Assignment Answer Sheet

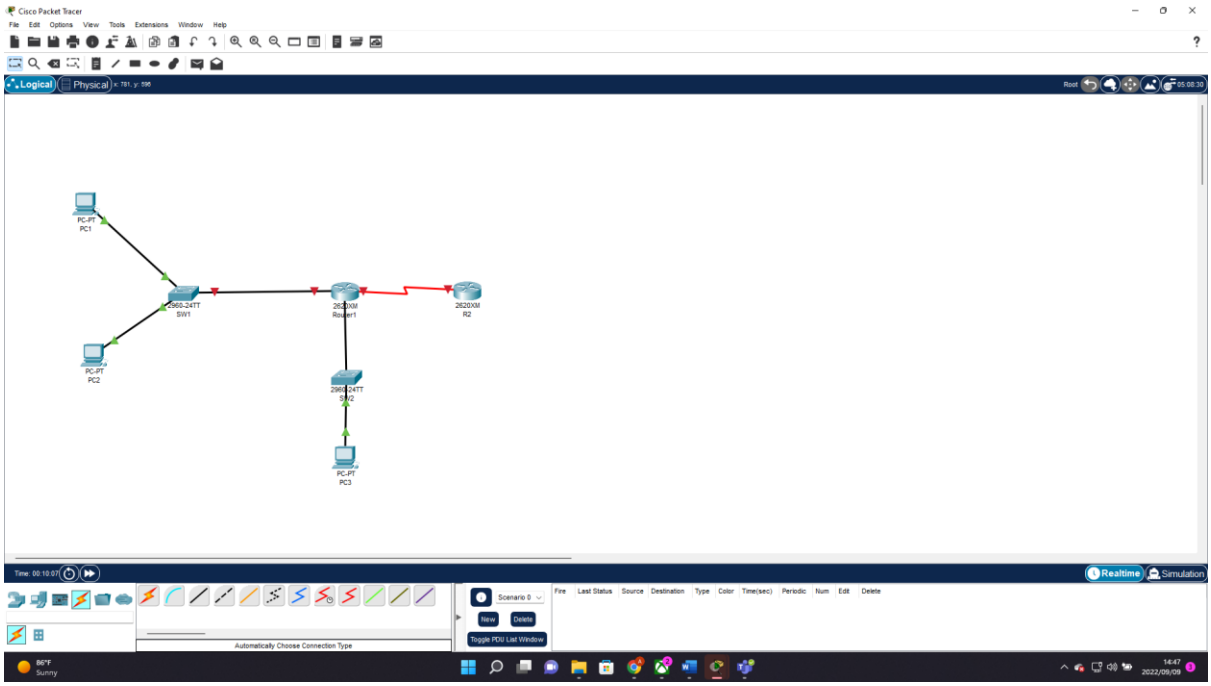
Campus	Pretoria	**Faculty**	IT
Module Code	ITNSA2-B33	**Module Name**	
Student Name	Arno Moller		
Student Number	CC96ZRRS5		
Lecturer Name	Khonde, Fabrice		

