Interested in learning more about security?

# SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Securing IP Routing and Remote Access on Cisco Routers

Cisco equipment comprises a large part of the Internet's infrastructure and is used by many large companies. Routers provide physical connectivity between networks by virtue of their physical attachments to either local area networks (LANs) or wide area networks (WANs). Cisco router has several vulnerabilities that could allow hackers to disrupt Internet traffic, intercept sensitive information such as passwords and credit card numbers or redirect traffic from web sites. Securing the router is the first thing that syst...

Copyright SANS Institute

Author Retains Full Rights

AD

**SECURING IP ROUTING AND TELNET ACCESS ON CISCO ROUTERS**

**1.0 Overview**

**2.0 What exactly is IP routing?**

**3.0 Why do we need to secure IP routing?**

- **3.1 IP Spoofing**
- **3.2 Denial of Service Attack (DoS)**
- **3.3 Unauthorized Routing Updates**

**4.0 What is Remote Access?**

- **4.1 Telnet Access on Cisco router**
- **4.2 HTTP Server Access on Cisco router**

**5.0 How to secure remote access?**

- **5.1 Using Access Control Lists (ACLs)**
- **5.2 Using Authentications and Secure Shell (SSH)**
- **5.3 Using Console Port Timeouts**
- **5.4 Disable HTTP server configuration**
- **5.5 Enable TACACS+ or Radius Authentication**

**6.0 Summary**

**7.0 References**

© SANS Institute 2001, Author retains full rights

**Securing IP Routing and Remote Access on Cisco Routers**

## 1.0 Overview

Cisco equipment comprises a large part of the Internet's infrastructure and is used by many large companies. Routers provide physical connectivity between networks by virtue of their physical attachments to either local area networks (LANs) or wide area networks (WANs).

Cisco router has several vulnerabilities that could allow hackers to disrupt Internet traffic, intercept sensitive information such as passwords and credit card numbers or redirect traffic from web sites. Securing the router is the first thing that system administrator needs to do before any network to be implemented. Securing IP routing and remote access are ways of securing your routers.

## 2.0 What exactly is IP routing?

The IP router allows you to control the flow of routing data to and from the routing tables. Every IP router maintains a table of current routing information. The routing table manager receives routing updates from the network through the Internet protocols running on the router. Periodically, the routing table manager issues routing updates through the protocols.

IP routing protocols are divided into classes:

1. Interior Gateway Protocols (IGP)

An IGP is a protocol for exchanging routing information between gateways (hosts with routers) within an autonomous network (for example, a system of corporate local area networks). The routing information can then be used by the Internet Protocol (IP) or other network protocols to specify how to route transmissions. The interior routing protocols supported are:

- i) Routing Information Protocol (RIP)
- ii) Internet Gateway Routing Protocol (IGRP)
- iii) Enhanced Internet Gateway Routing Protocol (EIGRP)
- iv) Open Shortest Path First (OSPF)
- v) Intermediate System to Intermediate System (IS-IS)

2. Exterior Gateway Protocols (EGP)

Exterior Gateway Protocol (EGP) is a protocol for exchanging routing information between two neighbor gateway hosts (each with its own router) in a network of autonomous systems. EGP is commonly used between hosts on the Internet to exchange routing table information. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. Each router polls its neighbor at intervals between 120 to 480 seconds and the neighbor responds by sending its complete routing table. The exterior routing protocols supported are:

- i) Border Gateway Protocol (BGP)
- ii) Exterior Gateway Protocol (EGP)

## 3.0 Why do we need to secure IP routing?

### 3.1 IP Spoofing

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

IP spoofing is when an attacker compromises the routing packets to redirect a file or transmission to a different destination. The routing packets of most Internet file transfers are transmitted in the clear, making it easy for an attacker to modify source data or change the destination of information. The technique is also effective in disguising an attacker's identity, preventing victims from identifying the original perpetrator.

