Information Security Management

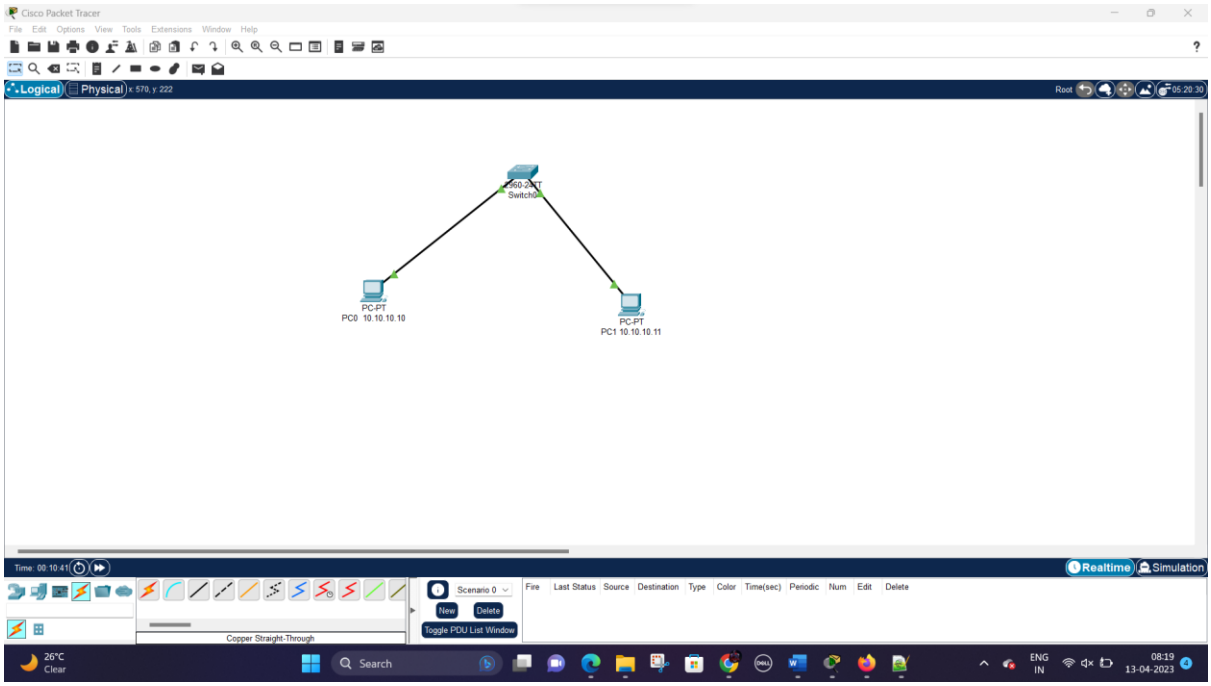
LABFAT

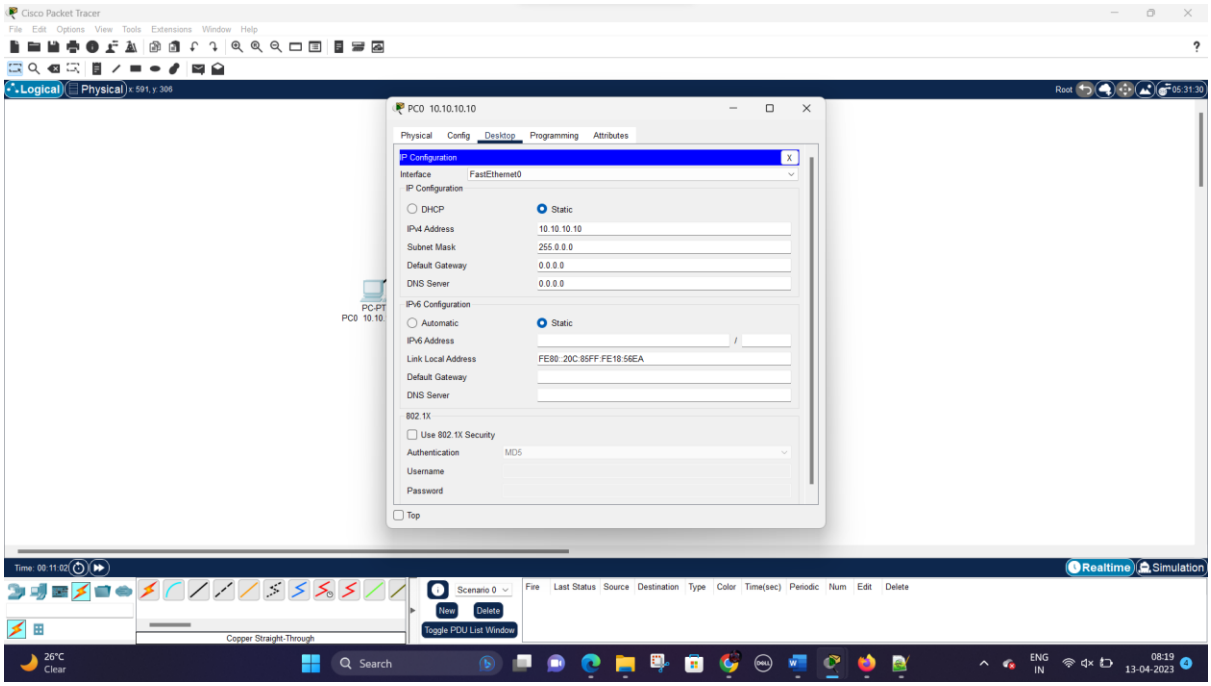
Name-Devansh Bajpai

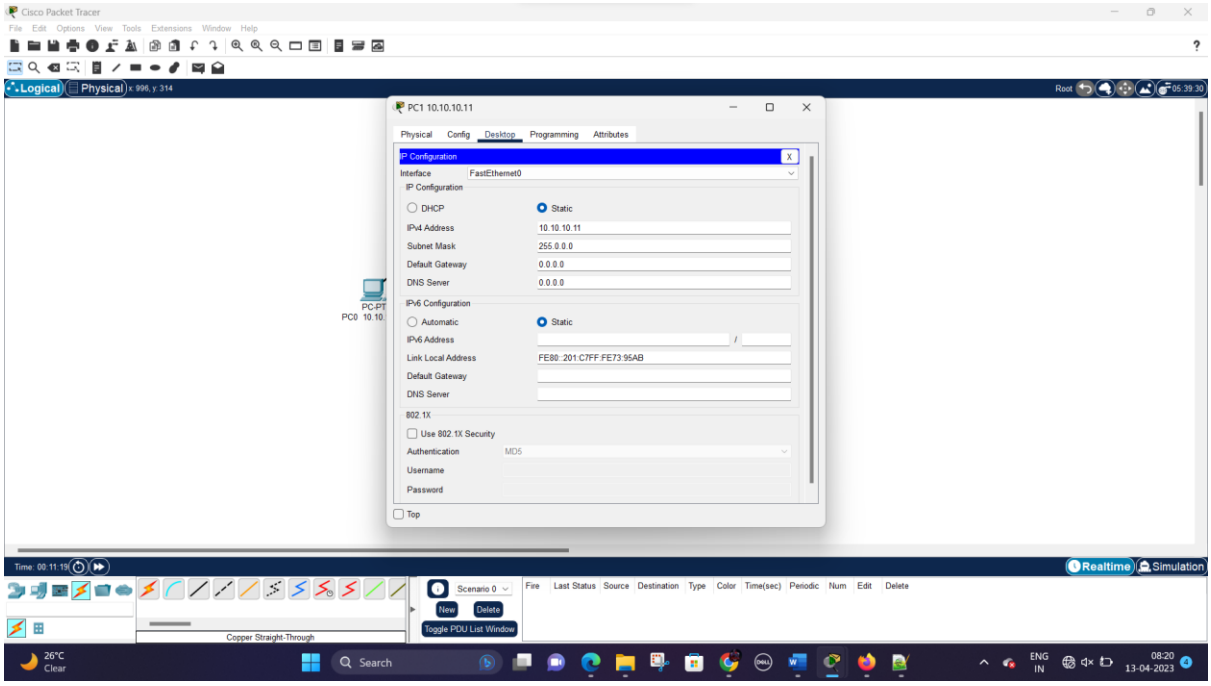
Regno-20BCE0807

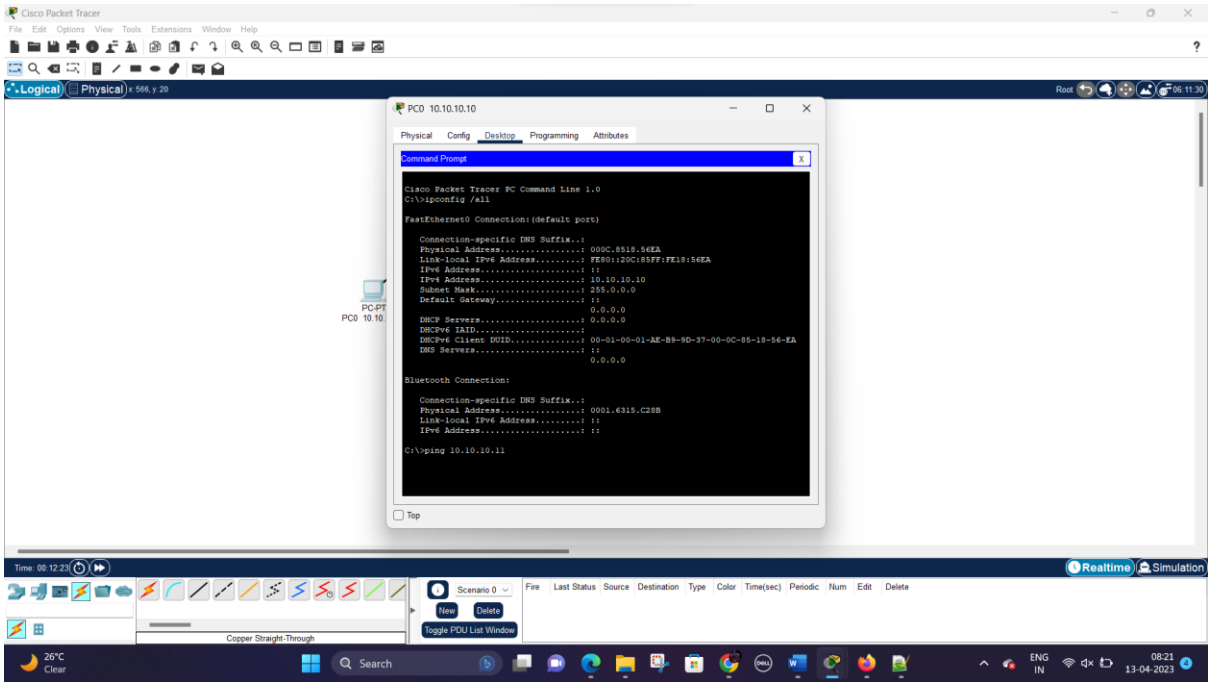
Q-1:

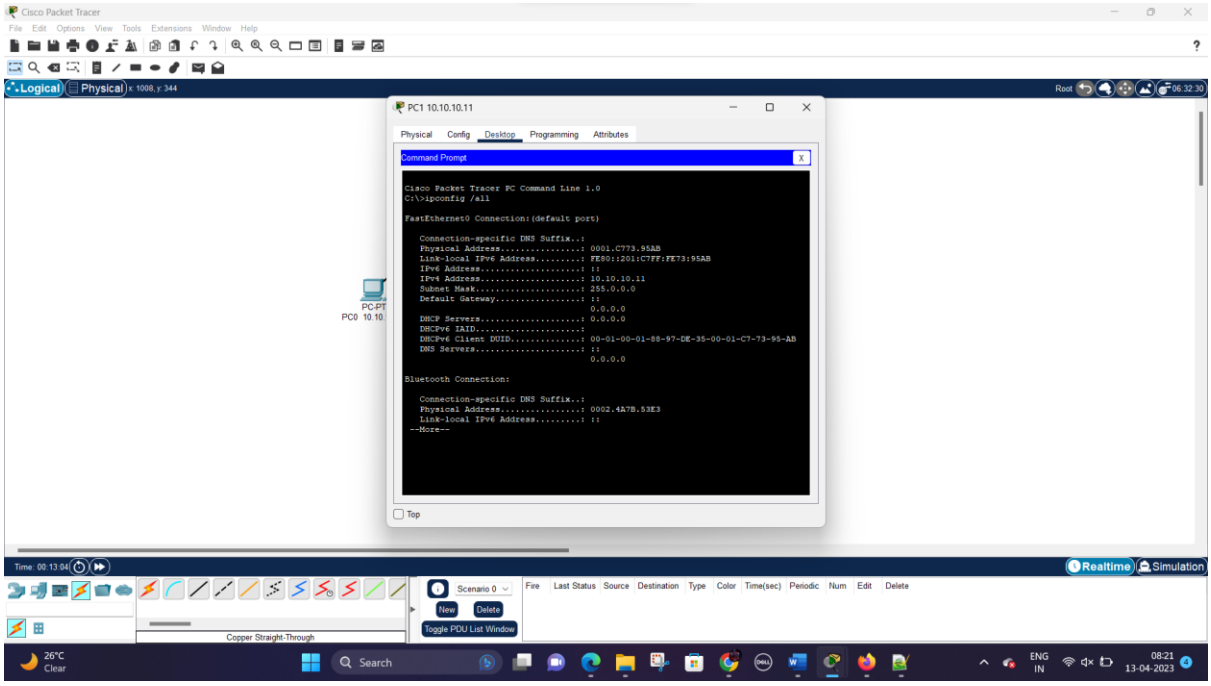
Demonstrate the Port security using the CISCO packet tracer and deploy the security policies in it. Test your network security w.r to the security policy.

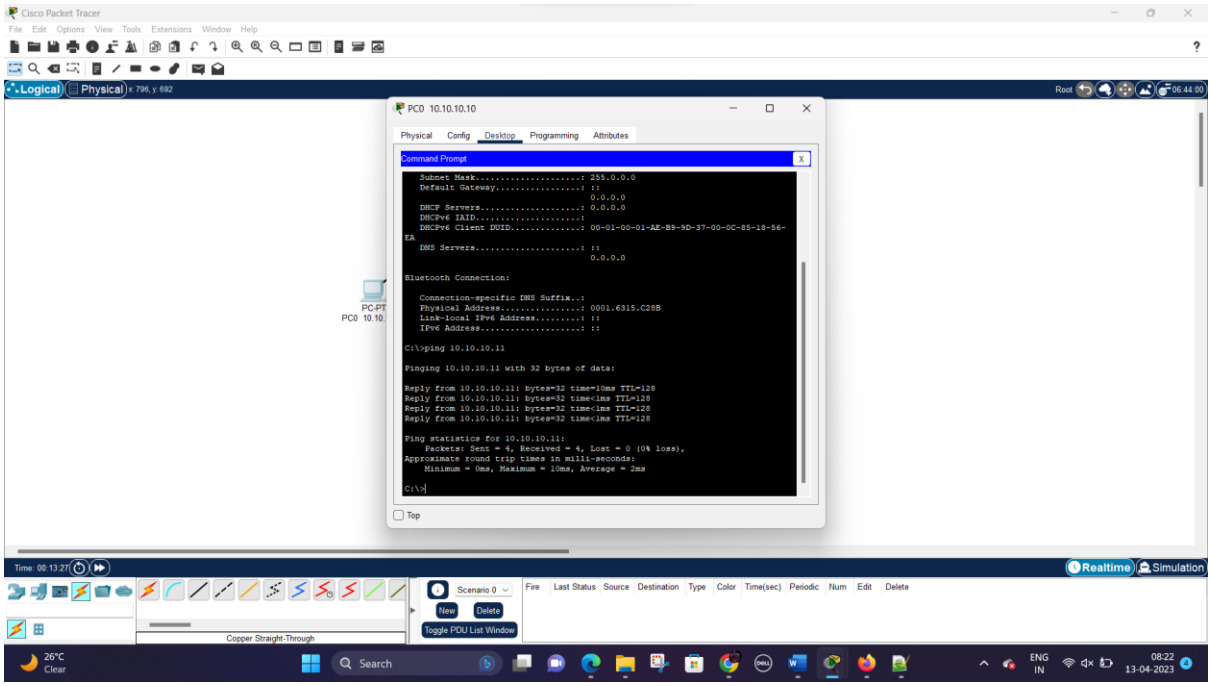


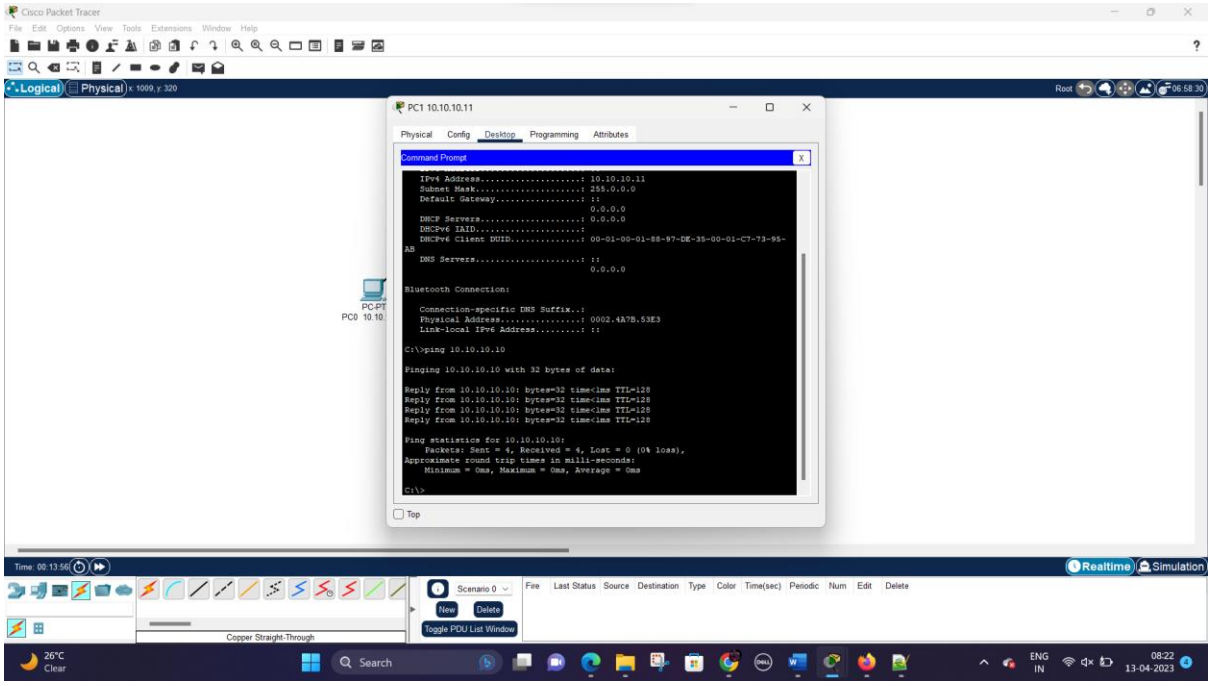

Cisco Packet Tracer
PC0 10.10.10.10
Physical Config Desktop Programming Attributes
IP Configuration
Interface FastEthernet0
DHCP
Static
IPv4 Address 10.10.10.10
Subnet Mask 255.0.0.0
Default Gateway 0.0.0.0
DNS Server 0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address FE80::20C:85FF:FE18:56EA
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication MD5
Username
Password
Top
Logical Physical
Root
Realtime Simulation
Copper Straight-Through
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
26°C Clear
Search
ENG IN
08:19 13-04-2023