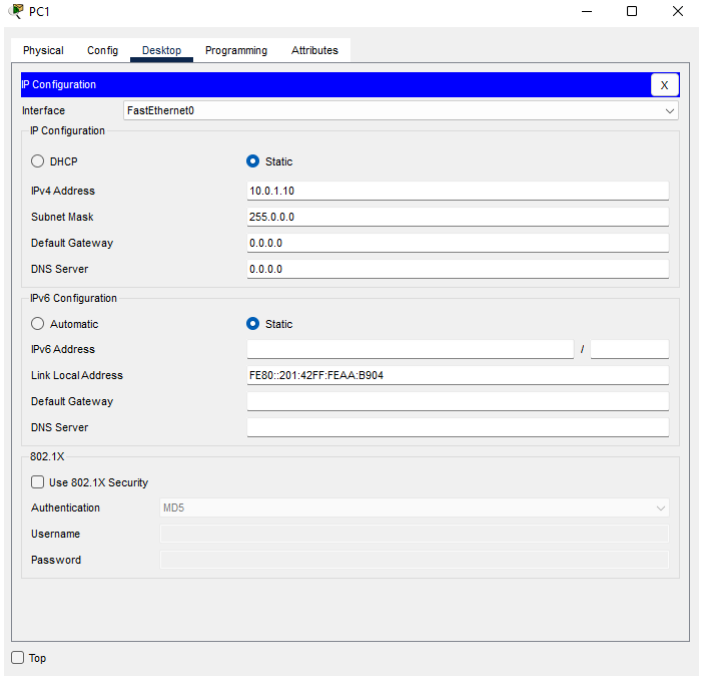
Declaration

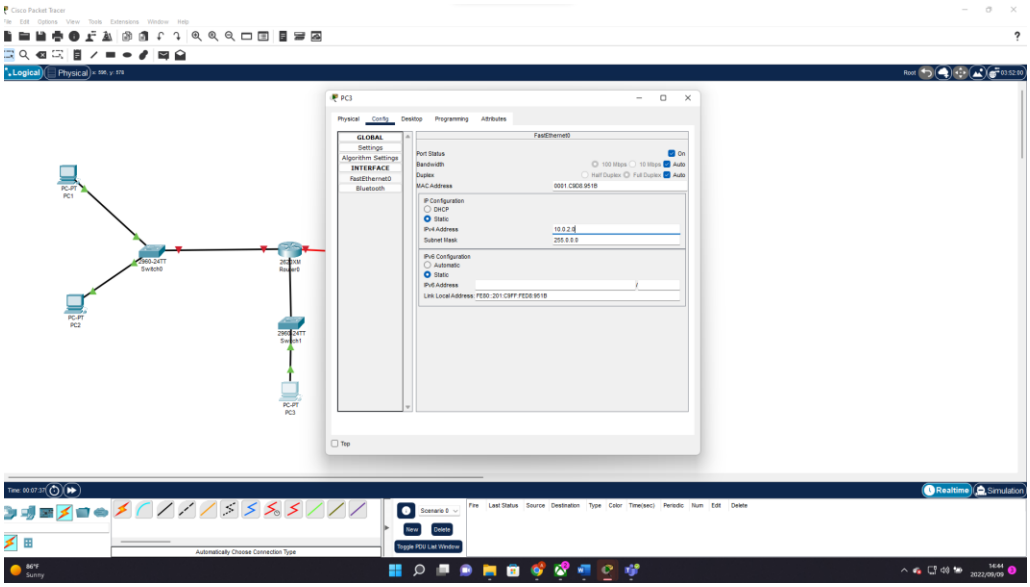
"I declare that this assignment is my own original work except for source material explicitly acknowledged, and that the same or related material has not been previously, or is being simultaneously, submitted for this or any other course. I also acknowledge that I am aware of the Institution's policy and regulations on honesty in academic work as set out in the Pearson Institute of Higher Education Conditions of Enrolment, and of the disciplinary guidelines applicable to breaches of such policy and regulations."

