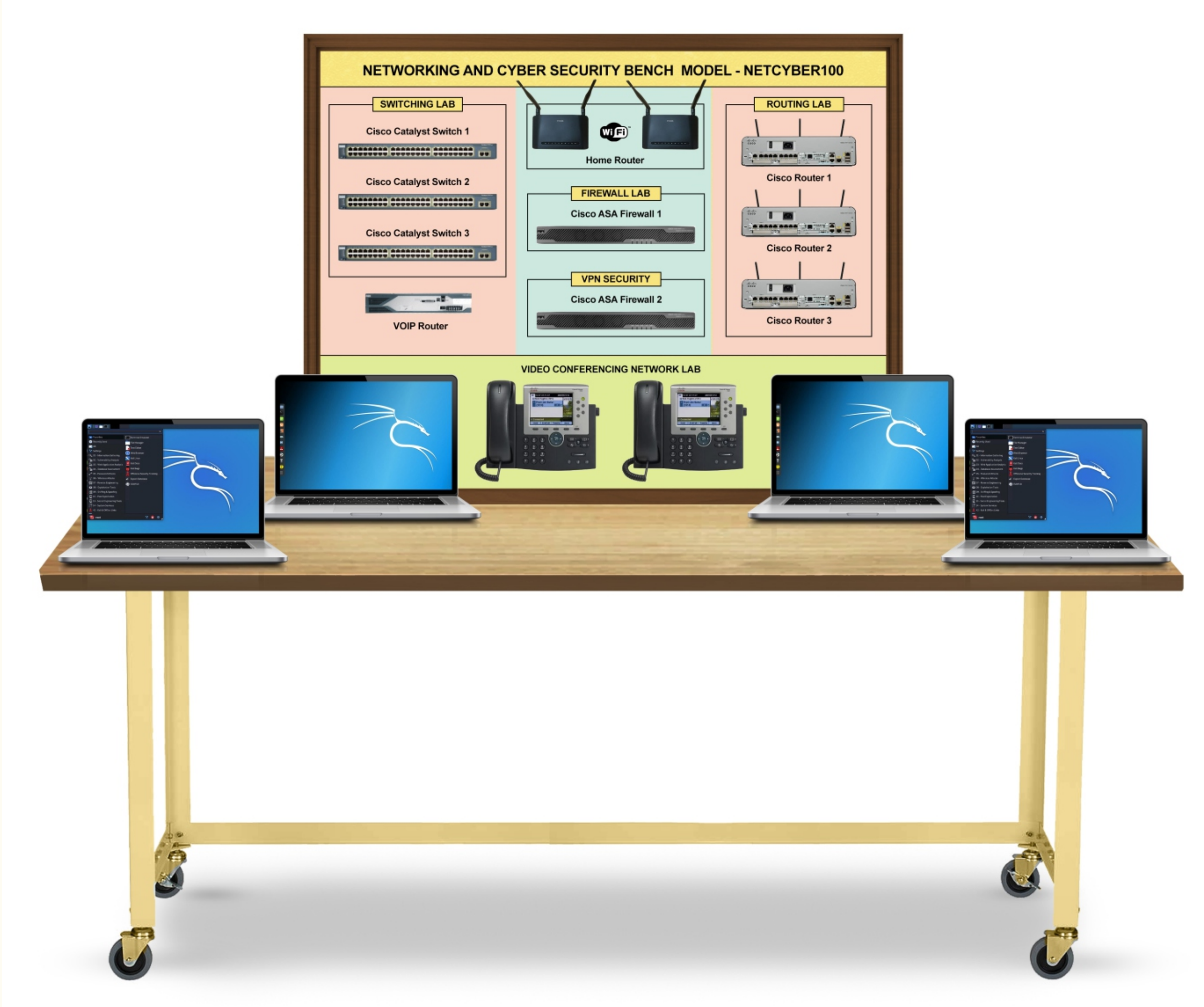
SIGMA

FIREWALL, VPN, ROUTER, INTERNET & CYBER SECURITY TRAINER MODEL- CYBERNET100

This trainer has been designed with a view to provide practical and experimental knowledge of a Computer, Internet, Routing and Cyber Security.



Sigma Trainers and Kits
E-113, Jai Ambe Nagar,
Near Udgam School,
Thaltej,
AHMEDABAD - 380054.
INDIA.

