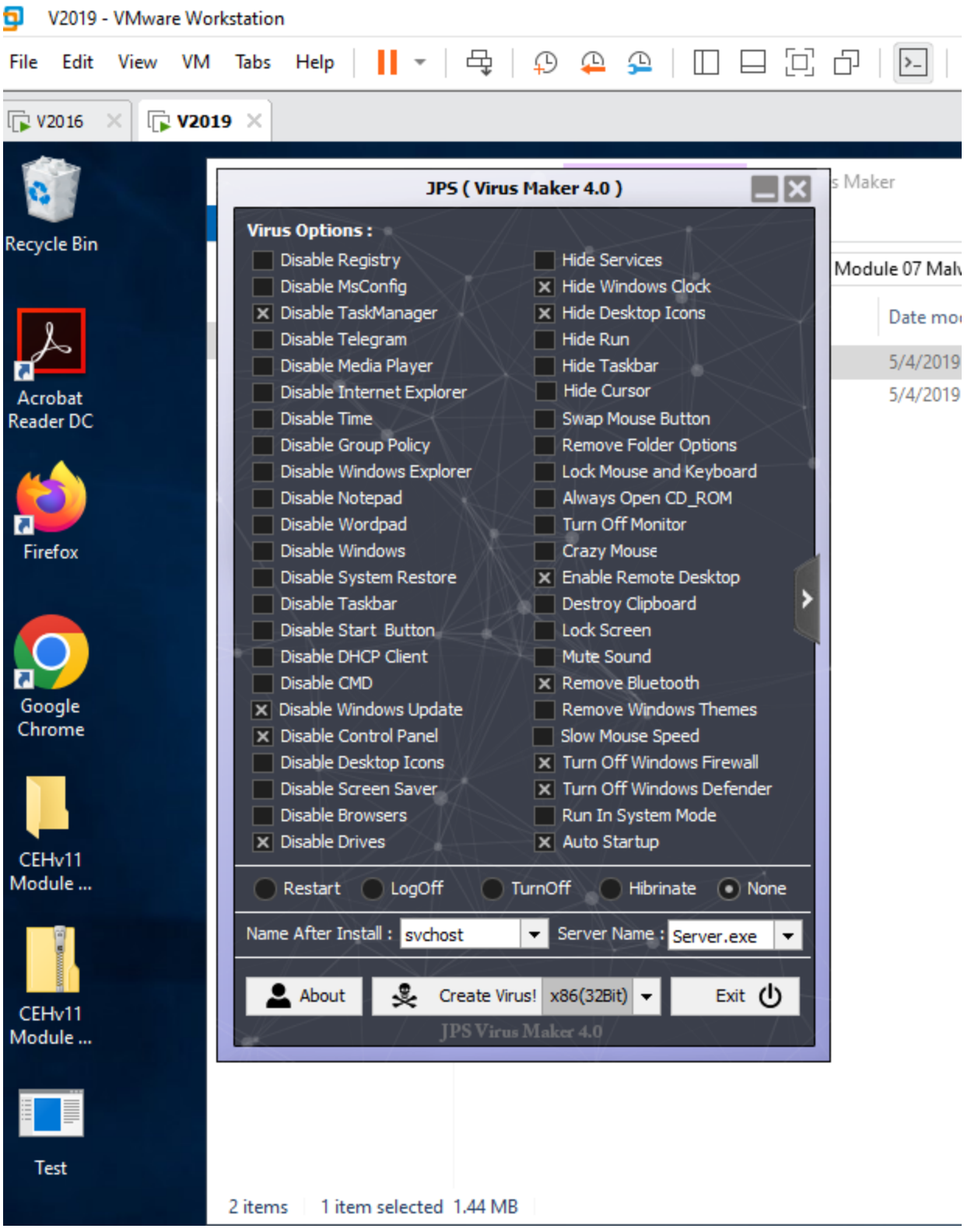
2. Infect the Target System using a Virus

