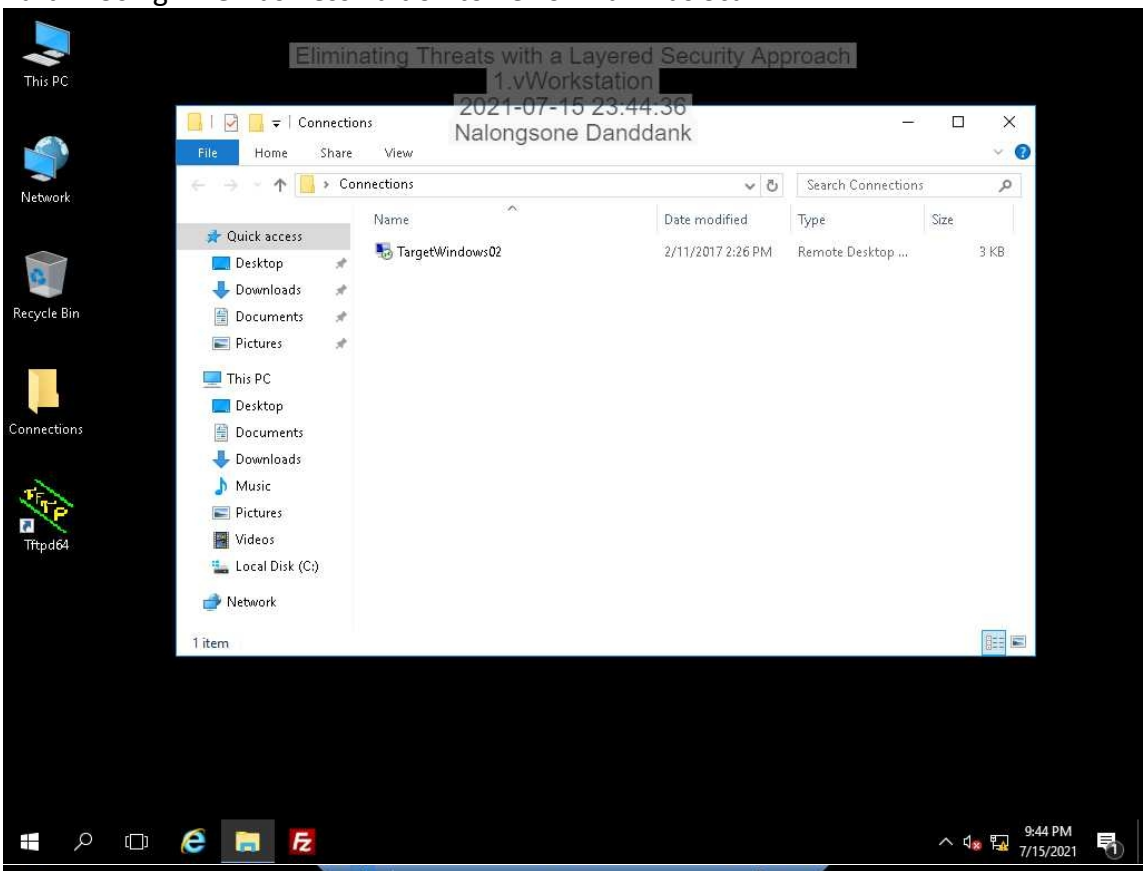
Nalongsone Danddank Student ID : 14958950 StarID: jf3893pd
Email: nalongsone.danddank@my.metrostate.edu\

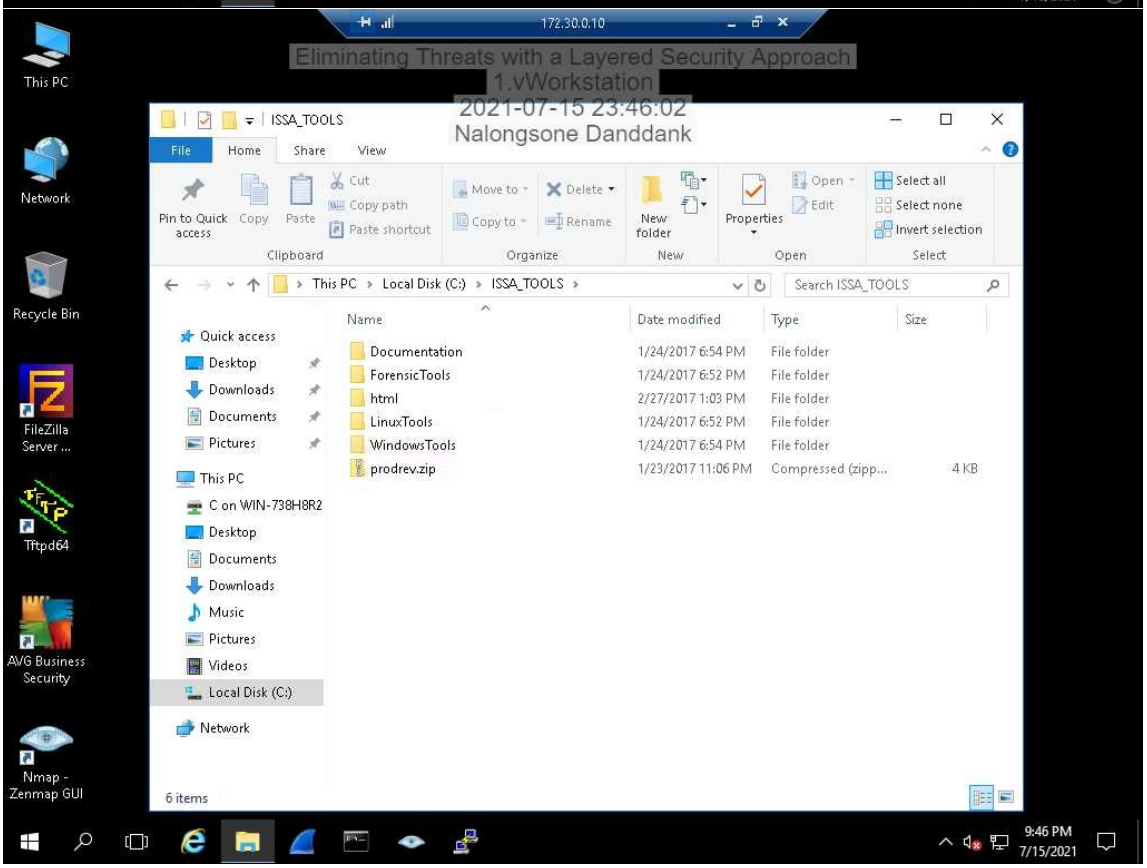
ICS382/CYBR332-51 —Computer Security

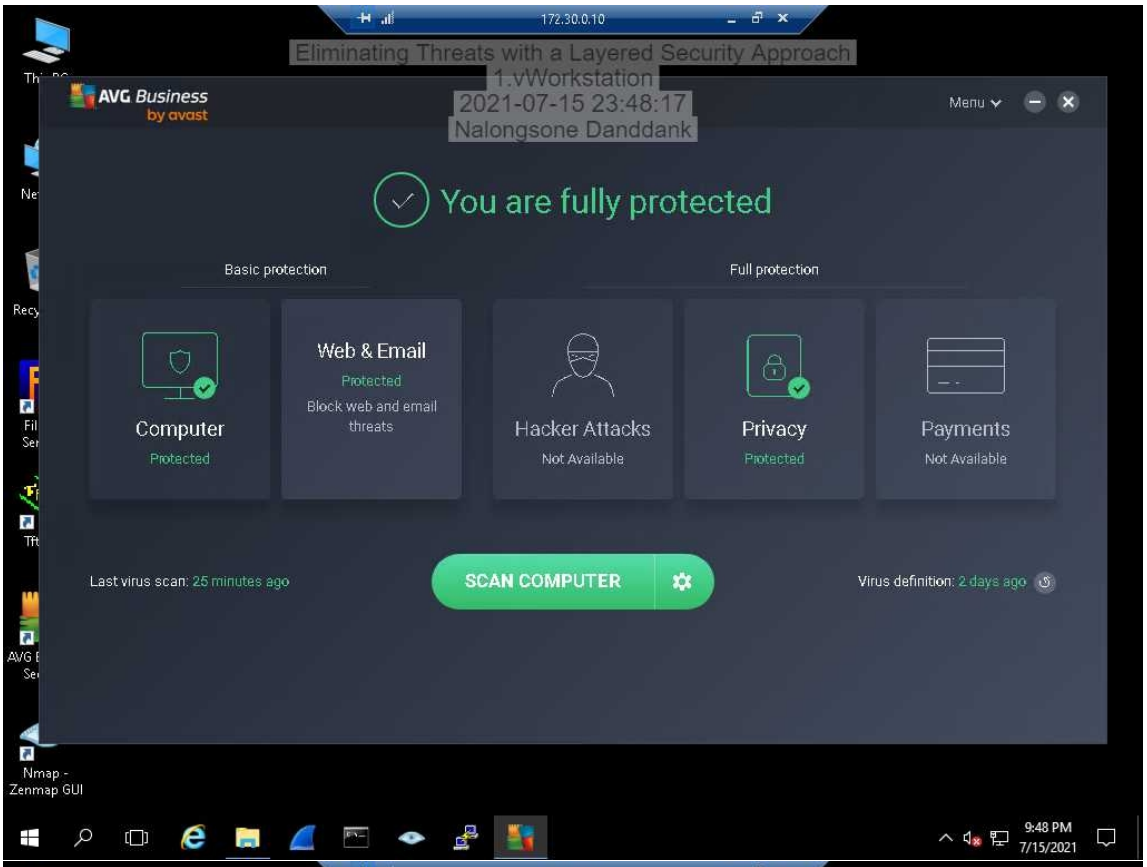
Lab #9 Report

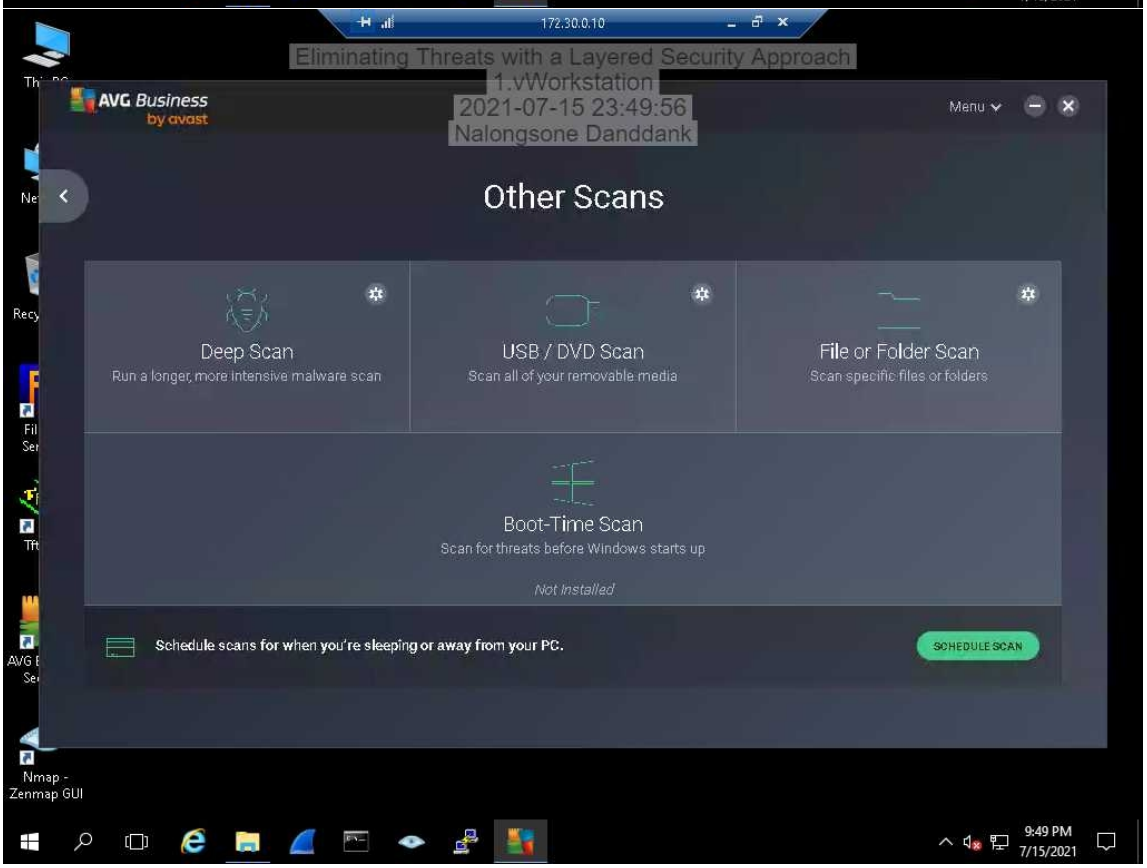
ELIMINATING THREATS WITH A LAYERED SECURITY APPROACH

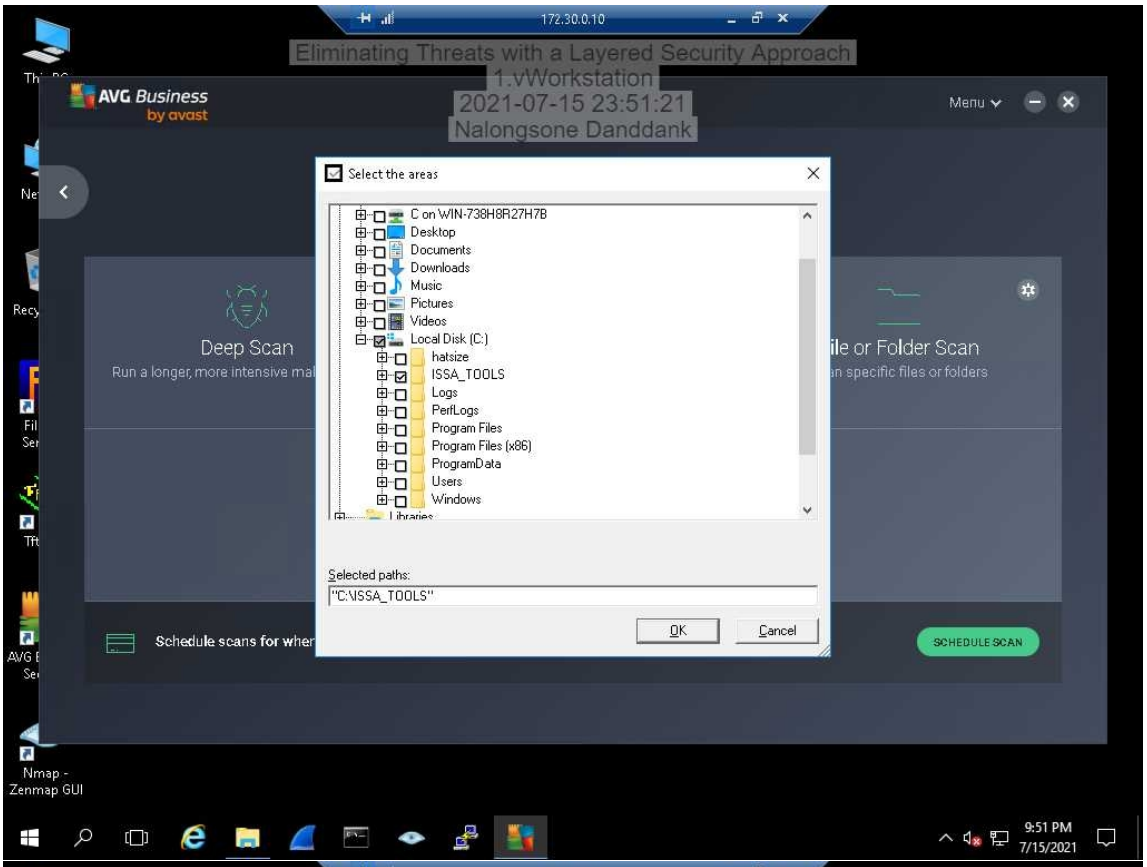
Part 1: Using AVG Business Edition to Perform a Virus Scan.