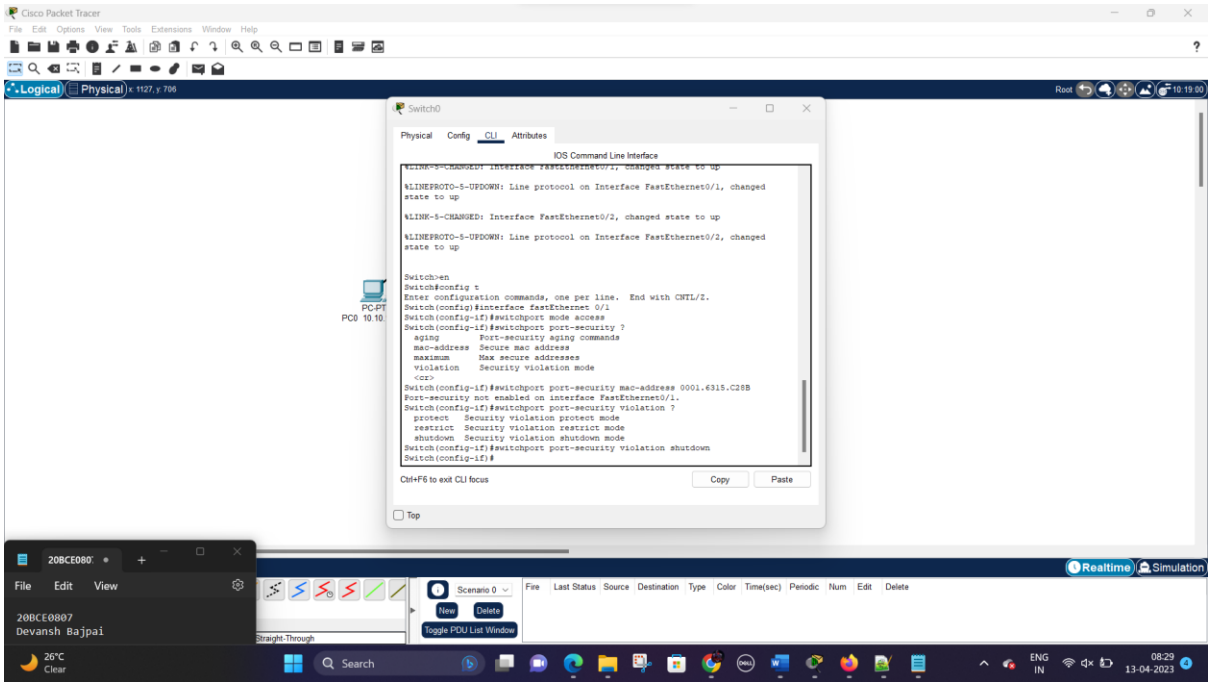

Cisco Packet Tracer
PC1 10.10.10.11
Physical Config Desktop Programming Attributes
IP Configuration
Interface FastEthernet0
DHCP
Static
IPv4 Address 10.10.10.11
Subnet Mask 255.0.0.0
Default Gateway 0.0.0.0
DNS Server 0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address FE80::201:C7FF:FE73:95AB
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication MD5
Username
Password
Top
Logical Physical
Root
Realtime Simulation
Copper Straight-Through
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
26°C Clear
Search
ENG IN
08:20 13-04-2023

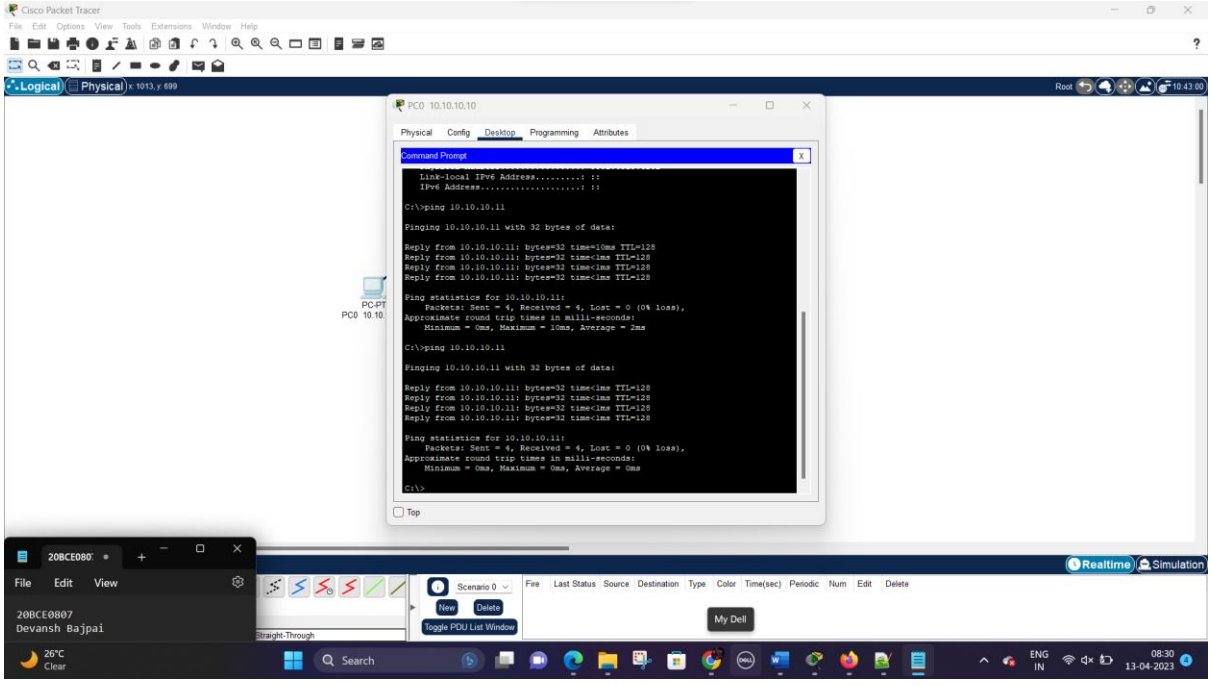

Cisco Packet Tracer
PC0 10.10.10.10
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix..:
Physical Address.....: 000C.8518.56EA
Link-local IPv6 Address.....: FE80::20C:85FF:FE18:56EA
IPv6 Address.....: ::
IPv4 Address.....: 10.10.10.10
Subnet Mask.....: 255.0.0.0
Default Gateway.....: ::
0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-AE-B9-9D-37-00-0C-85-18-56-EA
DNS Servers.....: ::
0.0.0.0
Bluetooth Connection:
Connection-specific DNS Suffix..:
Physical Address.....: 0001.6315.C28B
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
C:\>ping 10.10.10.11
Top
PC-PT
PC0 10.10
Logical Physical
Root
Time: 00:12:23
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Copper Straight-Through
26°C
Clear
Search
ENG
IN
08:21
13-04-2023