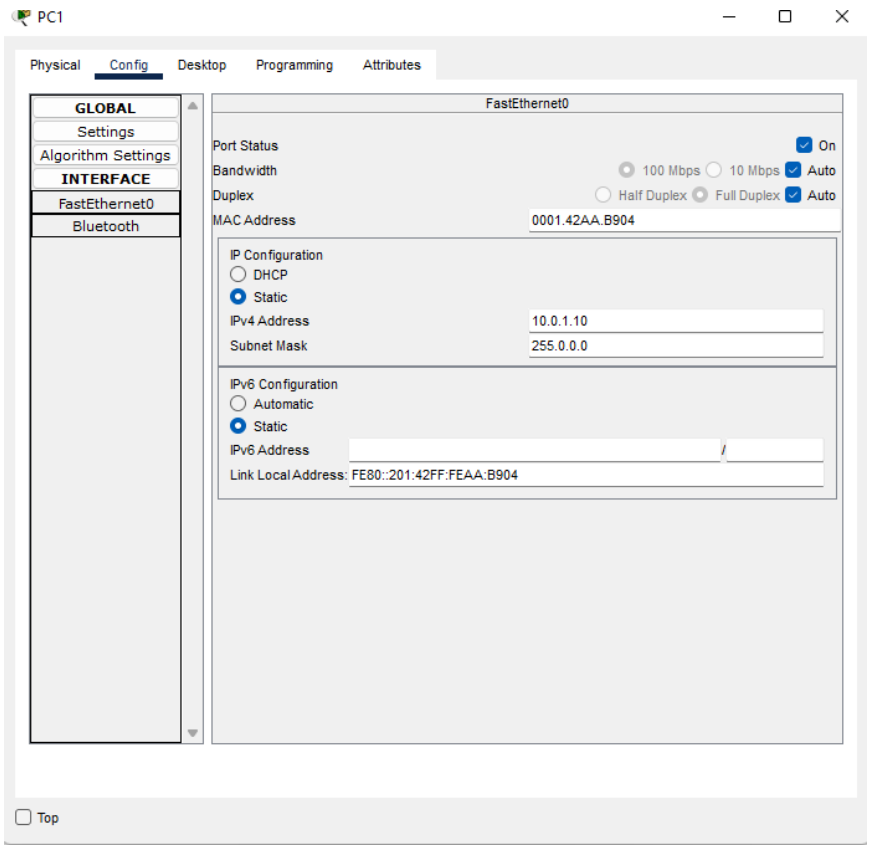
Start writing from here

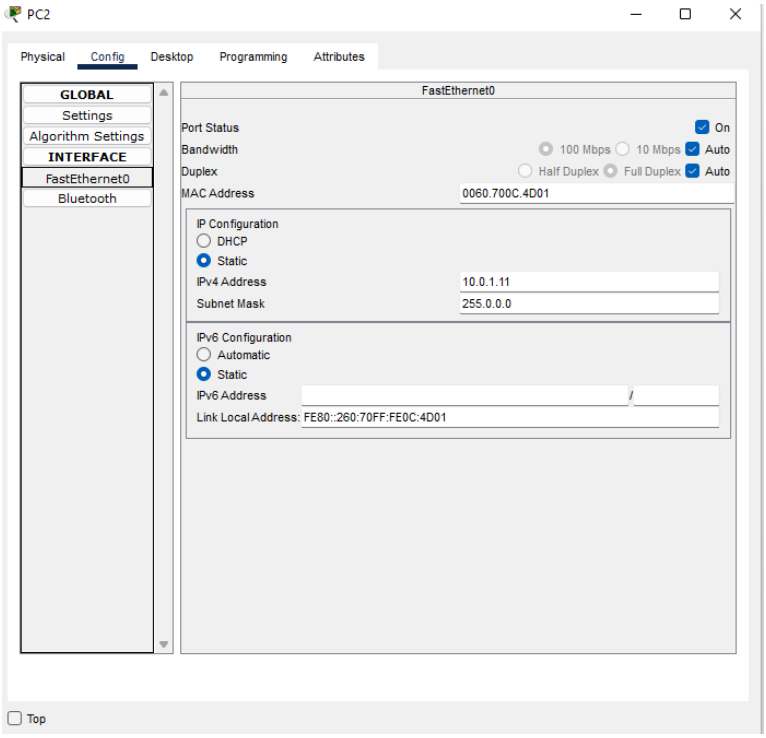
Question 1




PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
10.0.1.10
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::201:42FF:FEAA:B904
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top