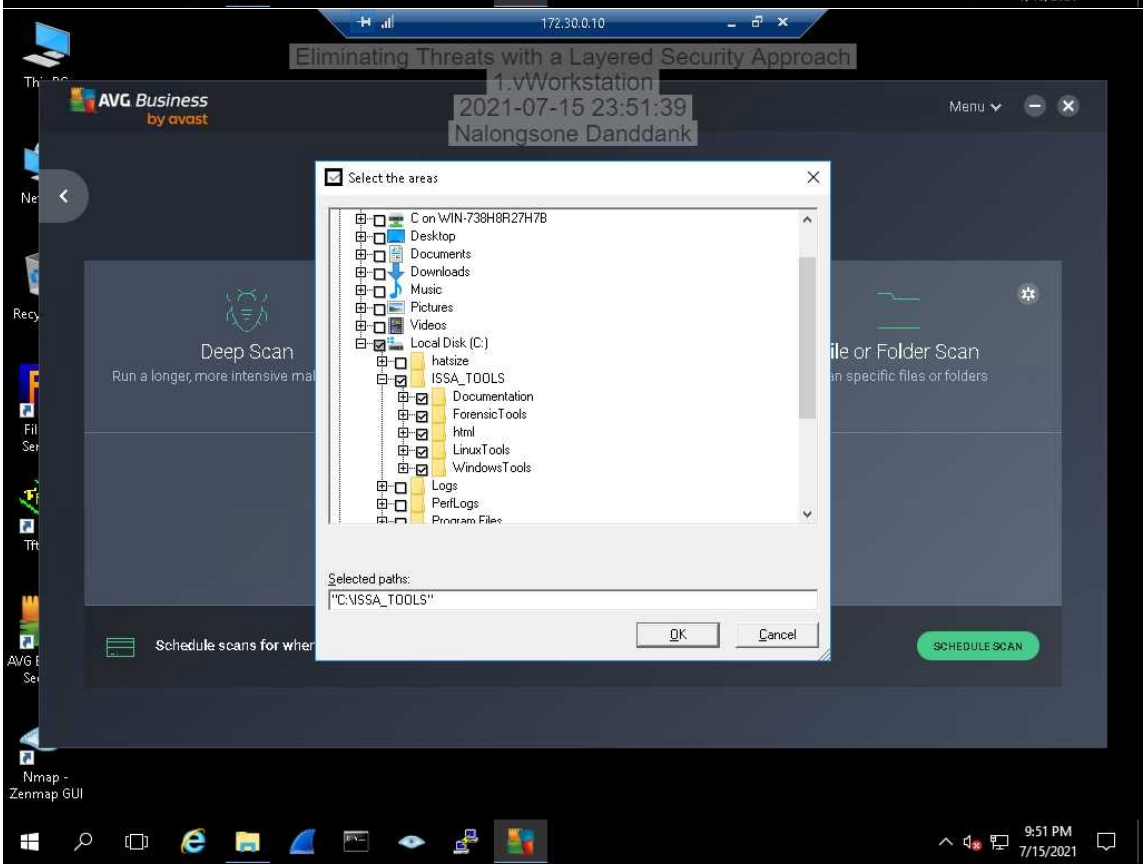


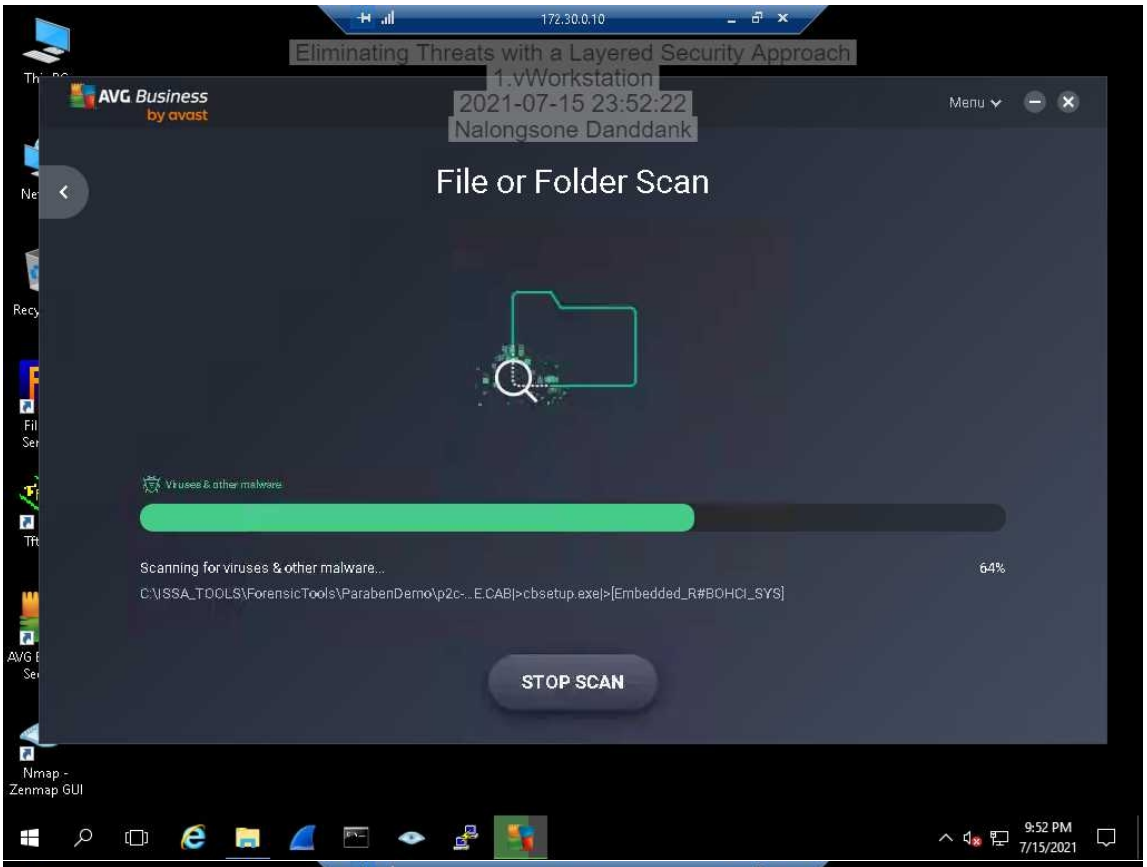


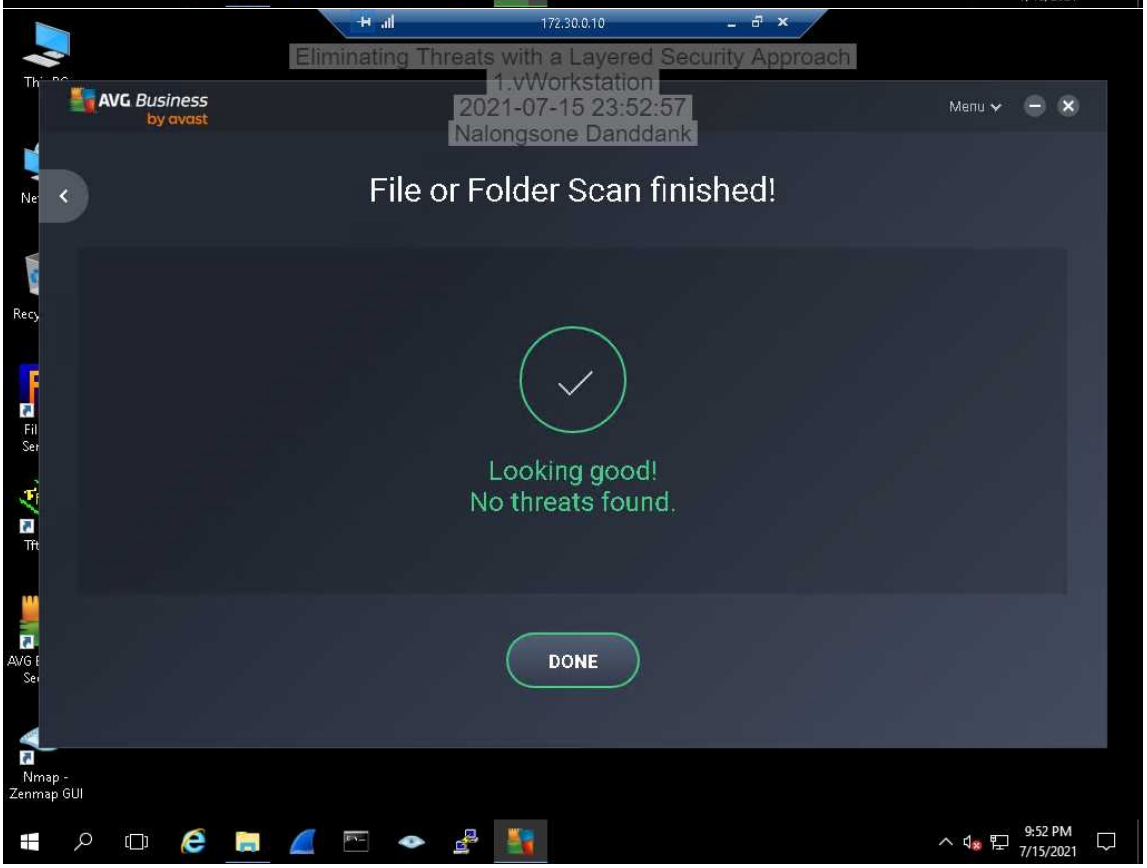

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-15 23:48:17
Nalongsone Danddank
AVG Business by avast
Menu
You are fully protected
Basic protection
Full protection
Web & Email
Protected
Block web and email threats
Computer
Protected
Hacker Attacks
Not Available
Privacy
Protected
Payments
Not Available
Last virus scan: 25 minutes ago
SCAN COMPUTER
Virus definition: 2 days ago
9:48 PM
7/15/2021

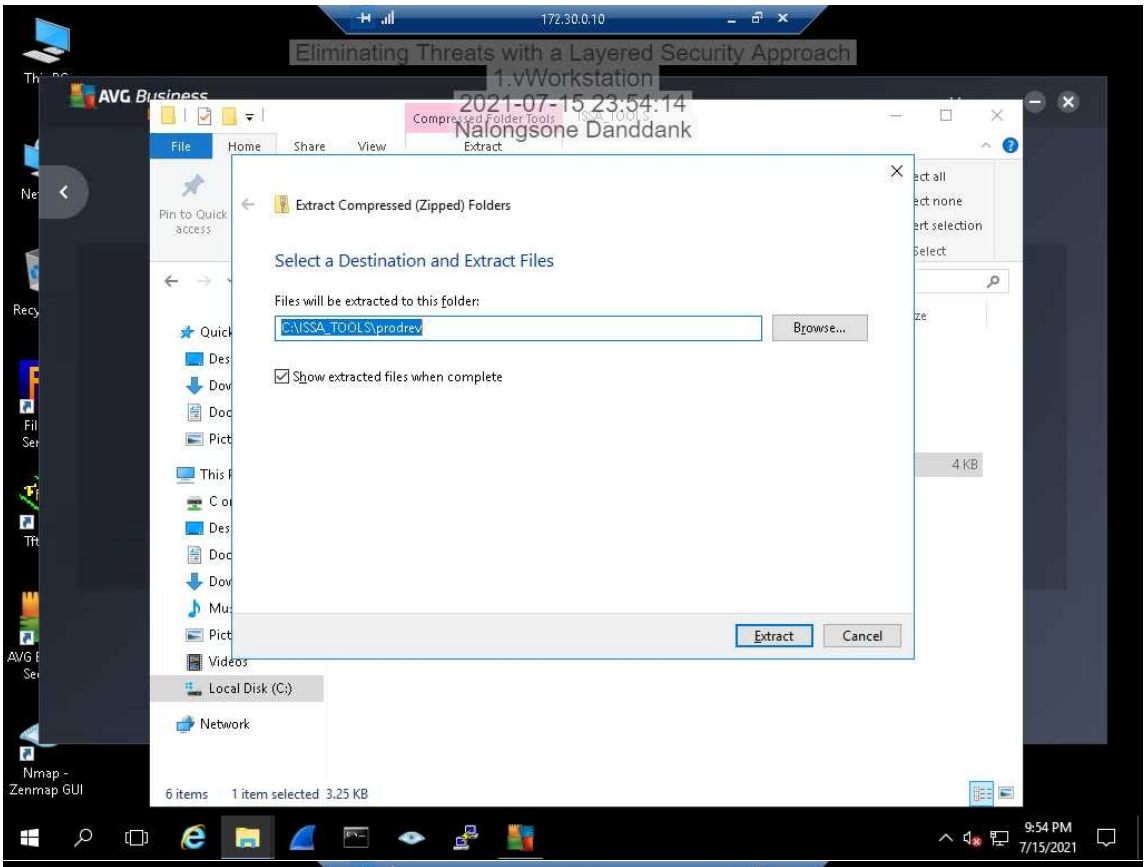

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-15 23:49:56
Nalongsone Danddank
AVG Business by avast
Menu
Other Scans
Deep Scan
Run a longer, more intensive malware scan
USB / DVD Scan
Scan all of your removable media
File or Folder Scan
Scan specific files or folders
Boot-Time Scan
Scan for threats before Windows starts up
Not Installed
Schedule scans for when you're sleeping or away from your PC.
SCHEDULE SCAN
9:49 PM
7/15/2021

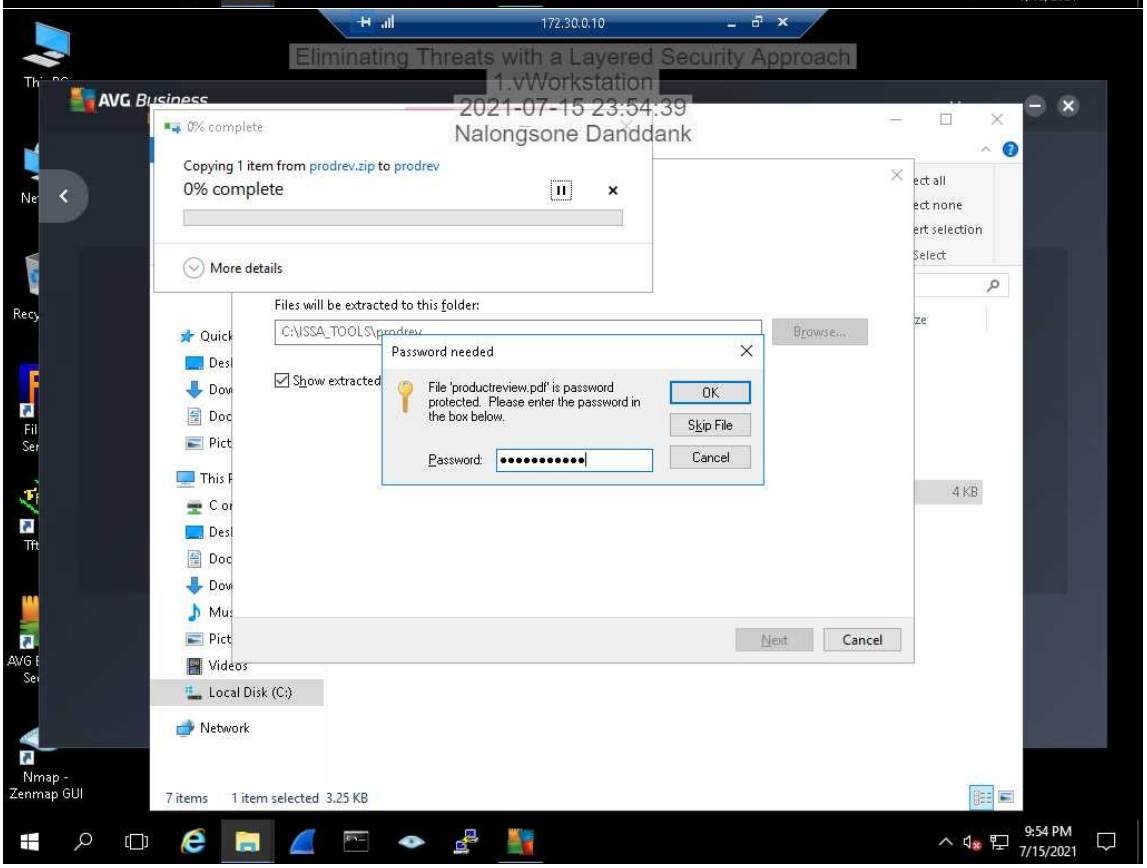

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-15 23:51:21
Nalongsone Danddank
AVG Business by avast
Menu
Select the areas
C on WIN-738H8R27H7B
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
hatsize
ISSA_TOOLS
Logs
PerfLogs
Program Files
Program Files (x86)
ProgramData
Users
Windows
Selected paths:
"C:\ISSA_TOOLS"
OK
Cancel
Deep Scan
Run a longer, more intensive mal
ile or Folder Scan
n specific files or folders
Schedule scans for wher
SCHEDULE SCAN
Nmap - Zenmap GUI
9:51 PM
7/15/2021

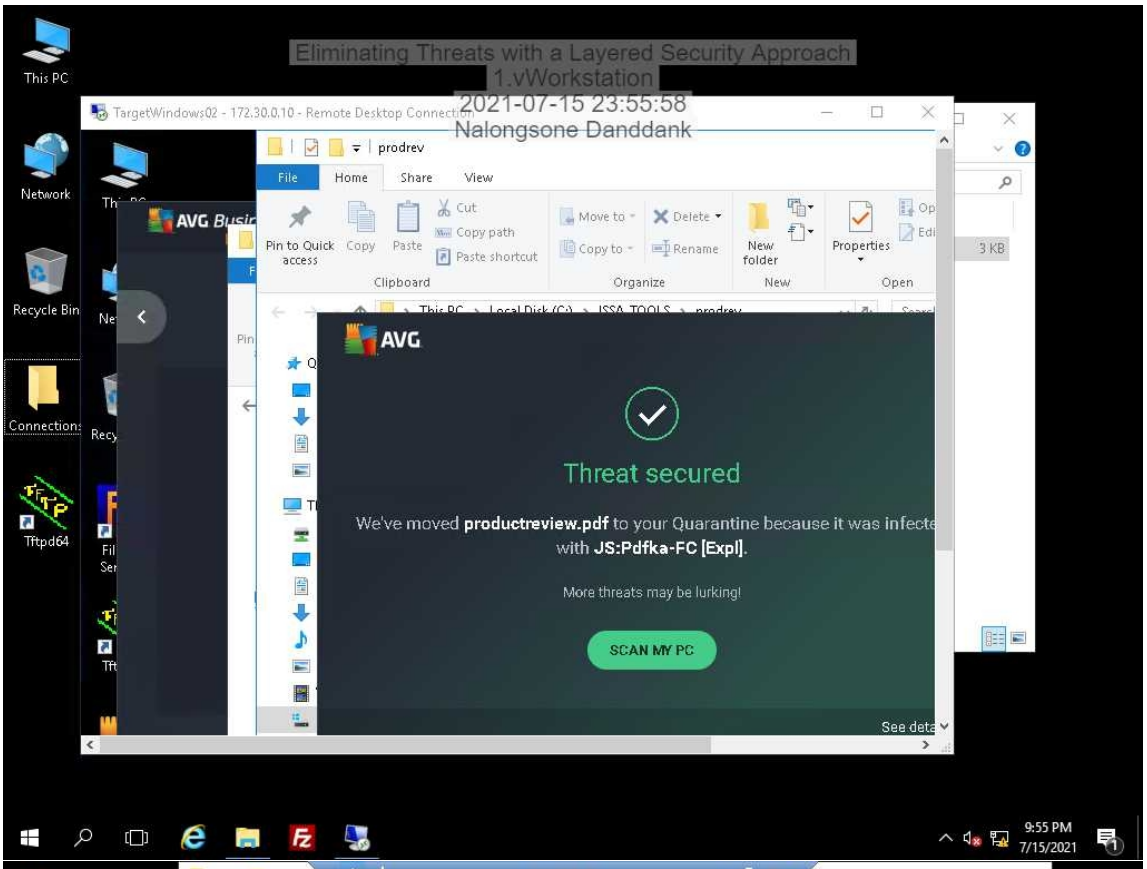

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-15 23:51:39
Nalongsone Danddank
AVG Business by avast
Menu
Select the areas
C on WIN-738H8R27H7B
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
hatsize
ISSA_TOOLS
Documentation
ForensicTools
html
LinuxTools
WindowsTools
Logs
PerfLogs
Selected paths:
"C:\ISSA_TOOLS"
OK
Cancel
Deep Scan
Run a longer, more intensive mal
ile or Folder Scan
n specific files or folders
Schedule scans for wher
SCHEDULE SCAN
Nmap - Zenmap GUI
9:51 PM
7/15/2021