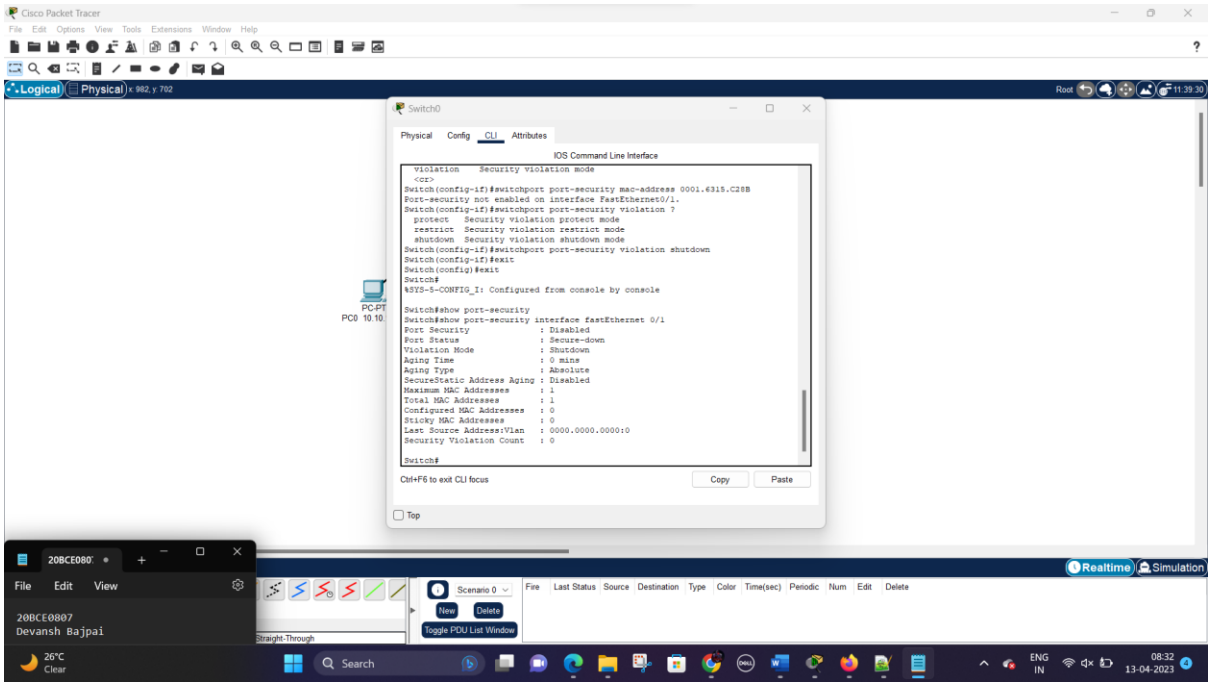

Cisco Packet Tracer
PC1 10.10.10.11
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all
FastEthernet0 Connection:(default port)
Connection-specific DNS Suffix..:
Physical Address.....: 0001.C773.95AB
Link-local IPv6 Address.....: FE80::201:C7FF:FE73:95AB
IPv6 Address.....: ::
IPv4 Address.....: 10.10.10.11
Subnet Mask.....: 255.0.0.0
Default Gateway.....: ::
0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-88-97-DE-35-00-01-C7-73-95-AB
DNS Servers.....: ::
0.0.0.0
Bluetooth Connection:
Connection-specific DNS Suffix..:
Physical Address.....: 0002.4A7B.53E3
Link-local IPv6 Address.....: ::
--More--
Top
PC-PT
PC0 10.10
Logical Physical
Root
Time: 00:13:04
Realtime Simulation
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Copper Straight-Through
26°C
Clear
Search
ENG
IN
08:21
13-04-2023


Cisco Packet Tracer
PC0 10.10.10.10
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Subnet Mask.....: 255.0.0.0
Default Gateway.....: ::
0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-AE-B9-9D-37-00-0C-85-18-56-EA
DNS Servers.....: ::
0.0.0.0
Bluetooth Connection:
Connection-specific DNS Suffix..:
Physical Address.....: 0001.6315.C28B
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
C:\>ping 10.10.10.11
Pinging 10.10.10.11 with 32 bytes of data:
Reply from 10.10.10.11: bytes=32 time=10ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Ping statistics for 10.10.10.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 2ms
C:\>
Top
Logical
Physical
Root
Realtime
Simulation
Copper Straight-Through
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
26°C
Clear
Search
ENG
IN
08:22
13-04-2023

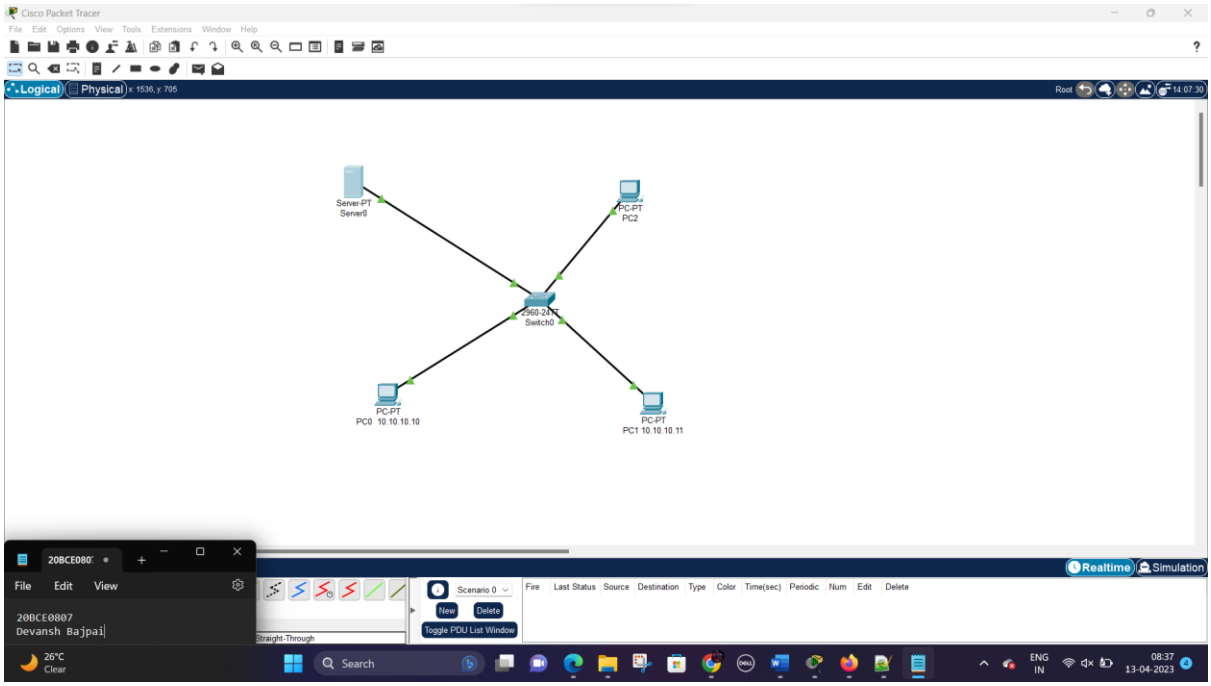

Cisco Packet Tracer
PC1 10.10.10.11
Physical
Config
Desktop
Programming
Attributes
Command Prompt
IPv4 Address.....: 10.10.10.11
Subnet Mask.....: 255.0.0.0
Default Gateway.....: ::
0.0.0.0
DHCP Servers.....: 0.0.0.0
DHCPv6 IAID.....:
DHCPv6 Client DUID.....: 00-01-00-01-88-97-DE-35-00-01-C7-73-95-AB
DNS Servers.....: ::
0.0.0.0
Bluetooth Connection:
Connection-specific DNS Suffix..:
Physical Address.....: 0002.4A7B.53E3
Link-local IPv6 Address.....: ::
C:\>ping 10.10.10.10
Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Ping statistics for 10.10.10.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top
Logical
Physical
Root
Realtime
Simulation
Copper Straight-Through
Scenario 0
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Delete
26°C
Clear
Search
ENG
IN
08:22
13-04-2023

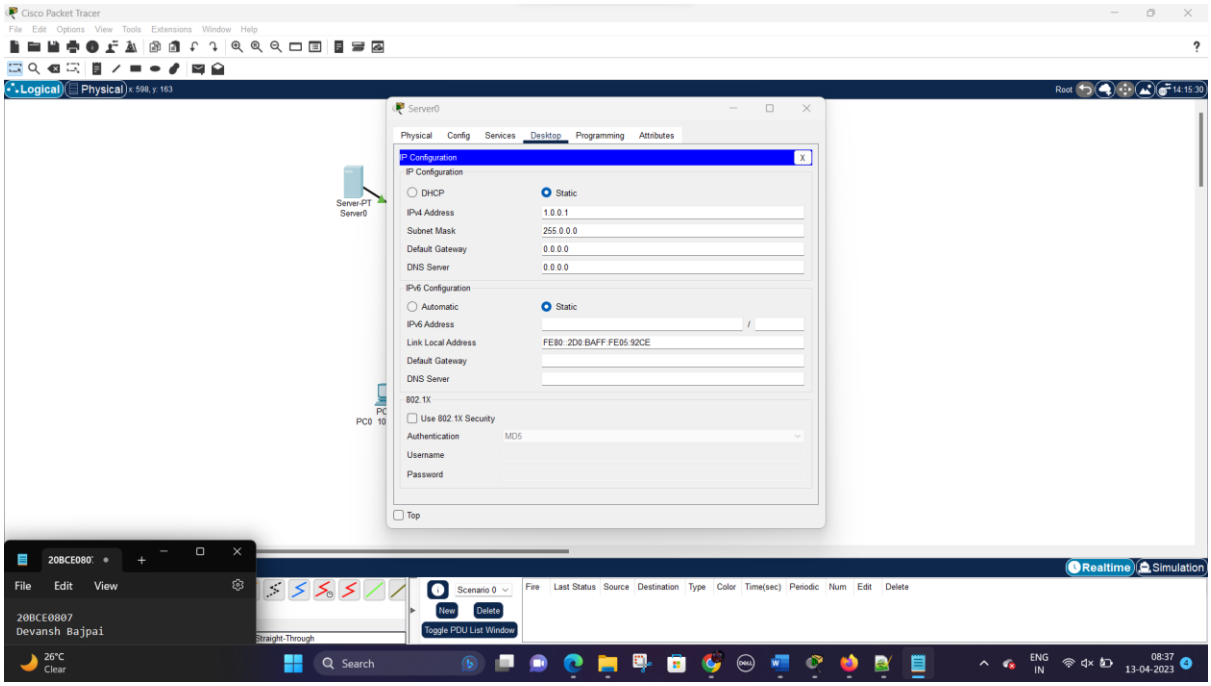

Cisco Packet Tracer
Switch0
Physical Config CLI Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security ?
aging Port-security aging commands
mac-address Secure mac address
maximum Max secure addresses
violation Security violation mode
<cr>
Switch(config-if)#switchport port-security mac-address 0001.6315.C28B
Port-security not enabled on interface FastEthernet0/1.
Switch(config-if)#switchport port-security violation ?
protect Security violation protect mode
restrict Security violation restrict mode
shutdown Security violation shutdown mode
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top
PC-PT
PC0
20BCE0807
File Edit View
20BCE0807
Devansh Bajpai
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Straight-Through
26°C
Clear
Search
ENG
IN
08:29
13-04-2023