PC1
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.42AA.B904
IP Configuration
DHCP
Static
IPv4 Address
10.0.1.10
Subnet Mask
255.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::201:42FF:FEAA:B904
Top


PC2
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.700C.4D01
IP Configuration
DHCP
Static
IPv4 Address
10.0.1.11
Subnet Mask
255.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::260:70FF:FE0C:4D01
Top

Router1

Physical | Config | CLI | Attributes

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
Serial0/0
Serial0/1

FastEthernet0/0

Port Status: On
Bandwidth: 100 Mbps / 10 Mbps / Auto
Duplex: Half Duplex / Full Duplex / Auto
MAC Address: 00E0.F70D.12CB

IP Configuration
IPv4 Address: 192.168.0.1
Subnet Mask: 255.255.255.0

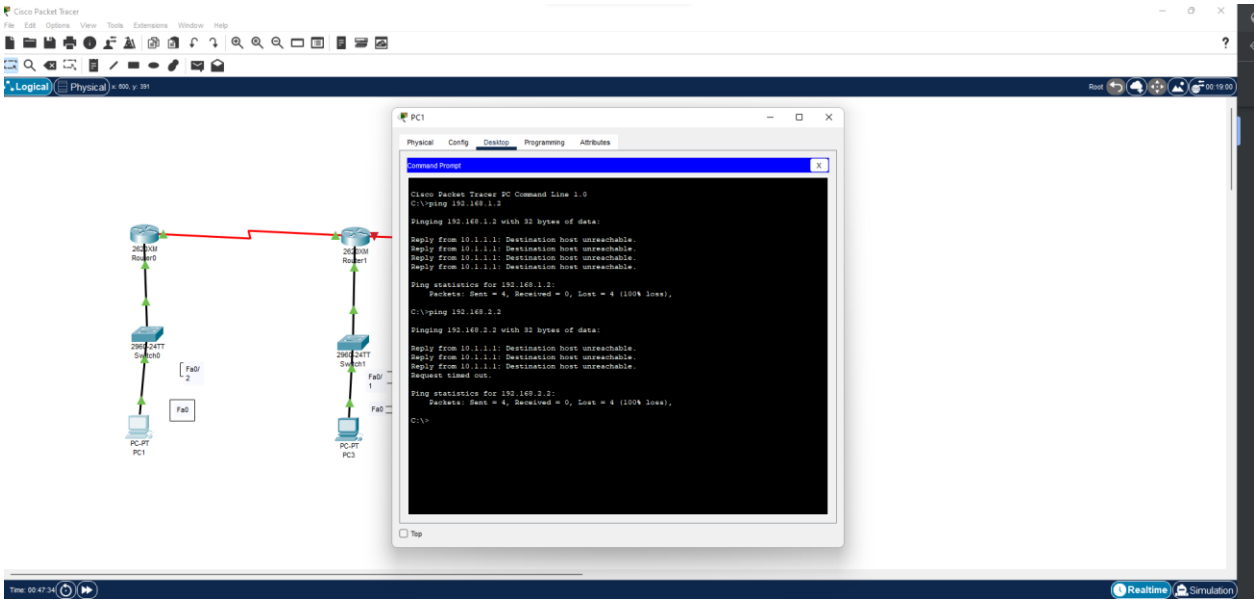
Tx Ring Limit: 10

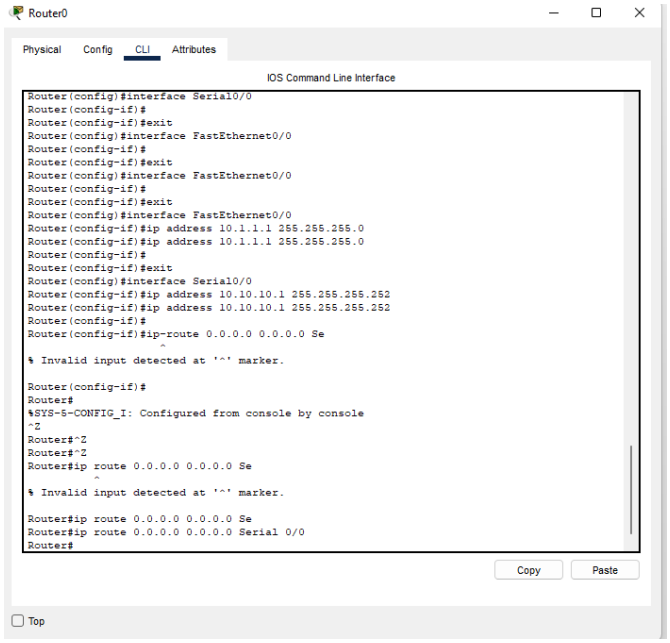
Equivalent IOS Commands

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#no ip address
Router(config-if)#no ip address
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#
```

Top

1.2





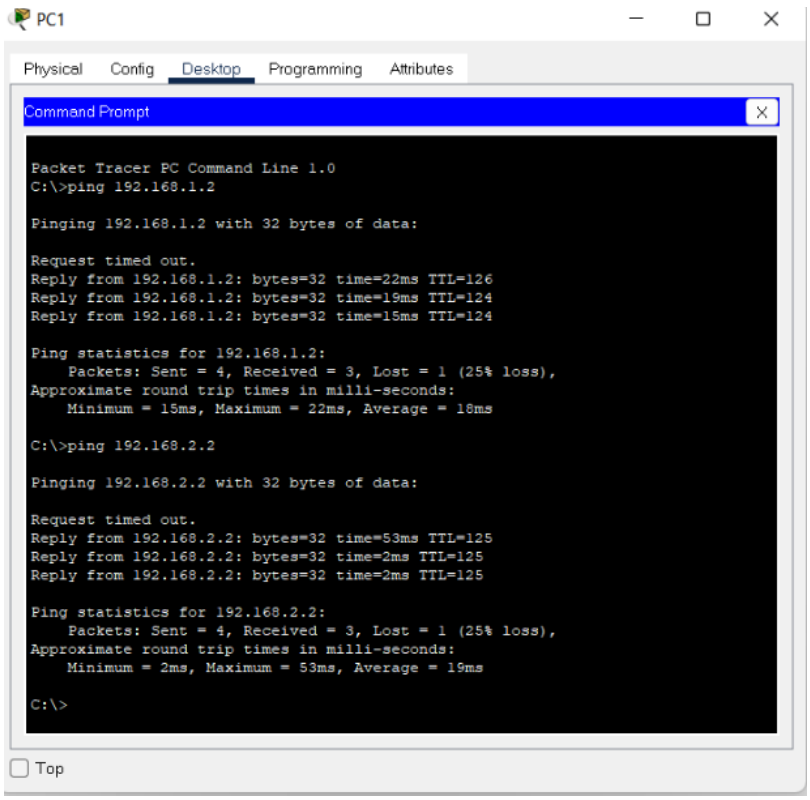
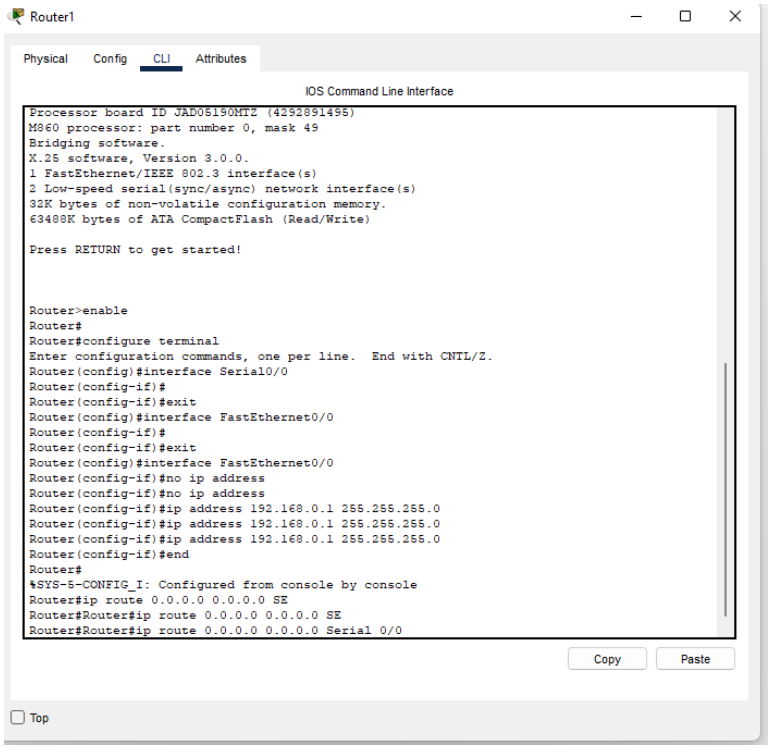


Figure 1PC1 cannot ping R2


Router1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)
Press RETURN to get started!
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#no ip address
Router(config-if)#no ip address
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#ip route 0.0.0.0 0.0.0.0 SE
Router#Router#ip route 0.0.0.0 0.0.0.0 SE
Router#Router#ip route 0.0.0.0 0.0.0.0 Serial 0/0
Copy
Paste
Top

Question 2

A method for protecting information or data that should only be accessed by authorized persons is cryptography. Algorithms are a collection of rule-based calculations that constitute the foundation of cryptography. These algorithms change the data into illegible, difficult-to-understand form. These particular cryptographic methods convert plaintext into cyphertext, which needs a key to be decoded, from the input plaintext. The cryptographic algorithm also creates this key. The encryption of the same plaintext will always be the same, as will the decryption key.