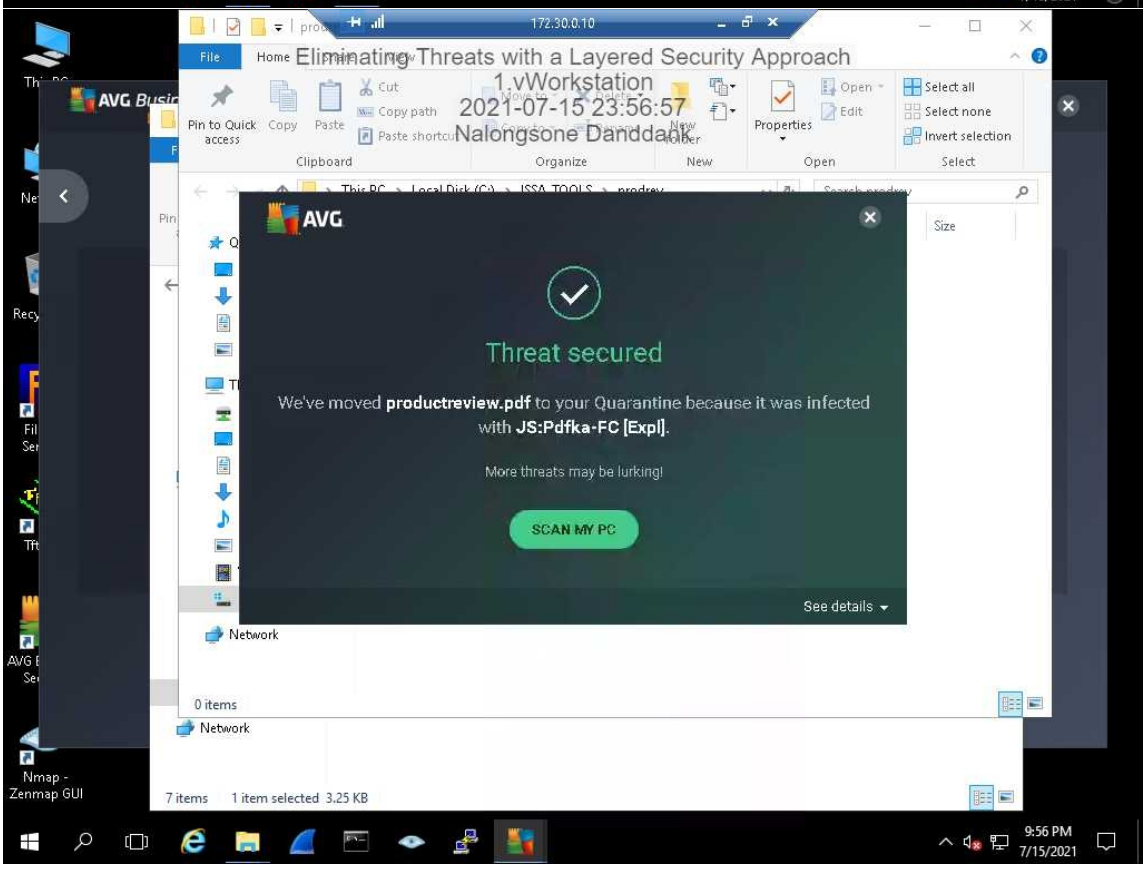

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-15 23:52:22
Nalongsone Danddank
AVG Business by avast
Menu
File or Folder Scan
Viruses & other malware
Scanning for viruses & other malware...
64%
C:\ISSA_TOOLS\ForensicTools\ParabenDemo\p2c-...E.CAB|>cbsetup.exe|>[Embedded_R#BOHCI_SYS]
STOP SCAN
Nmap - Zenmap GUI
9:52 PM
7/15/2021

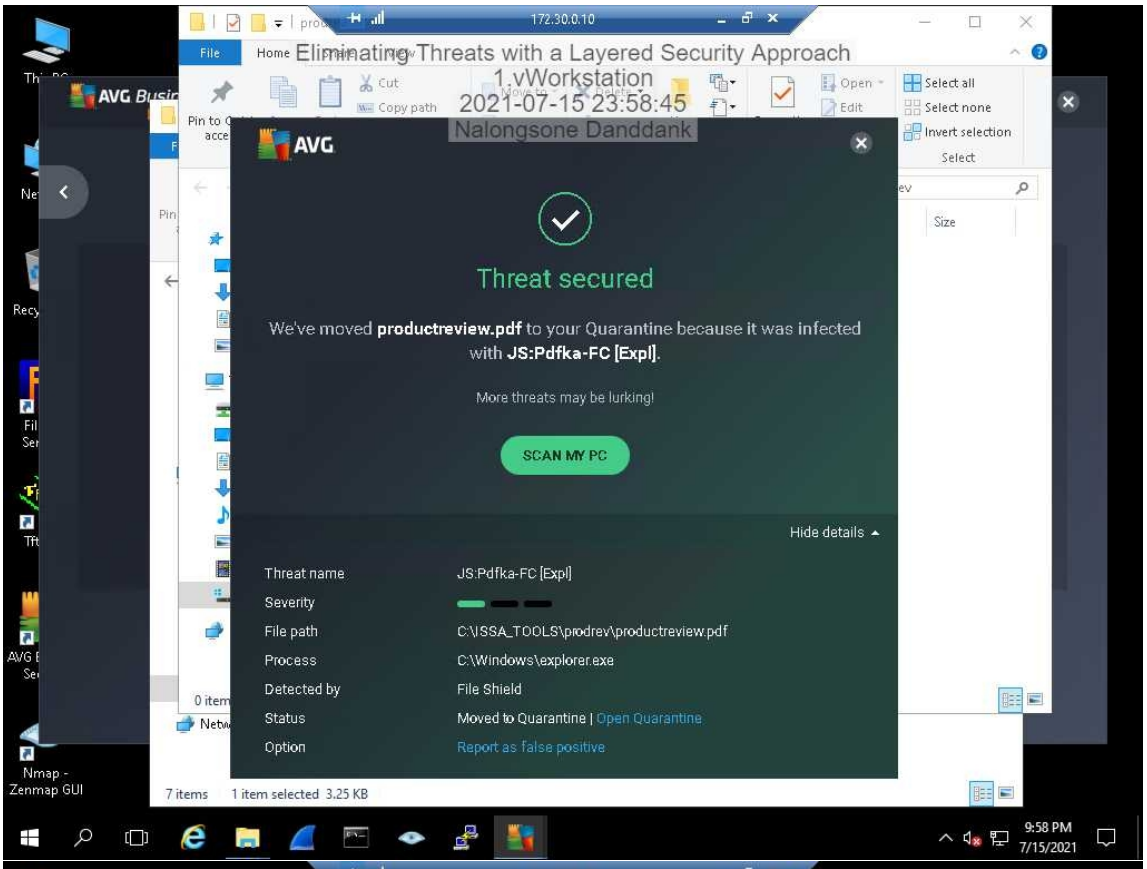

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-15 23:52:57
Nalongsone Danddank
AVG Business by avast
Menu
File or Folder Scan finished!
Looking good!
No threats found.
DONE
Nmap - Zenmap GUI
9:52 PM
7/15/2021

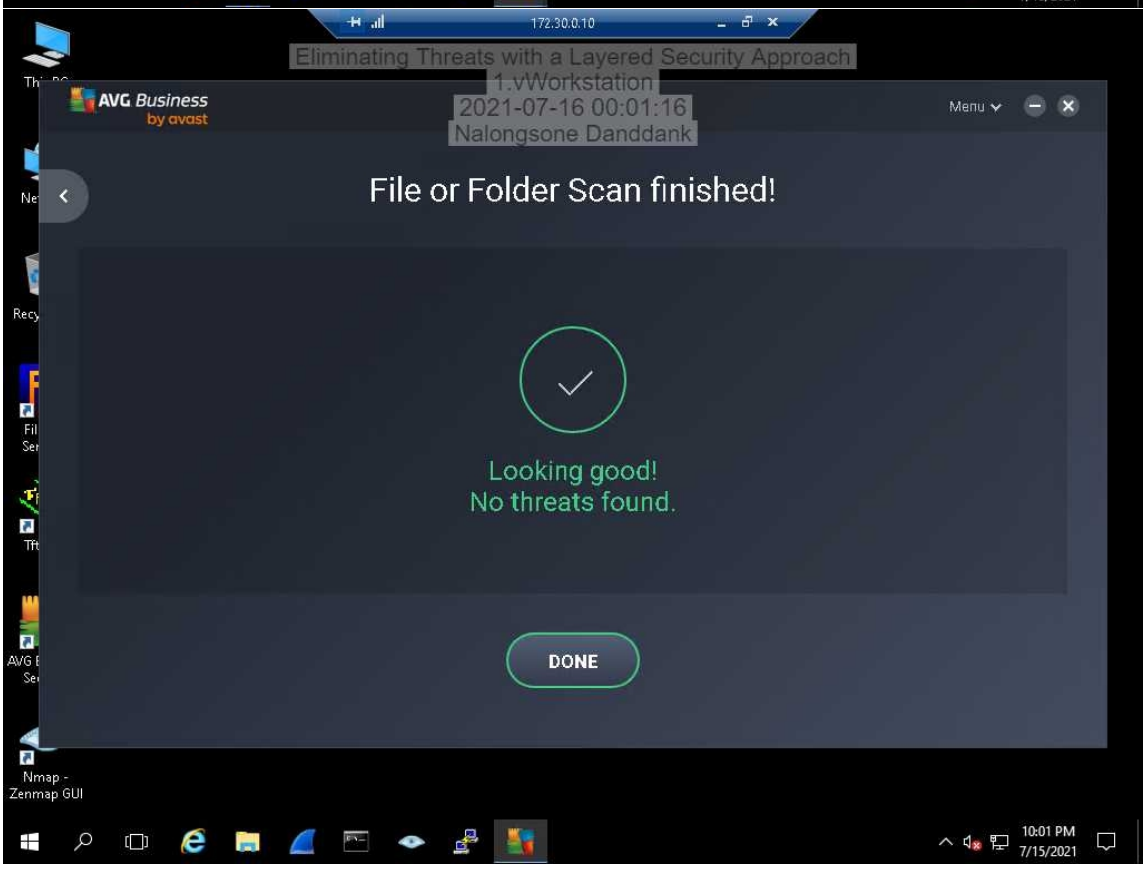

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-15 23:54:14
Nalongsone Danddank
AVG Business
Extract Compressed (Zipped) Folders
Select a Destination and Extract Files
Files will be extracted to this folder:
C:\ISSA_TOOLS\prodrev
Browse...
Show extracted files when complete
Extract
Cancel
6 items
1 item selected 3.25 KB
9:54 PM
7/15/2021

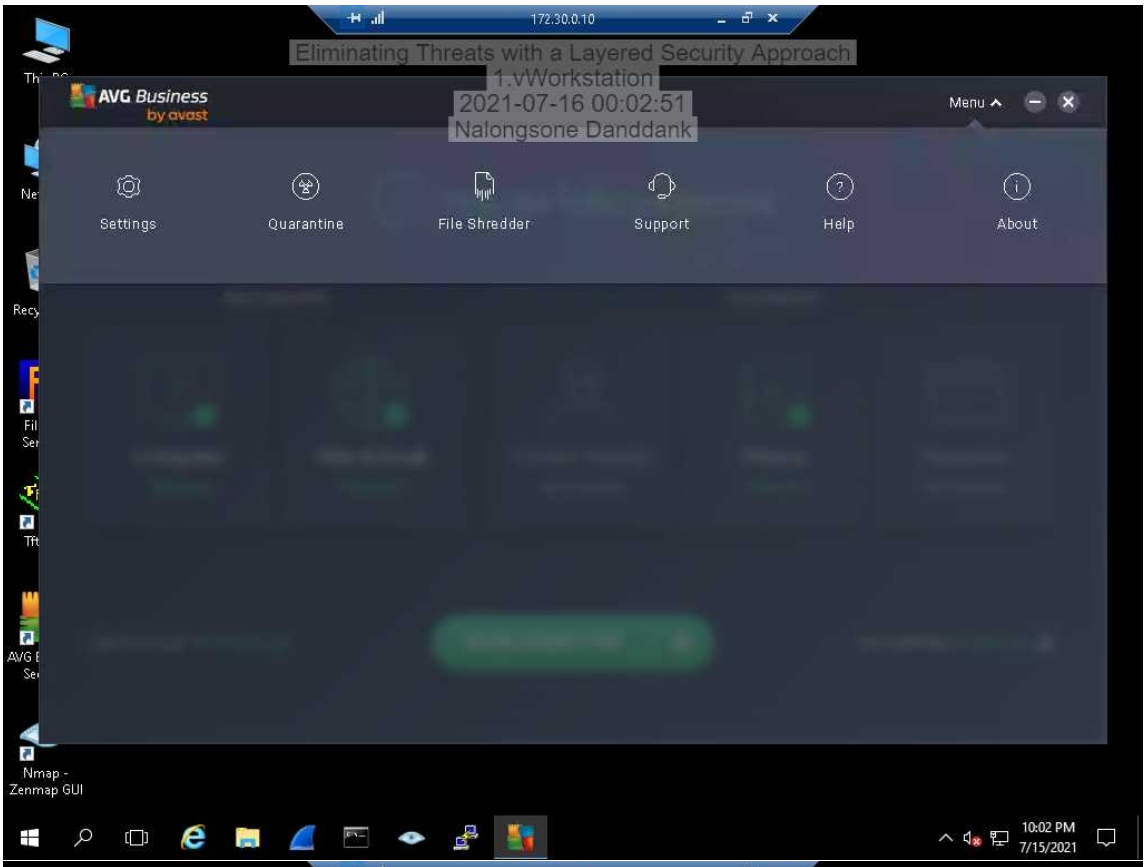

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-15 23:54:39
Nalongsone Danddank
AVG Business
0% complete
Copying 1 item from prodrev.zip to prodrev
0% complete
More details
Files will be extracted to this folder:
Browse...
Password needed
File 'productreview.pdf' is password protected. Please enter the password in the box below.
Password:
OK
Skip File
Cancel
Next
Cancel
7 items
1 item selected 3.25 KB
9:54 PM
7/15/2021

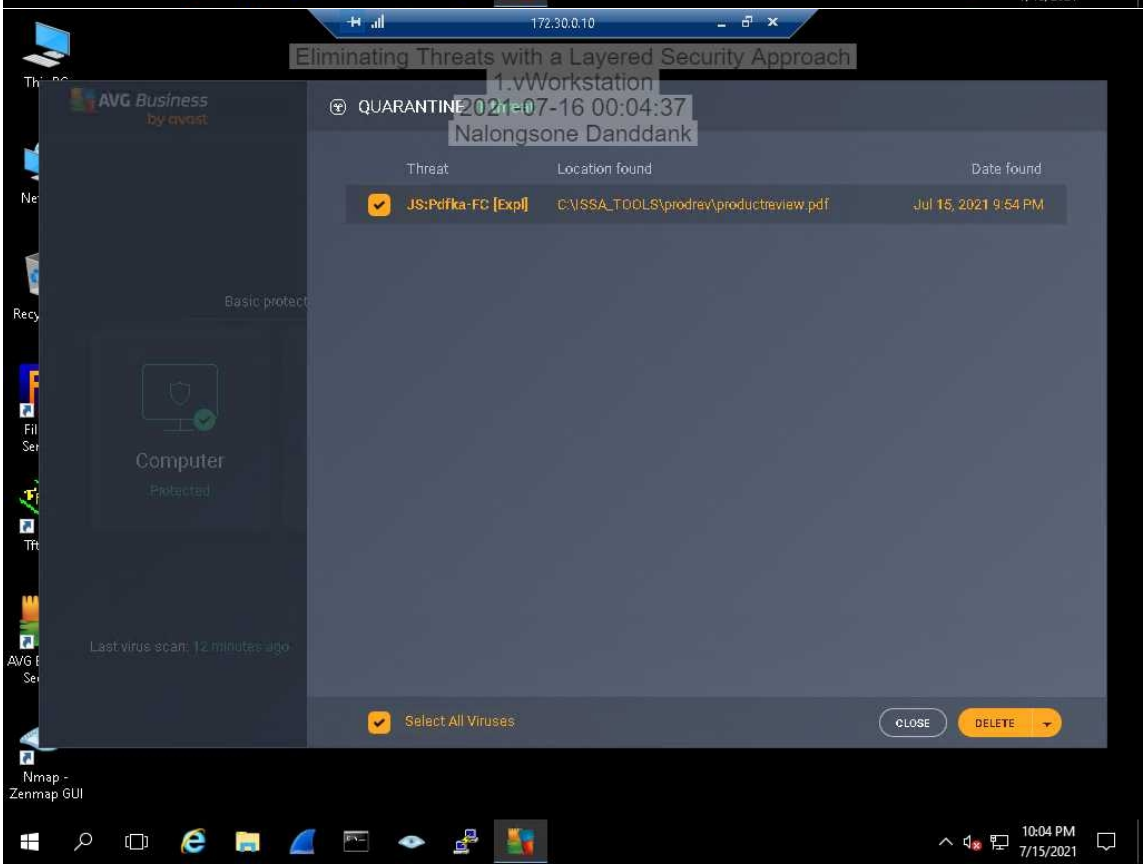

Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-15 23:55:58
Nalongsone Danddank
TargetWindows02 - 172.30.0.10 - Remote Desktop Connection
prodrev
File
Home
Share
View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Move to
Copy to
Delete
Rename
New folder
Properties
Clipboard
Organize
New
Open
AVG
Threat secured
We've moved productreview.pdf to your Quarantine because it was infecte
with JS:Pdfka-FC [Expl].
More threats may be lurking!
SCAN MY PC
See deta
This PC
Network
Recycle Bin
Connections
Tftpd64
3 KB
9:55 PM
7/15/2021