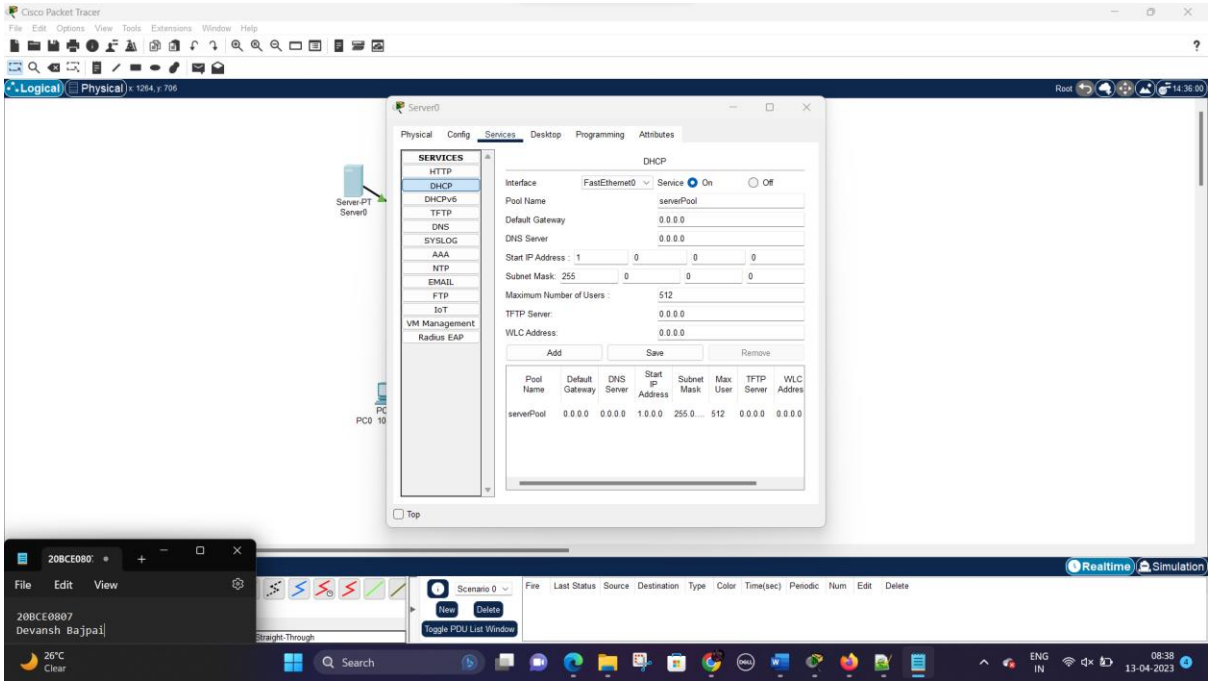

Cisco Packet Tracer
PC0 10.10.10.10
Physical Config Desktop Programming Attributes
Command Prompt
Link-local IPv6 Address.....: ::
IPv6 Address.....: ::
C:\>ping 10.10.10.11
Pinging 10.10.10.11 with 32 bytes of data:
Reply from 10.10.10.11: bytes=32 time=10ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Ping statistics for 10.10.10.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 10ms, Average = 2ms
C:\>ping 10.10.10.11
Pinging 10.10.10.11 with 32 bytes of data:
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Ping statistics for 10.10.10.11:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
Top
PC-PT
PC0
20BCE0807
File Edit View
20BCE0807
Devansh Bajpai
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
My Dell
Straight-Through
26°C
Clear
Search
ENG
IN
08:30
13-04-2023