The solution to preventing IP spoofing is securing transmission packets and establishing screening policies. Point-to-point encryption will prevent unauthorized users from reading the packets thus preserving the confidentiality of the data. Authentication can prove that a legitimate source, and not a spoofed middleman, sent the contents of the packet. In either case, any attempt to tamper with the packets would leave some telltale sign to warn system administrator.

Anti-spoofing rules, which basically tell the server to reject any external packets that appear to come from an internal IP address, will cut down on most spoof attacks. Non-predictable sequence numbering, or making the SYN/ACK dialogue more difficult to predict, will also reduce the chances of a session being intercepted and hijacked.

Anti-spoofing using access lists.

*access-list 101 deny any any log*
*access-list 101 deny 202.9.64.0 0.0.0.255 any log*

For the example above, 202.9.64.0 is the internal IP address of the network.
The first access list is to filter out all ICMP packets, regardless of source and destination address. The second access list will deny incoming packets that have the internal IP address from coming in.

Anti-spoofing using RPF checks

Cisco IOS software versions that supports Cisco Express Forwarding (CEF) will drop packets arriving on an interface with a source address. This requires strictly symmetric routing patterns. This feature is known as a reverse path forwarding (RPF) check.

*ip verify unicast rpf*

The above command will discard spoofed IP packets in symmetric routing environments with CEF only.

### 3.2 Denial of Service Attack (DoS)

A DoS attack takes place when availability to a resource is intentionally blocked or degraded due to maliciousness. In other words, the attack impedes the availability of the resource to its regular authorized users. Degradation of service occurs when the attacker causes the performance of the system or network to deteriorate due to overloading of the target system.

The *smurf* DoS performs a network level attack against the target host. This attack relies on the intermediary, in this case the router. The attacker, spoofing the source IP address of the target host, generates a large amount of ICMP echo traffic directed towards IP broadcast addresses. The router, also known as *smurf* amplifier, converts the IP broadcast to a layer 2

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

broadcast and send it on its way. Each host that receives the broadcast responds back to the real source IP with an echo reply. Depending on the number of hosts on the network both the router and the target host can be inundated with traffic resulting in degraded network service availability.

To prevent your network from being used as *smurf* amplifier, you need to filter packets sent to the broadcast address of your network. An IP directed broadcast is a packet that is sent to the broadcast address which the sending machine is not directly attached. Directed broadcast is routed as a *unicast* packet until it arrives at the target subnet. The last router on the chain only that is connected directly to the target subnet can identify a directed broadcast.

Apply "no ip directed-broadcast" on every interface of every router. By applying this you can prevent *smurf* attacks. Cisco IOS version 12.0 and above is configured by default to this configuration however version prior to 12.0 needs to be applied into the router configuration. Below is how to apply the command.

```
KL-4500#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
KL-4500(config)#int e0
KL-4500(config-if)#no ip directed-broadcast
KL-4500(config)#int s0
KL-4500(config-if)#no ip directed-broadcast
KL-4500(config-if)#^Z
```

The above configurations show how to disable the *ip directed-broadcast* on interface *Ethernet 0* and *Serial 0*.

SYN flood is another type of DoS attack. How it works? An attacker sends a TCP SYN segment with an unreachable spoofed source address to an open port on the target. The target response with SYN ACK to the unreachable host and the TCP handshake never completes. The target's connection queue quickly gets filled with half open connections in the SYN_RCVD state.

Cisco IOS has a mechanism called *TCP Intercept* that is available for many routers. The *TCP intercept* feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the *TCP intercept*software intercepts TCP synchronization (SYN) packets from clients to servers that match an extended access list.

Sample of *TCP Intercept* configuration.

```
access-list 101 permit tcp any 202.9.64.0 0.0.0.255
ip tcp intercept list 101
```

The above configuration defines extended IP access list 101. TCP intercept packets for all TCP servers on the 202.9.64.0/24 subnet:

### 3.3 Unauthorized Routing Updates

The other way on how to secure unauthorized routing updates is to use neighbor authentication. This security features is utilized whenever routing updates are exchanged

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

between the neighbor routers. Neighbor authentication makes sure that your router will receive reliable routing information from the other neighbor routers. Routing information can be easily spoofed and injected into the backbone.