In our daily lives, cryptography is utilized in places like

Financial transactions: All of our online banking transactions are encrypted to prevent unauthorized access.

End-to-end encryption. A texting app uses end-to-end encryption. End-to-end encryption encrypts content particularly when it is sent from one user to another.

Email: All emails are transmitted with encryption.

There are four primary goals of cryptography:

Non-repudiation: This refers to the idea that both the sender and the recipient will have evidence of delivery, making it impossible for either party to claim they did not process the information.

Authentication: PKI or digital signatures can be used to confirm a person's identification (Public Key Infrastructure)

Confidentiality: Maintaining the privacy of sensitive information that can only have access by being authorized by the owner of the intellectual data.

As stated above cryptography is used in our day-to-day life. The types of Cryptography we have are secure and trustworthy. Passwords saved by companies will be encrypted before they are stored in their databases. The encryption used is stated below:

Symmetric Key Encryption: With this encryption, a single key will be generated and used to both encrypt and decrypt the plaintext.

Hash functions: The information cannot be encrypted or decrypted using any key. It converts a very large number into a very small integer that can be used as the hash table's index.

Asymmetric Key Encryption: This encryption employs the usage of two distinct keys, a public key for encrypting plaintext and a private key for decrypting cyphertext.

Integrity: This refers to the fact that a third party cannot change or delete the data.

Cryptography can be used to write plain text in to cypher text. For example the plaintext; “Work is hard for everyone.”

Cyphertext: Aopz pz dypaalu mvy hu lehtwsl!

Question 3

The attack used in the above scenario is a botnet attack. It can be identified with the hacker using the system and different PC’s (Bots) to target the victim’s laptop. A botnet attack is a specific type of malware attack that targets the victim computer by employing a network of botnets or zombies.