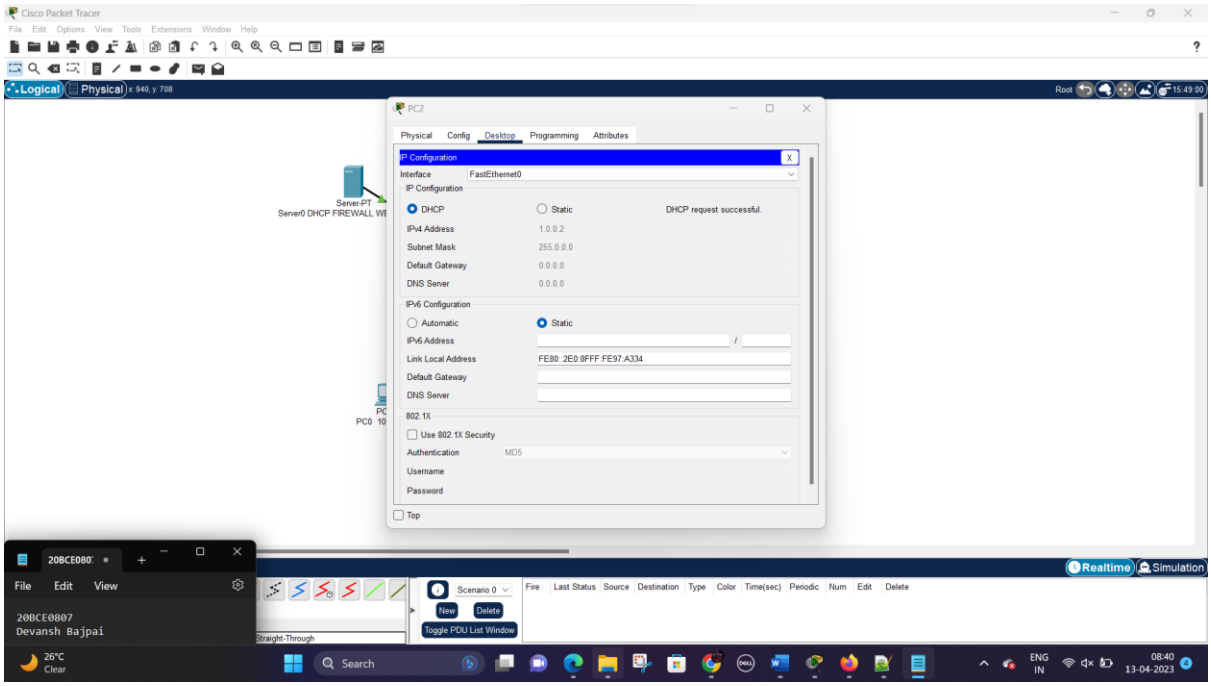


Firewall Configuration for Rule set up and Testing

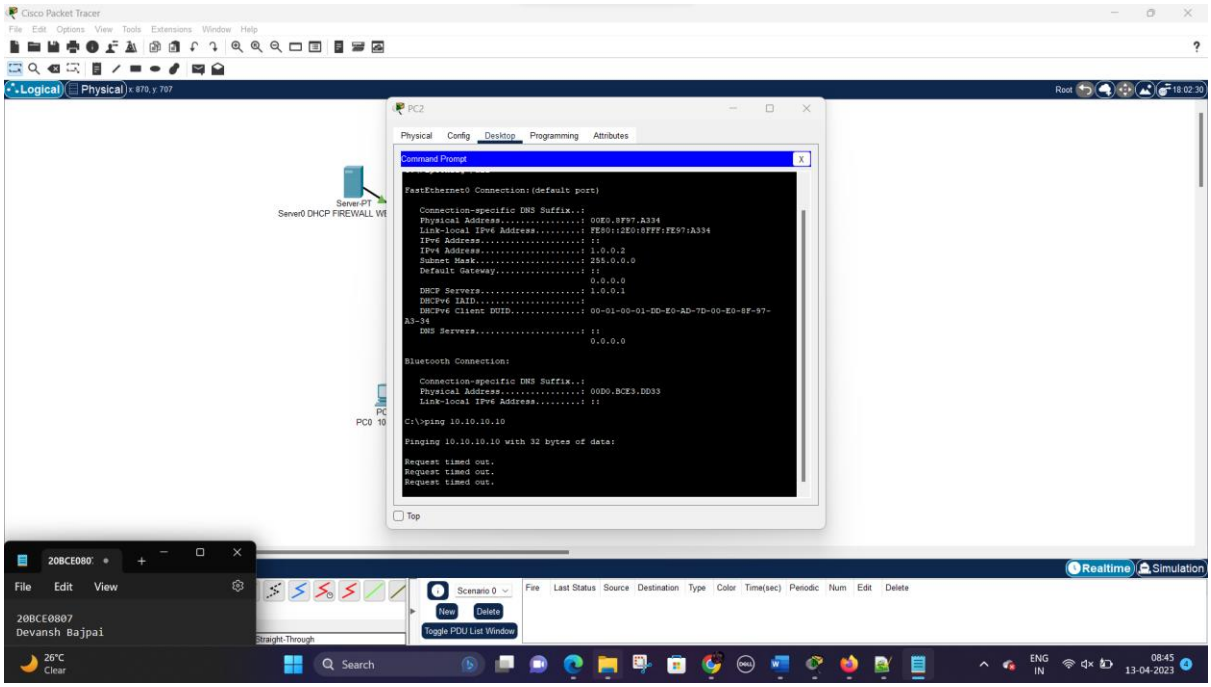


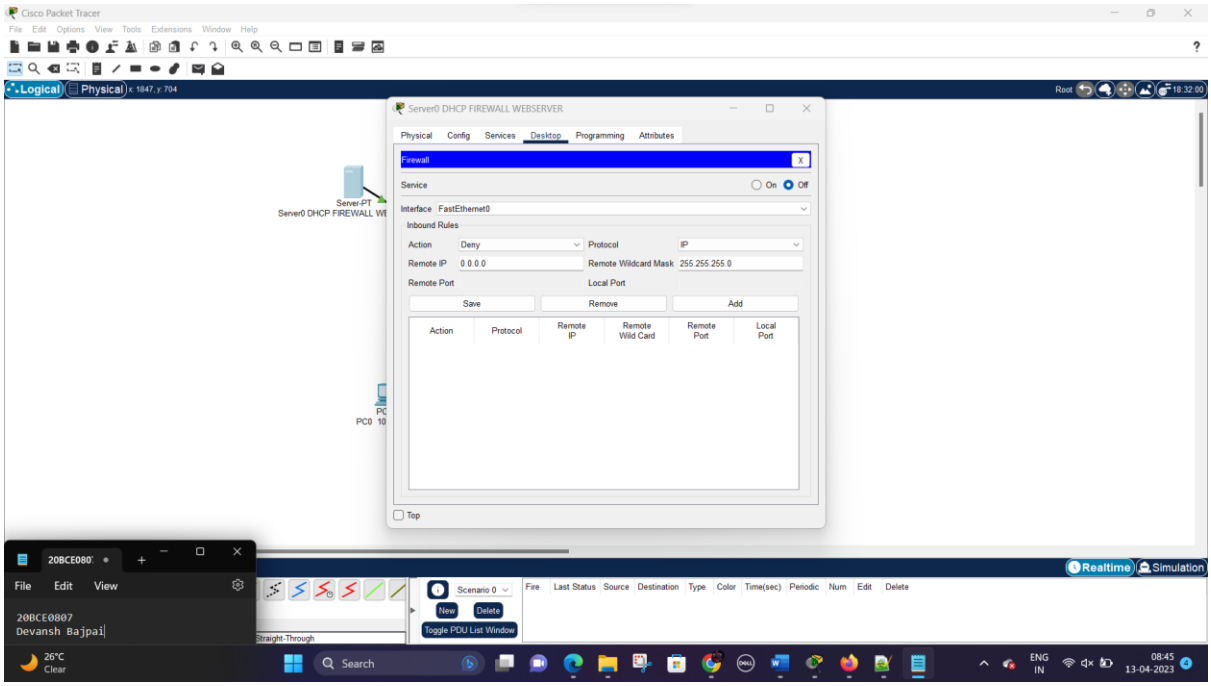

Cisco Packet Tracer
Server0
Physical Config Services Desktop Programming Attributes
IP Configuration
DHCP
Static
IPv4 Address 1.0.0.1
Subnet Mask 255.0.0.0
Default Gateway 0.0.0.0
DNS Server 0.0.0.0
IPv6 Configuration
Automatic
Static
Link Local Address FE80::2D0:BAFF:FE05:92CE
802.1X
Use 802.1X Security
Authentication MD5
Username
Password
Top
20BCE0807
Devansh Bajpai
Realtime Simulation


Cisco Packet Tracer
Server0
Physical Config Services Desktop Programming Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DHCP
Interface FastEthernet0 Service On Off
Pool Name serverPool
Default Gateway 0.0.0.0
DNS Server 0.0.0.0
Start IP Address : 1 0 0 0
Subnet Mask: 255 0 0 0
Maximum Number of Users : 512
TFTP Server: 0.0.0.0
WLC Address: 0.0.0.0
Add Save Remove
Pool Name Default Gateway DNS Server Start IP Address Subnet Mask Max User TFTP Server WLC Address
serverPool 0.0.0.0 0.0.0.0 1.0.0.0 255.0.... 512 0.0.0.0 0.0.0.0
Top
20BCE0807
Devansh Bajpai
Realtime Simulation