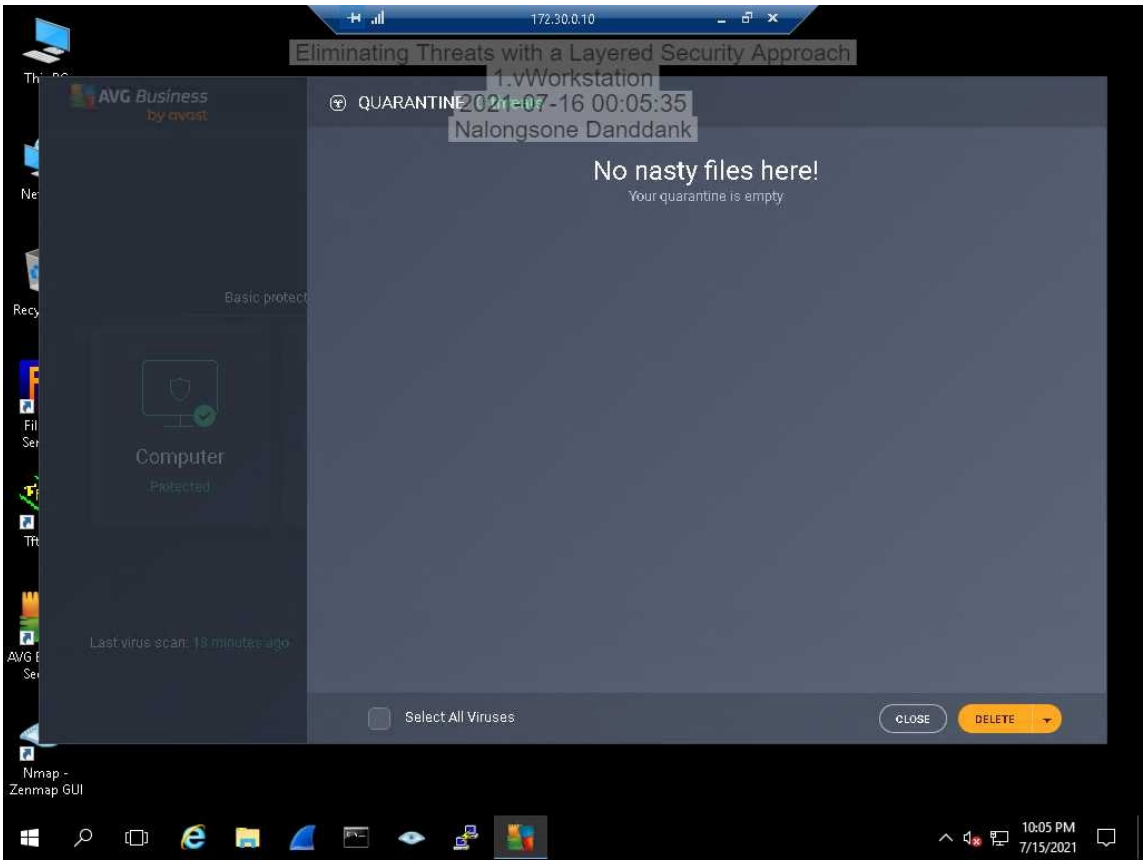

Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-15 23:56:57
Nalongsone Danddank
172.30.0.10
File
Home
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Properties
Open
Edit
Select all
Select none
Invert selection
Clipboard
Organize
New
Open
Select
AVG
Threat secured
We've moved productreview.pdf to your Quarantine because it was infected
with JS:Pdfka-FC [Expl].
More threats may be lurking!
SCAN MY PC
See details
Size
Network
0 items
Network
7 items
1 item selected 3.25 KB
Nmap - Zenmap GUI
9:56 PM
7/15/2021


172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-15 23:58:45
Nalongsone Danddank
AVG
Threat secured
We've moved productreview.pdf to your Quarantine because it was infected with JS:Pdfka-FC [Expl].
More threats may be lurking!
SCAN MY PC
Hide details
Threat name JS:Pdfka-FC [Expl]
Severity
File path C:\ISSA_TOOLS\prodrev\productreview.pdf
Process C:\Windows\explorer.exe
Detected by File Shield
Status Moved to Quarantine | Open Quarantine
Option Report as false positive
7 items 1 item selected 3.25 KB
9:58 PM
7/15/2021

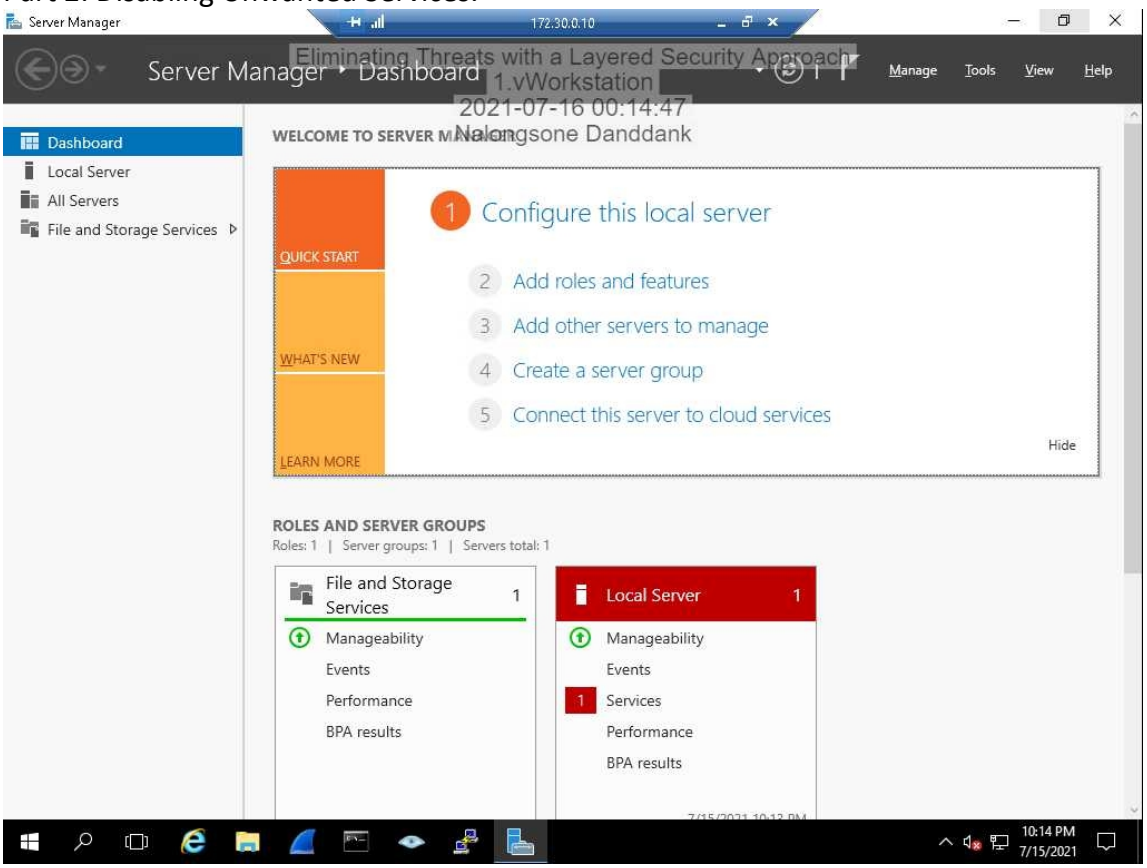

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:01:16
Nalongsone Danddank
AVG Business by avast
Menu
File or Folder Scan finished!
Looking good!
No threats found.
DONE
10:01 PM
7/15/2021

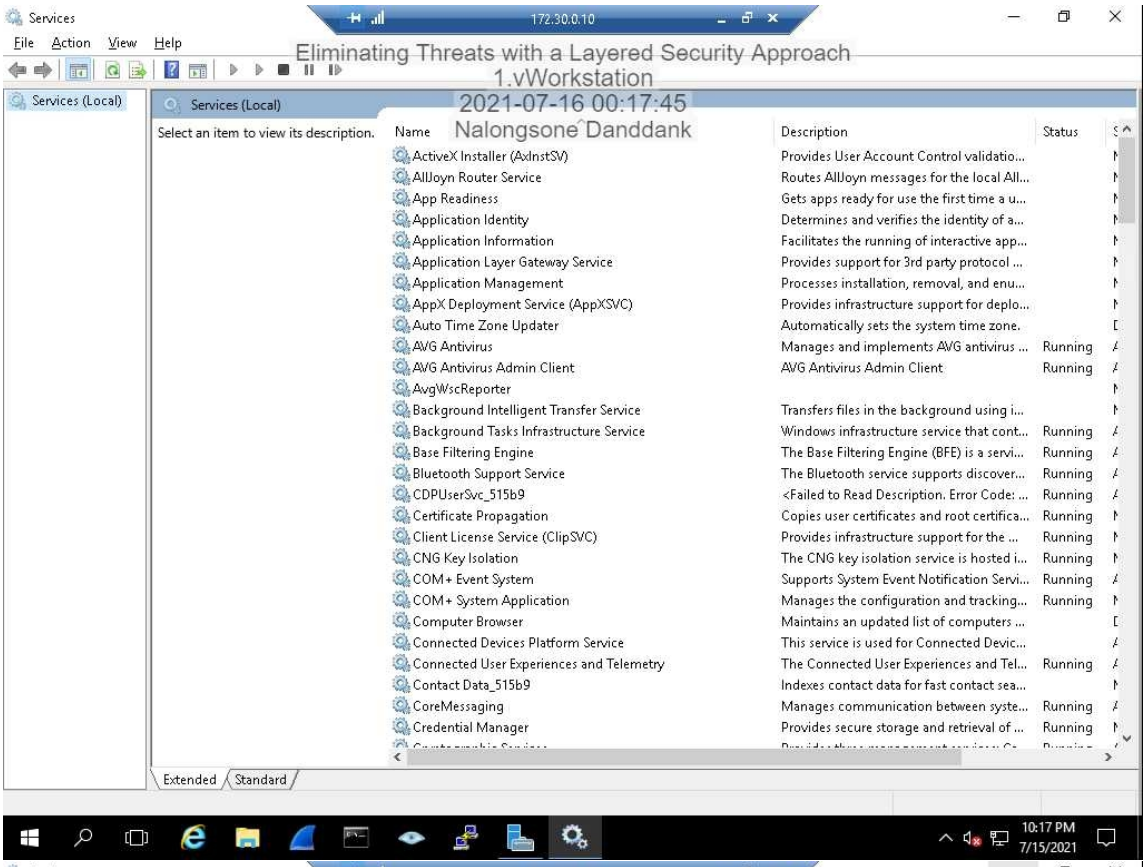

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:02:51
Nalongsone Danddank
AVG Business by avast
Menu
Settings
Quarantine
File Shredder
Support
Help
About
Nmap - Zenmap GUI
10:02 PM
7/15/2021

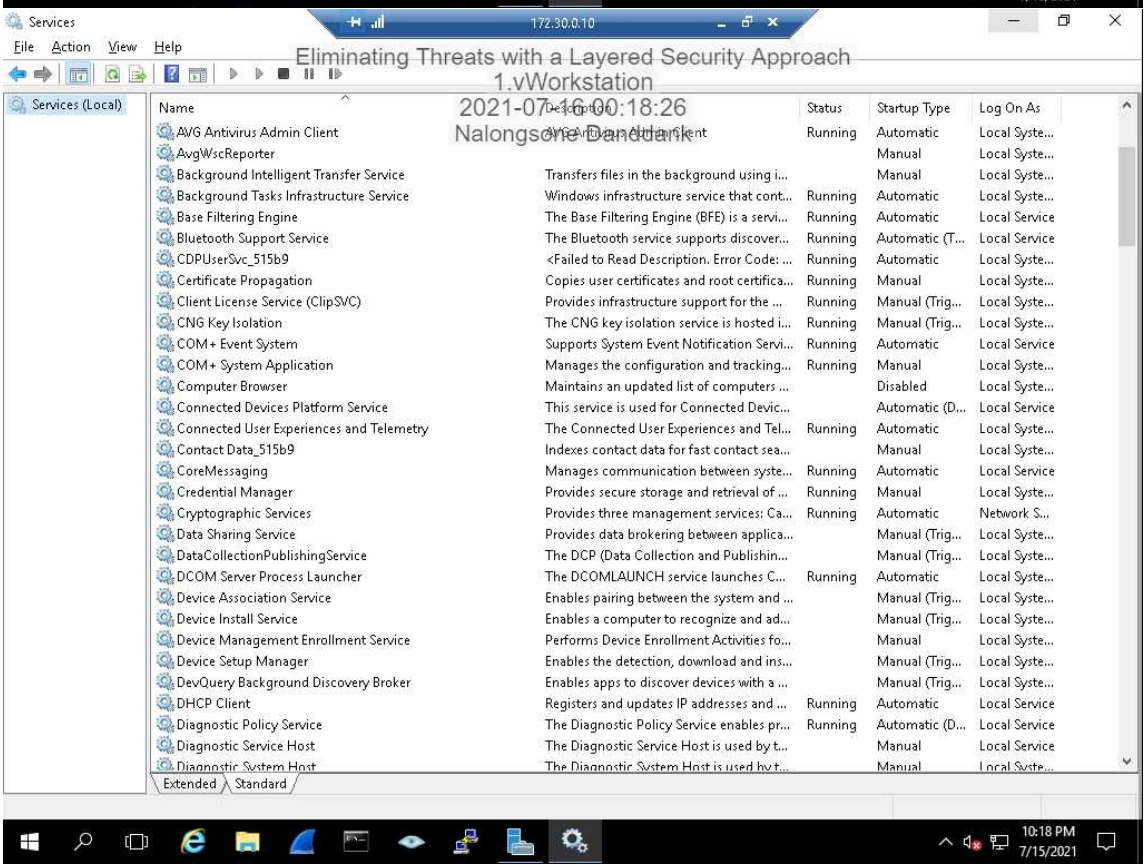

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:04:37
Nalongsone Danddank
AVG Business by avast
QUARANTINE
Threat
Location found
Date found
JS:Pdfka-FC [Expl]
C:\ISSA_TOOLS\prodrev\productreview.pdf
Jul 15, 2021 9:54 PM
Computer
Protected
Last virus scan: 12 minutes ago
Select All Viruses
CLOSE
DELETE
Nmap - Zenmap GUI
10:04 PM
7/15/2021

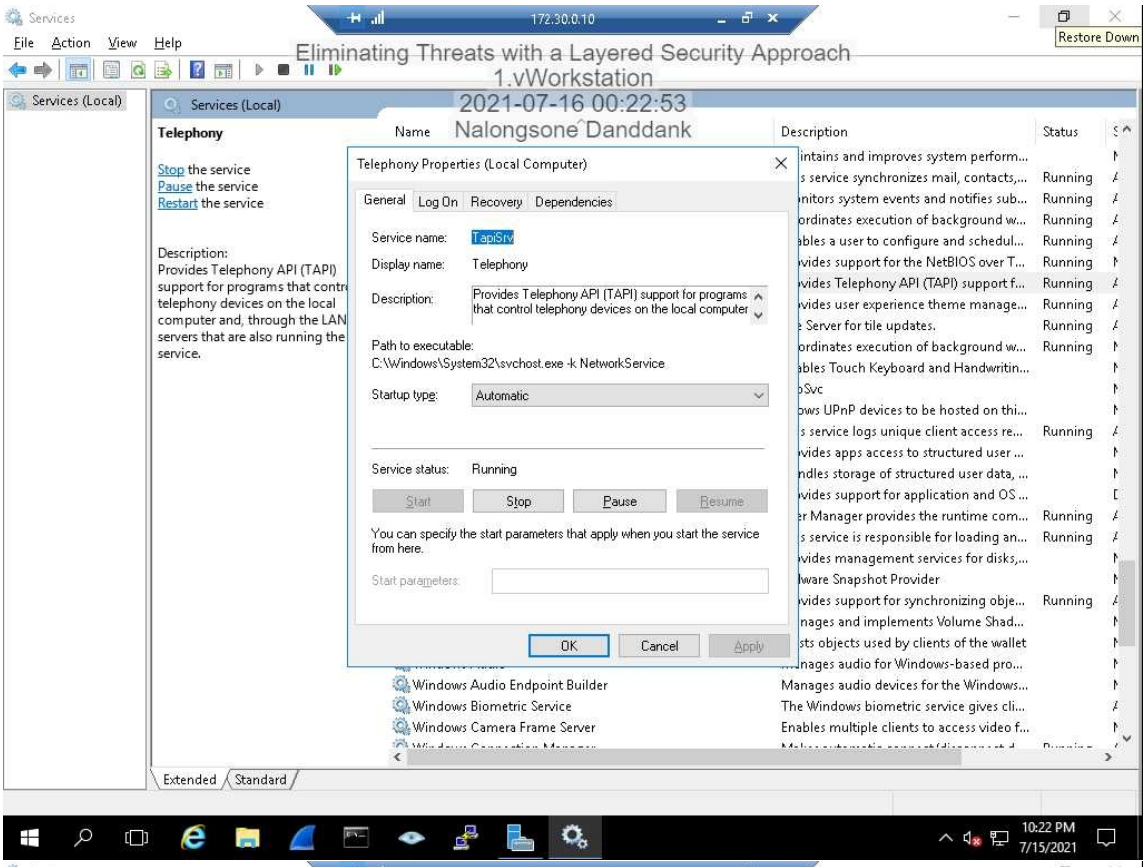


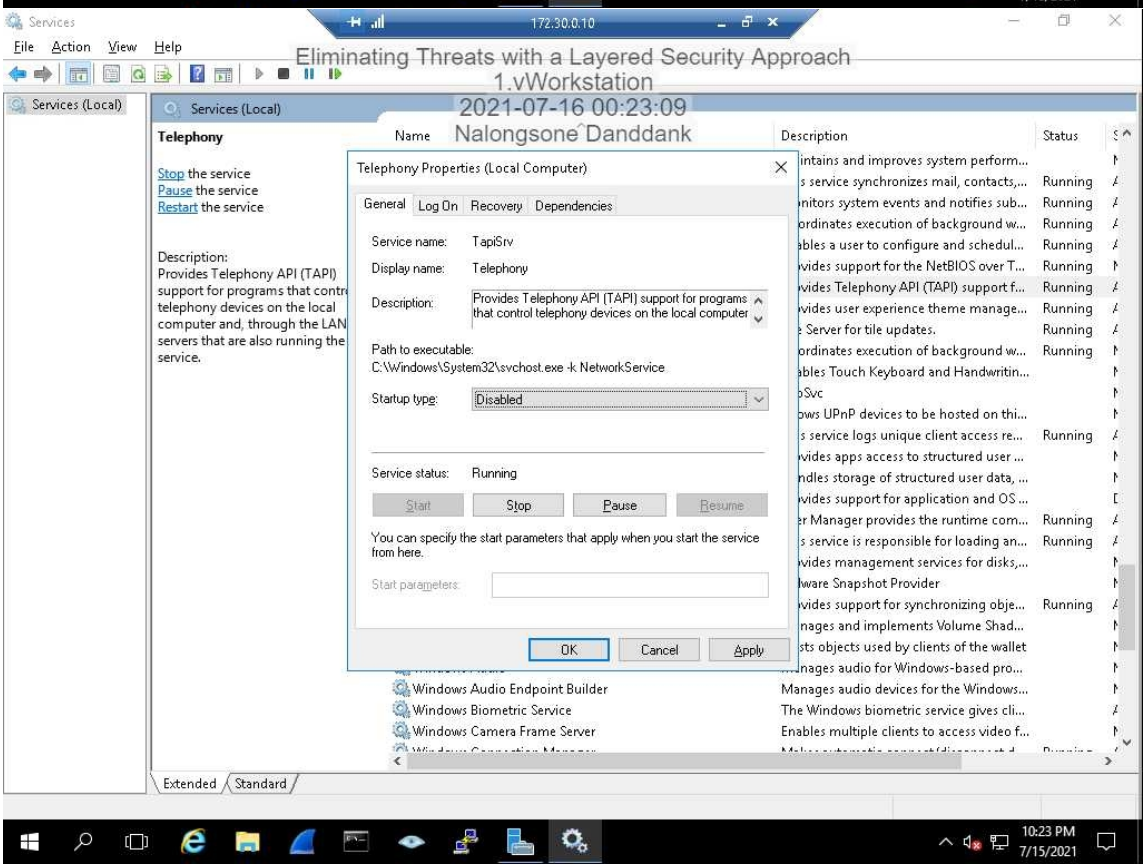
Part 2: Disabling Unwanted Services.