It is strongly recommend that users prevent their routers from receiving unauthorized or deliberately malicious route updates. RIPv2, IS-IS, DRP Server Agent, OSPF, EIGRP and BGP are the only routing protocol that supports neighbor authentication. Make sure after applying neighbor authentication you configure neighbor router for neighbor authentication. Otherwise it will not work since this work in pair.

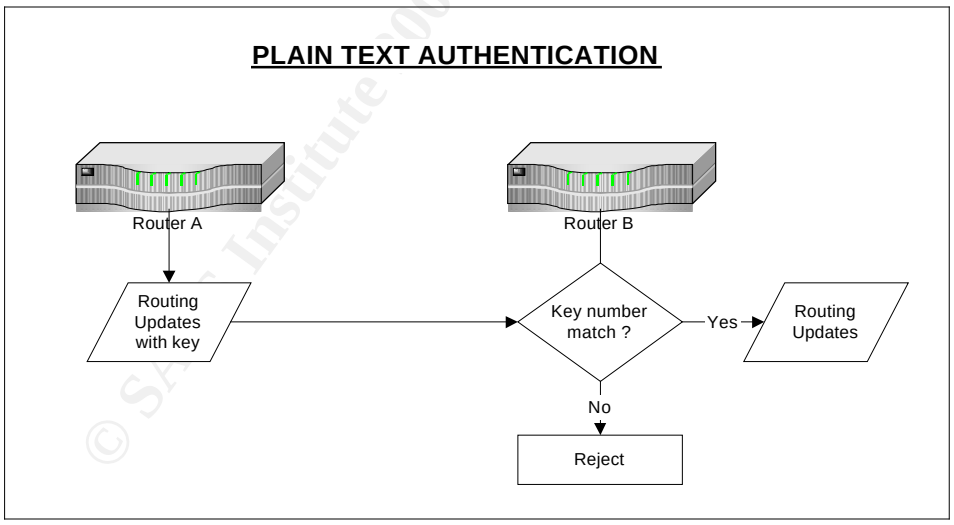
There are two types of neighbor authentication:

1. Plain Text Authentication
2. Message Digest Algorithm Version 5 (MD5)

Plain Text Authentication

Each participating neighbor router shares a secret key, which is specified on each router during configuration. Multiple keys can be specified but a key number must identify each key.

How it works? Let's say we have 2 routers, router A and router B. In this case, router A want to send a routing update with a key and the corresponding key number to router B which is the neighbor router. Router B will check the received key against its own key stored in its own memory. If the two key match, router B will accept the routing update packet. Otherwise the routing packet is rejected.




MD5 Authentication

MD5 authentication works similarly to plain text authentication. The only difference in MD5 is the key number never sent over the wire. In MD5, it will use an algorithm to produce "message digest" of the key. This is also known as "hash". The message digest is then sent making sure that nobody can eavesdrop on the line during transmission.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