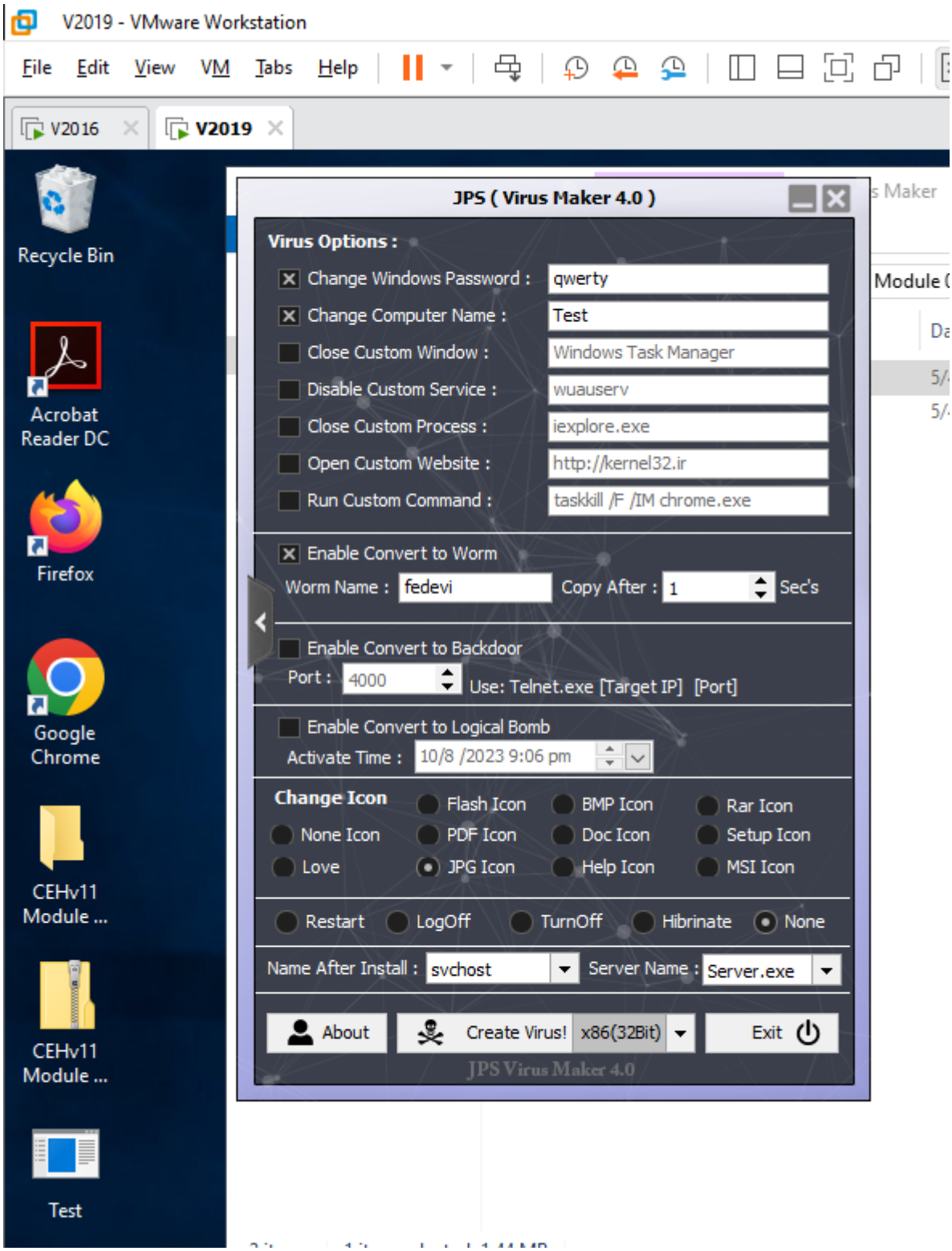
2.1 Create a Virus using the JPS Virus Maker Tool and Infect the Target System - Open Windows Server 2019