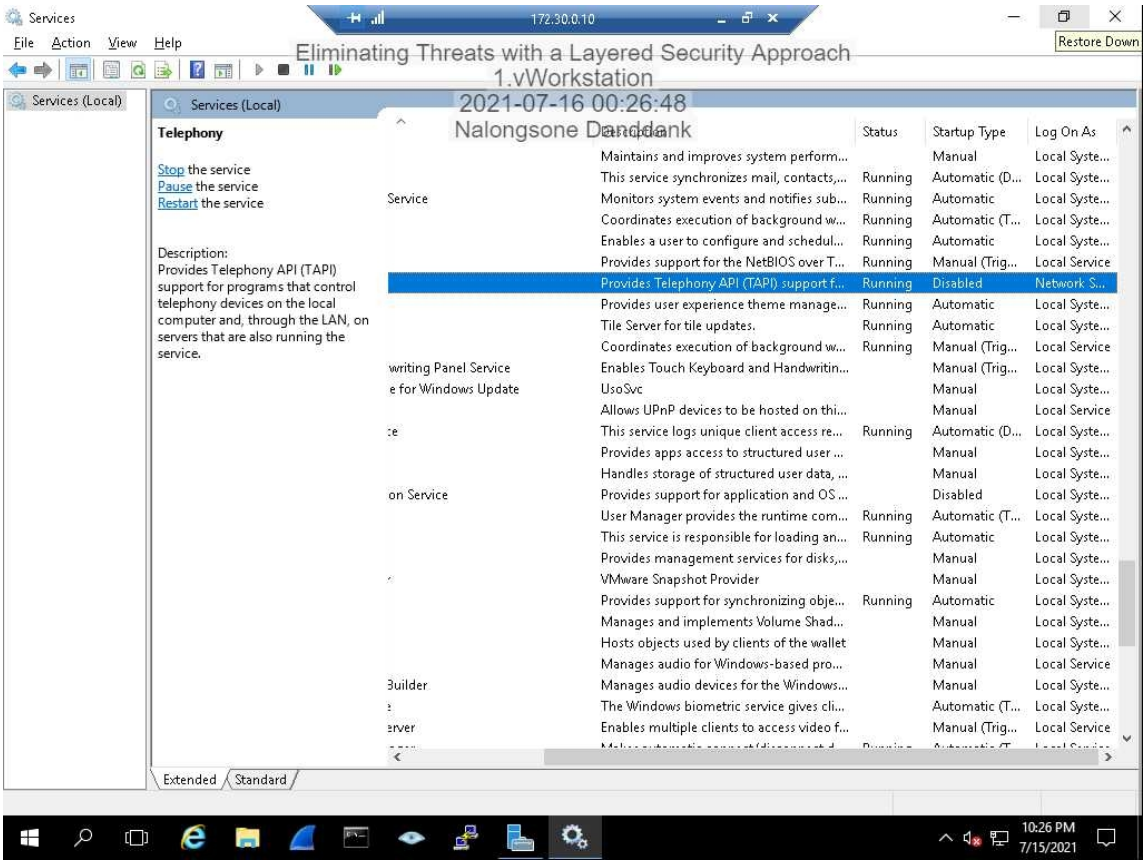



Services
File Action View Help
172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:17:45
Nalongsone Danddank
Services (Local)
Select an item to view its description.
Name
Description
Status
ActiveX Installer (AxInstSV)
Provides User Account Control validatio...
AllJoyn Router Service
Routes AllJoyn messages for the local All...
App Readiness
Gets apps ready for use the first time a u...
Application Identity
Determines and verifies the identity of a...
Application Information
Facilitates the running of interactive app...
Application Layer Gateway Service
Provides support for 3rd party protocol ...
Application Management
Processes installation, removal, and enu...
AppX Deployment Service (AppXSVC)
Provides infrastructure support for deplo...
Auto Time Zone Updater
Automatically sets the system time zone.
AVG Antivirus
Manages and implements AVG antivirus ...
Running
AVG Antivirus Admin Client
AVG Antivirus Admin Client
Running
AvgWscReporter
Background Intelligent Transfer Service
Transfers files in the background using i...
Background Tasks Infrastructure Service
Windows infrastructure service that cont...
Running
Base Filtering Engine
The Base Filtering Engine (BFE) is a servi...
Running
Bluetooth Support Service
The Bluetooth service supports discover...
Running
CDPUserSvc_515b9
<Failed to Read Description. Error Code: ...
Running
Certificate Propagation
Copies user certificates and root certifica...
Running
Client License Service (ClipSVC)
Provides infrastructure support for the ...
Running
CNG Key Isolation
The CNG key isolation service is hosted i...
Running
COM+ Event System
Supports System Event Notification Servi...
Running
COM+ System Application
Manages the configuration and tracking...
Running
Computer Browser
Maintains an updated list of computers ...
Connected Devices Platform Service
This service is used for Connected Devic...
Connected User Experiences and Telemetry
The Connected User Experiences and Tel...
Running
Contact Data_515b9
Indexes contact data for fast contact sea...
CoreMessaging
Manages communication between syste...
Running
Credential Manager
Provides secure storage and retrieval of ...
Running
Extended
Standard
10:17 PM
7/15/2021

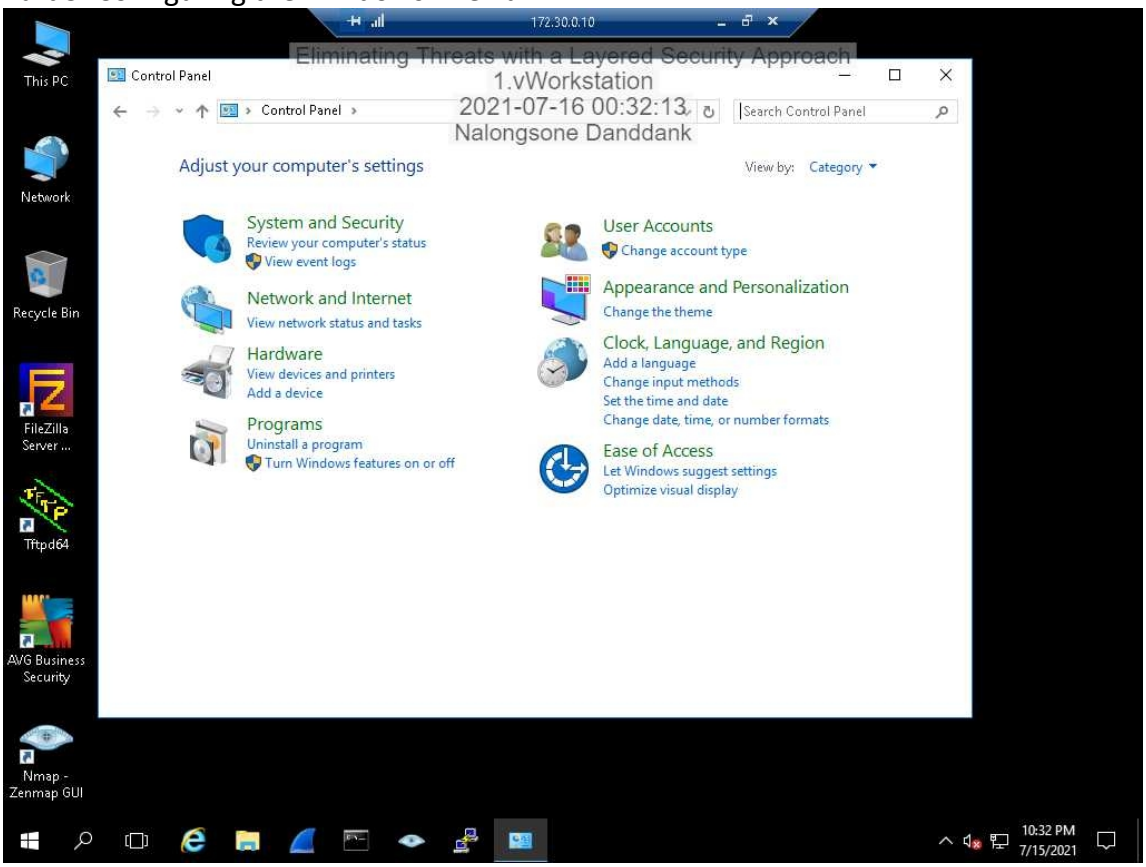

Services
File Action View Help
172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:18:26
Nalongsone Danddank
Services (Local)
Name
Description
Status
Startup Type
Log On As
AVG Antivirus Admin Client
Running
Automatic
Local Syste...
AvgWscReporter
Manual
Local Syste...
Background Intelligent Transfer Service
Transfers files in the background using i...
Manual
Local Syste...
Background Tasks Infrastructure Service
Windows infrastructure service that cont...
Running
Automatic
Local Syste...
Base Filtering Engine
The Base Filtering Engine (BFE) is a servi...
Running
Automatic
Local Service
Bluetooth Support Service
The Bluetooth service supports discover...
Running
Automatic (T...
Local Service
CDPUserSvc_515b9
<Failed to Read Description. Error Code: ...
Running
Automatic
Local Syste...
Certificate Propagation
Copies user certificates and root certifica...
Running
Manual
Local Syste...
Client License Service (ClipSVC)
Provides infrastructure support for the ...
Running
Manual (Trig...
Local Syste...
CNG Key Isolation
The CNG key isolation service is hosted i...
Running
Manual (Trig...
Local Syste...
COM+ Event System
Supports System Event Notification Servi...
Running
Automatic
Local Service
COM+ System Application
Manages the configuration and tracking...
Running
Manual
Local Syste...
Computer Browser
Maintains an updated list of computers ...
Disabled
Local Syste...
Connected Devices Platform Service
This service is used for Connected Devic...
Automatic (D...
Local Service
Connected User Experiences and Telemetry
The Connected User Experiences and Tel...
Running
Automatic
Local Syste...
Contact Data_515b9
Indexes contact data for fast contact sea...
Manual
Local Syste...
CoreMessaging
Manages communication between syste...
Running
Automatic
Local Service
Credential Manager
Provides secure storage and retrieval of ...
Running
Manual
Local Syste...
Cryptographic Services
Provides three management services: Ca...
Running
Automatic
Network S...
Data Sharing Service
Provides data brokering between applica...
Manual (Trig...
Local Syste...
DataCollectionPublishingService
The DCP (Data Collection and Publishin...
Manual (Trig...
Local Syste...
DCOM Server Process Launcher
The DCOMLAUNCH service launches C...
Running
Automatic
Local Syste...
Device Association Service
Enables pairing between the system and ...
Manual (Trig...
Local Syste...
Device Install Service
Enables a computer to recognize and ad...
Manual (Trig...
Local Syste...
Device Management Enrollment Service
Performs Device Enrollment Activities fo...
Manual
Local Syste...
Device Setup Manager
Enables the detection, download and ins...
Manual (Trig...
Local Syste...
DevQuery Background Discovery Broker
Enables apps to discover devices with a ...
Manual (Trig...
Local Syste...
DHCP Client
Registers and updates IP addresses and ...
Running
Automatic
Local Service
Diagnostic Policy Service
The Diagnostic Policy Service enables pr...
Running
Automatic (D...
Local Service
Diagnostic Service Host
The Diagnostic Service Host is used by t...
Manual
Local Service
Diagnostic System Host
The Diagnostic System Host is used by t...
Manual
Local Syste...
Extended
Standard
10:18 PM
7/15/2021

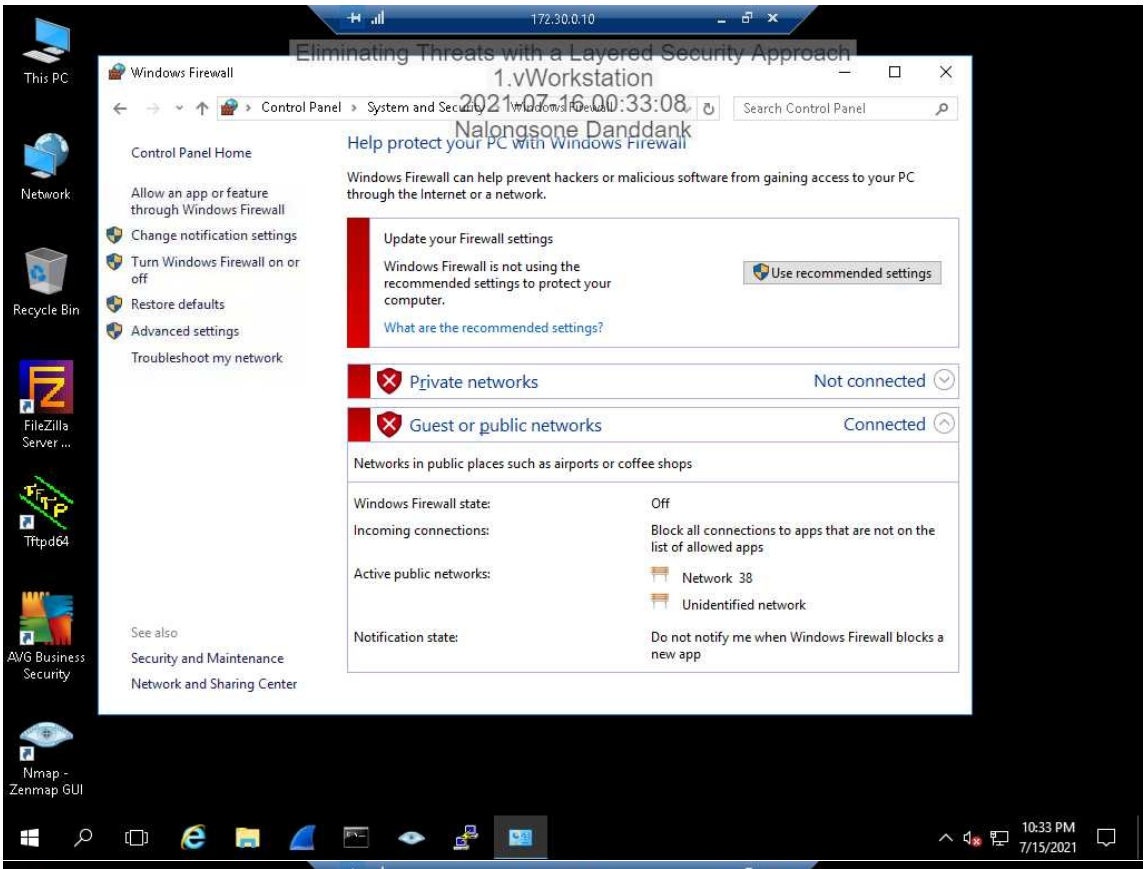

Services
File Action View Help
172.30.0.10
Restore Down
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:22:53
Nalongsone Danddank
Services (Local)
Telephony
Stop the service
Pause the service
Restart the service
Description:
Provides Telephony API (TAPI) support for programs that contr
telephony devices on the local
computer and, through the LAN
servers that are also running the
service.
Name
Description
Status
Telephony Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name: TapiSrv
Display name: Telephony
Description: Provides Telephony API (TAPI) support for programs that control telephony devices on the local computer
Path to executable:
C:\Windows\System32\svchost.exe -k NetworkService
Startup type: Automatic
Service status: Running
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply
Windows Audio Endpoint Builder
Manages audio devices for the Windows...
Windows Biometric Service
The Windows biometric service gives cli...
Windows Camera Frame Server
Enables multiple clients to access video f...
Extended
Standard
10:22 PM
7/15/2021