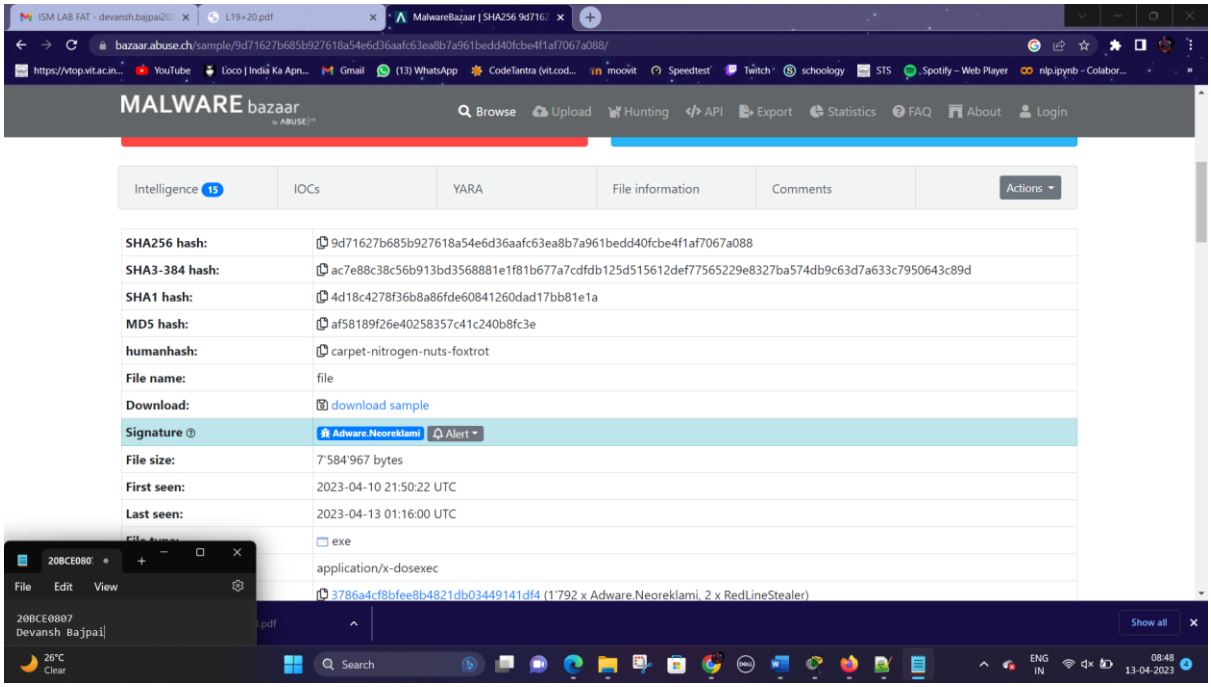
Testing the firewall



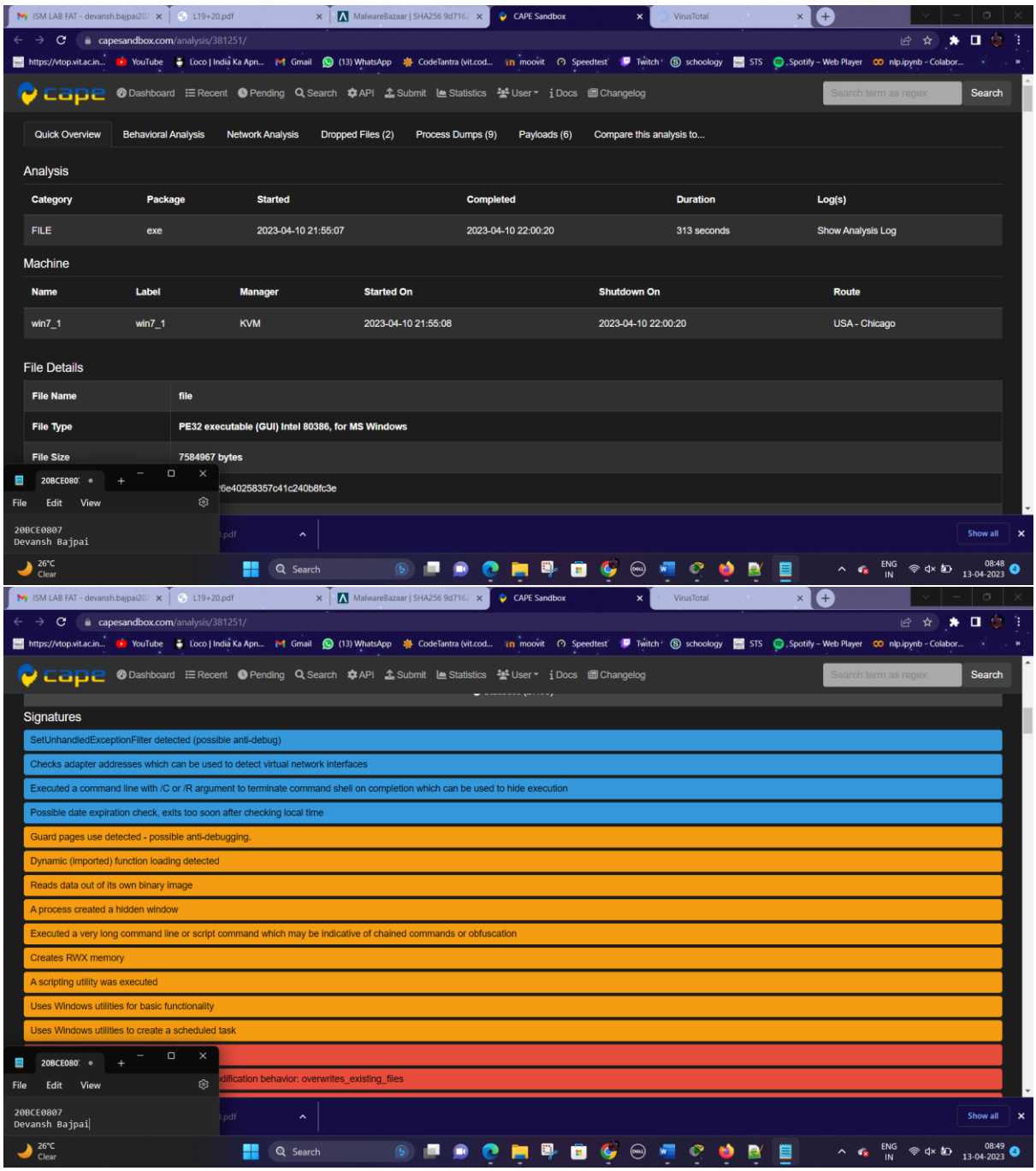


Q2-MALWARE ANALYSIS

1. Adware

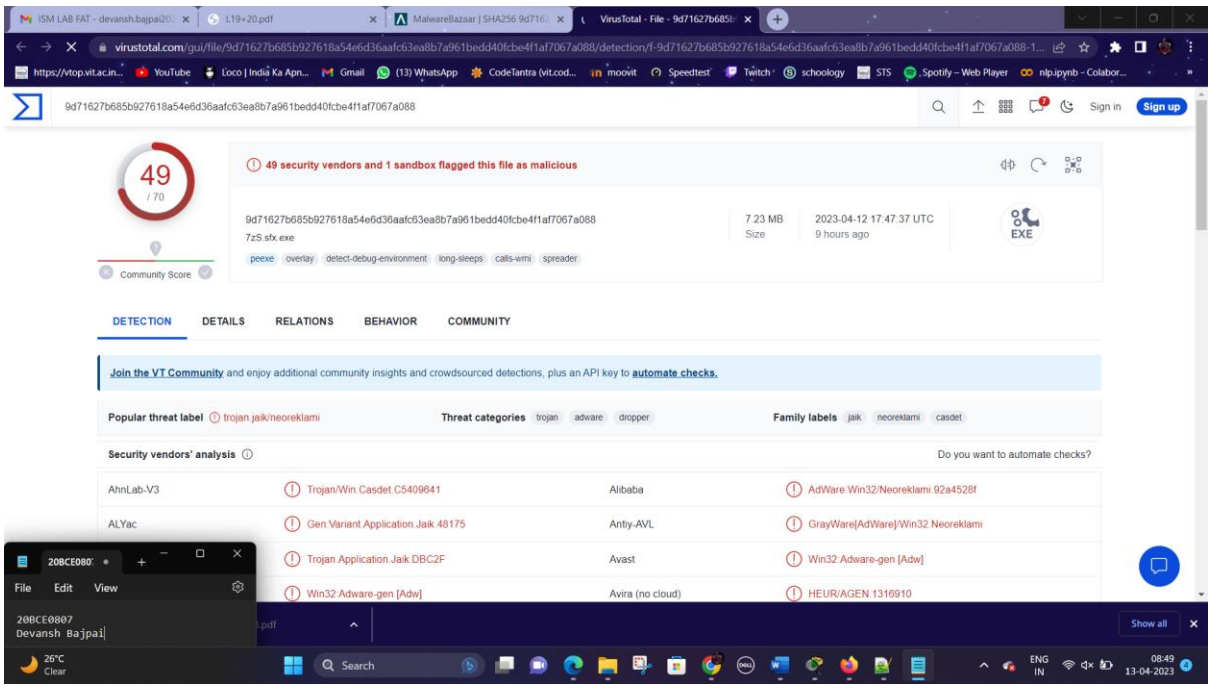


Sandbox

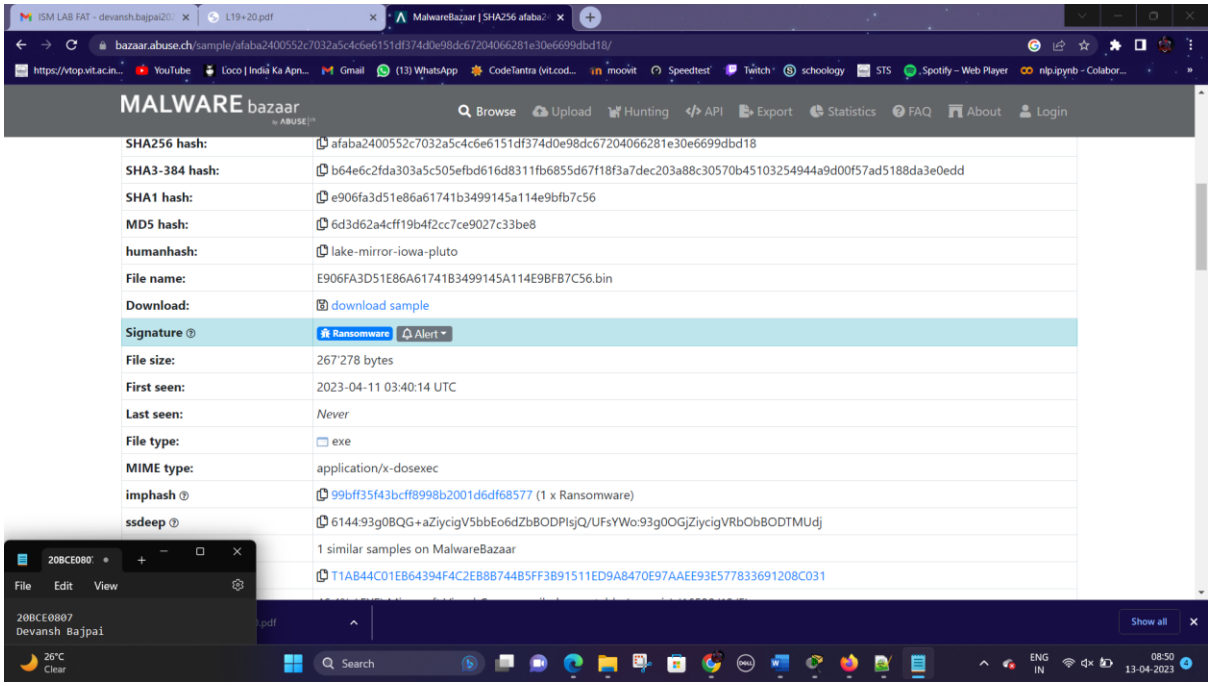

capesandbox.com/analysis/381251/
Dashboard
Recent
Pending
Search
API
Submit
Statistics
User
Docs
Changelog
Search term as regex
Search
Quick Overview
Behavioral Analysis
Network Analysis
Dropped Files (2)
Process Dumps (9)
Payloads (6)
Compare this analysis to...
Analysis
Category
Package
Started
Completed
Duration
Log(s)
FILE
exe
2023-04-10 21:55:07
2023-04-10 22:00:20
313 seconds
Show Analysis Log
Machine
Name
Label
Manager
Started On
Shutdown On
Route
win7_1
win7_1
KVM
2023-04-10 21:55:08
2023-04-10 22:00:20
USA - Chicago
File Details
File Name
file
File Type
PE32 executable (GUI) Intel 80386, for MS Windows
File Size
7584967 bytes
6e40258357c41c240b8fc3e
20BCE0807
File
Edit
View
20BCE0807
Devansh Bajpai
Show all
Search
ENG
IN
08:48
13-04-2023

capesandbox.com/analysis/381251/
Dashboard
Recent
Pending
Search
API
Submit
Statistics
User
Docs
Changelog
Search term as regex
Search
Signatures
SetUnhandledExceptionFilter detected (possible anti-debug)
Checks adapter addresses which can be used to detect virtual network interfaces
Executed a command line with /C or /R argument to terminate command shell on completion which can be used to hide execution
Possible date expiration check, exits too soon after checking local time
Guard pages use detected - possible anti-debugging.
Dynamic (imported) function loading detected
Reads data out of its own binary image
A process created a hidden window
Executed a very long command line or script command which may be indicative of chained commands or obfuscation
Creates RWX memory
A scripting utility was executed
Uses Windows utilities for basic functionality
Uses Windows utilities to create a scheduled task
dification behavior: overwrites_existing_files
20BCE0807
File
Edit
View
20BCE0807
Devansh Bajpai
Show all
Search
ENG
IN
08:49
13-04-2023