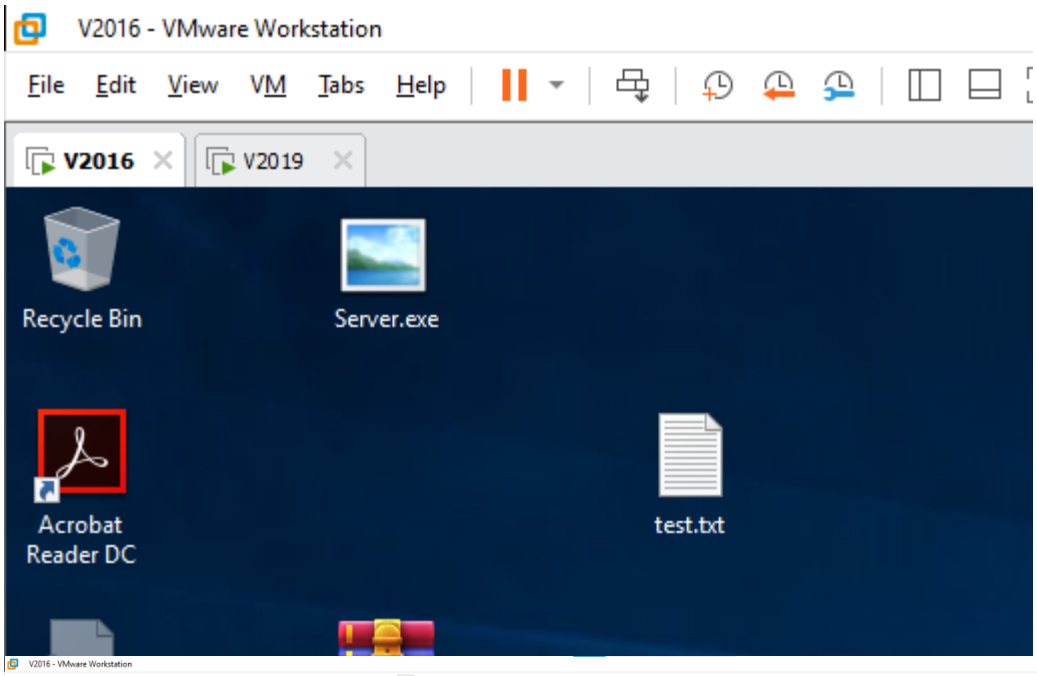


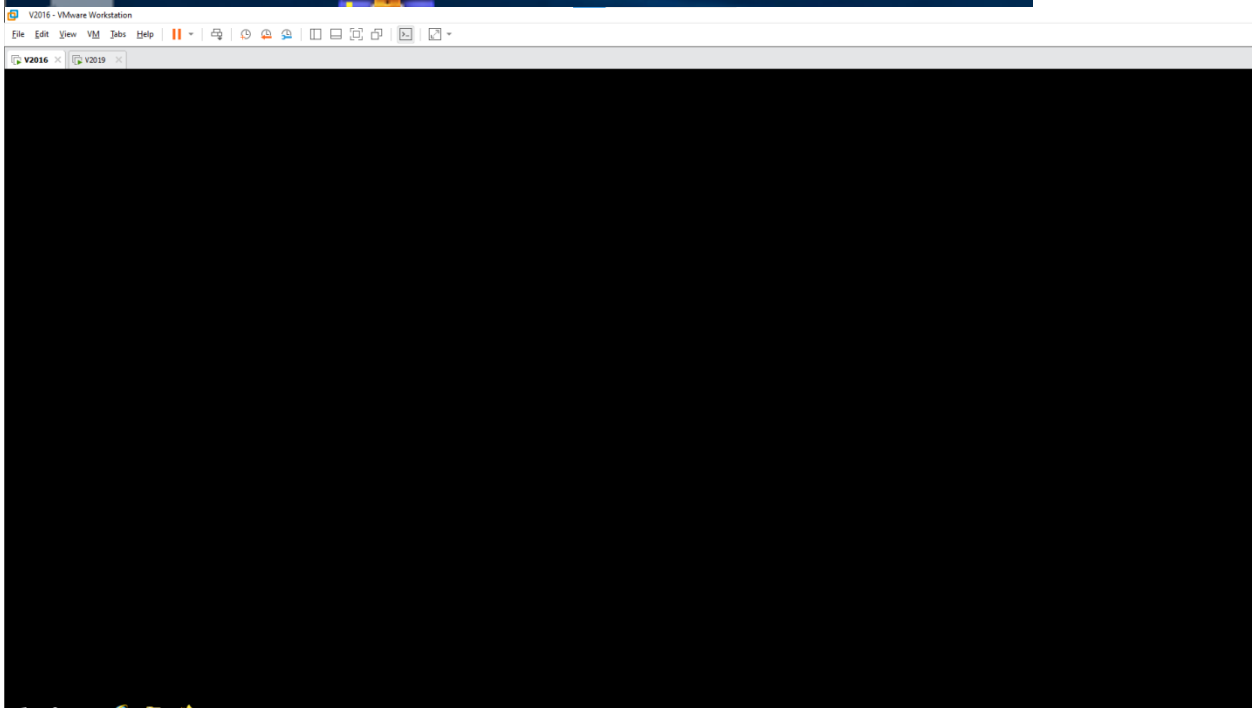

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
JPS Virus Maker
File Home Share View
CEHv11 Module 07 Malware Threats › CEHv11 Module 07 Malware Threats › Virus Maker › JPS Virus Maker
Search JPS Virus Maker
Quick access
Desktop
Downloads
Documents
Pictures
Images
System32
This PC
Network
Name
Date modified
Type
Size
JPS
5/4/2019 2:08 PM
Application
1,480 KB
ReadMe
5/4/2019 2:05 PM
Text Document
2 KB
2 items