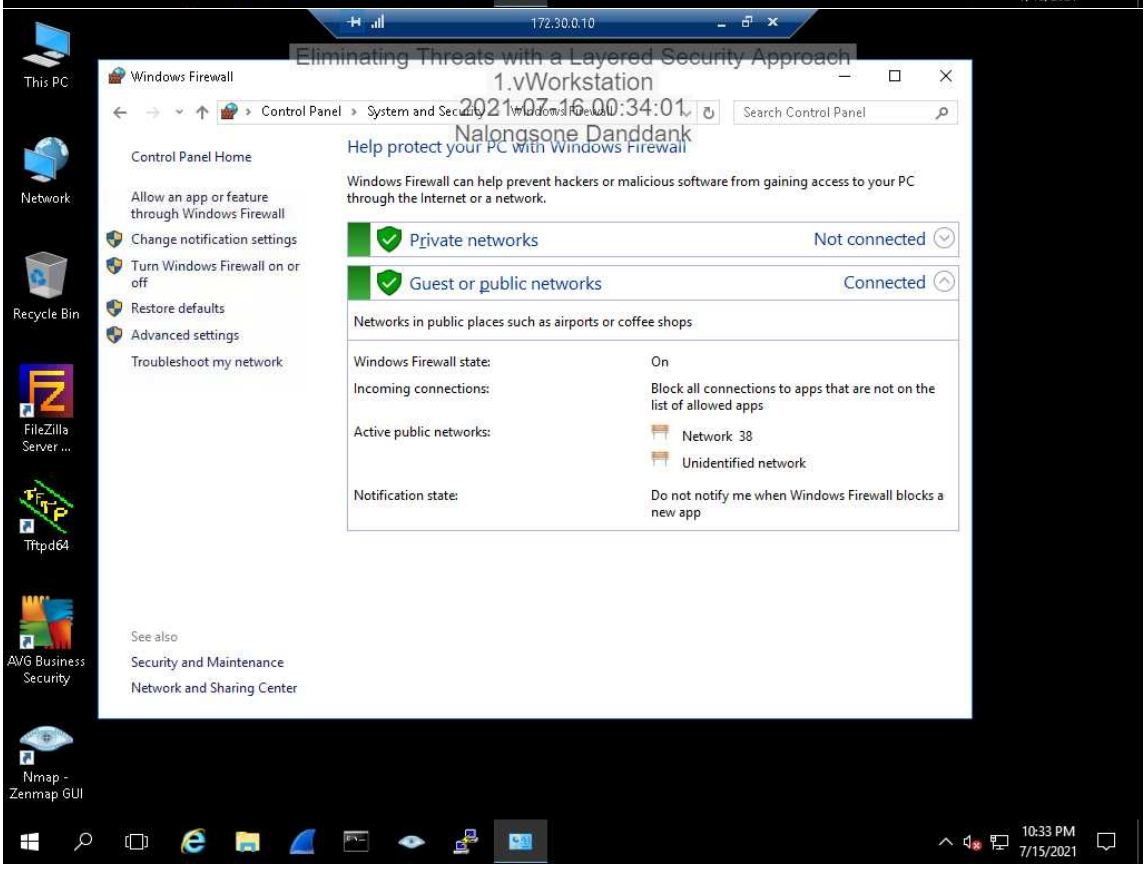

Services
File Action View Help
172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:23:09
Nalongsone Danddank
Services (Local)
Telephony
Stop the service
Pause the service
Restart the service
Description:
Provides Telephony API (TAPI) support for programs that contr
telephony devices on the local
computer and, through the LAN
servers that are also running the
service.
Name
Description
Status
Telephony Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name: TapiSrv
Display name: Telephony
Description: Provides Telephony API (TAPI) support for programs that control telephony devices on the local computer
Path to executable:
C:\Windows\System32\svchost.exe -k NetworkService
Startup type: Disabled
Service status: Running
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply
Windows Audio Endpoint Builder
Manages audio devices for the Windows...
Windows Biometric Service
The Windows biometric service gives cli...
Windows Camera Frame Server
Enables multiple clients to access video f...
Extended
Standard
10:23 PM
7/15/2021

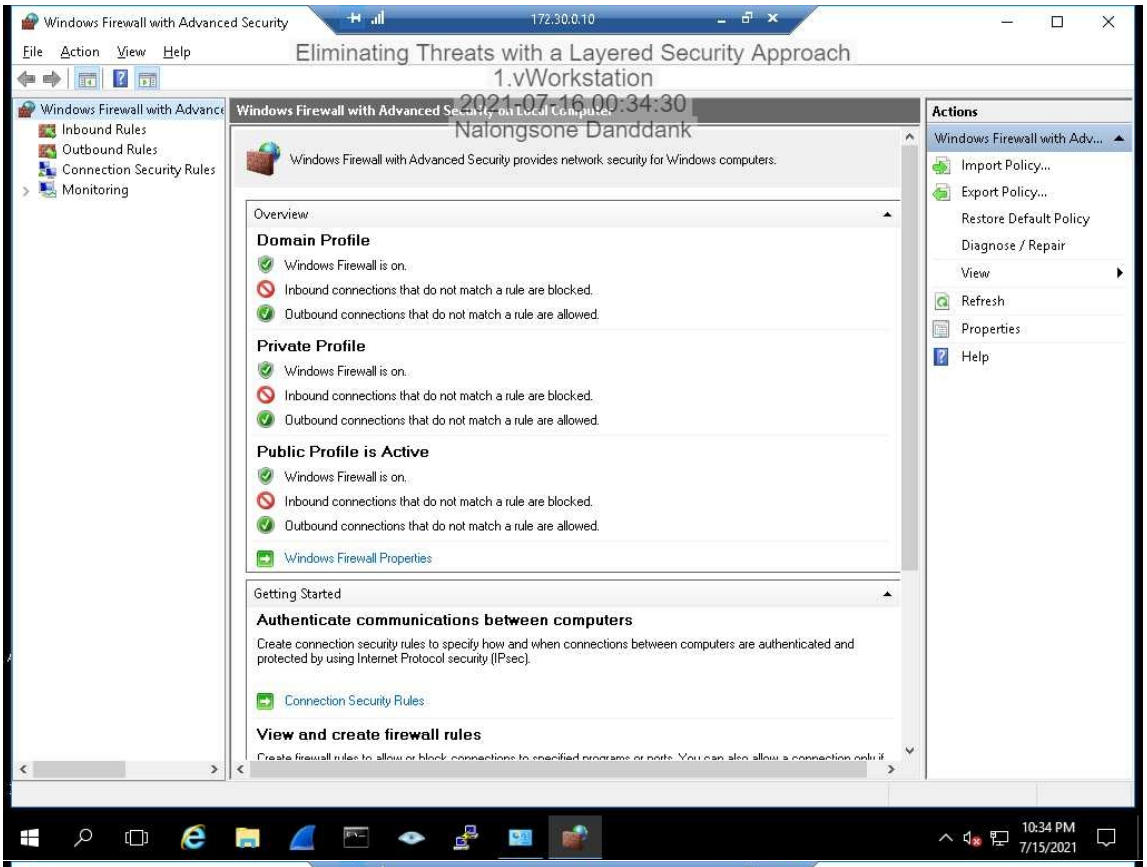


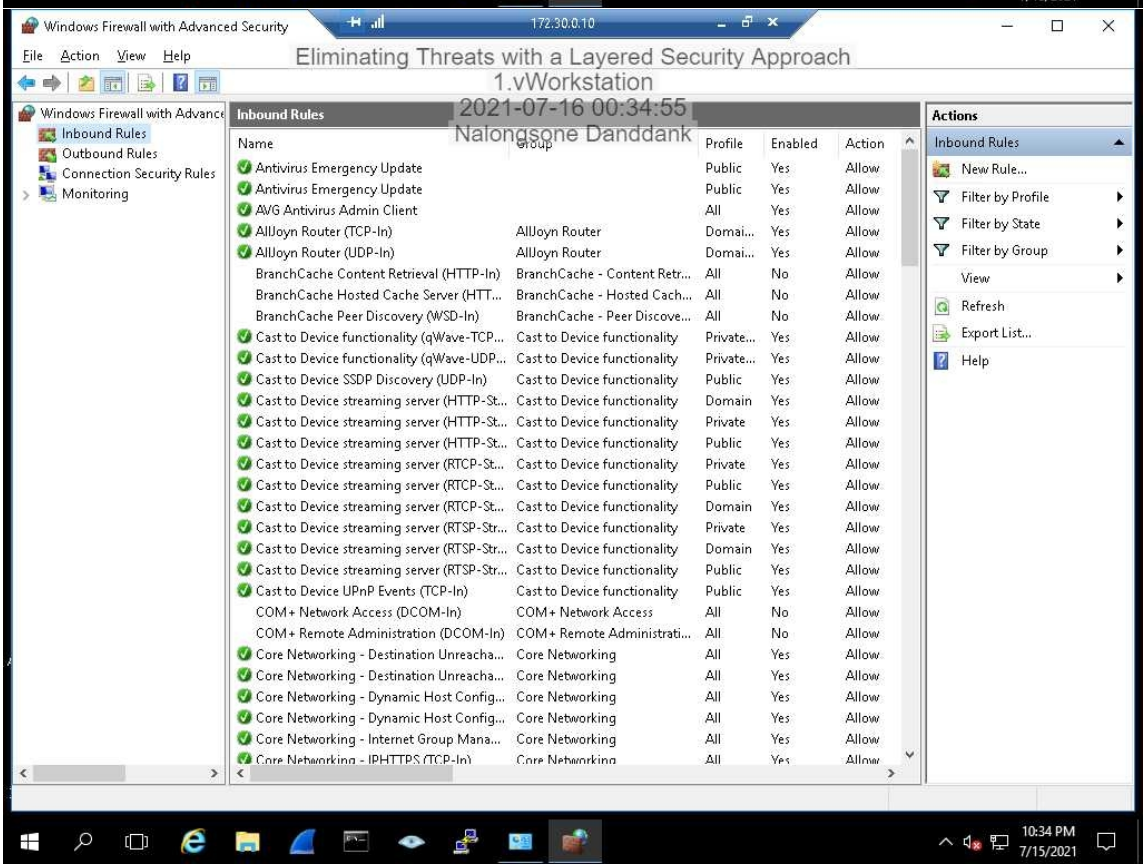
Part 3: Configuring the Windows Firewall.

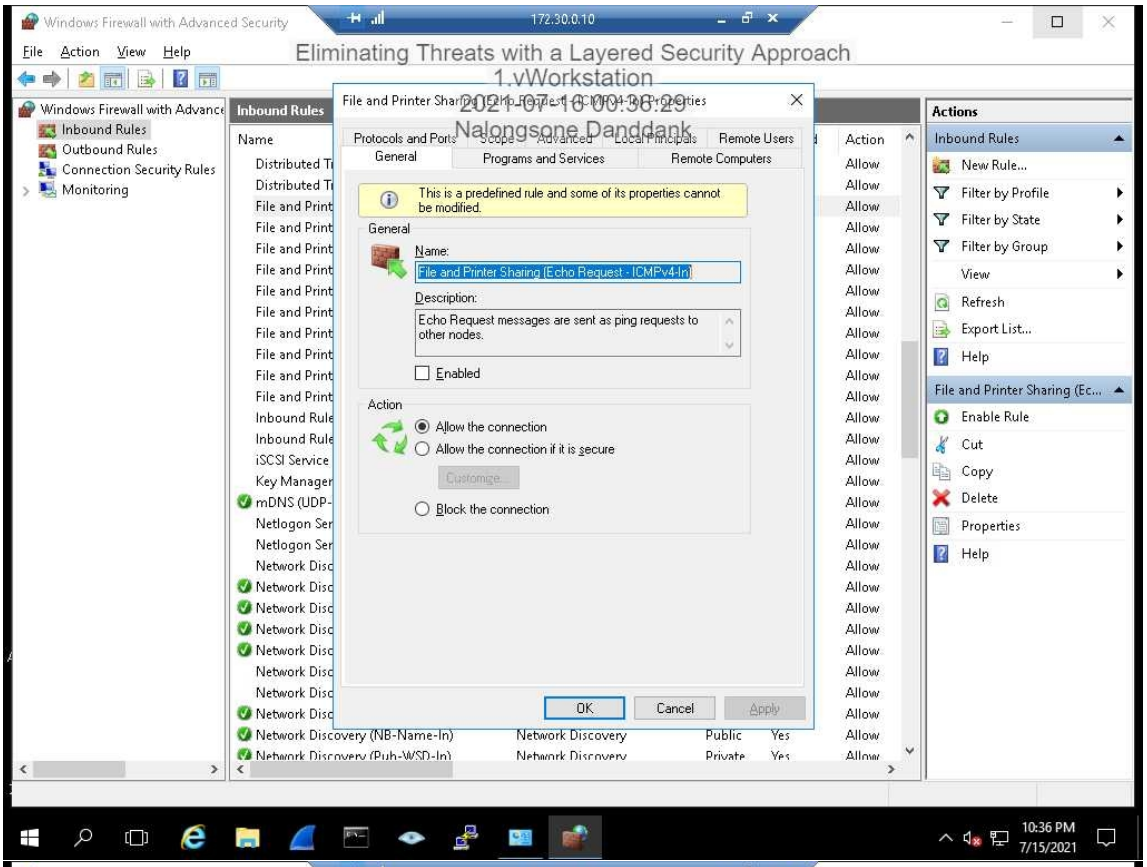


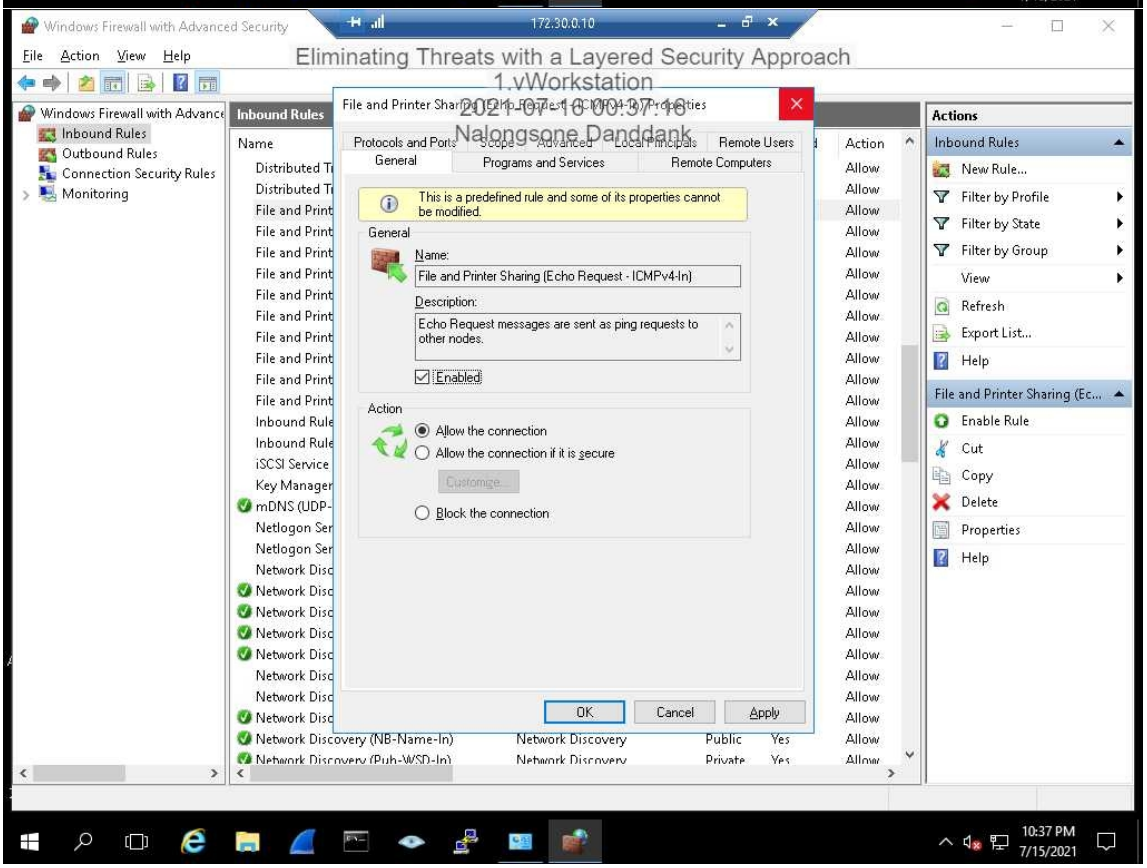

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:33:08
Nalongsone Danddank
Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Update your Firewall settings
Windows Firewall is not using the recommended settings to protect your computer.
Use recommended settings
What are the recommended settings?
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state:
Off
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active public networks:
Network 38
Unidentified network
Notification state:
Do not notify me when Windows Firewall blocks a new app
See also
Security and Maintenance
Network and Sharing Center
This PC
Network
Recycle Bin
FileZilla Server ...
Tftpd64
AVG Business Security
Nmap - Zenmap GUI
10:33 PM
7/15/2021

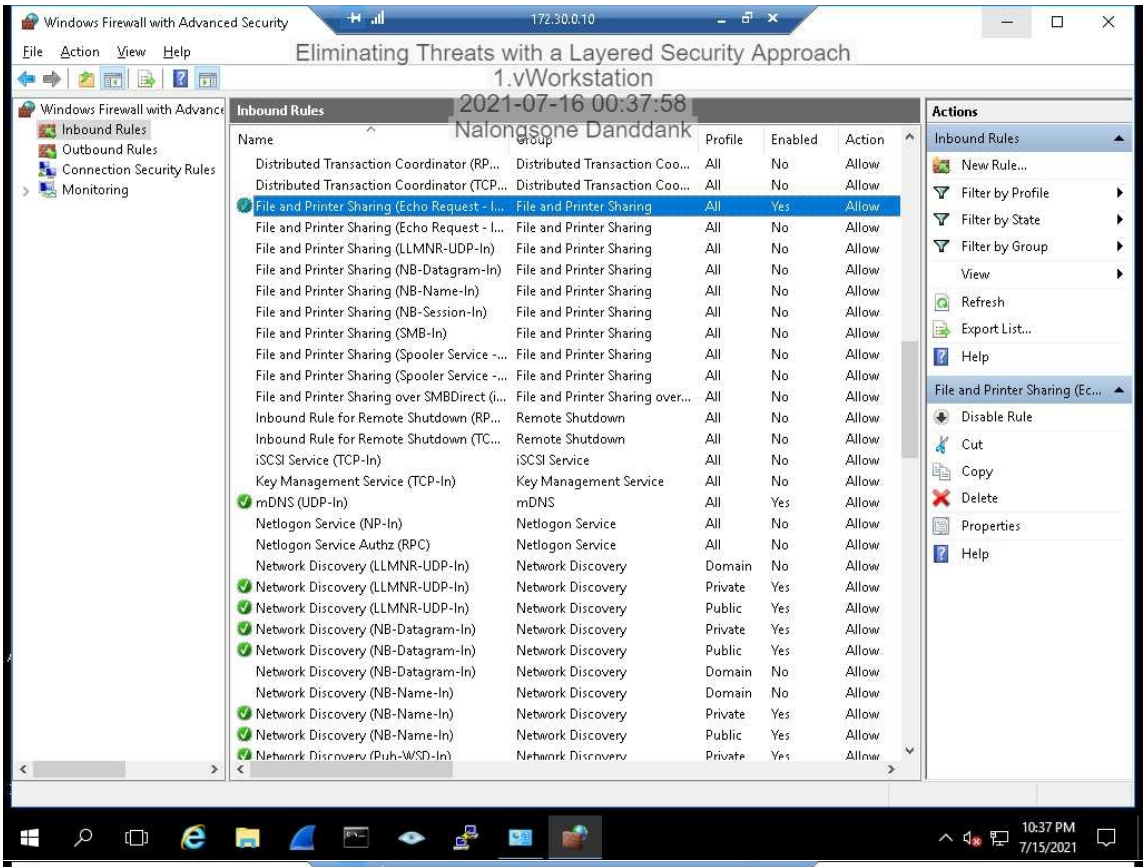

172.30.0.10
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:34:01
Nalongsone Danddank
Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your PC with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.
Private networks
Not connected
Guest or public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state:
On
Incoming connections:
Block all connections to apps that are not on the list of allowed apps
Active public networks:
Network 38
Unidentified network
Notification state:
Do not notify me when Windows Firewall blocks a new app
See also
Security and Maintenance
Network and Sharing Center
This PC
Network
Recycle Bin
FileZilla Server ...
Tftpd64
AVG Business Security
Nmap - Zenmap GUI
10:33 PM
7/15/2021