Phone(O): +91-79-26852427
Phone(F): +91-79-26767512
Mobile : +91-9824001168
Email : sales@sigmatrainers.com
: drluhar@gmail.com
Web : www.sigmatrainers.com

Dealer:-

SPECIFICATIONS

1. Hardware

Following Parts are assembled on a Bench

1. PC	4 Nos
2. Router	3 Nos
3. Switches	2 Nos
4. Firewall	1 No
5. Wifi Router	1 No
6. Wifi USB card	2 Nos.
7. RJ 45 Cross Cable	20 Nos
8. RJ 45 Straight Cable	20 Nos
9. Heavy Duty Work Bench	2 Nos
10. PCB Designing, SW Programming for all experiments and Manufacturing labour Cost provided	
11. Installing & Commissioning	Free
12. Training on the Trainer	10 days

. 13. All other cables, Adaptors and Accessories : As required

14. Standard Accessories : 1. Trainer.

2. Practical Manual

3. Drivers and Operating Systems

4. E-Books for Routers - 20 Nos.

5. Mp4 Video Class - 40 Nos

EXPERIMENTS

1. ROUTING EXPERIMENTS

1. Aim to Understand the basic working of Router on internet and Ip address.
2. Aim to Configure the Router interfaces with Ip addresses.
3. Aim to Understand the ICMP and perform PING between two Routers.
4. Aim to Configure the Static Routing between two Routers and understand the Routing table.
5. Aim to Configure the Default Routing between two Routers and understand the Route table.
6. Aim to Configure the RIP Routing between Routers and understand the Routing table.
7. Aim to Configure the EIGRP Routing between Routers and understand the topology.
8. Aim to Configure the OSPF Routing between Routers and understand the Routing table.
9. Aim to Configure the BGP Routing in topology to understand the working of protocol.
10. Aim to Configure the MPLS Routing between Routers to understand the multiprotocol Routing.

2. ROUTING SECURITY EXPERIMENTS

1. Aim to Configure the username and password on Router.
2. Aim to Understand and Configure the telnet access on Router.
3. Aim to Understand and perform the ssh access on Router.
4. Aim to Understand and perform the Standard access-list on Router.
5. Aim to Understand and perform the Extended access-list on Router.
6. Aim to Understand and Configure the HTTP server for Network.
7. Aim to Understand and Configure the FTP server for Network.
8. Aim to Understand and Configure the access-list to filter http traffic for IP's.
9. Aim to Understand and Configure the access-list to filter ICMP traffic for IP's.
10. Aim to Understand and Configure the tftp server for Emergency backup.
11. Aim to Understand and Configure the NAT on Network Topology.
12. Aim to Configure the DHCP Service .
13. Aim to Understand and Configure the DHCP Snooping.
14. Aim to Understand and Configure the MD5 password Authentication on Routers.
15. Aim to Configure ARP inspection.

3. VPN EXPERIMENTS

1. Aim to Configure the GRE based VPN in topology.
2. Aim to Configure the IPsec VPN between Routers.
3. Aim to Configure the SSL VPN in the Network Topology.

4. FIREWALL EXPERIMENTS

1. Aim to Understand the Basic Architecture and Working of Firewall.
2. Aim to Understand the Zone Working and Security levels in Firewall.
3. Aim to Understand and Configure the Firewall Interfaces with IP's.
4. Aim to Configure the Zones and Security levels for them.
5. Aim to Configure the Firewall and Other device with IP's.
6. Aim to Configure Routing on Firewall and Other device's.
7. Aim to Configure the ICMP policy on Firewall to allow Inside traffic.
8. Aim to Configure the HTTP policy on Firewall to allow Http Traffic.
9. Aim to configure the DNS policy on Firewall.
10. Aim to Configure the Static NAT on Firewall for Inside Zone.
11. Aim to Configure the Dynamic NAT on Firewall for Inside Zone.
12. Aim to Configure the Twice NAT in Firewall for Inside and Outside Zone.
13. Aim to Configure the access-list for traffic flow lower security levels to higher.
14. Aim to Configure the telnet on outside or inside.
15. Aim to Configure the SSH on outside or inside.
16. Aim to Configure the ASA lan-to-lan vpn.
17. Aim to Configure Traffic Filtering using access-list.

5. CYBERSECURITY EXPERIMENTS

1. Aim to Understand what is mac-address and how to change it.(Defensive)
2. Aim to Understand and Perform the basic packet sniffing.(Offensive)
3. Aim to Understand and Perform the DE-authentication attack.(Offensive)
4. Aim to Understand and Perform the WEP-Cracking. (Offensive)
5. Aim to Understand the WPA/WPA2 handshake capturing. (Offensive)
6. Aim to Perform Cracking WPA using wordlists. (Defensive)
7. Aim to Perform Device discovery on the same network. (Defensive and Offensive)
8. Aim to Perform the scan on discovered devices for vulnerability and open ports using nmap. (Offensive)
9. Aim to Perform gaining access or revershell using netcat. (Offensive)
10. Aim to Perform Information Gathering using tools like Maltego. (Defensive and Offensive)
11. Aim to Understand and Practice using METASPLOIT. (Offensive and Defensive)
12. Aim to Understand and Website testing using Burpsuite. (Offensive)
13. Aim to Understand and Perform Remote code execution on DVWA. (Offensive)
14. Aim to Understand and Perform the XSS on DVWA. (Offensive)
15. Aim to Understand and Perform the SQL injection on DVWA. (Offensive)