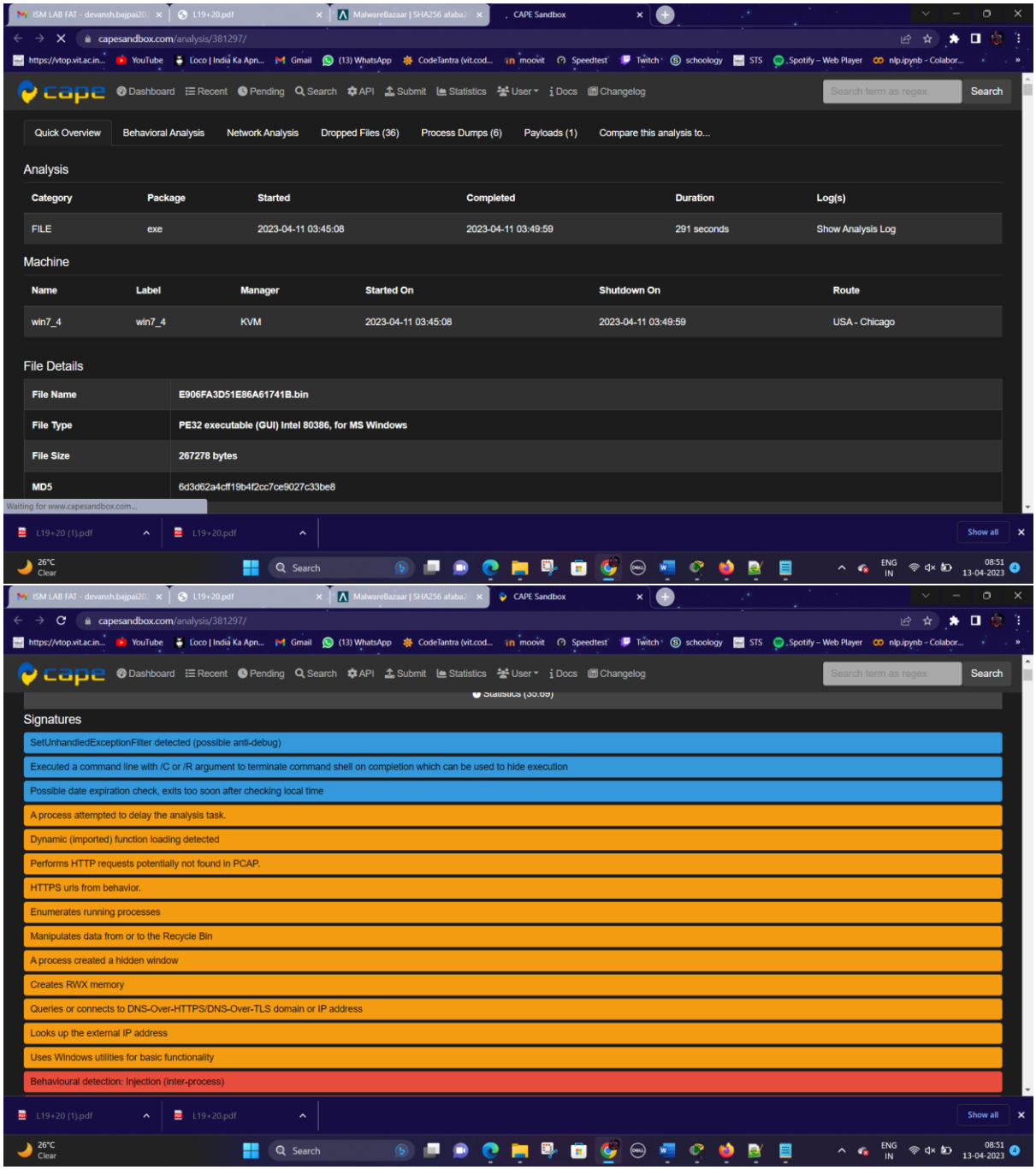
VirusTotal



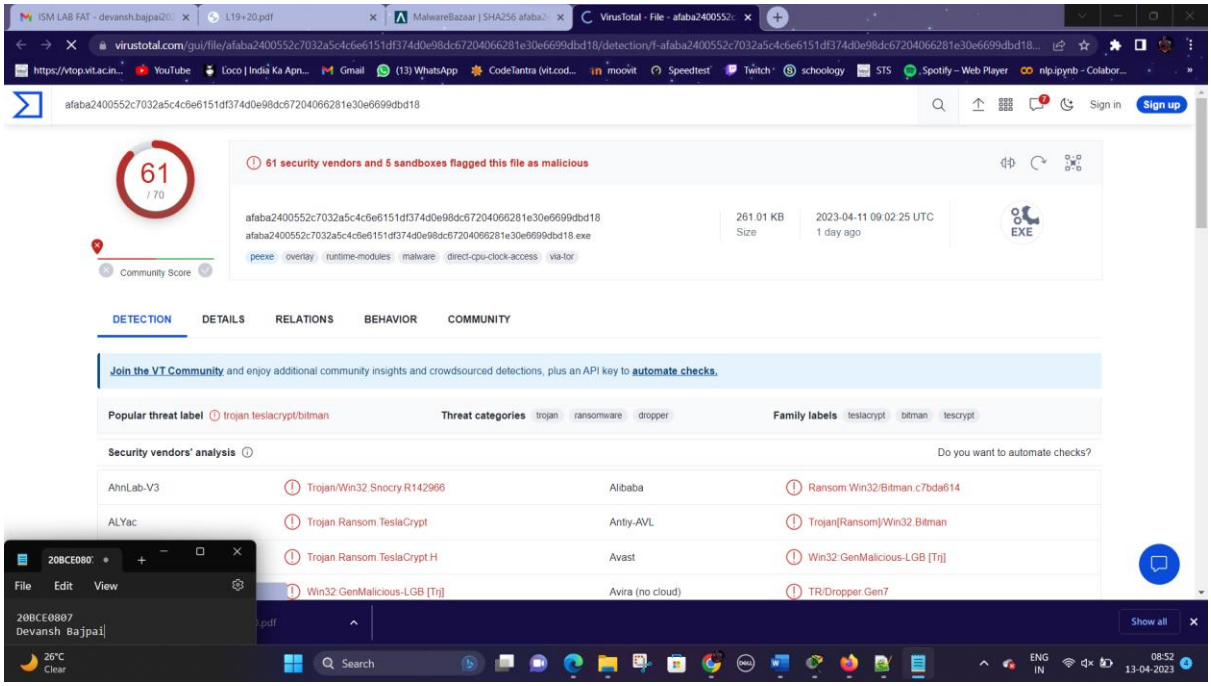
2.Ransomware



Sandbox


capesandbox.com/analysis/381297/
cape
Dashboard
Recent
Pending
Search
API
Submit
Statistics
User
Docs
Changelog
Search term as regex
Search
Quick Overview
Behavioral Analysis
Network Analysis
Dropped Files (36)
Process Dumps (6)
Payloads (1)
Compare this analysis to...
Analysis
Category
Package
Started
Completed
Duration
Log(s)
FILE
exe
2023-04-11 03:45:08
2023-04-11 03:49:59
291 seconds
Show Analysis Log
Machine
Name
Label
Manager
Started On
Shutdown On
Route
win7_4
win7_4
KVM
2023-04-11 03:45:08
2023-04-11 03:49:59
USA - Chicago
File Details
File Name
E906FA3D51E86A61741B.bin
File Type
PE32 executable (GUI) Intel 80386, for MS Windows
File Size
267278 bytes
MD5
6d3d62a4cff19b4f2cc7ce9027c33be8
Waiting for www.capesandbox.com...
L19+20 (1).pdf
L19+20.pdf
Show all
26°C
Clear
Search
ENG
IN
08:51
13-04-2023

capesandbox.com/analysis/381297/
cape
Dashboard
Recent
Pending
Search
API
Submit
Statistics
User
Docs
Changelog
Search term as regex
Search
Signatures
SetUnhandledExceptionFilter detected (possible anti-debug)
Executed a command line with /C or /R argument to terminate command shell on completion which can be used to hide execution
Possible date expiration check, exits too soon after checking local time
A process attempted to delay the analysis task.
Dynamic (imported) function loading detected
Performs HTTP requests potentially not found in PCAP.
HTTPS urls from behavior.
Enumerates running processes
Manipulates data from or to the Recycle Bin
A process created a hidden window
Creates RWX memory
Queries or connects to DNS-Over-HTTPS/DNS-Over-TLS domain or IP address
Looks up the external IP address
Uses Windows utilities for basic functionality
Behavioural detection: Injection (inter-process)
L19+20 (1).pdf
L19+20.pdf
Show all
26°C
Clear
Search
ENG
IN
08:51
13-04-2023


ISM LAB FAT - devansh.bajpai20
L19+20.pdf
MalwareBazaar | SHA256 afaba2
VirusTotal - File - afaba2400552
virustotal.com/gui/file/afaba2400552c7032a5c4c6e6151df374d0e98dc6720406628 1e30e6699dbd18/detection/f-afaba2400552c7032a5c4c6e6151df374d0e98dc6720406628 1e30e6699dbd18...
https://vtop.vit.ac.in...
YouTube
Loco | India Ka Apn...
Gmail
(13) WhatsApp
CodeTantra (vit.cod...
moovit
Speedtest
Twitch
schoology
STS
Spotify – Web Player
nlp.ipynb - Colabor...
afaba2400552c7032a5c4c6e6151df374d0e98dc6720406628 1e30e6699dbd18
Sign in
Sign up
61
/ 70
61 security vendors and 5 sandboxes flagged this file as malicious
afaba2400552c7032a5c4c6e6151df374d0e98dc6720406628 1e30e6699dbd18
afaba2400552c7032a5c4c6e6151df374d0e98dc6720406628 1e30e6699dbd18.exe
peexe
overlay
runtime-modules
malware
direct-cpu-clock-access
via-tor
261.01 KB
Size
2023-04-11 09:02:25 UTC
1 day ago
EXE
Community Score
DETECTION
DETAILS
RELATIONS
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.teslacrypt/bitman
Threat categories
trojan
ransomware
dropper
Family labels
teslacrypt
bitman
tescrypt
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3
Trojan/Win32.Snocry.R142966
Alibaba
Ransom:Win32/Bitman.c7bda614
ALYac
Trojan.Ransom.TeslaCrypt
Antiy-AVL
Trojan[Ransom]/Win32.Bitman
Trojan.Ransom.TeslaCrypt.H
Avast
Win32:GenMalicious-LGB [Trj]
Win32:GenMalicious-LGB [Trj]
Avira (no cloud)
TR/Dropper.Gen7
20BCE080
File
Edit
View
20BCE0807
Devansh Bajpai
Show all
26°C
Clear
Search
ENG
IN
08:52
13-04-2023