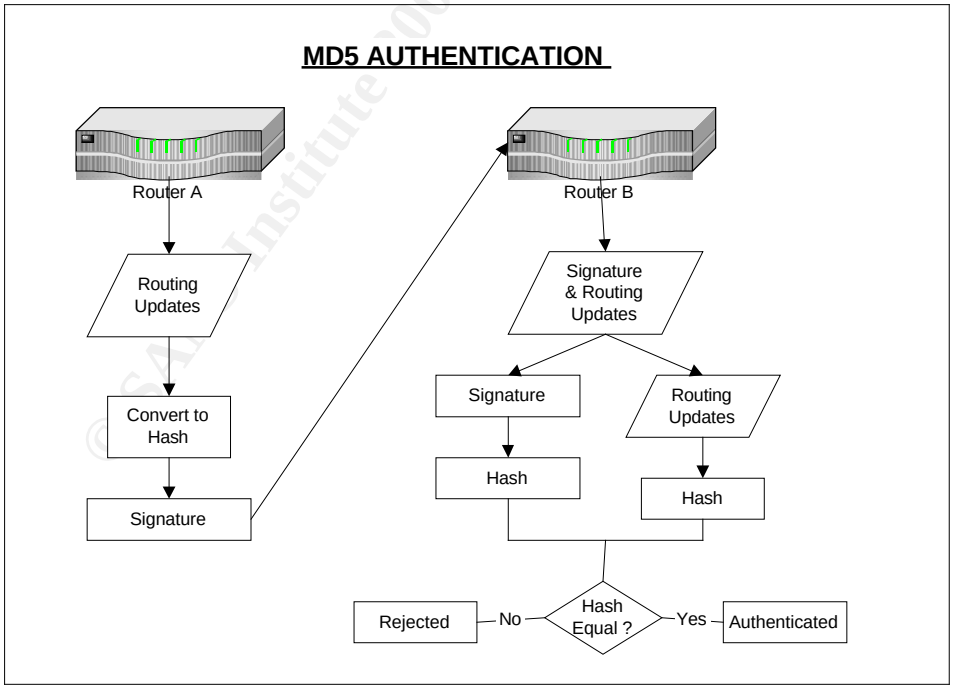
Sample BGP protocol Neighbor Authentication configuration.

```
router bgp 9290
 no synchronization
 network 192.168.1.0 mask 255.255.255.0
 neighbor 192.168.63.65 remote-as 4788
 neighbor 192.168.63.65 soft-reconfiguration inbound
 neighbor 192.168.63.65 send-community
 neighbor 192.168.63.65 route-map community1 out
 neighbor 192.168.63.65 password test
```

Sample OSPF protocol Neighbor Authentication configuration.

```
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
 ip ospf message-digest-key 50 md5 test
 no ip directed-broadcast
!
router ospf 5
 network 192.168.1.0 0.0.0.255 area 0
 area 0 authentication message-digest
```

For the above OSPF configuration, 50 (Message-digest-key) represent the key ID meanwhile "test" is the MD5 key. This will be entered on the Ethernet interface. The command "area 0 authentication message-digest" will turn on MD5 authentication for the OSPF backbone area.




© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

## 4.0 What is Remote Access?

Remote access is the ability to get access to a computer or a network from a remote distance. Home users get access to the Internet through remote access to an Internet service provider (ISP). Dial-up connection through desktop, notebook, or handheld computer modem over regular telephone lines is a common method of remote access. Remote access is also possible using a dedicated line between a computer or a remote local area network and the "central" or main corporate local area network.

### 4.1 Telnet Access on Cisco router

Telnet is one way of doing a remote access. Telnet programs are a type of terminal emulation program, just like modem-based communications programs. The difference is that telnet allows you to access other IP based hardware through the Internet, rather than by dialing directly. Telnet programs “talk” to other Internet-connected hardware using what's called the "telnet protocol" for communication. This protocol specifies how telnet programs should send data back and forth, allowing for interactive text sessions.

Administrative functions can be achieved using telnet to access the router or physically through the console port or remotely through a VTY (virtual terminal). Most Cisco IOS have support 5 VTY ports on the router. This means on 5 telnet sessions is allowed at one concurrent time. Telnet is widely used among system administrator to remotely access the router. Cisco IOS 12.0S software release is supported with Secure Shell (SSH) that makes the telnet session more secure. There are a few solutions on how to secure telnet access.

### 4.2 HTTP Server Access on Cisco router

The HTTP server was introduced to extend router management to the worldwide Web. This mean the administrator can update or make changes remotely via web. Recently Cisco has released an advisory regarding IOS HTTP authorization vulnerability. This vulnerability allows an intruder sending a crafted URL to execute privileged commands on Cisco router if local authentication database is used. The intruder will then be able to exercise complete control over the device.