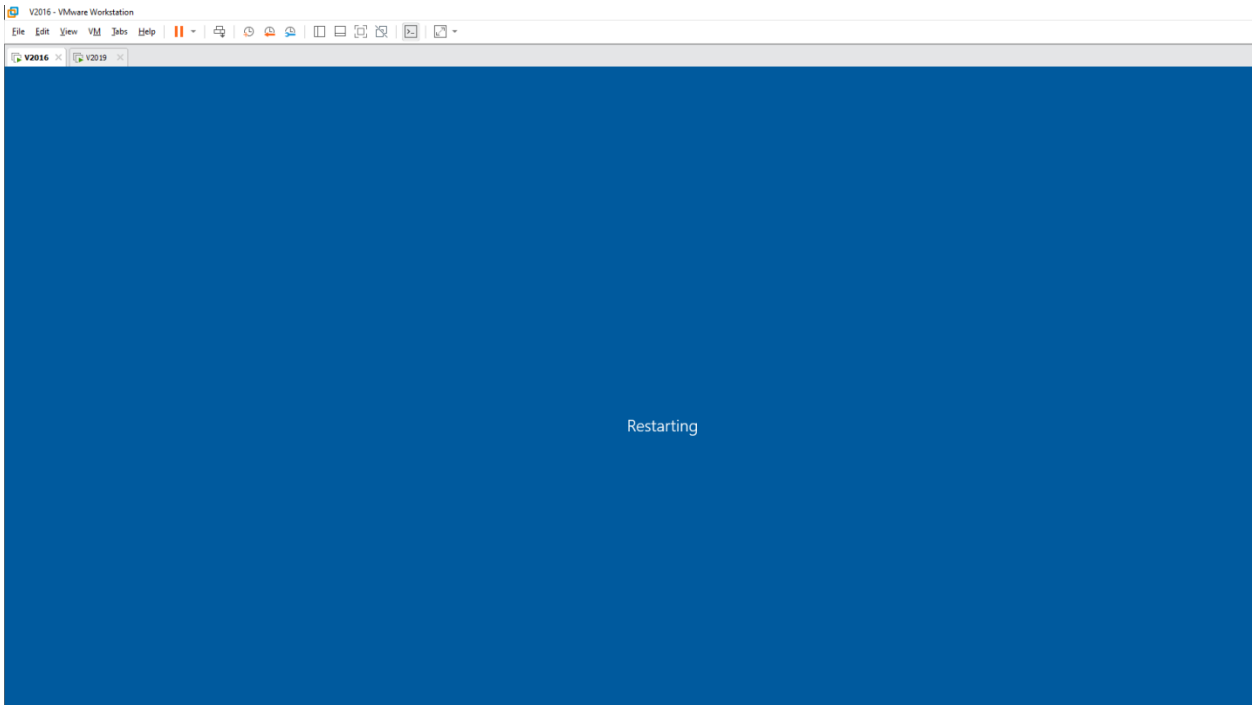

V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
JPS (Virus Maker 4.0)
Virus Options :
Disable Registry
Disable MsConfig
Disable TaskManager
Disable Telegram
Disable Media Player
Disable Internet Explorer
Disable Time
Disable Group Policy
Disable Windows Explorer
Disable Notepad
Disable Wordpad
Disable Windows
Disable System Restore
Disable Taskbar
Disable Start Button
Disable DHCP Client
Disable CMD
Disable Windows Update
Disable Control Panel
Disable Desktop Icons
Disable Screen Saver
Disable Browsers
Disable Drives
Hide Services
Hide Windows Clock
Hide Desktop Icons
Hide Run
Hide Taskbar
Hide Cursor
Swap Mouse Button
Remove Folder Options
Lock Mouse and Keyboard
Always Open CD_ROM
Turn Off Monitor
Crazy Mouse
Enable Remote Desktop
Destroy Clipboard
Lock Screen
Mute Sound
Remove Bluetooth
Remove Windows Themes
Slow Mouse Speed
Turn Off Windows Firewall
Turn Off Windows Defender
Run In System Mode
Auto Startup
Restart LogOff TurnOff Hibrinate None
Name After Install : svchost
Server Name : Server.exe
About
Create Virus!
x86(32Bit)
Exit
JPS Virus Maker 4.0
Module 07 Malware Threats
Date modified
5/4/2019 2:08 PM
5/4/2019 2:05 PM


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
JPS (Virus Maker 4.0)
Virus Options :
Disable Registry
Disable MsConfig
Disable TaskManager
Disable Telegram
Disable Media Player
Disable Internet Explorer
Disable Time
Disable Group Policy
Disable Windows Explorer
Disable Notepad
Disable Wordpad
Disable Windows
Disable System Restore
Disable Taskbar
Disable Start Button
Disable DHCP Client
Disable CMD
Disable Windows Update
Disable Control Panel
Disable Desktop Icons
Disable Screen Saver
Disable Browsers
Disable Drives