Botnet attacks is designed to generate a lot of network traffic, hang the victim machine or the entire network, and prevent legitimate users from accessing the system.

Botnet hosts, often known as bots, are infected hosts that are utilized to attack the target computer. PC-PT BOT1, BOT2, BOT3, and BOT4 are the 4 bots.

The hacker who plans and launches the attack. The attacker device in this instance is a laptop running PT Hacker.

The server that manages communication among the infected botnets is known as the server controller. In the image above, Server PT is the Server controller.

Botnets can be identified using the following indications:

1. Abnormal increase in the CPU load

2. Excessive network traffic that result in the network block

3.Excessive usage of memory and other resources.

4. Non-native and unusual network traffic.

The following signs can be used to identify a botnet attack:

To identify suspicious inbound packets and identify malware attack patterns, use signature-based detection. However, the malware pattern saved in the botnet database can be used to accomplish the signature-based detection. With this method, the brand-new packets cannot be found.

The method known as "flow-based detection" keeps track of a network's activity by looking at the source and destination ip addresses of packets.

Common signs are also known:

An abnormal rise in CPU load, unexpected and foreign network traffic, network block caused by excessive network traffic and excessive use of resources, including memory.

The following techniques can be used to mitigate the attack:

Analyse and keep an eye on network traffic within the company. A more accurate view of the network can be obtained using monitoring tools like Nagios.

Keep a zero-trust policy in place to defend against attacks that involve the identification of any single bot request and step-by-step examination.

Strong password hygiene policy: Always use strong passwords to protect sensitive data and preserve data privacy.

Watch over and secure all unreliable access points that could behave artificially.