Cisco IOS software starting with release 11.3 and later are vulnerable. For a more detailed discussion on Cisco IOS HTTP authorization vulnerability please visit this site http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html.

## 5.0 How to secure remote access?

There are a few ways on how to secure remote access whether it’s by telnet access, HTTP server access or Cisco TFTP access.

### 5.1 Using Access Control Lists (ACLs)

System administrator can restrict the telnet sessions to be from a trust source networks or IP addresses. This can be done using Access Control Lists (ACLs). By default there are no access controls on any of the VTY ports. This will add a layer of difficulty for hackers to attempt break-ins. The hacker needs to be in the trusted network to gain access to the router.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Example of ACLs:

*access-list 55 permit tcp 202.9.64.0 0.0.0.255 any log*
*access-list 55 deny tcp any any range 0 65535 log*
*access-list 55 deny udp any any range 0 65535 log*
*access-list 55 deny ip any any log*

The above access list defines a network 202.9.64.0/24 as the only network allowed to access the VTYs. The above configuration will also log TCP, UDP and IP attempts to the *syslog* file. Both valid and unauthorized scanning or break-in will be logged with the TCP/IP information.

### 5.2 Using Authentications

The other layer of difficulty that can be apply is to implement *username and password*. By default, password is the only authentication to log into a router. Using a *username and password* increases the level of effort need to use brute force to crack the password. Each user that has the access to the router get a separate user-id.

Example of configuring authentication:

*username admin1 password 01030C540A080F1C2243*
*username admin2 password 01030C540A080F1C2243*
*!*
*line vty 0 4*
*login local*
*!*

The above configuration shows that user "admin1" and "admin2" has been created. Telnet session will prompt for *username* and *password* to access the router. Each user needs to specify their password in order to use telnet session. A *username and password* makes brute force techniques harder but not impossible.

### 5.3 Using Console Port Timeouts

Leaving the terminal logged into the router can caused a use up of the available VTY ports. To handle this, configure shorter inactivity timeouts. By default the timeout applied to all connections to the Console, AUX and VTY on a Cisco router is 10 minutes. This can be control by applying the *exec-timeout* command on the router. Enabling *TCP keepalives* on incoming connections will ensure that any remote connection that crash or get disconnected will not use up the remaining router VTY ports.

Example *exec-timeout and TCP keepalives*:

*line con 0*
*exec-timeout 5 0*
*line aux 0*
*exec-timeout 5 0*
*line vty 0 4*
*exec-timeout 5 0*

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

*service tcp-keepalives-in*

Based on the above configuration, the router will disconnect console port, auxiliary port and VTY connections, which have been idle for more that 5 minutes and 0 seconds.

### 5.4 Disable HTTP server configuration

The workaround for this vulnerability is to disable HTTP server on the Cisco router configuration. Below is how to disable the HTTP server configuration.

*KL-4500#conf t*
*Enter configuration commands, one per line. End with CNTL/Z.*
*KL-4500(config)#no ip http server*
*KL-4500(config-if)#^Z*

### 5.5 Enable TACACS+ or Radius Authentication

The IOS HTTP server authentication vulnerability can be controlled. Place the Terminal Access Controller Access Control System (TACACS+**)** or Radius Authentication system to replace the local authorization database. An information and documentation regarding TACACS+ or Radius can be found at http://www.cisco.com/warp/public/480/tacplus.shtml.

## 6.0 Summary

Configuring a secure IP routing and telnet access should be a must in a Cisco router environment in order to improve security. Many other features, such as packet logging and quality of service features, can be used to increase network security against various attacks. Securing the router is the first thing that needs to be completed before any tools used to defend the network are implemented.