Hide Services
Hide Windows Clock
Hide Desktop Icons
Hide Run
Hide Taskbar
Hide Cursor
Swap Mouse Button
Remove Folder Options
Lock Mouse and Keyboard
Always Open CD_ROM
Turn Off Monitor
Crazy Mouse
Enable Remote Desktop
Destroy Clipboard
Lock Screen
Mute Sound
Remove Bluetooth
Remove Windows Themes
Slow Mouse Speed
Turn Off Windows Firewall
Turn Off Windows Defender
Run In System Mode
Auto Startup
Restart LogOff TurnOff Hibrinate None
Name After Install : svchost
Server Name : Server.exe
About
Create Virus! x86(32Bit)
Exit
JPS Virus Maker 4.0
Module 07 Mal
Date mo
5/4/2019
5/4/2019
2 items 1 item selected 1.44 MB


V2019 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Acrobat Reader DC
Firefox
Google Chrome
CEHv11 Module ...
CEHv11 Module ...
Test
JPS (Virus Maker 4.0)
Virus Options :
Change Windows Password : qwerty
Change Computer Name : Test
Close Custom Window : Windows Task Manager
Disable Custom Service : wuauserv
Close Custom Process : iexplore.exe
Open Custom Website : http://kernel32.ir
Run Custom Command : taskkill /F /IM chrome.exe
Enable Convert to Worm
Worm Name : fedevi
Copy After : 1 Sec's
Enable Convert to Backdoor
Port : 4000
Use: Telnet.exe [Target IP] [Port]
Enable Convert to Logical Bomb
Activate Time : 10/8 /2023 9:06 pm
Change Icon
Flash Icon
BMP Icon
Rar Icon
None Icon
PDF Icon
Doc Icon
Setup Icon
Love
JPG Icon
Help Icon
MSI Icon
Restart
LogOff
TurnOff
Hibrinate
None
Name After Install : svchost
Server Name : Server.exe
About
Create Virus!
x86(32Bit)
Exit
JPS Virus Maker 4.0


V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Recycle Bin
Server.exe
Acrobat Reader DC
test.txt




V2016 - VMware Workstation
File Edit View VM Tabs Help
V2016
V2019
Restarting