Most organizations employ this tactic to stop the botnet attack, known as honeypots. One of the systems, which guards the other real servers from attacks, is configured with weaker security and is more open to assault.

Once there is an upsurge in traffic in the honeypot, the analyst may quickly identify the botnet attack and protect the legitimate servers. (Anon., 2020)

(Anon., 2022) (TechEngineer, 2015) (TechEngineer, 2015) (McMillan, 2015) (Singh, 2918) (Gargano, 2016) (Cisco, 2022) (Geeks for Geeks, 2022) (Geeks for Geeks , 2022)

Bibliography

Anon., 2020. *netwrix.* [Online]
Available at: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/
[Accessed 08 September 2022].

Anon., 2022. *Csico.* [Online]
Available at: https://auth.socialgoodplatform.com/auth/realms/skillsforall/protocol/openid-connect/auth?client_id=02159bbb62514124&openid=&response_type=code&state=4UiR0b8p
[Accessed 07 September 2022].

Cisco, 2022. *Cisco.* [Online]
Available at: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html
[Accessed 6 September 2022].

Gargano, P., 2016. *31 Days Before Your CCNA Security Exam: A Day-by-day Review Guide for the IINS 210-260 Certification Exam..* 1ste ed. s.l.:Cisco.

Geeks for Geeks , 2022. *Geeks for Geeks.* [Online]
Available at: https://www.geeksforgeeks.org/computer-networks-set-13/?ref=leftbar-rightbar
[Accessed 7 September 2022].

Geeks for Geeks, 2022. *Geeks for Geeks.* [Online]
Available at: https://www.geeksforgeeks.org/router-configuration-with-cisco-packet-tracer/
[Accessed 6 September 2022].

McMillan, T., 2015. *CCNA Security 210-260 Official Cert Guide: CCNA Sec 210-260 OCG..* Cisco ed. s.l.:s.n.

Singh, G. V. M. a. A. V., 2918. *CCNA Security 210-260 Certification Guide: Build your knowledge of network security and pass your CCNA Security exam (.* 1st ed. s.l.:Packt Publishing.

TechEngineer, 2015. *Youtube.* [Online]
Available at:
https://www.youtube.com/watch?v=JaJAbOFl_u4&t=603s&ab_channel=TechEngineerTV
[Accessed 06 September 2022].

TechEngineer, 2015. *Youtube.* [Online]
Available at: https://www.youtube.com/watch?v=vKXjzEEB-UE&ab_channel=TechEngineerTV
[Accessed 07 September 2022].