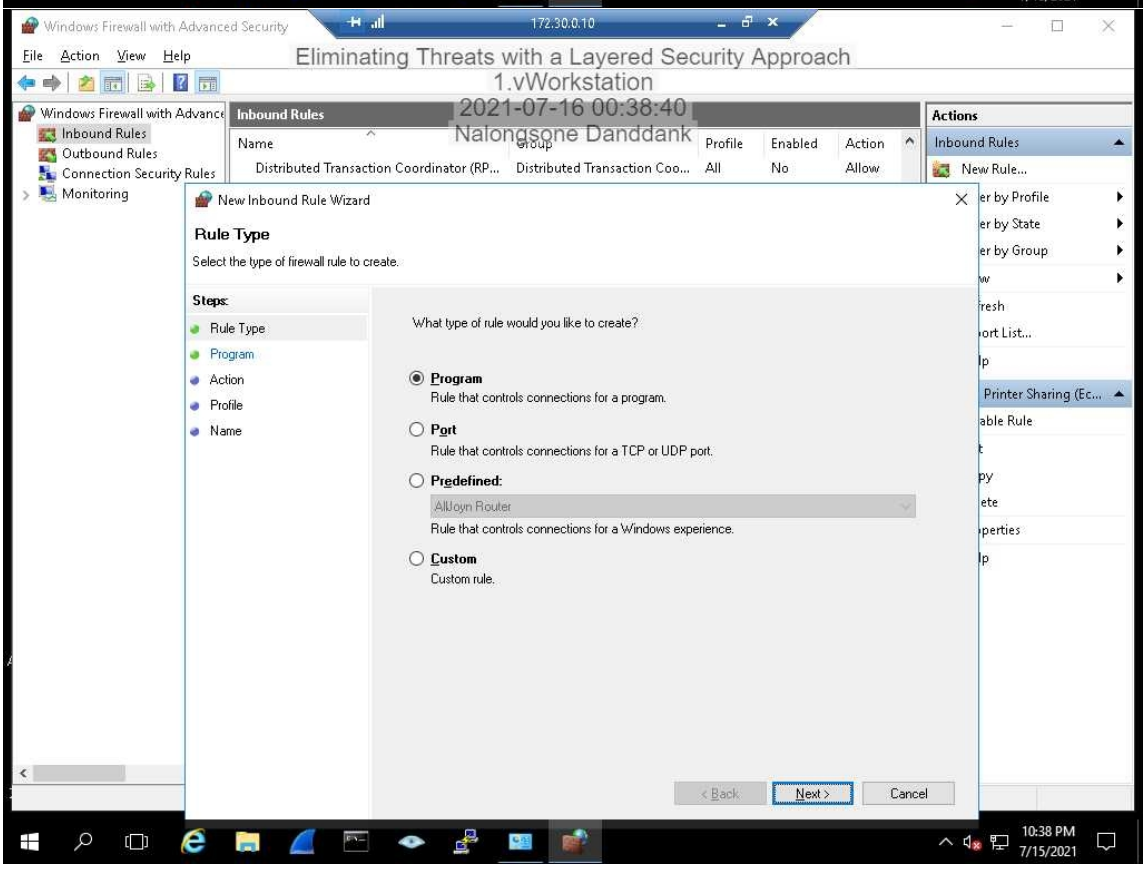

Windows Firewall with Advanced Security
172.30.0.10
File Action View Help
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:34:30
Nalongsone Danddank
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Windows Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile is Active
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Actions
Windows Firewall with Adv...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help
10:34 PM
7/15/2021

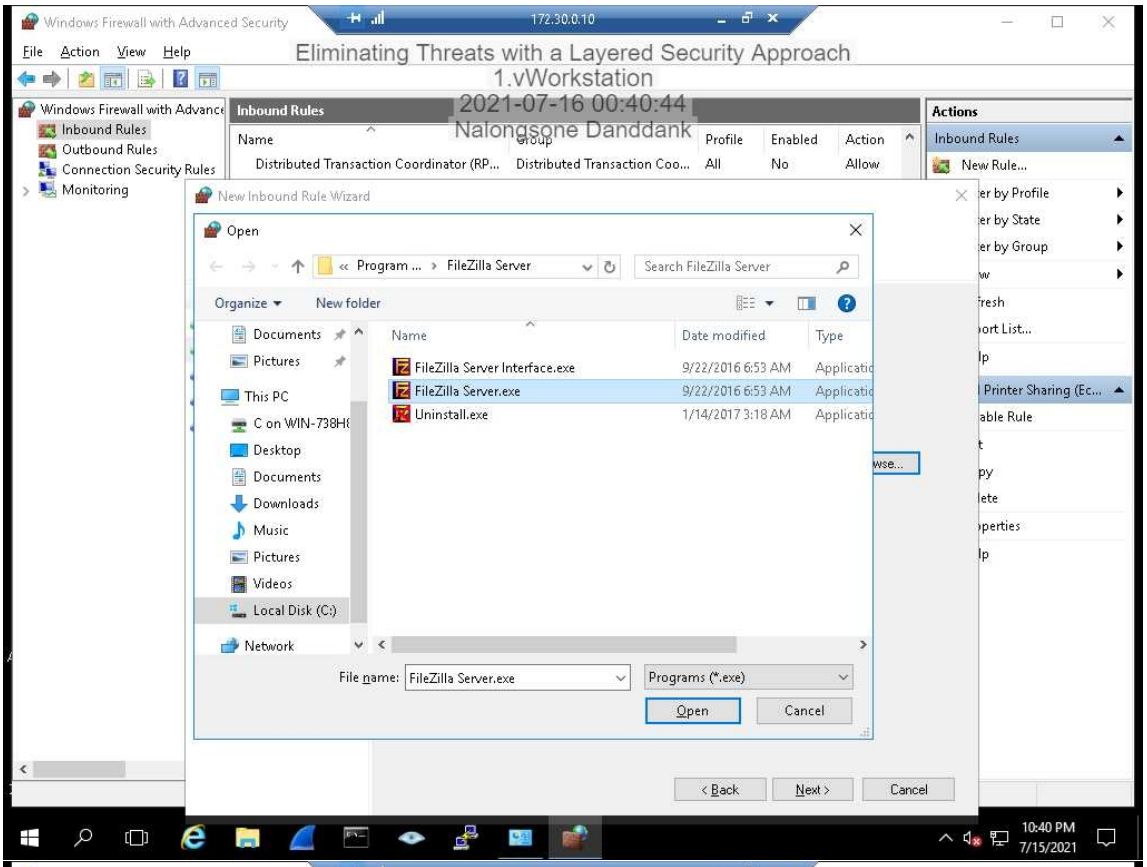

Windows Firewall with Advanced Security
172.30.0.10
File Action View Help
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:34:55
Nalongsone Danddank
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Antivirus Emergency Update Public Yes Allow
Antivirus Emergency Update Public Yes Allow
AVG Antivirus Admin Client All Yes Allow
AllJoyn Router (TCP-In) AllJoyn Router Domai... Yes Allow
AllJoyn Router (UDP-In) AllJoyn Router Domai... Yes Allow
BranchCache Content Retrieval (HTTP-In) BranchCache - Content Retr... All No Allow
BranchCache Hosted Cache Server (HTT... BranchCache - Hosted Cach... All No Allow
BranchCache Peer Discovery (WSD-In) BranchCache - Peer Discove... All No Allow
Cast to Device functionality (qWave-TCP... Cast to Device functionality Private... Yes Allow
Cast to Device functionality (qWave-UDP... Cast to Device functionality Private... Yes Allow
Cast to Device SSDP Discovery (UDP-In) Cast to Device functionality Public Yes Allow
Cast to Device streaming server (HTTP-St... Cast to Device functionality Domain Yes Allow
Cast to Device streaming server (HTTP-St... Cast to Device functionality Private Yes Allow
Cast to Device streaming server (HTTP-St... Cast to Device functionality Public Yes Allow
Cast to Device streaming server (RTCP-St... Cast to Device functionality Private Yes Allow
Cast to Device streaming server (RTCP-St... Cast to Device functionality Public Yes Allow
Cast to Device streaming server (RTCP-St... Cast to Device functionality Domain Yes Allow
Cast to Device streaming server (RTSP-Str... Cast to Device functionality Private Yes Allow
Cast to Device streaming server (RTSP-Str... Cast to Device functionality Domain Yes Allow
Cast to Device streaming server (RTSP-Str... Cast to Device functionality Public Yes Allow
Cast to Device UPnP Events (TCP-In) Cast to Device functionality Public Yes Allow
COM+ Network Access (DCOM-In) COM+ Network Access All No Allow
COM+ Remote Administration (DCOM-In) COM+ Remote Administrati... All No Allow
Core Networking - Destination Unreacha... Core Networking All Yes Allow
Core Networking - Destination Unreacha... Core Networking All Yes Allow
Core Networking - Dynamic Host Config... Core Networking All Yes Allow
Core Networking - Dynamic Host Config... Core Networking All Yes Allow
Core Networking - Internet Group Mana... Core Networking All Yes Allow
Core Networking - IPHTTPS (TCP-In) Core Networking All Yes Allow
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
10:34 PM
7/15/2021

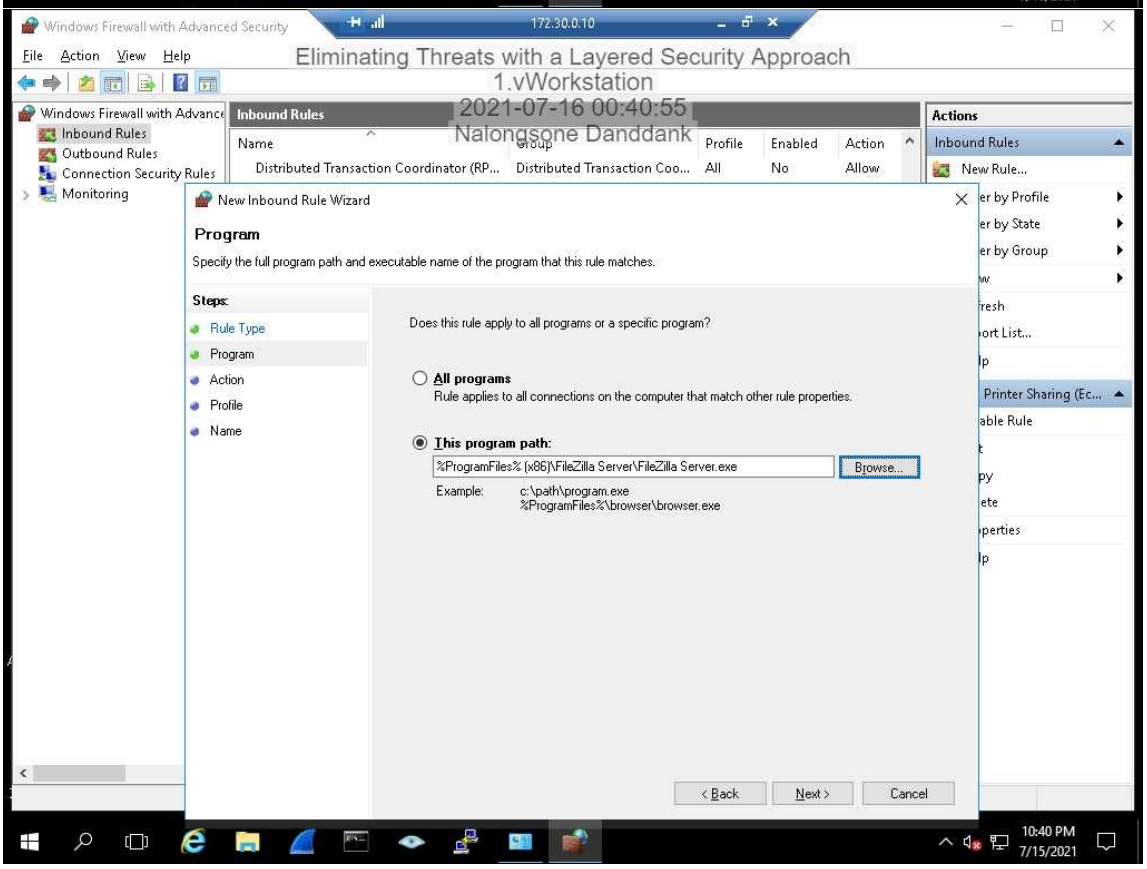

Windows Firewall with Advanced Security
172.30.0.10
File Action View Help
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:36:29
Nalongsone Danddank
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Action
Actions
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
File and Printer Sharing (Ec...
Enable Rule
Cut
Copy
Delete
Properties
Help
File and Printer Sharing (Echo Request - ICMPv4-In) Properties
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
General
Programs and Services
Remote Computers
This is a predefined rule and some of its properties cannot be modified.
General
Name:
File and Printer Sharing (Echo Request - ICMPv4-In)
Description:
Echo Request messages are sent as ping requests to other nodes.
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
OK
Cancel
Apply
Network Discovery (NB-Name-In)
Network Discovery
Public
Yes
Allow
10:36 PM
7/15/2021

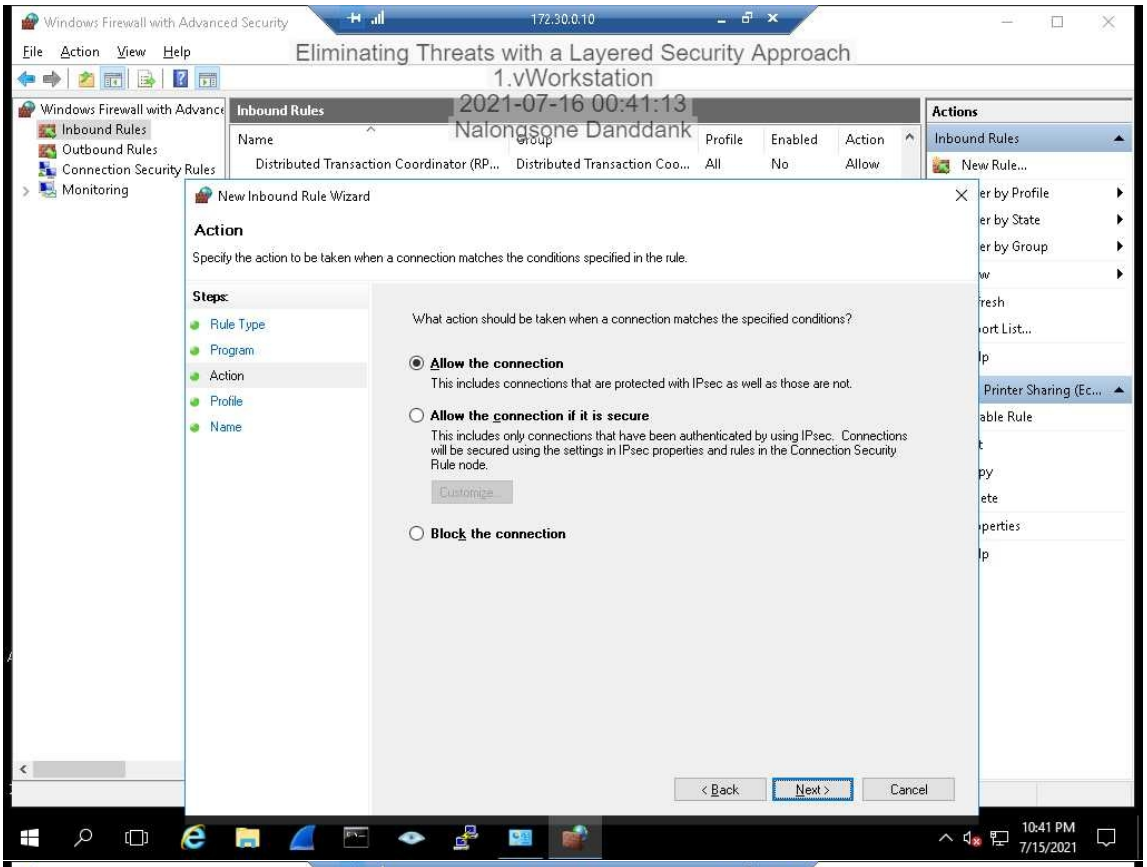

Windows Firewall with Advanced Security
172.30.0.10
File Action View Help
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:37:16
Nalongsone Danddank
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Action
Actions
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
File and Printer Sharing (Ec...
Enable Rule
Cut
Copy
Delete
Properties
Help
File and Printer Sharing (Echo Request - ICMPv4-In) Properties
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
General
Programs and Services
Remote Computers
This is a predefined rule and some of its properties cannot be modified.
General
Name:
File and Printer Sharing (Echo Request - ICMPv4-In)
Description:
Echo Request messages are sent as ping requests to other nodes.
Enabled
Action
Allow the connection
Allow the connection if it is secure
Customize...
Block the connection
OK
Cancel
Apply
Network Discovery (NB-Name-In)
Network Discovery
Public
Yes
Allow
10:37 PM
7/15/2021

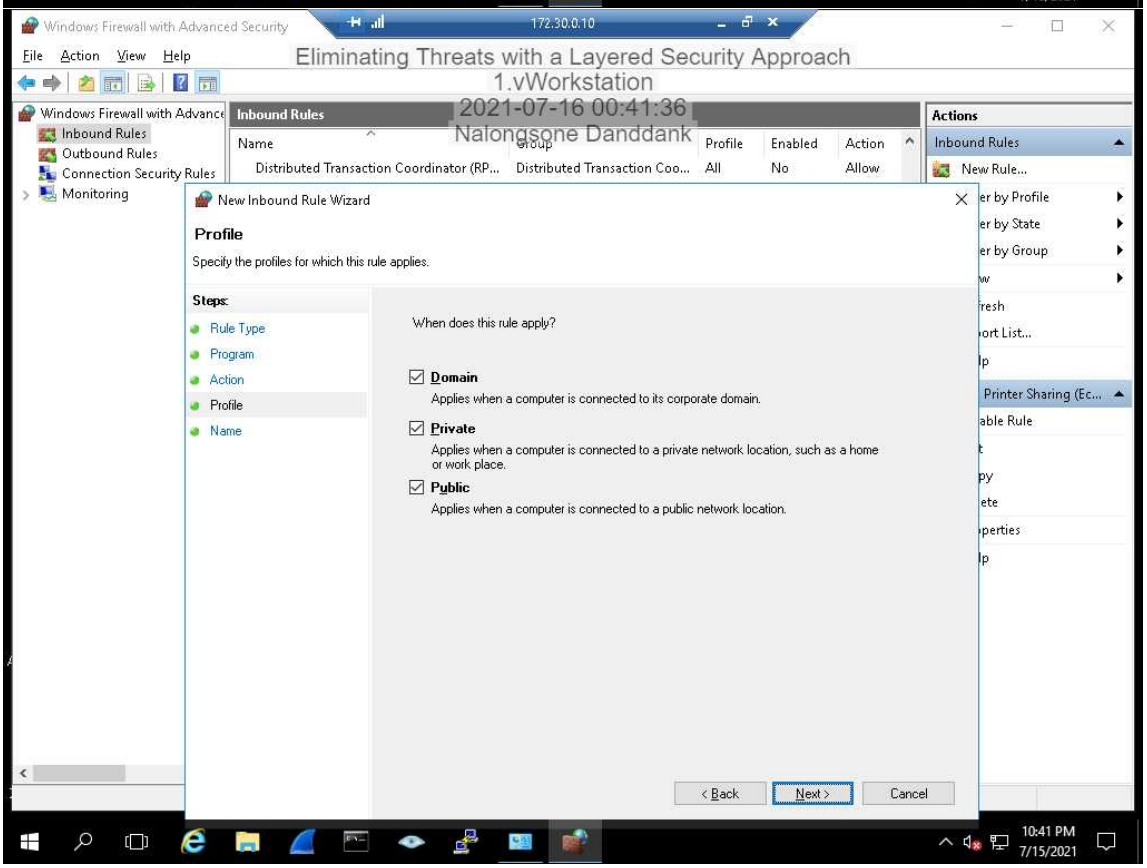

Windows Firewall with Advanced Security
172.30.0.10
File Action View Help
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:37:58
Nalongsone Danddank
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Distributed Transaction Coordinator (RP... Distributed Transaction Coo... All No Allow
Distributed Transaction Coordinator (TCP... Distributed Transaction Coo... All No Allow
File and Printer Sharing (Echo Request - I... File and Printer Sharing All Yes Allow
File and Printer Sharing (Echo Request - I... File and Printer Sharing All No Allow
File and Printer Sharing (LLMNR-UDP-In) File and Printer Sharing All No Allow
File and Printer Sharing (NB-Datagram-In) File and Printer Sharing All No Allow
File and Printer Sharing (NB-Name-In) File and Printer Sharing All No Allow
File and Printer Sharing (NB-Session-In) File and Printer Sharing All No Allow
File and Printer Sharing (SMB-In) File and Printer Sharing All No Allow
File and Printer Sharing (Spooler Service -... File and Printer Sharing All No Allow
File and Printer Sharing (Spooler Service -... File and Printer Sharing All No Allow
File and Printer Sharing over SMBDirect (i... File and Printer Sharing over... All No Allow
Inbound Rule for Remote Shutdown (RP... Remote Shutdown All No Allow
Inbound Rule for Remote Shutdown (TC... Remote Shutdown All No Allow
iSCSI Service (TCP-In) iSCSI Service All No Allow
Key Management Service (TCP-In) Key Management Service All No Allow
mDNS (UDP-In) mDNS All Yes Allow
Netlogon Service (NP-In) Netlogon Service All No Allow
Netlogon Service Authz (RPC) Netlogon Service All No Allow
Network Discovery (LLMNR-UDP-In) Network Discovery Domain No Allow
Network Discovery (LLMNR-UDP-In) Network Discovery Private Yes Allow
Network Discovery (LLMNR-UDP-In) Network Discovery Public Yes Allow
Network Discovery (NB-Datagram-In) Network Discovery Private Yes Allow
Network Discovery (NB-Datagram-In) Network Discovery Public Yes Allow
Network Discovery (NB-Datagram-In) Network Discovery Domain No Allow
Network Discovery (NB-Name-In) Network Discovery Domain No Allow
Network Discovery (NB-Name-In) Network Discovery Private Yes Allow
Network Discovery (NB-Name-In) Network Discovery Public Yes Allow
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
File and Printer Sharing (Ec...
Disable Rule
Cut
Copy
Delete
Properties
Help
10:37 PM
7/15/2021

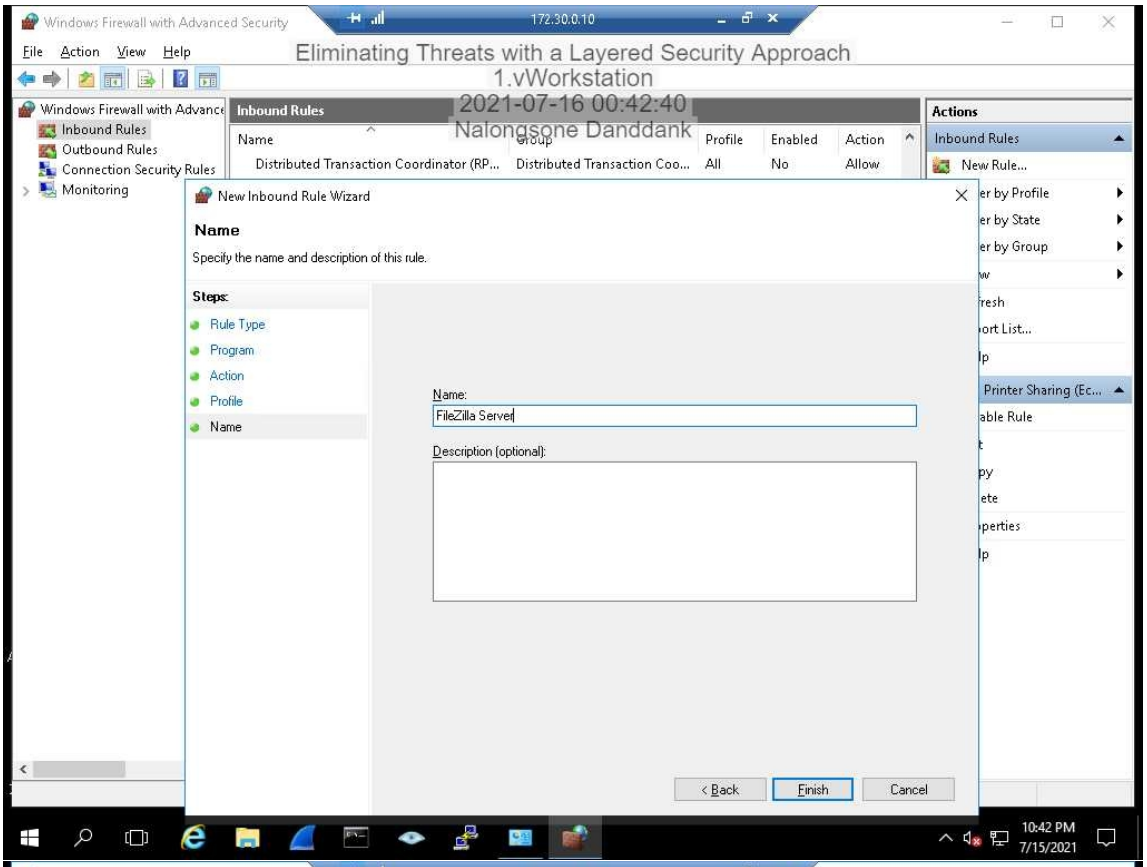

Windows Firewall with Advanced Security
172.30.0.10
File Action View Help
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:38:40
Nalongsone Danddank
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Name
Group
Profile
Enabled
Action
Distributed Transaction Coordinator (RP... Distributed Transaction Coo... All No Allow
New Inbound Rule Wizard
Rule Type
Select the type of firewall rule to create.
Steps:
Rule Type
Program
Action
Profile
Name
What type of rule would you like to create?
Program
Rule that controls connections for a program.
Port
Rule that controls connections for a TCP or UDP port.
Predefined:
AllJoyn Router
Rule that controls connections for a Windows experience.
Custom
Custom rule.
< Back
Next >
Cancel
Actions
Inbound Rules
New Rule...
10:38 PM
7/15/2021

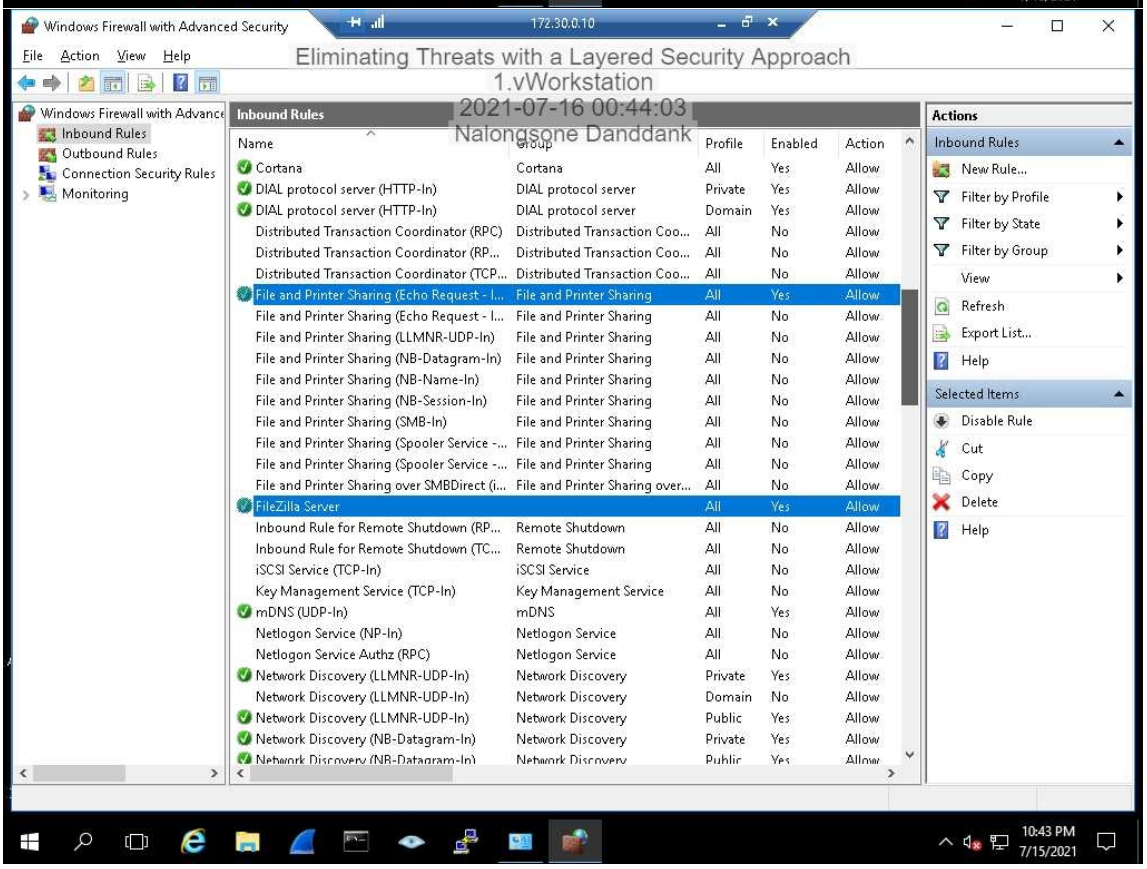

Windows Firewall with Advanced Security
172.30.0.10
File Action View Help
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:40:44
Nalongsone Danddank
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Name
Profile
Enabled
Action
Distributed Transaction Coordinator (RP...
Distributed Transaction Coo...
All
No
Allow
Actions
New Rule...
New Inbound Rule Wizard
Open
Program ... › FileZilla Server
Search FileZilla Server
Organize
New folder
Documents
Pictures
This PC
Desktop
Downloads
Music
Videos
Local Disk (C:)
Network
Name
Date modified
Type
FileZilla Server Interface.exe
9/22/2016 6:53 AM
FileZilla Server.exe
9/22/2016 6:53 AM
Uninstall.exe
1/14/2017 3:18 AM
File name: FileZilla Server.exe
Programs (*.exe)
Open
Cancel
< Back
Next >
Cancel
10:40 PM
7/15/2021


Windows Firewall with Advanced Security
172.30.0.10
File Action View Help
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:40:55
Nalongsone Danddank
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Name
Profile
Enabled
Action
Distributed Transaction Coordinator (RP...
Distributed Transaction Coo...
All
No
Allow
Actions
New Rule...
New Inbound Rule Wizard
Program
Specify the full program path and executable name of the program that this rule matches.
Steps:
Rule Type
Program
Action
Profile
Name
Does this rule apply to all programs or a specific program?
All programs
Rule applies to all connections on the computer that match other rule properties.
This program path:
%ProgramFiles% (x86)\FileZilla Server\FileZilla Server.exe
Browse...
Example:
c:\path\program.exe
%ProgramFiles%\browser\browser.exe
< Back
Next >
Cancel
10:40 PM
7/15/2021


Windows Firewall with Advanced Security
172.30.0.10
File Action View Help
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:41:13
Nalongsone Danddank
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Distributed Transaction Coordinator (RP...
Distributed Transaction Coo...
All
No
Allow
Actions
Inbound Rules
New Rule...
New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
< Back
Next >
Cancel
10:41 PM
7/15/2021


Windows Firewall with Advanced Security
172.30.0.10
File Action View Help
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:41:36
Nalongsone Danddank
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enabled
Action
Distributed Transaction Coordinator (RP...
Distributed Transaction Coo...
All
No
Allow
Actions
Inbound Rules
New Rule...
New Inbound Rule Wizard
Profile
Specify the profiles for which this rule applies.
Steps:
Rule Type
Program
Action
Profile
Name
When does this rule apply?
Domain
Applies when a computer is connected to its corporate domain.
Private
Applies when a computer is connected to a private network location, such as a home or work place.
Public
Applies when a computer is connected to a public network location.
< Back
Next >
Cancel
10:41 PM
7/15/2021


Windows Firewall with Advanced Security
172.30.0.10
File Action View Help
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:42:40
Nalongsone Danddank
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Name
Group
Profile
Enabled
Action
Distributed Transaction Coordinator (RP...
Distributed Transaction Coo...
All
No
Allow
Actions
New Inbound Rule Wizard
Name
Specify the name and description of this rule.
Steps:
Rule Type
Program
Action
Profile
Name
Name:
FileZilla Server
Description (optional):
< Back
Finish
Cancel
10:42 PM
7/15/2021


Windows Firewall with Advanced Security
172.30.0.10
File Action View Help
Eliminating Threats with a Layered Security Approach
1.vWorkstation
2021-07-16 00:44:03
Nalongsone Danddank
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Name
Group
Profile
Enabled
Action
Cortana
Cortana
All
Yes
Allow
DIAL protocol server (HTTP-In)
DIAL protocol server
Private
Yes
Allow
DIAL protocol server (HTTP-In)
DIAL protocol server
Domain
Yes
Allow
Distributed Transaction Coordinator (RPC)
Distributed Transaction Coo...
All
No
Allow
Distributed Transaction Coordinator (RP...
Distributed Transaction Coo...
All
No
Allow
Distributed Transaction Coordinator (TCP...
Distributed Transaction Coo...
All
No
Allow
File and Printer Sharing (Echo Request - I...
File and Printer Sharing
All
Yes
Allow
File and Printer Sharing (Echo Request - I...
File and Printer Sharing
All
No
Allow
File and Printer Sharing (LLMNR-UDP-In)
File and Printer Sharing
All
No
Allow
File and Printer Sharing (NB-Datagram-In)
File and Printer Sharing
All
No
Allow
File and Printer Sharing (NB-Name-In)
File and Printer Sharing
All
No
Allow
File and Printer Sharing (NB-Session-In)
File and Printer Sharing
All
No
Allow
File and Printer Sharing (SMB-In)
File and Printer Sharing
All
No
Allow
File and Printer Sharing (Spooler Service -...
File and Printer Sharing
All
No
Allow
File and Printer Sharing (Spooler Service -...
File and Printer Sharing
All
No
Allow
File and Printer Sharing over SMBDirect (i...
File and Printer Sharing over...
All
No
Allow
FileZilla Server
All
Yes
Allow
Inbound Rule for Remote Shutdown (RP...
Remote Shutdown
All
No
Allow
Inbound Rule for Remote Shutdown (TC...
Remote Shutdown
All
No
Allow
iSCSI Service (TCP-In)
iSCSI Service
All
No
Allow
Key Management Service (TCP-In)
Key Management Service
All
No
Allow
mDNS (UDP-In)
mDNS
All
Yes
Allow
Netlogon Service (NP-In)
Netlogon Service
All
No
Allow
Netlogon Service Authz (RPC)
Netlogon Service
All
No
Allow
Network Discovery (LLMNR-UDP-In)
Network Discovery
Private
Yes
Allow
Network Discovery (LLMNR-UDP-In)
Network Discovery
Domain
No
Allow
Network Discovery (LLMNR-UDP-In)
Network Discovery
Public
Yes
Allow
Network Discovery (NB-Datagram-In)
Network Discovery
Private
Yes
Allow
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Selected Items
Disable Rule
Cut
Copy
Delete
Help
10:43 PM
7/15/2021

End.