## 7.0 References


Cisco. "Improving Security on Cisco Routers".
URL: http://www.cisco.com/warp/public/707/21.html#routing

Malaysian Computer Emergency Response Team (MyCERT). "Building Bastion Routers Using Cisco IOS".
URL: http://www.mycert.mimos.my/resource/bastionrouter.htm

Cisco. "Defining Strategies to Protect Against TCP SYN Denial of Service Attacks".
URL: http://www.cisco.com/warp/public/707/4.html

Cisco. "PSIRT Advisories".
URL: http://www.cisco.com/warp/public/707/advisory.html

Liquifried. "Securing OSPF".
URL: http://www.liquifried.com/docs/security/securingospf.html

Network Security Library. "Cisco Router Security Overview".
URL: http://www.secinf.net/info/fw/cisco/cisco.html


© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Cisco. “Cisco ISP Essentials”.
URL: http://www.cisco.com/public/cons/isp/documents/IOSEssentialsPDF.zip

Cisco. “Cisco Security Advisory: IOS HTTP Authorization Vulnerability”
http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html

CERT Coordination Centre. “CERT® Advisory CA-2001-14 Cisco IOS HTTP Server Authentication Vulnerability”
http://www.cert.org/advisories/CA-2001-14.html

CERT Coordination Centre. “Vulnerability Note VU#812515: Cisco IOS HTTP server authentication vulnerability allows remote attackers to execute arbitrary commands”
http://www.kb.cert.org/vuls/id/812515

Whatis.com.
URL: http://www.whatis.com

Wright, Robert. “IP Routing Premier” Macmillan Technical Publishing, 1998

Halabi, Bassam. “Internet Routing Architectures” New Rides Publishing, 1997

Russell, Ryan and Cunningham, Stace. “Hack Proofing Your Network Internet Tradecraft” Syngress Media Inc., 2000

© SANS Institute 2001, Author retains full rights

Last Updated: May 26th, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **SANS Malaysia @ MCMC 2013** | **Cyberjaya, MY** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **SANS Pen Test Berlin 2013** | **Berlin, DE** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **Industial Control Systems Security Training - Houston** | **Houston, TXUS** | **Jun 10, 2013 - Jun 15, 2013** | **Live Event** |
| **Security Impact of IPv6 Summit 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 16, 2013** | **Live Event** |
| **SANSFIRE 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 22, 2013** | **Live Event** |
| **SANS Canberra 2013** | **Canberra, AU** | **Jul 01, 2013 - Jul 13, 2013** | **Live Event** |
| **Digital Forensics & Incident Response Summit 2013** | **Austin, TXUS** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS London Summer 2013** | **London, GB** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS Rocky Mountain 2013** | **Denver, COUS** | **Jul 14, 2013 - Jul 20, 2013** | **Live Event** |
| **SANS Mumbai 2013** | **Mumbai, IN** | **Jul 22, 2013 - Jul 27, 2013** | **Live Event** |
| **SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification** | **Washington, DCUS** | **Jul 22, 2013 - Jul 26, 2013** | **Live Event** |
| **SANS San Francisco 2013** | **San Francisco, CAUS** | **Jul 29, 2013 - Aug 03, 2013** | **Live Event** |
| **SANS SEC 560: Network Penetration Testing @ Bangalore 2013** | **Bangalore, IN** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **SANS Boston 2013** | **Boston, MAUS** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **Critical Security Controls Summit** | **Washington, DCUS** | **Aug 12, 2013 - Aug 18, 2013** | **Live Event** |
| **Industrial Control Systems Security Training - DC** | **Washington, DCUS** | **Aug 12, 2013 - Aug 16, 2013** | **Live Event** |
| **SANS Thailand 2013** | **Bangkok, TH** | **Aug 19, 2013 - Aug 31, 2013** | **Live Event** |
| **SANS Virginia Beach 2013** | **Virginia Beach, VAUS** | **Aug 19, 2013 - Aug 30, 2013** | **Live Event** |
| **Mobile Device Security Summit 2013** | **OnlineCAUS** | **May 30, 2013 - Jun 06, 2013** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |